SPL
Sermaye Piyasası
Lisanslama Sicil ve
Eğitim Kuruluşu

Lisanslama Sınavları
Çalışma Notları

Bilgi Sistemleri İşletimi

2022

Hazırlayanlar:
Sermaye Piyasası Kurulu Uzmanları, Cem ERGÜL,
Nezihe UYGUN, Ceren TOSUN, Ceyhun TOKMAK


SPL
Sermaye Piyasası
Lisanslama Sicil ve
Eğitim Kuruluşu

Sermaye Piyasası
Lisanslama Sicil ve
Eğitim Kuruluşu

Bilgi Sistemleri İşletimi

Ders Kodu: 1022

- Bilgi Sistemleri Bağımsız Denetim Sınavı

31 Aralık 2024

Bu çalışma notu Sermaye Piyasası Kurulu uzmanları, Cem ERGÜL, Nezihe UYGUN, Ceren TOSUN ve Ceyhun TOKMAK tarafından hazırlanmıştır.

SINAV ALT KONU BAŞLIKLARI
BİLGİ SİSTEMLERİ İŞLETİMİ

1. Bilgi Sistemleri Altyapısı
- **1.1.** Bilgi Sistemleri Altyapısı Elemanları
- **1.2.** Bilgi Sistemleri Altyapısı Teknolojileri

2. Bilgi Sistemleri Operasyonları
- **2.1.** Hizmet Yönetimi
- **2.2.** Gözetim, Kapasite ve Performans Yönetimi

3. Bilgi Sistemleri Sürekliliği
- **3.1.** Bilgi Sistemleri Sürekliliği Kavramları
- **3.2.** Bilgi Sistemleri Süreklilik Planının Yönetimi

İÇİNDEKİLER

KISALTMALAR

AC	:Alternating Current (Alternatif Akım)
AI	: Artificial Intelligence (Yapay Zeka)
Altcoin	: Alternative Coin
ALU	:Arithmetic Logic Unit (Aritmetik Mantık Birimi)
AM	:Application Management (Uygulama Yönetimi)
API	: Application Programming Interface (Uygulama Programlama Arayüzü)
BT, BS	**:**Bilgi Teknolojileri, Bilgi Sistemleri
CCM	:Cloud Controls Matrix (Bulut Kontrol Matrisi)
CI	:Configuration Item (Yapılandırma Öğesi)
CM	:Configuration Management (Yapılandırma Yönetimi)
CMDB	:Configuration Management Database (Yapılandırma Yönetimi Veri tabanı)
CPU	:Central Processing Unit (Merkezi İşlem Birimi, MİB)
CRAMM	:CCTA Analysis and Management Method (CCTA Risk Analizi ve Yönetim Yöntemi)
CSA	:Cloud Security Alliance (Bulut Güvenliği İttifakı)
DAS	:Direct Access Storage (Doğrudan Bağlı Depolama)
DDOS	: Distributed Denial of Service (Dağıtılmış Hizmet Reddi)
DFD	:Data Flow Diagram (Veri Akış Şeması)
DHCP	:Dynamic Host Configuration Protocol (Dinamik Ana Bilgisayar Yapılandırma Protokolü)
DKIM	:Domain Keys Identified Mail (Alan Anahtarı Tanımlı Posta)
DLT	: Distributed Ledger Technology (Dağıtık Defter Teknolojisi)
DLP	: Data Loss Prevention (Veri Kaybı Önleme)
DMARC	:Domain-Based Message Authentication, Reporting & Conformance (Etki Alanı Tabanlı İleti Kimlik Doğrulaması, Raporlama ve Uygunluk)
DNS	: Domain Name System (Alan Adı Sunucusu)
DOS	: Denial of Service (Hizmet Reddi)
DW	:Data Warehouse (Veri Ambarı)
FTA	:Fault Tree Analysis (Hata Ağaç Analizi)
FTP	: File Transfer Protocol (Dosya Transfer Protokolü)
GPU	:Graphics Processing Unit (Grafik İşlemci Birimi)
HSM	:Hardware Security Modüle (Donanım Güvenlik Modülü)
IaaS	:Infrastructure as a Service (Hizmet Olarak Altyapı)
ICO	: Initial Coin Offering (İlk Kripto Varlık Arzı)
IDS	:Intrusion Detection System (Saldırı Tespit Sistemi)
IOSCO	:International Organization of Securities Commissions (Uluslararası Menkul Kıymet Komisyonları Örgütü)
IOT	: Internet of Things (Nesnelerin İnterneti)
IPO	: Initial Public Offering (İlk Halka Arz)
IPS	:Intrusion Prevention System (Saldırı Engelleme Sistemi)
ISP	:Internet Service Provider (İnternet Servis Sağlayıcı)
IOT	:Internet of Things (Nesnelerin İnterneti)
IPE	:Information Produced by the Entity (İşletme Tarafından Üretilen Bilgiler).
ITGI	:Information Technology Governance Institute (Bilgi

	Teknolojisi Yönetişimi Enstitüsü)
ITIL	:Information Technology Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi)
IUC	:Information Used by the Company (İşletmenin ilgili kontrolleri gerçekleştirirken/çalıştırırken kullandığı bilgiler, kontrolde kullanılan bilgiler)
KYC	: Know Your Customer (Müşterini Tanı)
LAN	: Local Area Network (Yerel Alan Ağı)
Mac OS	: Macintosh işletim sistemi
ML	: Machine Learning (Makine Öğrenmesi)
MAO	:Maximum Acceptable Outages (Maksimum Kabul EdilebilirKesinti)
MITM	: Man In The Middle (Ortadaki Adam)
MPC	: Multi Party Computation (Çok Taraflı Hesaplama)
MTPOD	:Maximum Tolerable Period of Distruption (Maksimum Tahammül Edilebilir Kesinti Süresi)
NAC	:Network Access Control (Ağ Erişim Kontrolü)
NAS	:Network Attached Storage (Ağa Bağlı Depolama)
NCM	:Network Configuration Management (Ağ Konfigürasyonu Yönetimi)
NFT	: Non Fungible Token (Nitelikli Fikri Tapu)
2FA	: 2 Factor Authentication (2 Faktörlü Kimlik Doğrulama)
NTP	: Network Time Protocol (Ağ Zaman Protokolü)
OLA	: Operational Level Agreement (İş Birimleriyle Mutabakat)
P2P	: Peer-to-peer (Eşler arası)
PaaS	: Platform as a Service (Hizmet Olarak Platform)
PC	: Personel Computer (Kişisel Bilgisayar)
PoW	: Proof of Work (İş Kanıtı)
PoS	: Proof of Stake (Hisse Kanıtı)
PUKÖ-PDCA	: Plan-Do-Check-Act (Planla-Uygula-Kontrol et-Önlem al ()
RFID	: Radio Frequency Identification (Radyo Frekans Tanımlama)
RPO	: Recovery Point Objective (Kurtarma Noktası Hedefi)
RTO	: Recovery Time Objective (Kurtarma Süresi Hedefi)
RWA	: Real World Assets (Gerçek Dünya Varlıkları)
SaaS	: Software as a Service (Hizmet Olarak Yazılım)
SAN	: Storage Area Network (Depolama Alan Ağı)
SCM	: Supply Chain Management (Tedarik Zinciri Yönetimi)
SDO	: Service Delivery Objective (Hizmet Sağlama Hedefi)
SIEM	: Security Information and Event Management (Güvenlik Bilgi ve Olay Yönetimi)
SMTP	:Simple Mail Transfer Protocol (Basit Posta Aktarım Protokolü)
SLA	:Service Level Agreement (Hizmet Seviyesi Anlaşması/Sözleşmesi)
SNMP	:Simple Network Management Protocol (Basit Ağ Yönetimi Protokolü)
SSD	: Solid State Drive (Katı Hal Sürücü)
SOA	: Service Outage Analysis (Hizmet Kesintisi Analizi)
SPOC	: Single Point of Contact (Tek İletişim Noktası)

SQL	: Structured Query Language (Yapılandırılmış Sorgu Dili)
TOP	: Technical Observation Post (Teknik Gözlem Mevki)
USB	: Universal Serial Bus (Evrensel Seri Veri Yolu)
URL	:Uniform Resource Locator (Tekdüzen Kaynak Bulucu/Konumlayıcı)
VTYS	: Veri Tabanı yönetim Sistemi
WAN	: Wide Area Network (Geniş alan Ağı)
VMS	:Vulnerability Management Service (Güvenlik Açığı Yönetimi Hizmeti)
WRT	:Work Recovery Time (İş Kurtarma Süresi)

Bu kitapta; bilgi sistemleri işletimine ilişkin bilgi sistemleri altyapısı, bilgi sistemleri operasyonları ve bilgi sistemleri sürekliliği konularına yer verilmektedir.

1. BİLGİ SİSTEMLERİ ALTYAPISI

Günümüzde tüm kurum ve kuruluşlar faaliyetlerini sürdürmek için bilgi sistemleri çözümlerine ihtiyaç duymaktadır. Bilgi sistemleri altyapısı ile ifade edilmek istenen bir işletmede kullanılan tüm bilgi sistemleri çözümlerinin "işletilmesini, çalıştırılmasını" sağlayan bileşenlerdir. İş süreçlerinin beklendiği şekilde yürütülmesi için bilgi sistemleri altyapısı iş ihtiyaçlarına uygun şekilde ve belirli kriterlere göre yönetilmelidir. Bu bölümde, bilgi sistemlerinin altyapı unsurları incelenmiş ve yönetimi için Sermaye Piyasası Kurulu mevzuatı, uluslararası kabul görmüş standartlar ve en iyi uygulama örneklerine göre benimsenmesi gereken yaklaşımlar ele alınmıştır.

Günümüzde çok geniş bir çerçevede ele alınan "bilgi sistemleri" ifadesinin çıkış noktası aslında "bilgisayar" kavramıdır. Bu kavram çok basit olarak "*kullanıcıdan veriyi alan, işleyen, saklayan ve kullanıcıya tekrar sunan elektronik bir cihaz*"dır. İlerleyen bölümlerde, bu basit tanımın gelişen teknoloji ve çeşitlenen kullanım alanlarıyla ortaya çıkan farklı türleri incelenecektir.

Mimari

Bilgisayar mimarisi, bilgisayarın işletim sistemi ile etkileşime giren, hiyerarşik yapıda düzenlenmiş bir dizi devre ve mantık katmanı olarak görülebilir. Hiyerarşinin temelinde bazı gömülü kodlar (firmware) içeren bilgisayar donanımı bulunur. Hiyerarşideki bir sonraki seviye çekirdek (kernel) fonksiyonlarını içermektedir. Çekirdeğin işlevleri, işletim sistemi ile ilişkili aşağıdaki konuları içeren temel işlemlerle ilgilidir:

- Kesinti işleme yönetimi
- İşlem oluşturma/öldürme
- İşlem durum değişimi
- Görev dağıtımı
- İşlem senkronizasyonu
- İşlemler arası iletişim
- Girdi/çıktı (I/O) işlemleri desteği
- Belleğin tahsisi ve yeniden tahsisi /serbest bırakılması desteği

Çekirdek çoğu kullanıcının erişiminin kısıtlandığı son derece ayrıcalıklı bir alandır. Çekirdeğin üzerinde kullanıcıları destekleyen çeşitli işletim sistemi işlemleri vardır. Sistem yazılımı olarak adlandırılan bu işlemler, bilgisayar sistemini çalıştırmak, kontrol etmek ve sürdürmek için kullanılan programların toplamıdır. Sistem yardımcı uygulamalarından ve programlarından oluşan sistem yazılımı, sistemin bütünlüğünü sağlar, bilgisayardaki programların ve olayların akışını kontrol eder ve bilgisayarla olan arayüzleri yönetir. Bilgisayar için geliştirilen yazılımların (örneğin erişim kontrol yazılımı, veri iletişimi, veri tabanı yönetimi, çevre birimlerinin yönetimi, ağ yönetimi ve diğer tüm yardımcı (utility) programlar) işletim sistemi ile uyumlu olması gerekir

1.1. Bilgi Sistemleri Altyapısı Elemanları

Bilgi sistemleri altyapısı en genel anlamda donanım ve yazılımdan oluşmaktadır. Donanım, "fiziksel" bir cihaz veya bir cihazın parçasıdır. En genel tabirle her bilgisayarın elle tutulup gözle görülen fiziksel parçaları donanımdır. Yazılım ise, herhangi bir bilgisayarın/donanımın bir işi nasıl yapması gerektiğini tarif eden komutlardır. Fiziksel olarak düşünüldüğünde sadece bir kelime işlemci dokümanındaki satırlardan oluşan yazılımlar, bilgisayar donanımlarının "iş görmesini" sağlar. Donanım ve yazılım bileşenlerinin tümü "bilgi sistemleri altyapısı" olarak ifade edilir. Altyapı bileşenleri çeşitli kategorilere göre sınıflandırılabilir, aşağıda çok temel bir sınıflandırma örneği verilmiştir:

• Kullanıcı donanımları (dizüstü/masaüstü bilgisayar, tablet, akıllı telefon ve benzeri mobil cihazlar),

• Sunucu donanımları (sunucu bilgisayarlar, depolama ortamları),

• Ağ (iletişim) donanımları (yönlendiriciler, güvenlik duvarları, anahtarlar),

• Yazılımlar (işletim sistemleri, ağ yazılımları, her türlü uygulamalar)

Bu bileşenlerin yapısı ve yönetimi ile ilgili temel bilgiler aşağıda ele alınmıştır.

1.1.1. Temel Donanım Bileşenleri

Yukarıda yapılan tanıma göre bilgisayarlar/donanımlar kendilerine tarif edilen bir işi yaparlar. Bu işi yapmak için de kendilerine iletilen veriler üzerinde yine kendilerine iletilen komutları işletirler. Yaptıkları işten bağımsız olarak tüm donanımların bazı ortak birimleri vardır. Bunlar:

• Çevre birimleri (Peripheral devices): Veriyi ve komutları dış dünyadan almak ve sonuçları tekrar dış dünyaya iletmek için kullanılırlar. Tüm çevre birimleri merkezi işlem birimi tarafından yönetilir.

o Giriş birimleri: Klavye, mouse, mikrofon, kamera, pen vb.

o Çıkış birimleri: Ekran, yazıcı, ses sistemi vb.

• Merkezi işlem birimi (Central processing unit-CPU): Veri ve komutları işlemek için kullanılır. Hiçbir donanım, merkezi işlem birimi ya da daha yaygın kullanımıyla "işlemci" olmaksızın herhangi bir "iş" yapamaz.

Merkezi işlem biriminin de birden çok alt birimi vardır:

o Aritmetik mantık birimi (Arithmetic logic unit-ALU): Matematiksel ve mantıksal işlemleri gerçekleştirmek için kullanılan birimdir.

o Kontrol birimi (Control unit): İşlemciye gönderilen komut ve veri trafiğini yöneten, komutları işletilmesi için aritmetik mantık birimine gönderen ve sonuçları alan birimdir. İşlemci içindeki ve dışındaki birimlerin eş zamanlı çalışması için gerekli kontrol sinyalleri de kontrol birimi tarafından üretilir.

o Ön bellek (cache): İşlemci içinde belli bir anda işletilen komutları ve işlenen/üretilen veriyi tutan bir tür yüksek hızlı bellektir.

• Depolama birimi (Storage unit): İşlenecek veya işlenmiş verinin depolandığı birimdir. Türünden bağımsız tüm depolama ortamları merkezi işlem birimi tarafından yönetilir. Aslında depolama birimleri de bir tür "çevre birimidir", ancak kendi içinde çok fazla çeşitlilik gösterdiği için ayrı bir madde olarak belirtilmesi uygun görülmüştür. Depolama birimleri kabaca ikiye ayrılır:

o Ana bellek (Random Access Memory-RAM): Bir bilgisayarın birincil depolama ünitesidir. Her türlü bilgisayarda değişik tür ve kapasitede ana bellek bulunur. En büyük özellikleri geçici olması ve yüksek hızlı olmasıdır. Burada geçicilik ile kast edilen, bilgisayar/donanım kapatıldıktan sonra ana bellekte tutulan veriye/komuta bir daha erişilememesidir. Genel olarak ana bellek ne kadar büyük olursa işlemler o kadar hızlı gerçekleştirilir. Ana bellek olmadan bir bilgisayar çalışamaz.

o İkincil depolama (secondary storage): Ana belleğin aksine, her tür verinin kalıcı olarak tutulduğu bir depolama türüdür ancak ana belleğe göre hızı çok daha düşüktür. Bir bilgisayarın çalışması için şart değildir ancak verinin kalıcı olarak saklanması için şarttır. Bu depolama ortamlarının bazıları bir defaya mahsus yazılabilir şekildedir. İkincil depolama ortamları dâhili veya harici olabilmektedir.

Bunlar da kendi içinde farklı kategorilere ayrılır:

▪ Manyetik depolama ortamları: En eski sabit diskler (HDD), kartuşlar

▪ Optik depolama ortamları: CD, DVD, Blu-ray diskler

▪ Solid-state depolama ortamları (SSD): SSD diskler (manyetik sabit disklerin yerine), SD hafıza kartları, USB'ler.

Son yıllarda yaşanan gelişmeler ve maliyetlerdeki düşüşler grafik işleme birimleri (GPU) kullanımını da hızla artırmaktadır. Genellikle ekran kartı üzerinde yer alan grafik işleme birimleri, merkezi işlemciden daha fazla aritmetik mantık birimi içerirler ve bilgisayar grafiklerini işlemek ve göstermekte son derece verimlidir. Klasik merkezi işlem birimlerine göre çok daha yüksek hız, verim (daha az hafıza kullanarak) ve işlem kapasitesi sunan grafik işlem birimleri büyük veri, yapay zekâ ve blok zincir gibi teknolojileri mümkün kılmıştır.

1.1.2. Bilgisayar Türleri

Önceki bölümde bilgisayarların en temel bileşenleri ele alınmıştır: Merkezi işlem birimi, çevre birimleri ve depolama birimleri. Bilgisayarları birçok farklı kategoride incelemek mümkündür. İlerleyen bölümlerde bilgisayarlar önce büyüklükleri sonra da mimarilerine göre sınıflandırılarak incelenecektir:

1.1.2.1. Büyüklüklerine Göre Bilgisayarlar

Süper Bilgisayarlar

Süper bilgisayar, genel amaçlı bir bilgisayara kıyasla yüksek performans düzeyi ve kapsamlı işlem gücü gerektiren, büyük miktarda veri işleyen veya çok karmaşık matematiksel hesaplamalar yapılan alanlarda (bilimsel ve teknik araştırmalar-hesaplamalar, mühendislik çalışmaları gibi) kullanılmak üzere tasarlanmış çok yüksek işlem hızına sahip, çok büyük ve pahalı bilgisayarlardır. Genellikle birkaç özel uzman sistem veya uygulama programına tahsis edilmektedirler.

Ana çatı (Mainframe) bilgisayarlar:

Ana bilgisayarlar, en yüksek düzeyde güvenlik ve güvenilirlikle günlük 1 trilyona kadar işlem yapmak üzere tasarlanmış bilgisayarlardır. Özünde, büyük miktarda belleğe ve milyarlarca basit hesaplamayı ve işlemi gerçek zamanlı olarak işleyen işlemcilere sahip yüksek performanslı bilgisayarlardır. Ana bilgisayar, yüksek esneklik, güvenlik ve çeviklik gerektiren ticari veri tabanları, işlem sunucuları ve uygulamalar için kritik öneme sahiptir. Bu bilgisayarların yetenekleri oldukça geniş olup genellikle paralel uygulamaları çalıştıran arka plan ve gerçek zamanlı (çevrimiçi) programları destekleyebilen kendi özel işletim sistemleri bulunmaktadır. Ana bilgisayarlar geleneksel olarak büyük kuruluşların ana veri işleme ve veri ambarı kaynağı olmuştur.

Mini Bilgisayarlar:

Mini bilgisayarlar büyüklük, güç ve kapasite bakımından mainframe bilgisayarlar ile mikro bilgisayarlar arasındadır ancak "mini bilgisayar" ifadesi artık kullanılmamaktadır. Bu bilgisayarlar günümüzde küçük-orta büyüklükte sunucular olarak sınıflandırılabilirler. Sunucu kavramı, eşzamanlı olarak birden çok kullanıcıyı (örneğin kurumsal sistemler) destekleyebilen çok işlemcili sistemleri tarif etmektedir. Bu bilgisayarların işletim sistemleri ve sistem yazılımları genellikle ticari ürünlerdir.

Kişisel bilgisayarlar (Personal Computers-PC):

Bireysel kullanıcılar için tasarlanmış, uygun fiyatlı ve mikro işlemci teknolojisine dayanan PC'ler veya iş istasyonları (work station) olarak adlandırılan küçük bilgisayar sistemleridir. Bir diğer adı "mikro bilgisayar"dır. Bunlar yaygın olarak word, excel ve elektronik posta gibi ofis otomasyon işlevleri, küçük veri tabanı yönetimi, web tabanlı uygulamalarla etkileşim ve kişisel grafik, ses, görüntüleme, tasarım, web erişimi ve eğlence gibi diğer işlevler için kullanılmaktadır. Tek kullanıcılı sistemler olarak tasarlanmasına rağmen, bu bilgisayarlar genellikle bir ağ oluşturmak için birbirine bağlanabilmektedir. Kişisel bilgisayarlar da birden çok alt türe ayrılabilir.

İnce istemci (Thin Client) bilgisayarlar:

Bunlar genellikle en az donanım özelliğiyle (disksiz iş istasyonu gibi) yapılandırılan ve işlem yapabilmek veya uygulama kullanabilmek için bir sunucu bilgisayara erişmek zorunda olan kişisel bilgisayarlardır. Geleneksel kişisel bilgisayarlar gibi kendi kaynak ve uygulamaları yoktur.

Masaüstü bilgisayarlar (Desktop computers):

Kişisel bilgisayarların ilk ortaya çıkması masaüstü bilgisayarın hayatımıza girmesi şeklinde olmuştur. Bu bilgisayarlar genellikle sabit bir yerde olup taşınabilir değildirler.

Dizüstü bilgisayarlar (Laptop computers):

Dizüstü bilgisayarlar kolayca taşınabilen ve normal bir alternatif akım (AC) bağlantısı veya şarj edilebilir bir pil takımı ile çalışan hafif (5 kilogramın altında) kişisel bilgisayarlardır. Masaüstü bilgisayarlara benzer yetenekte, benzer işlemci, bellek ve disk depolama kapasitesine sahip olup pil paketi sayesinde elektrik kesintilerine karşı dayanıklıdırlar.

Taşınabilir oldukları için hırsızlığa karşı savunmasız olup cihazlar içindeki bilgiyi almak, yerel alan ağı (LAN) içine girmek veya uzaktan bağlantıyı ele geçirmek için çalınabilirler.

Akıllı telefonlar, tabletler ve taşınabilir cihazlar:

Kullanıcıların dizüstü bilgisayarın yerine küçük bir bilgi işlem aygıtı kullanmalarını sağlayan el aygıtlarıdır. Bazı kullanımları arasında görev planlayıcı, telefon ve adres defteri, yapılacaklar listeleri oluşturma ve izleme, bir masraf yöneticisi, e-okuyucu, web tarayıcısı ve diğer işlevler bulunur. Bu tür cihazlar aynı zamanda bilgisayar, telefon / faks ve ağ özelliklerini bir araya getirerek her zaman ve her yerde kullanılabilmektedir. Taşınır (mobil) cihazlar ayrıca önemli bilgileri yedeklemek veya aktarmak için bilgisayarla arayüz oluşturabilir. Benzer şekilde, bir PC'den elde edilen bilgiler taşınabilir bir cihaza indirilebilir.

1.1.2.2. Ağ Mimarisine Göre Bilgisayarlar

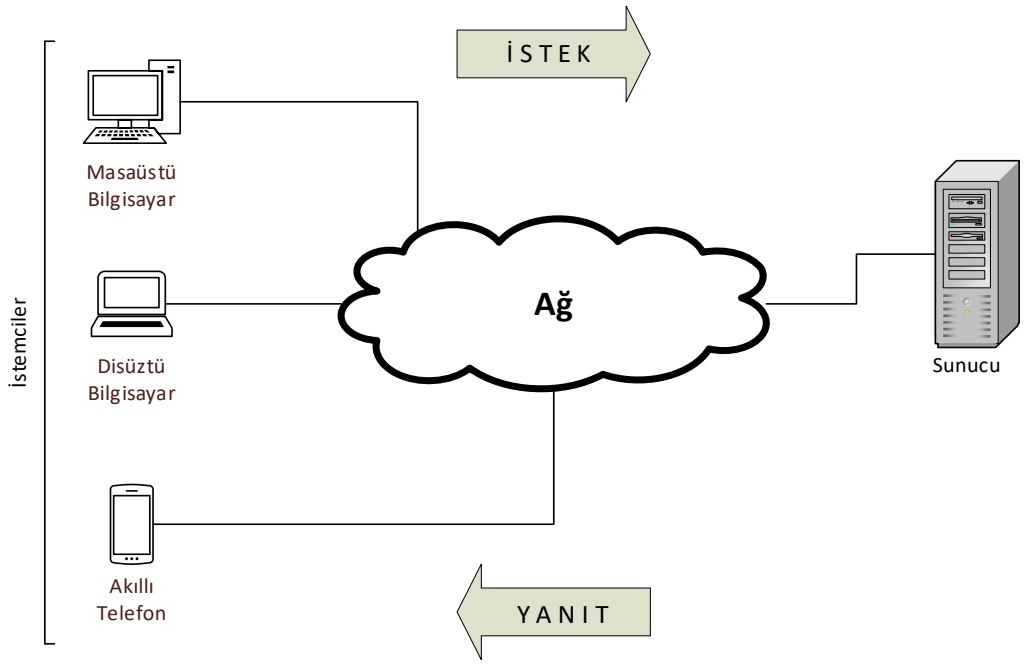
Bilgisayarlar kullandıkları ağ mimarisine göre iki kategoriye ayrılır:

Eşler arası model (Peer-to-peer, P2P):

Merkezi bir otoritenin katılımı olmadan taraflar arasında bilgi, veri veya varlık alışverişi/paylaşımı gerçekleştirmek için kullanılır. Dijital eşler arası bir ağda, her kullanıcı (teorik olarak) ağın sahibi ve ortağıdır. Bu tür bir ağ neredeyse her türlü bilgi veya dosya paylaşım süreci için kullanılabilir.

İstemci Sunucu Mimarisi

Günümüzde çok yaygın olarak kullanılan istemci-sunucu mimarisi, tipik olarak bir veri merkezinde bulunan, bir ağa bağlı bir veya birden çok sunucu ve bu sunuculardan hizmet alan birden çok istemci (client) makineye dayanmaktadır. Bu mimaride sunucular, yüksek hacimli belirli görevleri işlemek üzere tasarlanmış bilgisayarlar olarak düşünülebilir, P2P mimarinin aksine sunucu ve istemci bilgisayarlar ne yapı ne de görev olarak birbirine "eş" değildir. Sunucular sistemi "yönetir". Mimarinin basit bir anlatımı Şekil-1'de verilmiştir.



Şekil 1: İstemci-sunucu yapısı

İstemciler ise, sunucudan bir hizmet talep etmek için ilgili sunucuya paketler gönderir. Sunucu bu istekleri aldığında, üç işlemden birini yapabilir: Paketi kabul edebilir, paketi reddedebilir veya sessizce bağlantıyı kesebilir (paketi bırakabilir). Talepleri ve verilen cevapları yani veri akışını kontrol etmek için "bağlantı noktaları (port)" kullanımına dayanan istemciler ve sunucular, doğru bağlantı noktalarından birbirlerine istek göndermelidir. Genellikle sunuculardaki her farklı türde talep için farklı bağlantı noktaları bulunur. Bir istemciden bir sunucuya "yanlış" bir bağlantı noktası baz alınarak bir paket gönderilirse sunucu genellikle gönderilen paketleri sessizce "bırakır".

İstemci-sunucu mimarisinin tüm verilerin tek bir yerde toplanması, daha az bakım maliyeti gerektirmesi, ortaklaşa kullanılacak uygulamaların merkezi olarak yönetilebilmesi, veri kurtarmanın mümkün olması, istemci ve sunucuların kapasitesinin ayrı ayrı değiştirilebilmesi gibi avantajları bulunmaktadır.

İstemci-sunucu mimarisinde istemciler, sunucuda varsa veya sunucuya bir şekilde yüklendiyse virüslere, truva atlarına ve solucanların bulaşmasına açıktır. Sunucu, hizmet reddi (Denial of Service - DOS) saldırılarına eğilimlidir. Veri paketlerinin iletim sırasında değiştirilebilmesi, kimlik avı veya oturum açma kimlik bilgilerinin veya kullanıcının diğer yararlı bilgilerinin ele geçirilmesi ve ortadaki adam (Man In The Middle -MITM) saldırıları vb. dezavantajları bulunmaktadır.

İstemci-sunucu mimari günümüzde bilgi sistemleri çözümlerini kullanan ve birden çok kullanıcısı olan neredeyse tüm işletmelerde görülen bir modeldir. Bu modelde sunucu sistemler birden çok farklı fonksiyonu yerine getirmek durumundadır. İşletmenin büyüklüğü, işlemlerin çeşitliliği ve kullanıcı sayısına da bağlı olarak sunucular tarafından yerine getirilecek fonksiyonlar (görevler), sunucular arasında paylaşılır. Ancak sunucuların görevlerine göre ayrılması yeterli olmaz, görevlere göre ayrılan sunuculara, atandığı göreve uygun "sunucu yazılımlarının" yüklenmesi gerekir. Görevlerine göre sunucu sınıfları bir sonraki bölümde verilmiştir.

1.1.2.3. Görevlerine Göre Sunucu Bilgisayarlar

Uygulama Sunucusu

Uygulama sunucusu, bir veya birden çok uygulamayı barındırmak ve işletmek için kullanılan sunuculardır. Burada söz konusu olan uygulamaların genellikle fazla kaynak gereksinimi vardır ve birden çok kullanıcı tarafından paylaşılır. Burada sunucu, uygulamanın istemciler tarafından erişilebilir olmasından sorumludur. İstemcilerden gelen talepleri kendi üzerindeki ilgili uygulamaya gönderir ve uygulamadan gelen cevapları da talep eden istemciye geri döndürür. Uygulamaların karmaşıklığına göre uygulama sunucusunun arkasında çalışan başka sunucular da olabilir (örneğin veri tabanı sunucusu).

Web Sunucusu

Web sunucusunun görevi bir web sitesinin (internet sitesinin) içeriğini talep eden kullanıcıya sunmaktır. Bir kullanıcı, istemci bilgisayarındaki web tarayıcısında (web browser) bir "URL" (Uniform Resource Locator) yani bir "adres" yazıp "enter" düğmesine bastığında web tarayıcısı, ulaşılmak istenen web sitesinin yer aldığı İnternet'e bağlı web sunucusunu bularak ilgili sayfayı çağırır. Web sunucu, talep edilen dosyaları web tarayıcıya göndererek yanıt verir. Bu işlemden sonra tarayıcı, istenen sayfayı kullanıcıya göstermek için bu dosyaları çalıştırır. Web sunucusu da aslında bir uygulama sunucusudur: Web sitesi uygulamasını çalıştırır.

Web sunucuları, istemcilerden çeşitli istekler alır. Bunların en çok kullanılan ikisi "GET" ve "POST" istekleridir. Bir "GET" isteği, istemcinin yalnızca bilgi almak istediği ve sunucuya gönderecek verisi bulunmadığı zaman kullanılır. Bir "POST" isteği ise, istemcinin sunucuya gönderecek verisi olduğu ve buna bir yanıt beklediği zaman kullanılır. Örneğin, bir web sunucusunda form doldurmak ve gönder düğmesine tıklamak, istemciden sunucuya bir "POST" isteğidir.

Bazı popüler web sunucu yazılımları arasında Microsoft IIS, Apache, Nginx vb. sayılabilir. Web sunucuları için kullanılan bazı bağlantı noktaları (port) ise şunlardır: HTTP için 80 (şifrelenmemiş) ve HTTPs için 443 (şifreli).

Veri Tabanı Sunucuları

Veri tabanları, yoğun miktarda verinin iş ihtiyaçlarına uygun şekilde saklanması, işlenmesi ve yönetilmesi için kullanılan yazılımlardır. Genellikle veri tabanı yönetim sistemleri olarak adlandırılır. Günümüzde hemen tüm işletmelerde veri tabanı yönetim sistemleri kullanılmaktadır.

Veri tabanı sunucuları veri tabanı yönetim sistemlerini barındırmak ve işletmek amacıyla kullanılır. Veri tabanı yönetim sistemleri genellikle çok fazla kaynak tüketir bu sebeple diğer fonksiyonlardan ayrı bir sunucuda işletilmesi gerekir.

Veri tabanı bağlantılı uygulamalarda veri tabanı sunucusunun yanı sıra genellikle uygulama sunucuları da kullanılır. Uygulama sunucuları, kullanıcıların talep ettiği verileri almak için veri tabanı sunucusuna bağlanırlar. Güvenlik, performans ve yönetim kolaylığı gibi sebeplerle uygulama ve veri tabanı sunucularının farklı olması iyi bir uygulamadır.

Sık kullanılan veri tabanı yönetim sistemlerine örnek olarak Microsoft SQL, Oracle, HANA, DB2, MySQL, MariaDB örnek verilebilir. Veri tabanı yönetim sistemleri veriyi organize etme ve işleme/kullanma biçimlerine göre değişik şekilde sınıflandırılırlar.

Dosya ve Yazıcı Sunucuları

Dosya sunucusu, bir işletmede çeşitli işlemler için kullanılan tüm dosyaların saklandığı ve kullanıcılar tarafından paylaşıldığı bir sunucudur. Bu sunucu formunun ana avantajı, kullanıcıların dosyaları gereksiz tekrara düşmeden paylaşabilmesi ve saklanan dosyaların yedekleme işlemlerinin kolaylıkla yapılabilmesidir. Kullanıcılar sunucuya yetkileri çerçevesinde erişirler. Dosya izinleri ise yöneticiler tarafından kararlaştırılır ve kontrol edilir. Genellikle tüm işletmelerde dosya sunucuları kullanılır.

Yazıcı sunucusu ise, kullanıcıların baskı isteklerini yöneten ve yazıcı kuyruğunun durum bilgilerini son kullanıcılar ve ağ yöneticilerinin kullanımına sunan bir yazılım, ağ aygıtı veya

bilgisayardır. Baskı sunucuları hem büyük kurumsal hem de küçük ofis veya ev ağlarında kullanılabilmektedir.

Elektronik Posta Sunucuları

Bir e-posta sunucusu, kullanıcılara dağıtılmak üzere (işletme içinden veya dışından) gelen e-postaları kabul eder, saklar ve aynı şekilde kullanıcılar tarafından gönderilen (işletme içine veya dışına) e-postaların gönderilme işlemini gerçekleştirir. E-posta almak ve göndermek için genellikle "Basit Posta Aktarım Protokolü" (SMTP) kullanarak kurumsal ağlar (LAN, WAN) ve internet üzerinden iletişimi gerçekleştirir. Yerinde (on-premise) ve bulutta e-posta servisleri mümkündür; bunların en yaygın olanlarına örnek olarak Microsoft Exchange Server verilebilir.

E-posta sunucuları için kullanılan bazı bağlantı noktaları (port) şunlardır: 25 (SMTP), 587 (Güvenli SMTP), 110 (POP3).

SMTP protokolü, piyasaya sürülmesinden bu yana çok az veya hiç güvenlik içermemiştir ve e-posta göndermek için kullanıldığında, e-posta adresleri veya sunucu sahteciliğine karşı çok az savunma sunmaktadır.

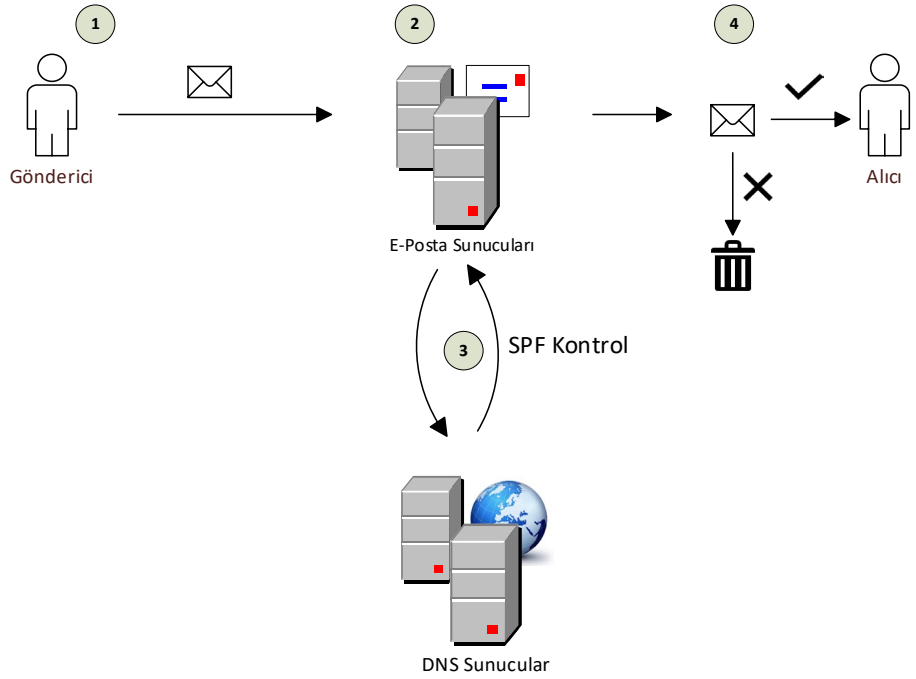
E-posta gönderimi ile ilgili kontroller

E-posta güvenliği, gizli verilerin dolandırıcılardan ve siber saldırganlardan korunması için tüm kuruluşların en büyük gereksinimidir. Son kullanıcıların, zararlı e-posta içeriklerinin dürüst bir kaynaktan geldiğini düşünerek kurumsal verilerin ele geçirilmesine sebep olduğu oltalama saldırıları bilgi güvenliği ihlallerinin başlıca sebeplerindendir. Tek bir kullanıcı bazı kötü niyetli e-posta eklerini tıklarsa, fidye yazılımı, kripto hırsızlığı, veri sızıntıları veya ayrıcalık yükseltme istismarları ile tüm kuruluşu tehlikeye atabilir. Ayrıca bu, e-posta sunucularının kara listeye alınmasına neden olabilmekte ve spam, kimlik sahtekârlığı ve kimlik avına da imkân tanımaktadır.

İş üretkenliğini ve iletişimi geliştirmek için kullanılan e-posta verilerinin güvence altına alınması için mesajlaşma sistemlerinin güvenliği sağlanmalıdır. Sunucuda yüklü olan zararlı yazılım araçlarının yanı sıra, e-posta mesajlarını güvenli hale getirmek için çeşitli tekniklerden yararlanılabilir.

Yıllar içinde e-posta güvenliği için birçok koruma protokolü geliştirilmiştir. Aşağıda bunlardan günümüzde yaygın olarak kullanılan 3 tanesi ele alınmıştır:

Gönderen Politikası Çerçevesi (Sender Policy Framework -SPF)



Şekil 2: SPF çalışma yöntemi

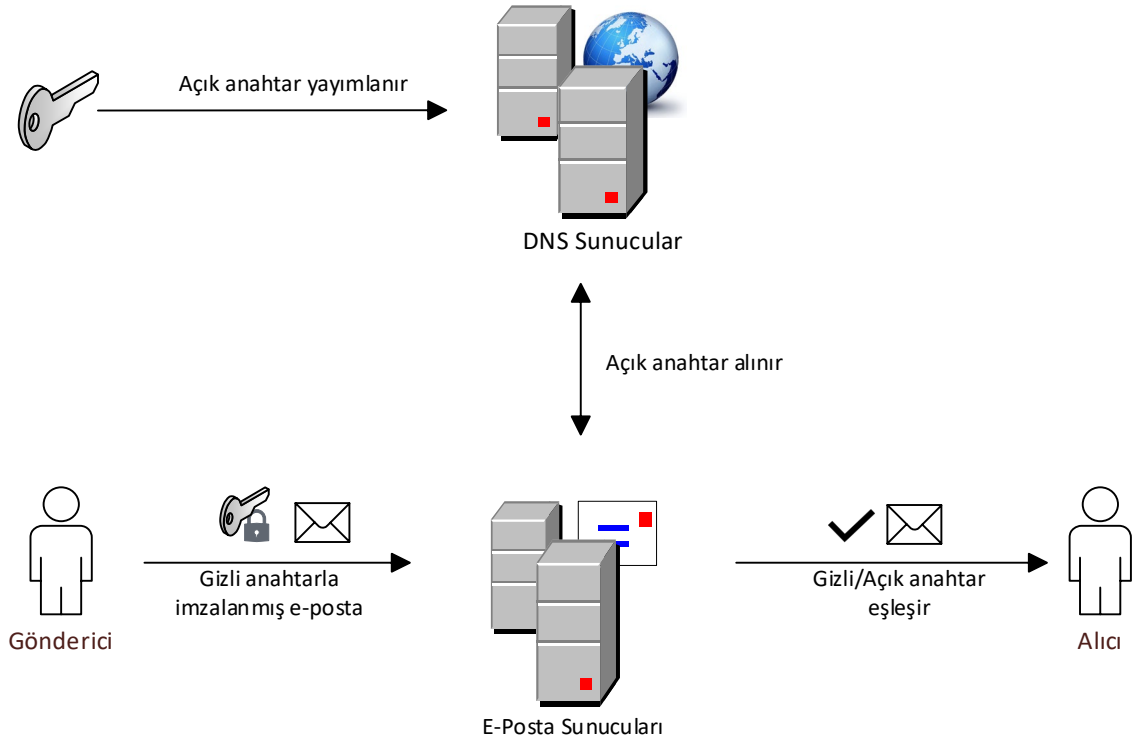
Gönderen Politikası Çerçevesi, kurumsal SMTP etki alanı için hangi e-posta sunucularının e-posta gönderme yetkisine sahip olduğunun belirlenmesine olanak tanımaktadır. Bir DNS girişi kullanarak belirli bir etki alanı için e-posta göndermesine izin verilen sunucuların listesini belirtir. Yalnızca yetkili etki alanı yöneticilerinin etki alanı için DNS bölge kayıtlarına erişimi olduğu fikrine dayanarak güvenlik sağlamaktadır.

SPF, TXT kaydı olarak eklenmekte ve kimlik sahtekârlığının (spoofing) önlenmesine yardımcı olmaktadır. Bir kullanıcı bir e-posta gönderdiğinde gönderen sunucu, SMTP mesaj başlığında "Kimden" alanında bir komut vermekte ve gönderen sunucunun bilgilerini içermektedir. Kuruluşların e-posta gönderebilecek yetkili sunucuları yapılandırmadığı durumda, alıcı e-posta sunucusu, mesajı SPAM olarak reddedebilir. Alıcı sunucunun mesajı SPAM olarak reddetmesinin nedeni, mesajın yetkili bir mesajlaşma sunucusundan geldiğini doğrulayamamasıdır. Sahte bir e-posta iletisi, iletinin asıl göndericisinden başka bir göndericiden geliyormuş gibi görünecek şekilde değiştirilmesiyle hazırlanmaktadır.

Kullanıcı e-posta'larını farklı bir adrese yönlendirirse SPF çalışmamaktadır. SPF'nin diğer DKIM ve DMARC e-posta kimlik doğrulama yöntemleriyle birlikte kullanılması önerilmektedir.

Alan Anahtarı Tanımlı Posta (DKIM)

Alan Anahtarı Tanımlı Posta (DKIM), bir kuruluşun aktarılmakta olan bir e-posta mesajının sorumluluğunu almasına ve alan kimliğinin doğrulanmasına yardımcı olmaktadır. DKIM, kriptografik kimlik doğrulamasından yararlanarak (genel/özel anahtar imzalama mekanizması) bir e-posta iletisinin geldiği görünen etki alanından geldiğini doğrulamaya yardımcı olan SPF'nin daha gelişmiş bir sürümüdür. SPF'den farklı olarak DKIM, alıcı sunucunun etki alanı için posta göndermesine izin verildiğini ve gönderildiğinden beri postanın kalitesinin değişmediğini doğrulamaktadır.



Şekil 3: DKIM çalışma yöntemi

DKIM ile e-posta işleminde gönderici sunucular, DKIM özel anahtarıyla bir imza oluşturur ve bunu e-posta başlığına (DKIM imza) ekler ve alan adını bir e-posta mesajıyla ilişkilendirmesi veya imzalaması için yetkilendirir. E-posta alıcıları, gönderen alanın DNS TXT kaydında DKIM ortak anahtarını arar ve bu daha sonra e-postaya eklenen DKIM imzasını doğrulamak için kullanılır. E-posta gövdesi içeriği değiştirilirse, e-posta imzası artık eşleşmeyecek ve doğrulama başarısız olacaktır. Bu

işlem, e-posta içeriğinin değiştirilmediğini ve e-postanın etki alanı onaylı bir sunucudan gönderildiğini doğrulamaktadır.

DKIM'in kendisi herhangi bir istenmeyen e-postayı doğrudan engellemez, filtrelemez veya tanımlamaz. E-posta mesajının çok daha iyi doğrulanması için DKIM'in SPF ile birlikte kullanılması önerilmektedir.

Etki Alanı Tabanlı İleti Kimlik Doğrulaması, Raporlama ve Uygunluk (DMARC)

Etki alanı tabanlı ileti kimlik doğrulaması, raporlama ve uygunluk (DMARC), göndericinin ve alıcının etki alanının sahte e-postaya karşı korumasını iyileştirmesine ve izlemesine olanak tanımak için raporlama yetenekleri ekleyen SPF ve DKIM protokolleri üzerine kurulmuş bir e-posta kimlik doğrulama protokolüdür. DMARC politikaları, DNS'de TXT kaydı olarak yayınlanmakta ve gönderici kuruluştan alınan bir e-posta iletisiyle e-posta alıcısının ne yapması gerektiğini duyurmaktadır.

Her iki araçta da kullanılabilen basit bir DMARC politikası belirterek hem SPF hem de DKIM öğeleri birleştirilebilir ve etki alanı yöneticisinin, aynı alan adına karşı alıcılar tarafından toplanan sahte posta mesajı istatistikleri hakkında bilgi göndermesine (etki alanlarının göreli kimlik sahtekârlığı düzeyleri, alan adından geldiğini iddia eden e-posta sahtekârlığını kimin yaptığı vb) olanak sağlayabilir.

Sonuç olarak, gerekli DNS TXT kayıtlarını yapılandırırken bir hata yapılması önemli e-postaların kaybolmasına neden olabileceğinden, bazı alan sahipleri yöntemleri uygulamamayı tercih edebilmektedirler. Buna rağmen, Google, Microsoft ve Yahoo gibi büyük e-posta alan sahipleri bu yaklaşımları uygulamışlardır.

Bu iki protokol değerlendirilirken dikkat edilmesi gereken noktalar:

- SPF ve DMARC protokollerinin çalışması için sahip olunan her alan ve alt alan için ayarlanması gerekir.
- Bu protokoller uygulanırken değişiklik yönetimine uygun bir süreç izlenmelidir. DMARC uygulaması sırasında tüm ayarların yayına geçmeden hemen önce yapıldığından emin olunmalıdır. Örneğin SPF, değişikliklerin bir test modunda ayarlanmasına olanak tanır; bu, alıcı etki alanlarının testi geçemeyen postaları engellemeyeceği anlamına gelir.
- E-posta sunucusuyla iletişimde olan tüm uygulamaların izlenmesi gerekmektedir. Kuruluşta uygulama içinden e-posta altyapısına bağlananlar tespit edilerek bunların doğru kimlik doğrulama yöntemlerini kullanacak şekilde ayarlanması sağlanmalıdır.

Vekil (Proxy) Sunucular

Bir vekil (Proxy) sunucu, istemcilerden gelen istekleri filtrelemek, performansı ve güvenliği artırmak için istemci ile sunucu arasında aracı görevi gören bir sunucu uygulamasıdır. Proxy sunucusu, hizmet istenirken istemci adına çalışır ve hedef sunucuya yapılan isteğin gerçek kaynağını potansiyel olarak maskeler. Şifrelenmiş verileri filtrelemek, denetim izlerini tutmak ve dinleme, hataları onarma, hizmetlere erişim, etki alanları arası kaynaklar, güvenlik gibi sebeplerle içerik kontrol yazılımı olarak kullanılmaktadır.

Bir web vekil sunucusu birçok protokolden birinde çalışabilir, ancak en popüler web proxy sunucusu türü, okul ve kurumsal web filtrelerini aşmak için tasarlanmıştır. Web trafiğinin tamamı tek bir IP adresi ve henüz bloke edilmemiş web sitesi üzerinde olduğundan, kullanıcılar bu filtreler aracılığıyla yasaklı sitelere erişim sağlayabilirler.

Kurumsal vekil sunucular da aynı etkiye sahiptir, ancak genellikle bir kuruluş tarafından yetkilendirilir. Kullanıcıların web trafiğini alır, genellikle daha sonra değerlendirilmek üzere günlüğe (log) kaydeder ve internete gönderir. Bu, kullanıcıların trafiğini bir araya getirir, böylece bir bilgisayar genel olarak diğerinden ayırt edilemez. Bu durum, kullanıcıların hedeflenmesini önlemek ve genellikle gönderilen ve alınan paketleri inceleyebilmek, önbelleğe alabilmek ve analiz edebilmek için bir kuruluş tarafından kasıtlı olarak yapılır.

Alan Adı Sunucusu (Domain Name Server - DNS)

Alan adlarını karşılık gelen IP adreslerine çevirmek için bir alan adı sunucusu kullanılır. Bu sunucu, internet tarayıcısında bir alan adı (URL) aratıldığında tarayıcının başvurduğu sunucudur. Bu sayede kullanıcılar IP adreslerini ezberlemek zorunda kalmamakta ve alan adresleri kurumların istediği şekilde belirlenebilmektedir.

Genellikle İnternet Servis Sağlayıcıları (Internet Service Provider -ISP), kullanıcılarına DNS sunucuları sağlar. Ancak bu arama hizmetini ücretsiz olarak sağlayan birçok kuruluş da vardır (IP 8.8.8.8'e sahip popüler Google DNS sunucusu gibi). Kullanıcılar yeni bir alan adı oluşturduğunda alan adı, diğer alt düzey DNS sunucularının (DNS sunucuları hiyerarşik bir temelde çalışır, bu nedenle diğerlerinden daha "yetkili" sunucular vardır) başvurduğu bir üst düzey DNS sunucusuna kaydedilir. DNS Sunucuları için kullanılan bağlantı noktaları: 53 (hem TCP hem de UDP protokollerinde).

Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP) Sunucusu

Bir dinamik ana bilgisayar yapılandırma protokolü (DHCP) sunucusu, istemci bilgisayarların ağ ayarlarını yapılandırmak için kullanılmaktadır. Büyük bir ağdaki istemci bilgisayarlarda statik IP adresini ve diğer ağ ayarlarını manuel olarak yapılandırmak yerine, ağdaki bir DHCP sunucusu bu ağ ayarlarını yerel ağdaki (LAN) bilgisayarlarda dinamik olarak yapar. DHCP sunucuları için kullanılan bağlantı noktası: UDP protokolünde 67.

Dosya Aktarım Protokolü (FTP) Sunucusu

FTP sunucuları veya “Dosya aktarım protokolü” sunucularının amacı, kullanıcılar arasında dosya alışverişi yapmaktır. İnternet servislerinin en eskilerinden biri olan dosya aktarım protokolü, bir veya daha fazla dosyanın bilgisayarlar arasında güvenli bir şekilde taşınmasını sağlarken, dosya güvenliği ve organizasyonunun yanı sıra aktarım kontrolü de sağlar. FTP sunucusu, alt dizinleri, oturum açmayı ve yönlendirme komutlarını destekleyen dosyaları aktarmak için kullanılır. Ayrıca, HTML sayfalarını HTTP sunucusuna yüklemek veya günlük (log) dosyalarını uzak bilgisayara indirmek için kullanılabilir.

Filezilla, WinSCP gibi erişim kontrol arayüzleri, kullanıcıların FTP sunucusunu başlatmasına veya durdurmasına ve yerel kullanıcı hesaplarını yönetmesine olanak tanır. FTP sunucusu hakkındaki bildirimi kullanıcı uygulamasına göndermek için kullanıcı geri arama işlevini kullanır.

Bu sunucular varsayılan olarak herhangi bir şifreleme türü sağlamaz, bu nedenle bu protokolün sıklıkla kullanılan birkaç güvenli sürümü vardır (örneğin, güvenli SSH protokolü üzerinden FTP olan sFTP). Bu tür sunucu, kullanıcıların bir FTP istemcisi aracılığıyla kimlik doğrulaması yaptıktan sonra dosyaları kendisine yüklemesine veya dosya indirmesine olanak tanır. Kullanıcılar ayrıca sunucunun dosyalarına göz atabilir ve istedikleri gibi tek tek dosyaları indirebilir. FTP sunucuları için kullanılan bazı bağlantı noktaları: FTP için 20, 21 ve sFTP için 22.

Atlama (jump) Sunucuları

Bir atlama sunucusu, ayrı güvenlik bölgelerindeki cihazlara erişmek ve bunları yönetmek için kullanılan, birbirinden farklı güvenlik seviyelerine sahip iki güvenlik bölgesini kapsayan ve bunlar arasında kontrollü bir erişime olanak veren, sıkılaştırılmış ve sürekli gözetim altında tutulan bir cihazdır. En yaygın örnek, bir DMZ'deki bir ana bilgisayarı güvenilir ağlardan veya bilgisayarlardan yönetmektir. En yaygın kullanımlarından biri, SSH ve yerel bir güvenlik duvarı ile yapılandırılmış, sıkılaştırılmış bir Unix (veya Unix benzeri) makinedir.

BS Denetçisinin dikkat etmesi gerekenler

Atlama sunucusu kullanımı, avantajlarının yanı sıra güvenlik risklerini de beraberinde getirmekte olup güvenliği artırmanın birkaç yolu vardır:

- Ağın alt bölümlere (VLAN) ayrılması ve bir güvenlik duvarı veya yönlendirici kullanılarak güvenceye alınması.

- Yüksek güvenlikli kimlik doğrulama kullanılması. (2FA gibi çok faktörlü kimlik doğrulama vb.)

- Atlama sunucusunda yer alan işletim sistemi ve yazılımın güncel tutulması.
- Atlama sunucusundan internet erişimine izin verilmemesi ya da en alt seviyede tutulması.
- Sunucuda çalışabilecek programların kısıtlanması.
- Erişim denetim listelerinin (Access control list-ACL) erişimi kısıtlamak için kullanılması.
- Şüpheli etkinliğin izlenmesi ve ilgili tarafların uyarılması için iz kaydının tutulması ve izlenmesi.
- Bir atlama sunucusunun temsil edebileceği yüksek düzeyde riske karşın bir VPN, uygun ve daha yüksek güvenlikli bir alternatif olabilmektedir.

Kimlik Doğrulama Sunucuları

Kimlik doğrulama sunucuları, bir uygulamaya veya hizmete bağlanan kullanıcıları ve kimliklerini doğrulayan bir ağ sunucusu türüdür. Amaç, kimlik doğrulama sunucusunun arkasındaki sunucuya, uygulamaya, depolama alanına veya diğer bilgi sistemleri kaynaklarına yalnızca yetkili ve kimliği doğrulanmış uç noktalardan erişim sağlanmasıdır. Bu uç noktalar son kullanıcı, bilgisayar, sunucu veya bir uygulama olabilmektedir. Kimlik doğrulama sunucusunun, erişim sağlamak isteyen her bir kullanıcı veya sistem için geçerli kimlik doğrulama bilgilerini sağlaması gerekmektedir.

Windows için kullanılan kimlik doğrulama sunucusuna LDAP, Unix sistemler için kullanılana örnek olarak Centrify verilebilir.

Ağ Zaman Protokolü (Network Time Protocol- NTP) Sunucusu

Ağ zaman protokolü, bilgisayarların saat bilgilerinin bir ağ dahilinde senkronize edilmesine yardımcı olan bir protokoldür. Bilgisayar ağlarındaki saatleri evrensel koordineli zaman (Coordinated Universal Time - UTC) ile senkronize etmek için kullanılmaktadır. Cihazların bir sunucudan zaman bilgisi (UTC) talep etmesini ve almasını sağlar, bu da atomik bir saatten kesin zamanı almaktadır. Bu uygulama tek görevi bu olan bir sunucuya yüklenebilir.

1.1.2.4. Yapısına Göre Sunucu Bilgisayarlar

Fiziksel Sunucular

Fiziksel sunucu, ilk sunucu donanımları ortaya çıktığı anda görmeye başladığımız adeta "elle tutulabilen" sunuculardır. Sahip olduğu kaynakları (ana belleği, merkezi işlem birimini, bunların üzerinde bulunduğu ana kartı (motherboard) sadece kendisi kullanır. Üzerinde sadece bir işletim sistemi çalışır. Yukarıda anlatıldığı gibi görevlere göre bir bölümleme yapıldığında genellikle her fiziksel sunucuya ayrı bir görev verilir (örneğin web sunucusu, veri tabanı sunucusu).

Sanal Sunucular

Bir fiziksel sunucuyu, üzerinde birden çok işletim sistemi çalıştırıp birden çok "sunucu" gibi göstermeye yarayan yazılımlar sayesinde elde edilen sunuculardır. "Sanallaştırma" yazılımları sayesinde bir fiziksel sunucu birden fazla sunucu şeklinde kullanılabilir, bu şekilde elde edilen her bir sunucuya "sanal sunucu" veya "sanal makina" denir. Bir fiziksel sunucuyu sanal sunuculara dönüştürmek için, fiziksel sunucuya işletim sistemi yerine "sanallaştırma yazılımı" yüklenir.

Sanal sunucular, üzerinde yer aldıkları fiziksel sunucunun kaynaklarını kullanırlar. Bir fiziksel sunucunun üzerindeki sanal sunucuların her birinde ayrı bir işletim sistemi çalışabilir. Bu şekilde elde edilen her sanal sunucuya farklı bir görev verilebilir.

Sanal sunucular, işletmeleri her bir görev için farklı birer fiziksel sunucu kullanmaları zorunluluğundan kurtarır. Özellikle nispeten daha az yoğunlukta kullanılan sunucuların birer sanal sunucu olarak fiziksel bir sunucuda birleştirilmeleri işletmelere maliyet avantajı sağlar. Sanal sunuculardan biri kullanılmadığında veya daha az kullanıldığında sahip olduğu kaynaklar daha yoğun

kullanılan sunuculara kaydırılabilir böylece kaynakların "boş" kalması önlenir. Bu şekilde işletmeler fiziksel sunucu maliyetinin çok altında sanal sunucular edinebilirler.

Bahsedilen bu maliyet avantajı ticari veri merkezleri için de geçerlidir. Veri merkezi şirketleri genellikle fiziksel sunuculara toptan satış fiyatına sahip olur, ardından fiziksel makineden "elde edilen" sanal sunucuları işletmelere kiralayarak maliyet avantajı sağlarlar. Veri merkezlerinden hizmet alan işletmeler de bu avantajdan faydalanmış olur. Veri merkezlerinin bu tasarımı sayesinde fiziksel makinelerin farklı müşteriler (işletmeler) ya da aynı müşterinin farklı ihtiyaçları tarafından paylaşımlı kullanılmasına olanak sağlanmaktadır. Bu durum maliyet avantajı sağladığı gibi (hem veri merkezine hem de işletmeye), yine her iki tarafa yönetim kolaylığı da sağlamaktadır. Ancak, güvenlik, log izleme, mevzuata uyum gibi konulardaki değerlendirmeler neticesinde farklı işletmeler arasında paylaşımlı kullanımın tercih edilmediği durumlar da olabilir.

Sanallaştırma kavramının detayları ve farklı kullanımları ilerleyen bölümlerde anlatılacaktır.

1.1.3. Diğer Cihaz ve Sistemler

Bilgi sistemleri altyapısının önemli unsurlarından biri de belirli görevlere atanmış ve diğer hizmetleri çalıştırma yeteneği bulunmayan cihazlardır. Kapasite, performans ve güvenlik nedenleriyle, bazı servislerin sunucular yerine cihazlarda çalıştırılması gerekmektedir. Bu duruma örnek olarak; Güvenlik duvarı (firewall), IDS, IPS, ağ anahtarları, ağ yönlendiricileri, özel sanal ağlar (VPN), ağ erişim kontrolü (NAC), ağ yük dengeleyici (load balancer), SIEM ürünleri (Qradar, Splunk, Arcsight, Elastic search, Guardium, Imperva, Cryptolog vb) ve parola saklama kasaları (password vaults) (Cyberark, Thycotic, Single Connect, Manage Engine PAM) verilebilir.

Donanım Güvenlik Modülü (Hardware Security Module- HSM)

Donanım güvenlik modülü, kriptografik anahtarların oluşturulması, depolanması ve korunmasından oluşan bir güvenlik hizmeti sunan elektronik cihazdır. Bu bir donanım, bilgisayardaki bir eklenti kartı veya harici bir kutu olabilmektedir.

Bu hizmeti yazılım (Yazılım güvenlik modülü) aracılığıyla da almak mümkün olmakla birlikte donanım modülü daha yüksek düzeyde güvenlik sağlamaktadır. HSM'ler, FIPS 140 ve Common Criteria EAL4+ gibi uluslararası güvenlik standartlarına uygun üretilmek ve kullanılmak zorundadır ve başlıca kriptografik API'leri desteklemektedir. Ayrıca doğrudan Oracle veya MS SQL Server gibi veri tabanı yönetim sistemleri tarafından da kullanılabilmektedirler.

Bir açık anahtar altyapısına güven duyulması için sertifikayı yayınlayan kuruluşun güvenilirliği dikkate alınmaktadır. Bu yetkili kuruluşlar, kök şifreleme imzalama anahtarına sahiptir. Bu anahtar, bu otoriteden sertifika alacak kişilerin açık anahtarlarını imzalamak için kullanılmaktadır. Daha da önemlisi, bu anahtar kendi açık anahtarını imzalar. Bu anahtarın güvenliği ihlal edildiğinde, sertifika yetkilisi tarafından imzalanan tüm sertifikalar şüpheli hale gelmekte ve sertifika yetkilisinin güvenilirliği yok edilmektedir. HSM, bu yüksek önemdeki anahtarların güvenli şekilde kullanılmasını ve korunmasını sağlamaktadır.

Radyo Frekans Tanımlama (Radio Frequency Identification- RFID)

Radyo frekansı tanımlama, sınırlı bir yarıçap içindeki etiketli nesnelerin tanımlanması için radyo dalgalarını kullanmaktadır. Etiket bir mikroçip ve bir antenden oluşmakta olup mikroçip, nesneyi tanımlamak için bilgileri ve kimliği birlikte depolarken anten, bilgileri bir RFID okuyucusuna iletmektedir.

Etiketi çalıştırmak için gereken güç iki modda elde edilebilmektedir. Pasif etiketlerde kullanılan ilk mod, okuyucudan gelen manyetik alandan güç çekmekte; aktif etiketlerde kullanılan ikinci ve daha pahalı mod, gücünü pillerden almakta ve bu nedenle daha yüksek frekanslar kullanabilmekte ve daha uzun iletişim mesafeleri elde edebilmektedir. Etkin bir etiket yeniden kullanılabilir ve daha fazla veri içerebilir.

Etiketler, hem doğrudan bir ürünü veya hem ürünü hem de taşıyıcısını tanımlamak için kullanılabilmektedir. İkincisi durumunda, bir nesnenin kimliği sisteme manuel olarak girilmekte (örn.

bir barkod kullanarak) ve öğeyi izlemek ve bulmak için stratejik olarak yerleştirilmiş radyo frekans okuyucularla birlikte kullanılmaktadır.

RFID uygulamaları

Varlık yönetimi: RFID tabanlı varlık yönetim sistemleri, etiketlenebilecek her öğenin envanterini yönetmek için kullanılır. RFID teknolojisini kullanan varlık yönetim sistemleri, kâğıt tabanlı veya barkod sistemlerine göre, optik görüş hattı veya fiziksel temas olmadan neredeyse aynı anda birden fazla öğenin tanımlayıcılarını okuyabilmeyi de sağlayan önemli avantajlar sunmaktadır.

İzleme: RFID varlık yönetim sistemleri, bir öğenin konumunu veya daha doğru bir ifadeyle, öğeyle ilişkili etiketin varlığını tespit eden son okuyucunun yerini belirlemek için kullanılmaktadır.

Orijinallik doğrulaması: Etiket, etiketli bir öğenin kaynağına ilişkin kanıt sağlamaktadır. Orijinallik doğrulaması, genellikle bir izleme uygulamasına dâhil edilmektedir.

Eşleştirme: Etiketlenmiş iki öğe birbiriyle eşleşmekte ve öğelerden biri daha sonra yanlış etiketlenmiş bir öğeyle eşleşirse bir sinyal tetiklenmektedir.

Süreç Kontrolü: İş süreçlerinin bir etiketle (veya etikete eklenmiş öğeyle) ilgili bilgileri kullanmasına ve özelleştirilmiş bir işlem gerçekleştirmesine olanak tanımaktadır.

Erişim Kontrolü: Bir bireyin bir tesise (örn. bir kampüs veya belirli bir bina) fiziksel olarak erişme yetkisine veya bir bilgi sistemine mantıksal olarak erişme yetkisine sahip olup olmadığını otomatik olarak kontrol etmek için RFID kullanılabilmektedir.

Tedarik Zinciri Yönetimi (SCM): SCM, üretimden dağıtıma ve perakende satışa kadar ürünlerin izlenmesini ve kontrolünü içermektedir. SCM genellikle varlık yönetimi, izleme, süreç kontrolü ve ödeme sistemleri gibi çeşitli uygulama türlerini bir araya getirmektedir.

RFID ile ilgili riskler

RFID ile ilişkili risklerden bazılarına aşağıda yer verilmiştir:

İş süreci riski: RFID sistem bileşenlerine yapılan doğrudan saldırılar, RFID sisteminin etkinleştirmek için tasarlandığı iş süreçlerini zayıflatabilmektedir.

İş zekâsı riski: Rakipler RFID tarafından üretilen bilgilere yetkisiz erişim sağlayabilir ve bilgileri RFID sistemini uygulayan kuruluşun çıkarına zarar vermek için kullanabilmektedir.

Gizlilik riski: Bir RFID sistemi, kişisel bilgileri orijinal olarak tasarlanan veya anlaşılan amaç dışında kullanırsa, kişisel güvenlik tehlikeye girebilir. Aktif etiketlerin kişisel mülkiyeti de bir gizlilik riskidir çünkü bu etiketli öğeler izlenebilir.

Dışsallık Riski: RFID teknolojisi, RFID ile ağa bağlı olmayan veya RFID ile birlikte konumlandırılmayan sistemler, varlıklar ve kişiler için bir tehdit oluşturabilmektedir. RFID'nin riski etkileyen önemli bir özelliği, RF iletişiminin operatörler ve kullanıcılar tarafından görülememesidir.

RFID'ler ile ilgili güvenlik önlemleri

Bir BS denetçisi, RFID'ye yönelik bazı güvenlik önlemlerinin alındığını kontrol etmelidir:

İdari: Bir idari kontrol RFID sisteminin güvenliğinin gözetimini içermelidir. Örneğin, kuruluş, RFID uygulamalarına yönelik mevcut politikaları ve güvenlik kontrollerini gerektiğinde güncellemelidir.

Operasyonel: Operasyonel kontrol, sistem yöneticileri ve kullanıcıları tarafından günlük olarak gerçekleştirilen eylemleri içermektedir. Örneğin RFID sistemleri, sistemlerin fiziksel güvenliğini ve doğru kullanımını sağlayan operasyonel kontrollere ihtiyaç duyabilir.

Teknik: Teknik kontrol, sistem içinde gerçekleştirilebilecek eylemlerin izlenmesine/kısıtlanmasına ilişkin teknolojinin kullanılmasıdır. RFID sistemleri, etiketlerdeki verilerin korunması veya şifrelenmesi, etiketlerin kendi kendini imha etmesini sağlama ve kablosuz iletişimlerin korunması veya şifrelenmesi gibi çeşitli nedenlerle teknik kontrollere ihtiyaç duyar.

1.1.4. Donanım Yönetim Süreçleri ve Değerlendirilmesi

1.1.4.1. Donanım Bakım Programları

Bilgi sistemleri altyapısında bulunan tüm donanımların düzgün çalışmasını sağlamak için rutin olarak bakımının yapılması gerekmektedir. Bakım gereksinimleri, donanımın türü, karmaşıklığı ve iş yüküne göre değişmektedir. Bakım faaliyetleri tedarikçi firma tarafından sağlanan özelliklere uygun olacak şekilde planlanmalıdır. Burada donanımdan kasıt; sunucular, kullanıcı makineleri, yazıcılar, ağ cihazları, depolama üniteleri gibi her türlü bilgisayar donanımı olabilir.

Bakım hizmeti, donanımın tedarikçisi, üreticisi, üçüncü taraflarca veya kurumun kendi personeli tarafından verilebilir. Özellikle kritik iş süreçlerinde kullanılan maliyeti yüksek donanımların bir sözleşme kapsamında bakım hizmeti altında olması beklenir. Kurum, garanti aşamasında olan donanımları için üretici/tedarikçi tarafından verilecek bakım hizmetini kullanabilir, bu süre sona erdiğinde yeni bakım anlaşmaları (üçüncü taraflarca verilenler dâhil) değerlendirilmelidir. Bir sözleşme çerçevesinde yürütülen bakım programı donanımın sigortası olarak düşünülebilir.

Bakım programlarının faydası aşağıdaki gibi özetlenebilir[1]:

- Donanımların hizmet dışı kalma süresini minimuma indirir, düzeltici bakım faaliyetlerinin oranını düşürür.
- Donanımların ömrünü uzatır,
- Donanımın en iyi performansta çalışmasını sağlar,
- Yasal düzenlemelere uyumsuzluk riskini düşürür, iş güvenliğine katkıda bulunur.

Donanım bakımı iki temel kategoriye ayrılabilir: Önleyici bakım ve düzeltici bakım.

- **Önleyici Bakım:** Donanımlarda henüz bir arıza ortaya çıkmadan yapılan bakım faaliyetleridir. Donanımda potansiyel problemlerin zamanında belirlenmesini sağlar, bu bakımdan vazgeçilmezdir.

Donanım bakım programı, bu bakımın performansını belgelemek için tasarlanmıştır. Bu aslen rutin bir bakım programıdır. Önleyici donanım bakım programları genellikle aşağıda belirtilen bilgileri içerir:

- Rutin bakım gerektiren her donanım kaynağı için tedarikçi bilgileri,
- Bakımın içeriğine ilişkin bilgiler,
- Bakımın maliyetine ilişkin bilgiler,
- Planlanmış, planlanmamış, gerçekleştirilmiş ve istisnai bakıma ilişkin bilgiler.

Bilgi sistemleri yönetimi, önleyici bakım programı çerçevesinde tedarikçi tarafından belirlenen bakım gereksinimlerinden sapmaları izlemeli, bu sapmanın nedenleri ve sonuçları üzerinde durmalıdır.

Bakım programının değerlendirmesi yapılırken ilk önce resmi bir bakım planının geliştirildiğinden, bilgi sistemleri yönetimi tarafından onaylandığından ve takip edildiğinden emin olunmalıdır. Bakım programının detayları incelenmeli ve tedarikçi/üreticinin önerilerine uygun olduğundan emin olunmalıdır.

Bütçeyi aşan veya aşırı olan bakım maliyetleri belirlenmelidir. Bunlar bakım prosedürlerine uyulmadığının veya donanımın ömrünün dolduğunun bir göstergesi olabileceğinden uygun sorgulama ve takip prosedürleri uygulanmalıdır.

Bakım faaliyetlerinin zamanlaması da önemlidir. Rutin bakım faaliyetleri kritik iş süreçlerinin çalışmakta olduğu zamanlara denk getirilmemeli, ilgili taraflara yapılacak bakım hakkında gerekli bilgiler verilmelidir. İstisnai (rutin olmayan) bakım faaliyetlerinde de yine ilgili taraflarla bilgi paylaşımı yapılmalı ve iş operasyonlarının sürekliliği ve bütünlüğü için mümkün olan tüm tedbirler alınmalıdır.

[1] https://www.flyability.com/blog/maintenance-management

• **Düzeltici Bakım:** Düzeltici bakım bir sorun ortaya çıktığında düzeltmek amacıyla yapılır. Burada bahse konu sorun, bilgi sistemleri biriminin hizmet masası/olay yönetimi seviyesinde çözülebilecek bir sorun da olabilir, üretici/satıcı seviyesinde yardım da gerektirebilir. Bakım süreçlerinin karmaşıklığı, söz konusu donanımlar çeşitlendikçe artabilir. Donanım bakımı süreci, yerine göre hizmet ve olay yönetimi personeli, mühendisler ve üretici/dağıtıcı firma personelinin işin içine girmesini gerektirebilir. Kurumun donanım bakım süreçlerinde yer alacak personelinin yetkinliği önemlidir.

Bakım sürecinin bir de güvenlik yönü vardır. Bakım faaliyetleri kurum dışı kişilerce gerçekleştiğinde söz konusu çalışmalar uzaktan erişim yöntemiyle veya kurum tesislerinde verilebilir. Her durumda kurumsal bilgiye erişim söz konusudur. Uzaktan erişim yönteminde karşı tarafa verilecek erişim izinleri dikkatle planlanmalı, yapılan işlemlerin kaydı tutulmalı ve kesinlikle iş bittiğinde izinler geri alınmalıdır. Bakım hizmeti bir sözleşme çerçevesinde ise sözleşmede gizlilikle ilgili hükümler mutlaka yer almalı, eğer sözleşme dışı (olay bazında) bir hizmet alınıyorsa da gizlilik anlaşması imzalanmalıdır. Kurum dışı bakım personeli mutlaka kurumdan ilgili çalışanların refakatinde olmalıdır (uzaktan bakım faaliyetleri dâhil).

BS denetçisi bu alanla ilgili denetim yaparken resmi bir bakım planının oluşturulduğunu kontrol etmelidir.

- Bu plan için yönetim onayı alınmış olmalıdır,
- Bakım işlemleri bu plan çerçevesinde yürütülmelidir,
- Bütçeyi aşan veya aşmış bakım maliyetlerini belirlemelidir, bunun sebeplerini sorgulamalıdır,
- Bakım sürecinin belirlenmiş yönergelere uygun işletilip işletilmediğini belirlemek için geçmiş bakım faaliyetlerini kanıtlarıyla beraber incelemelidir.

Bakım sürecinde güvenlik adımı mutlaka değerlendirilmelidir.

1.1.4.2. Donanım Performansını İzleme

Bilgi sistemleri altyapısında bulunan tüm donanımlar etkili ve verimli kullanımını garantilemek amacıyla uygun şekilde izlenmelidir. Performans izleme süreci proaktif ve sürekli işleyen bir süreçtir. Donanımın uygun araçlarla izlenmesini, raporlanmasını ve bu raporların yorumlanarak gereken aksiyonların alınmasını içerir. Sadece raporlama performans yönetimi için yeterli değildir. Diğer yandan performans raporlarından anlamlı bir sonuç çıkarabilmek için önce performans hedefleri ve amaçlar belirlenmelidir: Örneğin sistemin kabul edilebilir kesinti süresi nedir veya bakım maliyetlerini azaltmak hedeflenmekte midir? Bu hedeflere göre ölçülmesi gereken parametreler/sistemler ve eşik değerler belirlenir. Bu hedefler de aslında bilgi sistemlerinden beklenen hizmet seviyelerine karşı gelir (resmi bir SLA şeklinde veya resmi olmayan bir şekilde ifade edilmiş olabilir). Ancak bundan sonra elde edilen raporlar faydalı hale gelir.

Performans izleme süreci, kullanılan donanımların türü, sayısı, üretici farklılıkları ve kullanıldıkları iş süreçleri sebebiyle oldukça zahmetli ve çok fazla veri üreten bir süreç haline gelebilir. Burada iş süreçlerinin kritikliğine göre izlenecek sistemler arasında bir öncelik belirlemek, ayrıca elde edilen verideki her bulgu da büyük bir riske işaret etmeyeceği için tespit edilen bulgular arasında bir kritiklik seviyesi belirlemek uygun olacaktır.

Aşağıda bu amaçla kullanılabilecek bazı rapor türleri belirtilmiştir:

• **Erişilebilirlik raporları:** Bu raporlar, donanımların/bilgisayarın çalıştığı ve kullanıcılar veya diğer işlemler tarafından kullanılabileceği veya kullanılabildiği süreleri göstermektedir. Bu raporla ele alınan önemli bir endişe, kesinti süresi olarak adlandırılan normalden uzun erişim sıkıntılarıdır. Bu kesinti, yetersiz donanım kapasitesini, aşırı yükü, önleyici bakım ihtiyacını, yetersiz çevresel ekipmanı (örn. güç kaynağı veya klima) veya donanımın operatörleri için yetersiz eğitimi gösterebilir.

• **Donanım hata raporları:** Bu raporlar, merkezi işlem birimi, giriş/çıkış, güç ve depolama arızalarını belirtmektedir. Bu raporlar donanımın düzgün çalıştığından emin olmak, arızaları tespit

etmek ve düzeltici eylem başlatmak için bilgi sistemleri işletimi yönetimi tarafından gözden geçirilmelidir.

- **Varlık yönetimi raporları:** Bu raporlar işletmedeki her tür bilgisayar, sunucu, ağ cihazı, mobil cihaz ve diğer tüm donanımın envanterini sağlamaktadır. Varlık yönetimi uygulamaları açısından önemlidir. Varlık yönetimi ilerleyen bölümlerde detaylı şekilde açıklanacaktır.

- **Kullanım raporları:** Bu raporlar, donanımların kullanımını belgelemektedir. İşlemci kullanım yüzdesi, veri yolu yoğunluğu, disk ve teyp doluluk oranı gibi değerleri izlemek için kullanılır. Kullanım raporlarından belirlenen eğilimler, bilgi sistemleri yönetimi tarafından daha fazla veya daha az kaynağına gerek olup olmadığını tahmin etmek için kullanılmalıdır.

1.1.4.3. Donanım Tedarik Süreci

İşletmede donanım tedariki "*gerektiği zaman*" yaklaşımından farklı olarak belli bir planlama ile yapılmalıdır. Donanım tedarik planları yazılı olmalı ve değerlendirirken aşağıdaki hususların varlığı ve yeterliliği dikkate alınmalıdır:

- İş tarafının gereksinimlerine uyumu, bu uyumu sürekli kılmak için değişen iş ihtiyaçlarına bağlı olarak tedarik planının da güncelliğinin sağlanması,
- Kurumsal mimariyle ve bilgi sistemlerinin iş planlarıyla uyumu,
- İlgili iş birimlerinin sürece katkısı,
- Tedarik sırasında kullanılacak kriterlerin geliştirilip geliştirilmediği,
- Mevcut bilgi sistemleri altyapısının yeni donanımlara uygun olup olmadığının kontrolü, mevcut iş gücünün yeni donanıma ilişkin yetkinliği veya eğitim ihtiyacı,
- Teslim süresi de dâhil satın alma sürecine ilişkin bilgilerin belirlenip belirlenmediği.
- Üretici/dağıtıcılarla stratejik ilişkiler, risk yönetimi (donanım tedariki bir miktar risk içerebilir).

Donanım tedarik süreci değerlendirilirken de, ilk önce sürece ilişkin gerekli tüm politika ve prosedürlerin varlığı, üst yönetimce onayı, ilgili çalışanlara duyurulması ve farkındalığı dikkate alınmalıdır. Daha sonra örneklem yöntemiyle satın alınan donanımın bir önceki adımda belirlenen plan ve gereksinimlere uygun olup olmadığı değerlendirilmelidir.

Bunun yanı sıra satın alma öncesi fayda/maliyet analizinin yapılıp yapılmadığı ve satın alma sürecinin işletmenin satın alma birimi tarafından yönetilip yönetilmediği de kontrol edilmelidir. İşletmede tüm satın almaların belli bir birim tarafından yönetilmesi, süreçlerin tekrar edilebilir ve ölçülebilir olmasını, ihale ve mevzuat şartlarına uyum, toplu indirim gibi avantajlardan yararlanmayı sağlar.

1.1.5. Temel Yazılım Bileşenleri

1.1.5.1. İşletim Sistemleri

Bilgisayarlarda çalışan en önemli yazılım olan işletim sistemleri; bellek, işlemci ve ayrıca tüm yazılım ve donanımın yönetiminden sorumludur. Farklı uygulamaların aynı anda çalışırken merkezi işlem birimine (CPU, MİB), belleğe ve depolama birimlerine erişmeleri için bunları koordine eder. İşletim sistemi, bir bilgisayarda doğrudan donanımın üzerinde konuşlanmış, donanımı yöneten, kullanıcılara yönelik uygulamaları üzerinde barındıran ve bu uygulamalara hizmet veren, aynı zamanda kullanıcıya yönelik ara yüzü de bulunan bir yazılımdır. Kullanıcı/uygulama ile donanım arasında bir güvenli bölge olarak düşünülebilir. Üzerindeki tüm uygulamaların çalışmasını kontrol eder/yönetir. Kurumsal uygulamalar (muhasebe, insan kaynakları vb.), ofis yazılımları, elektronik posta yazılımları, veri tabanı yönetim sistemleri işletim sistem olmadan çalışamazlar. Pratik olarak bir işletim sistemi ile bilgisayar ayrılmaz bir ikilidir. Burada bilgisayar denince akla sadece bir masa üstü veya diz üstü değil, tüm sunucular, mainframe bilgisayarlar, kutu şeklinde donanımlar, tablet, cep telefonu gibi ürünler gelmelidir.

Bilgisayarı oluşturan temel bileşenler olan merkezi işlem birimi, bellek, ikincil depolama, giriş/çıkış sisteminin yönetimi tümüyle işletim sistemi tarafından sağlanır. Burada yönetimden kasıt kabaca kaynak taleplerine cevap verilmesi, işlerin senkronize edilmesi, hataların çözülmesidir.

İşletim sistemi üzerinde çalışan tüm diğer uygulamaların (ister kutu olarak satın alınmış olsun, ister kurum içinde geliştirilmiş olsun) hiçbir şekilde donanıma erişimi yoktur o zaman donanımla etkileşim nasıl gerçekleşecektir? Örneğin kullanıcının bir forma girdiği bilgiler nasıl diske yazılacak? Bu ve bunun gibi tüm işlevler için işletim sisteminin hizmet olarak sunduğu küçük programcıklar bulunur (application programming interface, API). Tüm uygulamalar da kodlarından bu programcıkları çağırır, bu şekilde donanımla etkileşime girerler, işletim sisteminden hizmet almış olurlar. Diğer yandan işletim sistemlerinin kullanıcılara dönük iki temel ara yüzü bulunmaktadır: Metin tabanlı komut satırı (command line interface-CLI) olarak veya her seviyede kullanıcıya yönelik grafik arayüz olarak.

İşletim sistemlerinin temel fonksiyonları aşağıdaki gibi gruplandırılabilir:

- İşlem (process) yönetimi: Herhangi bir program (örneğin bir kullanıcı uygulaması) çalışırken "iş/görev (process)" adını alır. Bir program çalışmak için öncelikle merkezi işlem birimine (MİB) ihtiyaç duyar. Ancak bir bilgisayarda belirli bir anda MİB erişimine ihtiyaç duyan birden çok iş olabilir (genelde olur). Bu şekilde MİB erişimi isteyen işler arasında öncelik belirleme, MİB'i işlere tahsis etme ve serbest bırakma, işler arası zaman uyumlama ve iletişimin sağlanması gibi faaliyetler işlem yönetiminin konusudur.

- Bellek (memory) yönetimi: Kısaca bilgisayarın ana belleğinin (RAM) yönetimidir. Belleğin işler arasında paylaştırılması, sanal bellek yönetimi (işlerin gereksinim duyduklarından daha az bellek ile çalışmalarını sağlamak, paging), kullanılabilir bellek bölümlerini işler arasında dağıtmak, işlerin belleğe erişimini yönetmek ve belleğin çalışmasını iyileştirmek gibi işlevler bellek yönetiminin konusudur.

- Aygıt (device) yönetimi: Bilgisayara bağlı olan tüm aygıtların (giriş/çıkış birimleri) yönetimidir. İşletim sistemi aygıtlarla iletişimi aygıtın kendi yönetim programı (device driver) aracılığı ile gerçekleştirir.

- Ağ yönetimi: Günümüzde özellikle iş ortamlarında, tek başına (stand alone) biçimde hiçbir ağa bağlı olmadan çalışan bilgisayar olsa bile çok azdır. Bu yüzden ağ yönetim fonksiyonları işletim sisteminin içinde düşünülebilir.

- Güvenlik yönetimi: Kısaca işletim sisteminin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamakla ilişkilidir. "İşletim Sistemi Bütünlüğü" adlı bölümde detaylı incelenmiştir.

- Kullanıcı arayüzü yönetimi: Kullanıcı arayüzleri, kullanıcıları (her seviyeden) ve işletim sistemini birbirine bağlar. Kullanıcılar bu şekilde doğrudan işletim sistemiyle etkileşime girer. Kabaca iki farklı kullanıcı arayüzü bulunmaktadır: Komut satırı ve grafik arayüzü.

İşletim sisteminin en temel bileşenine "kernel (çekirdek)" adı verilir. Bilgisayarın tüm birimleri (ana bellek, tüm aygıtlar, işlemci) üzerinde doğrudan kontrolü vardır. Uygulamalar (kullanıcı programları) ile bilgisayar donanımları arasındaki iletişimi yönetir. Bu bileşen genelde, işlem (process) yönetimi, bellek yönetimi ve aygıt yönetimi gibi daha temel fonksiyonlardan sorumludur. İşletim sistemi, kullanıcılar ile donanım arasındaki arayüz olarak düşünülebilir, bu durumda kernel, donanım ve yazılımlar arasındaki arayüzdür. Bilgisayarda gerçekleştirilen tüm işlemler mutlaka kernel üzerinden geçer.

İşletim sistemlerinin birçok türü bulunmakla birlikte kurumsal bilgi sistemleri ve kişisel bilgisayarlar için en yaygın üç işletim sistemi Microsoft Windows, Unix/Linux ve Mac OS'tur.

- **Windows**

Windows, Microsoft tarafından geliştirilen bir işletim sistemi olup ilk sürümünden bu yana kişisel bilgisayarlar için en popüler işletim sistemi olmuştur.

Windows'un her sürümü, varsayılan olarak ekranın altında görüntülenen bir görev çubuğu ve simgeler içeren bir masaüstünden oluşan bir grafik kullanıcı arayüzü ile gelir. Windows "Dosya Gezgini", kullanıcıların birden çok pencere açmasına, klasörlere göz atmasına ve dosya ve uygulamaları açmasına olanak tanımaktadır. Çoğu Windows sürümü, dosyalara, ayarlara ve Windows arama özelliğine hızlı erişim sağlayan bir "Başlat" menüsü içermektedir.

Windows, standart x86 donanımlarında çalışır ve Microsoft, işletim sistemini birden çok üreticiye lisanslar. Bu nedenle birçok farklı bilgisayar şirketi Windows işletim sistemini içeren bilgisayar satmaktadır.

Windows için yazılmış programlar ve uygulamalar .exe dosya uzantısına sahiptir. Windows'un 64 bit sürümleri hem 32 bit hem de 64 bit uygulamaları çalıştırırken, 32 bit sürümleri yalnızca 32 bit uygulamaları çalıştırır.

Günümüzde Windows işletim sisteminin sunucu sürümleri de mevcut olup pek çok işletmede yaygın olarak kullanılırlar.

- **Unix, Linux**

Unix işletim sistemi ilk olarak 1960'larda oluşturulmuştur. İlerleyen yıllarda üst düzey bilgi işlem merkezlerinde popüler hale gelmiştir. Tüketiciler arasında yaygınlaşması, pek çok hizmet başlangıçta Unix makinelerinde barındırıldığından, internetin yaygınlaşmasıyla daha da popülerlik kazanmış olup hala web sunucuları için en yaygın işletim sistemi olarak endüstriye öncülük etmektedir.

Linux, Unix benzeri bir işletim sistemidir. İşletmeler adına web sitelerini barındırma (web hosting) faaliyeti gösteren şirketler web sunucularına genellikle Linux kurar çünkü Linux tabanlı sunucuların kurulumu ve bakımı Windows tabanlı sunuculardan daha ucuzdur. Linux işletim sistemi özgürce dağıtıldığı için lisans ücreti yoktur. Bu, Linux sunucularının hiçbir ek ücret ödemeden yüzlerce hatta binlerce web sitesini barındırabileceği anlamına gelir. Windows sunucuları ise genellikle sunucuda barındırılan her web sitesi için kullanıcı lisansı gerektirmektedir.

Linux çeşitli dağıtımlarda mevcuttur. En popüler dağıtımlardan bazıları Red Hat Enterprise, CentOS, Debian, openSUSE ve Ubuntu'dur. Linux ayrıca Intel, PowerPC, DEC Alpha, Sun Sparc ve Motorola dâhil olmak üzere geçmişten günümüze çeşitli donanım platformlarını da desteklemiştir. Linux pek çok donanım türüyle uyumlu olduğundan, Linux işletim sisteminin varyasyonları bilgisayarların yanı sıra diğer birçok elektronik aygıt için de kullanılır. Bazı örnekler arasında cep telefonları, kablo kutuları ve oyun konsolları sayılabilir.

- **MacOS**

Macintosh İşletim Sistemi (Mac OS), Apple tarafından Apple Macintosh serisi bilgisayarlara kurulmak ve çalıştırılmak üzere tasarlanmış ve yayınlandığı tarihten itibaren birden çok farklı sürüm olarak piyasaya sürülen bir grafik kullanıcı arabirimi (GUI) tabanlı işletim sistemidir.

Mac OS, GUI tabanlı işletim sistemlerinin öncüsü olarak kabul edilir. Mac OS, Windows veya Linux işletim sistemine benzer işlevler ve hizmetler sağlayan tamamen yetenekli bir işletim sistemidir. Mac OS, Apple tarafından üretilen PC'lerde çalışacak şekilde tasarlanmıştır ve varsayılan olarak x86 mimarisini desteklememektedir.

Mobil cihazlar için yaygın işletim sistemleri

Günümüzde birçok türü bulunmakla birlikte mobil cihazlar için en yaygın işletim sistemleri Android ve iOS'tur.

- **Android**

Android işletim sistemi, öncelikle dokunmatik ekranlı cihazlar, cep telefonları ve tabletler için kullanılmak üzere Google tarafından yayınlanan bir mobil işletim sistemidir. Tasarımı, kullanıcıların sıkıştırma, kaydırma ve dokunma gibi genel hareketleri yansıtan parmak hareketleriyle mobil cihazları sezgisel olarak yönetmesine olanak tanımaktadır. Android'in temel çekirdeği Linux'a dayanmaktadır, ancak Google tarafından özelleştirilmiştir.

- **IOS**

IOS, Apple tarafından üretilen cihazlar için (iPhone, iPad, iPod Touch, Apple TV, vb) bir mobil işletim sistemidir. iOS, iPhone kullanıcılarının telefonlarıyla kaydırma ve dokunma gibi hareketleri kullanarak etkileşim kurmasını sağlar.

1.1.5.2. İşletim Sistemi Bütünlüğü

İşletim sistemi bütünlüğü, işletim sisteminin çok önemli bir gereksinimi ve yeteneği olup aşağıdaki özellikleri sağlamak için belirli donanım ve yazılım özelliklerinin kullanılmasını içerir:

- Kasıtlı/kasıtsız değişikliklerden kendini korumak.
- Ayrıcalıklı programlara kullanıcı programları tarafından müdahale edilmediğinden emin olmak.
- Etkili işlem izolasyonu sağlamak:
  - Eşzamanlı olarak çalışan birden çok işlem kazara veya kasten birbirini etkilemez ve birbirlerinin belleğine yazmaktan korunur (örn. talimatları değiştirmek, kaynakları paylaşmak vb.).
  - Süreçlerin işlevleri gerçekleştirmek için gerekenden daha fazla ayrıcalığa sahip olmadığı ve modüllerin yalnızca gerektiğinde ve yalnızca yeterli süre için daha ayrıcalıklı rutinleri çağırdığı durum olan en az ayrıcalık ilkesinin uygulanması.

İşletim sisteminde bütünlük, hem işletim sisteminin tasarımı aşamasında (yanlış bir tasarım istenmeden kötü sonuçlara yol açabilir), hem de işletimi aşamasında ele alınır.

İşletimsel (operasyonel) aşamada güvenliği ve bütünlüğü sağlamak için alınabilecek önlemler şu şekilde özetlenebilir (*bu önlemlerin detaylı açıklaması 1023 numaralı Bilgi Sistemleri Güvenliği çalışma notunda yer almaktadır*):

Zararlı yazılımlara karşı koruma, fiziksel ve çevresel koruma, etkin bir kimlik tanıma/yetkilendirme mekanizmasının kullanımı, bir ağda çalışan makinalar için ağ güvenlik önlemlerinin uygulanması. Bunlar genellikle önleyici kontrollerdir, bunun yanı sıra tespit edici kontroller olarak da iz kayıtlarının alınması, sızma testleri, erişim haklarının gözden geçirilmesi gibi süreçler işletilmelidir.

Sistem ve veri bütünlüğünü korumak için, işletim sisteminde verilen izinleri doğru ve tutarlı bir şekilde tanımlamak, uygulamak ve izlemek gerekir. Bilgi güvenliği yönetimi, ayrıcalıklı olmayan kullanıcıların ayrıcalıklı komutlar çalıştırabilme ve böylece tüm makinenin kontrolünü ele geçirme yeteneğini kazanmasını önlemek için uygun yetkilendirme tekniklerinin kullanılmasından sorumludur.

İşletim Sistemlerinin Denetimi

Kurumda işletim sistemlerinin denetiminde hem genel kontroller, hem de kullanılan ürüne göre spesifik kontroller incelenmelidir. Aşağıda belirtilen hususlar genel bir liste olarak düşünülebilir:

BS denetçisi tüm işletim sistemlerindeki sistem yapılandırma dosyalarını kontrol etmelidir. Unix, Linux ve Windows işletim sistemlerinde özel sistem yapılandırma dosyaları ve dizinleri yer alır. Yazılımsal zafiyetlerin varlığı veya sistemlerin en son güvenlik yamalarıyla yapılandırılması halinde kontrol ve güncellenme işlemlerinde hata oluşması gibi durumlar saldırganlar tarafından ele geçirilme riskine karşı sistemi savunmasız bırakabilir.

Önemli Windows sistem seçenekleri ve parametreleri, kayıt defteri (registry) olarak adlandırılan özel sistem yapılandırma dosyalarında ayarlanmaktadır. Bu nedenle kayıt defterinin gözden geçirilmesi, BS denetiminin önemli bir kontrol hedefidir. Kayıt defterinde yapılan değişikliklerin kontrollü yapılması kritiktir. Yapılan değişiklikler sistemlerin bütünlüğünü, gizliliğini ve erişilebilirliğini etkilemektedir. UNIX tabanlı işletim sistemlerinde de aynı sorunlar vardır. Çekirdek (kernel) işlemleri, sistem başlatma, ağ dosya paylaşımı ve diğer uzak hizmetler ile ilgili kritik sistem yapılandırma dosyaları ve dizinleri uygun şekilde korunmalı ve doğruluk açısından kontrol edilmelidir.

Bir BS denetçisi, denetimler esnasında işletmenin sistemlerine erişim için çalışanlarına, dış kaynak hizmeti aldığı taraflara ve müşterilerine sağladığı mobil hizmetlerde güvenlik önlemlerini uygun şekilde aldığına dair kanıtları gözden geçirmelidir.

Üreticilerin/destek sağlayıcıların önerdiği en son sürüm kullanılmalıdır. Sunucular güvenlik duvarı arkasında konuşlanmış olmalıdır. Zararlı yazılımlara karşı gerekli uygulamalar yüklü olmalı ve bunların devamlı güncelleme alması sağlanmalıdır.

İşletim sistemi üzerinde kullanıcı ekleme ve silme/etkisizleştirmeye ilişkin prosedürler incelenmelidir. Bu konu mutlaka yazılı ve onaylı bir şekilde mevcut olmalıdır. Sistemde rastgele seçilen kullanıcılar için (ki içlerinde her yetki seviyesinden birer örneğin olması gerekir) sürecin kanıtları aranır. Kurum, erişim yönetimi kapsamında muhakkak periyodik yetki kontrolleri de yapmalı ve bunun kanıtları denetimde sorgulanmalıdır.

Sistemde şifre yönetimi ile ilgili yapılandırma ayarları incelenmelidir. Şifre yönetimi ile ilgili hususların kullanıcılar tarafından da biliniyor olması gerekir.

Belli bir çalışma grubu için kısa süreliğine açılmış paylaşım alanları genelde grubun işi sonlandıktan sonra unutulur ve buradaki yetkiler geri alınmaz. Bu konuda periyodik gözden geçirme gerekir.

Sunucular üzerindeki açık portlar ve gerekçeleri sorgulanmalıdır. Sistemlere uygulanan sızma testleri gözden geçirilmeli ve zafiyetlerin son durumu öğrenilmelidir.

Sunucu bazında yüklü uygulamalar incelenmeli ve gerekçesi sorgulanmalıdır. Bu kapsamda sunucular üzerine servis olarak yüklenen birçok işin, gereksinim kalktıktan sonra da işlerliğini devam ettirdiği görülmüştür. Bu konu ayrıca incelenmelidir.

En önemli konulardan biri de, sunucular üzerinde operatör ve yetkili kullanıcıların yaptıkları işlemlerin iz kayıtlarının alınıp alınmadığıdır. Bu husus da süreci ile beraber incelenmelidir.

Sunucular üzerinde ortaya çıkan problemleri takip edebilmek amacıyla bir gözetim (monitoring) mekanizması mevcut olmalıdır. Bu konu kanıtlarıyla beraber incelenmelidir.

1.1.5.3. Sıkılaştırılmış Baz Konfigürasyonlar

İşletim sistemlerinin, birçok yaygın altyapı bileşeninin, sunucuların ve bulut hizmetlerinin yönetimi için konfigürasyon yönetimi bilgi güvenliğinin üç temel bileşeni olan gizlilik, bütünlük ve erişilebilirlik gereksinimlerinin sağlanması için üst düzeyde önem arz etmektedir. Kurumların sıkılaştırılmış ve test edilmiş baz konfigürasyonlar belirleyerek altyapı yönetimini sağlaması beklenmektedir.

Bunun için, dünya çapında kâr amacı gütmeyen bağımsız bir organizasyon olan The Center for Internet Security, Inc. (CIS®), günümüzde yaygın olarak kullanılmakta olan hemen her sistem ve sürümü için baz konfigürasyon önerilerini yayınlamaktadır. Bunlara örnek olarak aktif dizin parola parametreleri, veri tabanı sunucusunda kapalı olması gereken portlar, işletim sisteminde çalışması gereken servisler, bulut hizmet sağlayıcıları özelinde yönetim konsolu parametreleri gibi konular verilebilir.

BS denetçileri, ağ ve altyapı güvenliği denetimleri kapsamında, işletmenin baz konfigürasyon yaklaşımına göre, mevcut baz konfigürasyonları ve bunların yönetimi ile ilgili konuları değerlendirmelidir.

1.1.5.4. Sanallaştırma

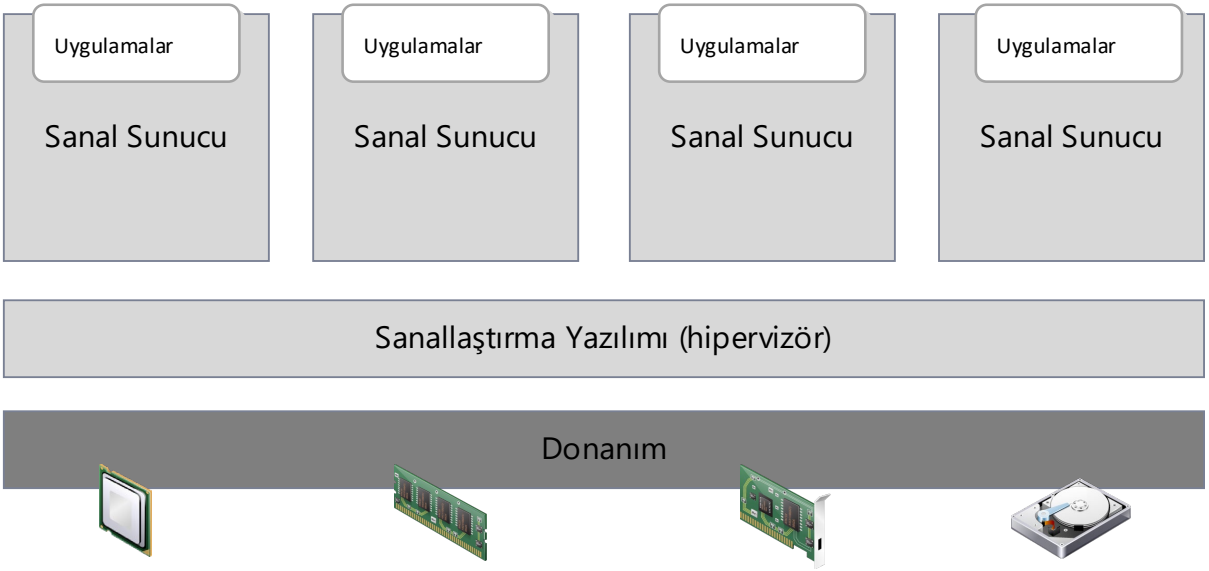
Sanallaştırma, donanıma bağlı kaynakların birçok kullanıcı veya ortam arasında dağıtılarak fiziksel bir makinenin tam kapasitesinin kullanılmasına olanak tanıyan teknolojiye verilen genel isimdir. Sanallaştırma ile bir sunucu bağımsız görevleri yerine getirebilecek iki ya da daha çok sayıda sunucuya bölünebilmektedir. Bu durum, eldeki donanımın daha verimli kullanımına olanak tanımaktadır. Ayrıca boşa çıkan sunucular sayesinde soğutma ve bakım maliyetlerinin azalması, başka görevler için yeniden kullanılabilmesi veya tamamen kullanımdan kaldırılması mümkün olabilmektedir.

Sanallaştırma teknolojisi, sanallaştırma yazılımı uygulamalarının ortaya çıkmasıyla yaygın olarak benimsenmiştir. İşletmeler bu sayede farklı bir satıcının ürününü/yazılımını kendi donanımında çalışmasına izin vermeyen fiziksel sunuculara alternatif bulmuş ve işletmeler çeşitli üreticilerin daha ucuz sunucuları, işletim sistemleri ve uygulamalarıyla güncellendikçe yetersiz fiziksel donanıma bağımlılıktan kurtulmuştur. Sanallaştırmanın yaygın olarak kullanımı, üretici bağımlılığını azaltmaya yardımcı olmuş ve bulut bilişimin temeli haline gelmiştir.

- **Sanallaştırma Yazılımı (Hipervizör)**

Sanallaştırma yazılımı, bir işletim sisteminin üzerine veya doğrudan donanıma kurularak fiziksel kaynakların sanal ortamlardan ayrılmasını sağlamaktadır. Sanallaştırma yazılımları fiziksel kaynakları sanal ortamlara bölmektedir.

Kullanıcılar sanal makinayla etkileşime girerek işlemlerini gerçekleştirmektedir. Sanal makina, tek bir veri dosyası olarak işlev görmekte ve elektronik ortamdaki herhangi bir dosya gibi bir bilgisayardan diğerine taşınabilmektedir.



Şekil 4: Sanallaştırma mimarisi örneği

Sanal ortamda çalışan bir kullanıcı veya program, fiziksel ortamdan ek kaynaklar gerektiren bir talimat verdiğinde sanallaştırma yazılımı isteği fiziksel sisteme iletmekte ve değişiklikleri önbelleğe almaktadır. Yaygın sanallaştırma türlerine aşağıda değinilmiştir:

Sunucu sanallaştırma

Bir sunucunun sanallaştırılması, sunucunun birden çok iş/görev yapmasına izin vermekte ve kaynaklarının birden çok işe hizmet etmek amacıyla kullanılabilmesi için bölümlere ayrılmasını sağlamaktadır.

İşletim sistemi sanallaştırma

İşletim sistemi sanallaştırması işletim sistemlerinin merkezi görev yöneticileri olan çekirdekte gerçekleşmektedir. Linux ve Windows ortamlarını yan yana çalıştırmanın kullanışlı bir yolu olup ayrıca sanal işletim sistemlerini bilgisayarlara aktarılabilmekte ve toplu donanım maliyetleri azaltılabilmektedir. Tüm sanal örnekler izlenebildiği ve izole edilebildiği için güvenliği artmakta, yazılım güncellemeleri gibi hizmetlere harcanan süre azalmaktadır.

Veri sanallaştırma

Veri sanallaştırma, işletmelerin verileri dinamik bir kaynak olarak ele almalarına olanak tanımakta ve birden çok kaynaktan gelen verileri bir araya getirebilen, yeni veri kaynaklarını kolayca barındırabilen ve verileri kullanıcı ihtiyaçlarına göre dönüştürebilen işlem yetenekleri sağlamaktadır.

Masaüstü sanallaştırma

Birden çok işletim sisteminin tek bir makineye dağıtılmasına olanak sağlayan masaüstü sanallaştırma, bir yöneticinin (veya otomatikleştirilmiş yönetim aracının) merkezi olarak masaüstü ortamlarını kopyalayarak aynı anda yüzlerce fiziksel makineye dağıtmasını mümkün kılmaktadır. Her makinede fiziksel olarak kurulan, yapılandırılan ve güncellenen geleneksel masaüstü ortamlarının aksine masaüstü sanallaştırma, yöneticilerin tüm sanal masaüstlerinde toplu yapılandırmalar, güncellemeler ve güvenlik kontrolleri gerçekleştirmesine olanak tanımaktadır. Çok kullanıcılı işletmelerde yönetim kolaylığı sağlar.

Ağ fonksiyonlarını sanallaştırma

Ağ fonksiyonlarının sanallaştırılması (NFV), bir ağın temel işlevlerini (dizin hizmetleri, dosya paylaşımı ve IP yapılandırması gibi) ayırarak bunların ortamlar arasında dağıtılmasına olanak sağlamaktadır. Yazılım işlevleri fiziksel makinelerden bağımsız olduğunda, belirli fonksiyonlar birlikte gruplanarak yeni bir ortama atanabilmektedir. Ağları sanallaştırmak, birden çok bağımsız ağ oluşturmak için gereken anahtarlar, yönlendiriciler, sunucular, kablolar ve diğer aygıtlar gibi fiziksel bileşenlerin sayısını azaltmakta ve özellikle telekomünikasyon endüstrisinde yaygın olarak kullanılmaktadır.

Sanal sunucu kullanımının riskleri[2]

Sanal ortamlara geçiş, yeni ortamın daha karmaşık olması ve güvenlik için yeni bir yaklaşım gerektirmesi nedeniyle birtakım riskleri de barındırmaktadır. Sanallaştırma yazılımlarının kendileri de gerekli güncelleme ve güvenlik açığı taramalarına tabi olmadıkları takdirde zafiyet yaratabilecektir.

BS denetçileri denetim planı hazırlarken sanal sunucular için oluşan riskleri göz önünde bulundurmalıdır. Oluşacak bu risklere örnek aşağıdakiler verilebilir:

- Kaynak kullanımı
- Aynı sunucuda yer alan farklı güvenlik seviyelerine sahip iş yükleri
- Sanal ağlar üzerinde görünürlük ve kontrol edilme periyodu ve süreci
- Sanal cihazların içerisinde yer alan hassas veriler ve korunması
- Çevrimdışı kalan sanal makinaların güvenliği

[2] Cloud Security Alliance, "Best Practices for Mitigating Risks in Virtualized Environments.", 2015.

Maliyet ve yönetim bakımından birçok avantaj sağlayan sanallaştırma teknolojisi, birçok kuruluşun bir arada aynı fiziksel sunucuda çalıştığı ortak/paylaşımlı bulut hizmeti modellerinde güvenlik açısından dezavantajlı olabilmektedir. Bir kuruluşun sistemlerinde yaşanabilecek bir güvenlik açığı, diğerlerinin de etkilenmesine sebep olabilir. Bu nedenle özellikle hassas verilerin, kritik uygulamaların ve veri tabanlarının çalıştığı sanal sunucuların, diğer kuruluşlarla aynı fiziksel sunucuda ve paylaşımlı olarak kullanılmaması önerilmektedir.

1.1.6. Veri Yönetişimi

Bilgi sistemlerinin kurumsal yönetim uygulamalarının bir parçası olarak ele alınarak iş hedefleriyle uyumlu bir şekilde kurumsal verinin güvenliğinin, performansının, etkinliğinin, doğruluğunun ve sürekliliğin sağlanması ancak etkin bir veri yönetişim çerçevesinin oluşturulması ve kurum genelinde uygulanmasıyla mümkün olmaktadır. Bu kapsamda ele alınması gereken en önemli başlıklardan biri verinin nasıl yönetileceğidir. Aşağıdaki hususlar veri yönetişimi süreçleri tasarlanırken göz önünde bulundurulmalıdır:

- Veri yönetimi stratejisinin, rollerin ve sorumlulukların tanımlanması ve duyurulması,
- İş süreçlerinde kullanılan terimlerin tutarlı bir sözlüğünün oluşturulması ve sürdürülmesi,
- Veri imha yaklaşımlarının belirlenmesi,
- Veri kalitesi stratejisinin belirlenmesi ve kalite değerlendirme yaklaşımının uygulanması,
- Verilerin profillenmesi için yöntem, süreç ve araçların oluşturulması,
- Meta veri yönetimi (veri sözlüğü-data dictionary) için süreçlerin ve altyapının oluşturulması,
- Veri yedekleme ve geri dönüş sürecinin yönetilmesi,
- Veri varlıklarının yaşam döngüsünün yönetilmesi,
- Veri arşivleme ve saklamanın desteklenmesi.[3]

1.1.6.1. Veri Yönetimi

Verilerin güvenli, verimli ve uygun maliyetli bir şekilde toplanması, saklanması ve kullanılmasını sağlayan veri yönetiminin amacı; kişilere, kuruluşlara ve paydaşlara, politika ve düzenlemeler dâhilinde veri kullanımının optimize edilmesinde yardımcı olmaktır.

Veri Kalitesi

Veri yönetiminin beklendiği şekilde gerçekleştirilmesi için en önemli unsurlardan biri veri kalitesinin sağlanmasıdır. COBIT 2019 çerçevesine göre veri kalitesi üç alt başlıkta değerlendirilmelidir. Her bir alt başlık ayrıca, çeşitli kalite kriterlerine ayrılmıştır.[4]

İçsel: Veri değerlerinin ne kadar gerçek veya gerçek değerlerle ne ölçüde uyumlu olduğunu ifade etmektedir:

- Kesinlik: Verinin ne kadar doğru ve güvenilir olduğu,
- Nesnellik: Verinin ne ölçüde tarafsız ve önyargısız olduğu,
- İnanılırlık: Verinin ne ölçüde doğru ve güvenilir olarak kabul edildiği,
- İtibar: Verinin kaynağı veya içeriği açısından ne ölçüde dikkate alındığı.

Bağlamsal: Verinin, kullanıcısının görevine ne ölçüde uygulanabilir olduğu ve kalitesinin kullanım bağlamına bağlı olduğunu kabul ederek anlaşılır ve açık bir şekilde sunulduğunu ifade etmektedir:

[3] COBIT 2019, Governance Management Objectives, ISACA, 2018.
[4] Information Reference Model: Quality Criteria for Information, COBIT 2019, Introduction and Methodology, 2018.

- İlgililik: Verinin eldeki görev için ne ölçüde uygulanabilir ve yararlı olduğu,
- Tamlık: Verinin eksik olmadığı ve eldeki görev için yeterli derinlik ve genişlikte olduğu,
- Geçerlilik: Eldeki görev için verilerin ne kadar güncel/geçerli olduğu,
- Yeterlilik: Veri hacminin eldeki görev için ne ölçüde yeterli olduğu,
- Özlülük: Verinin ne kadar öz/kısa bir şekilde sunulduğu,
- Tutarlılık: Verinin sunulduğu formatın tutarlılığı,
- Yorumlanabilirlik: Verilerin net şekilde tanımlanmış ve uygun dillerde, sembollerde ve birimlerde olduğu,
- Anlaşılabilirlik: Verinin ne kadar kolay anlaşıldığı,
- Manipüle edilebilirlik: Verinin manipüle edilmesinin ve farklı görevlere uygulanmasının ne ölçüde kolay olduğu,
- Güvenlik/gizlilik/erişilebilirlik: Bilginin ne ölçüde mevcut veya elde edilebilir olduğu,
- Kullanılabilirlik: Bilginin gerektiğinde ne ölçüde erişilebilir olduğu veya kolay ve hızlı bir şekilde döndürülebileceği,
- Gizlilik: Bilgiye erişimin yalnızca yetkili taraflarla kısıtlanması.

BS Denetçisi tarafından veri kalitesi sürecinin içermesi gereken konular aşağıdaki şekilde belirlenebilir:

- Veri değerlerinin doğru ve güvenilir olması,
- Verilerin tarafsız olması,
- Verilerin saklama politikasına uygun şekilde arşivlenmesi ve periyodik olarak kontrol edilmesi,
- Veri kalitesinin değerlendirildiğine ilişkin kontrollerin yapılması ve kayıtlarının saklanması,
- Veri kalitesi ölçümlerine ait periyodik olarak raporların oluşturulması,
- Veri kalitelerinin işletmeye ait stratejik hedefler ile uyumlu olması.

1.1.6.2. Veri Yaşam Döngüsü

Veri yaşam döngüsü yönetimi, verilerin bir kuruluştaki varlığı süresince geçtiği aşamaları tanımlamakta ve aşağıdaki öğeleri içermektedir:

Planlama: Veri kaynağının yaratılması, elde edilmesi ve kullanılmasının hazırlandığı aşamadır. Bu aşamadaki faaliyetler, ilgili iş süreçlerinde veri kullanımını anlamak, veri varlığının değerini ve ilişkili sınıflandırmasını belirlemek, hedefleri belirlemek ve veri mimarisini planlamaktır.

Tasarım: Verinin nasıl görüneceğini ve veriyi işleyen sistemlerin nasıl çalışması gerektiğini belirtmek için daha ayrıntılı çalışmanın yapıldığı aşamadır. Bu aşamadaki faaliyetler standartların ve tanımlarının (örn. veri tanımları, veri toplama, erişim, depolama prosedürleri, üst veri özellikleri) ve veri sınıflandırmasının geliştirilmesini ifade edebilir.

Geliştirme/tedarik: Veri kaynağının edinildiği aşama. Bu aşamadaki faaliyetler, veri kayıtlarının oluşturulması, verilerin satın alınması ve harici dosyaların yüklenmesi anlamına gelebilir.

Kullanım/işletim: Bu aşama şunları içerir:

- Saklama: Verilerin elektronik olarak veya basılı olarak (veya sadece insan belleğinde) tutulduğu aşamadır. Bu aşamadaki faaliyetler, verilerin elektronik biçimde (örn. elektronik dosyalar,

veri tabanları ve veri ambarları) veya basılı kopya olarak (örn. kâğıt belgeler) saklanmasını ifade edebilir.

• Paylaşma: Verinin bir dağıtım yöntemi ile kullanıma sunulduğu aşamadır. Bu aşamadaki faaliyetler, verinin erişilebildiği ve kullanılabileceği yerlere (örn. belgeleri e-posta ile dağıtma) ulaşmasında yer alan süreçleri ifade edebilir. Elektronik olarak tutulan veriler için bu yaşam döngüsü aşaması büyük ölçüde saklama aşamasıyla çakışabilir (örn. veri tabanı erişimi ve dosya/belge sunucuları aracılığıyla veri paylaşımı).

• Kullanım: Verinin iş hedeflerine ulaşmak için kullanıldığı aşamadır. Bu aşamadaki faaliyetler her türlü veri kullanımını ifade edebilir (örn. yönetimsel karar verme ve otomatik süreçleri çalıştırma, veri alma ve veriyi bir biçimden diğerine dönüştürme gibi faaliyetler). Veri modelinde tanımlandığı gibi veri kullanımı, kurumsal paydaşların rollerini üstlenirken, faaliyetlerini yerine getirirken ve birbirleriyle etkileşimde bulunurken veriye ihtiyaç duydukları amaçlar olarak düşünülebilir.

• İzleme: Veri kaynağının düzgün çalışmaya (yani değerli olmaya) devam etmesinin sağlandığı aşamadır. Bu aşamadaki faaliyetler, verilerin güncel tutulmasını ve diğer veri yönetimi faaliyetlerini (örn. veri ambarlarında yinelenen bilgileri geliştirme, temizleme, birleştirme ve ortadan kaldırma) ifade edebilir.

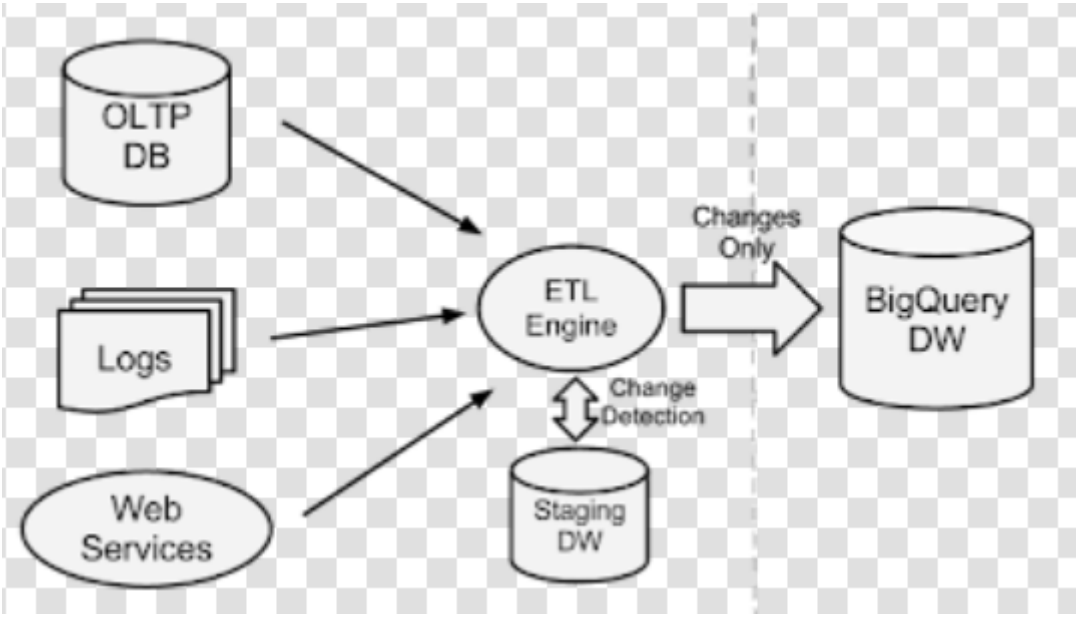
• Elden çıkarma: Veri kaynağının belirli bir süre için aktarıldığı veya tutulduğu, imha edildiği veya gerektiğinde bir arşivin parçası olarak işlendiği aşamadır. Bu aşamadaki faaliyetler, verinin saklanması, arşivlenmesi veya imha edilmesi anlamına gelebilir.

BS denetçisi, verilerin kalitesinin kuruluşun stratejik hedeflerine ulaşmasına imkân verip vermediğini değerlendirmelidir. Ayrıca kuruluşun uygulamalarının ve veri tabanı yönetim sistemlerinin yapılandırmasının kuruluş hedefleriyle uyumluluğunu gözden geçirmelidir. Örneğin, verilerin veri saklama politikası doğrultusunda kayıt altına alınması, arşivlenmesi veya imha edilmesi sağlanıyor mu?

Verilerin korunması için alınabilecek önlemler arasında kurum genelinde veri sınıflandırmasına göre ağ bölümlenmesinin uygulanması, veri kaybı önleme sistemleri ve ağ trafiğinin şifrelenmesi, yazılım, donanım ve verilerin bütünlüğünü doğrulamak için mekanizmaların mevcudiyeti, hareketsiz ve iletim halindeki verilerin şifrelenmesi sayılmaktadır.

Veri Akış Şeması (DFD)

Bir veri akış şeması (DFD), verilerin bir sistem tarafından girdiler ve çıktılar açısından nasıl işlendiğini, odak noktasına bilginin akışını, verilerin nereden geldiği, nereye gittiği ve nasıl depolandığını alarak göstermektedir. Bir bilgi sistemi aracılığıyla verinin "akışının" süreç yönlerini modelleyen grafiksel bir temsilidir. Genellikle sisteme genel bir bakış oluşturmak için kullanılmaktadır. DFD'ler ayrıca verinin nasıl işlendiğini görselleştirmek için kullanılmakta ve sisteme ne tür bilgilerin girileceğini ve sistemden hangi bilgilerin çıkacağını, verilerin nereden gelip nereye gideceğini ve verilerin nerede saklanacağını göstermektedir. Ancak süreçlerin zamanlaması hakkında bilgi veya süreçlerin sırayla mı yoksa paralel olarak mı çalışacağı hakkında bilgi içermemektedir.



Şekil 5: Veri Akış Şeması Örneği

1.1.6.3. Veri Tabanı Yönetim Sistemleri ve Veri Ambarı

Veri Tabanı Yönetim Sistemleri

Veri tabanı, verilerin organize edilmiş bir şekilde oluşturulması, saklanması ve yönetilmesini sağlayan yazılımların genel ismidir. Temel hedefleri uygulama programlarının ihtiyaç duyduğu verilerin düzenlenmesine, kontrol edilmesine ve kullanılmasına olanak sağlamaktır. Bunun yanı sıra, verilerin mükerrerliğinin en aza indirilmesi, erişilebilirlik süresinin artırılması ve hassas verilere yönelik güvenlik önlemlerinin alınmasına imkân vermesi de diğer kullanım amaçları arasında sayılabilir. Veri tabanı sistemleri günümüzde yönetim araçlarını da içerecek şekilde veri tabanı yönetim sistemi (database management systems, VTYS) olarak adlandırılırlar.

Veri Tabanı Türleri

Günümüzde kurumsal anlamda veri tabanı denince ilk olarak ilişkisel veri tabanları (relational databases) gelmektedir. Ancak tek veri tabanı türü bu değildir. Veri tabanları, veri organize etme ve saklama yöntemlerine göre türlere ayrılabildiği gibi, yönetim/sunum altyapısı olarak da birbirinden ayrılabilir. Aşağıda günümüzde sık kullanılan veri tabanı türlerine yer verilmiştir:

- **İlişkisel Veri Tabanları:** Veri tabanı sistemlerinde adeta bir çığır açan bu modelde veriler tablolar halinde tutulur. Örneği kurumdaki personeller bir personel tablosunda yer alabilir, bu durumda tablonun her satırı ayrı bir personeli temsil ederken, tablonun sütunları (kolonları) da personelin özelliklerini (attributes) temsil eder (her personelin adı, soyadı, kimlik numarası gibi). Bu modelde veri birbiriyle olan ilişkisiyle birlikte saklanır.

İlişkisel veri modeli oldukça yapılandırılmış (structured) bir modeldir, bu yüzden bazı kısıtlamalara uyum gerektirse de çok yönlü, çok taraflı ilişkileri kolaylıkla temsil etmeyi ve yönetebilmeyi sağlar. Günümüzde geleneksel kurumsal uygulamalar için neredeyse altın standart haline gelmiştir. Ancak farklı formatlarda, yapılandırılmamış veriyi saklamak için uygun değildir.

Bu veri tabanlarında verileri işleme, yönetme gibi işlevler için SQL (Yapılandırılmış Sorgu Dili, Structured Query Language) olarak bilinen bir dil geliştirilmiş olup ilişkisel veri tabanları üzerinde çalışmayı çok kolaylaştırmıştır.

- **NoSQL Veri Tabanları:** İlişkisel modelin aksine, yapılandırılmış olduğu kadar yapılandırılmamış veriyi de saklamak ve işlemek üzere geliştirilmiş bir veri tabanı modelidir. Burada veriyi saklamak için ilişkisel modelde olduğu gibi belli bir tablo/ilişki formatına dönüşüm gerekmez. Böylece büyük miktarda ve farklı formatlarda veri hızlıca yüklenip işlenebilir. Bu tür veri tabanları aynı zamanda dağıtık yapıda çalışabilir, veri birden çok yerde saklanabilir, bu da verinin erişilebilirliğini artırır.

NoSQL veri tabanlarını kullandığı veri modeline göre aşağıdaki gibi gruplayabiliriz:

- Key-Value (Anahtar-Değer): Bu modeli çok basit bir şekilde bir sözlük gibi düşünebiliriz. Veri tabanında saklanacak her verinin bir anahtarı (key) (örn: numarası, adı) ve karşılık gelen bir değeri (value) vardır. Bir sözlükteki her kelimenin (key) karşılık gelen bir açıklamasının (value) olması gibi. Burada anahtara karşılık gelen değer yapılandırılmamış bir veri olabilir. Web uygulamalarında çerezlerin saklanması bir örnek olarak gösterilebilir.

- Document (Doküman) Veri Tabanı: Burada her birim veri, bir doküman olarak saklanır. Dokümanlara bir anahtar değer ile ulaşılır. Dokümanların içinde genelde iç içe (anahtar, değer) şeklinde veriler saklanır. Yani bir dokümana erişerek birden çok (anahtar, değer) çiftine erişim mümkündür. Dokümanların iç yapıları değişebilir, esneklik vardır. MongoDB bu tür bir veri tabanına örnektir. Bu veri tabanının kullanım alanları arasında bloglar, e-ticaret uygulamaları gösterilebilir.

- Column Store (Kolon tabanlı) Veri Tabanı: Verileri satır (row) bazlı saklayan ve işleyen ilişkisel veri tabanlarının aksine, veriyi kolon (sütun) bazlı saklar. Burada, bir anahtar karşılığında sadece istenen kolondaki (veya bir grup kolondaki) tüm değerlere ulaşılır. Genelde çok okuma yapılan büyük veri tabanlarına yüksek performans sağlar. Veri ambarı ve iş zekâsı uygulamaları için çok kullanışlıdır.

o Graph (Çizge) Veri tabanı: Bu veri tabanı türünde veriler düğüm, veriler arasındaki ilişkiler de düğümleri birbirine bağlayan kenarlar olarak düşünülebilir. Her düğüm ve her kenarın bir belirteci (identifier) bulunmaktadır. Sosyal medya uygulamalarındaki veriler ve ilişkiler (örn: kişiler, kişilerin gönderileri, gönderileri beğenenler gibi) bu şekilde temsil edilebilir.

Veri Tabanı Denetimi

Veri tabanı kullanımı öyle ya da böyle artık bir zorunluluk arz ettiği için, buna özgü risklerden haberdar olunmalıdır. Veri tabanı hem bir tür yazılım olarak hem de kurumsal veri deposu olarak farklı risklere maruz kalmaktadır. Kurumun veri tabanı kullanımından kaynaklanan riskleri ne şekilde sınıflandırdığı ve yönettiği önemlidir. Kurumun bu konudaki risk yönetim süreci incelenmelidir.

Veri tabanı denetiminde aşağıdaki hususlar hem ilgili sürecin varlığı ve yeterliliği hem de işletimi açısından incelenmelidir:

- Kullanılan veri tabanının sürüm ve yama yönetimi. Güncel sürümler kullanılmalı, özellikle güvenlik yamaları test edilerek yüklenmiş olmalıdır. Diğer yandan kullanıcı/istemcilerin veri tabanına bağlanabilmeleri için istemcilerin bilgisayarlarına yüklenen çeşitli sürücülerin de sürüm kontrolünde ele alınması gerekir. Bu sürücüler, istemcilerin VTYS sunucusuna/uygulamalara bağlantısı noktasında elzemdir.

- Kapasite yönetimi: Eşik değerlerin belirlenmesi, bunlara ilişkin uyarı mekanizmasının kurulu olması. Veri tabanı büyümesinin takip edilmesi.

- Performans yönetimi: Veri tabanı uygulamalarından beklenen performans değerlerinin iş birimleriyle beraber belirlenmesi.

- Erişim haklarının yönetimi: Veri tabanına erişim hakları farklı bakış açılarıyla düzenlenmelidir:
  - Veri tabanına işletim, tasarım ve yönetim amacıyla erişim,
  - Veri tabanına uygulamalar aracılığıyla erişim,
  - Veri tabanının kurulu olduğu sunucuya işletim sistemi seviyesinde erişim,
  - Sunucunun yapılandırma ayarlarına erişim hakları,
  - Veri tabanının iz (log) kayıtlarına erişim.

- Kullanıcı Yönetimi: Periyodik hesap kontrolleri, kullanılmayan hesapların etkisizleştirilmesi, şifre yönetimi, jenerik hesapların varlığı, iş/görev değişikliğinin hesaplara yansıması, ayrıcalıklı hesaplar ve bunların yönetimi.

- Yapılandırma (konfigürasyon) Yönetimi: yapılandırma ayarları genellikle veri tabanı yönetim sistemi aracılığı ile düzenlenir (işletim sistemi seviyesinde yapılanlar da olabilir) ve bunu yapanlar genellikle veri tabanı yöneticileridir (sistem yöneticilerinden yardım alınabilir). Bu kapsamda, veri tabanının yapılandırma ayarlarının kim(ler) tarafından yapıldığı (bu hakka sahip olanlar), yapılandırma verisinin saklanması ve yedeklenmesi önemlidir. Yapılandırma değişikliklerinin kontrol altında tutulması ve (ilgili kişi ve gruplara önceden haber verilmesi, onay alınması, değişikliğin ilk önce test ortamında yapılması, üretime geçirilmesi gibi) değişim yönetimi pratikleri kapsamında yapılması önemlidir. Yapılandırma değişikliklerinin kanıtları bulundurulmalı, değişiklikler geriye doğru izlenebilmeli ve gerekçeleri sorgulanmalıdır.

- Şifreleme: Veri tabanı şifrelemede iki husus düşünülmelidir: Birincisi verinin hareket halindeyken (data in motion) şifrelenmesi yani ağ üzerinde dolaşırken şifrelenmesi ki bu husus genelde uygun ağ protokollerinin kullanımı ile sağlanacaktır. Ağ üzerindeki şifreleme hem verinin kendisini, hem de VTYS ile yapılacak iletişimde kullanılan kimlik tanıma/yetkilendirme verisini koruyacaktır.

Diğer husus ise verinin durağan haldeyken şifrelenmesidir (data at rest). Burada da iki farklı durum akla gelmelidir: Birincisi VTYS içindeki verinin şifrelenmesi. Diğeri ise yedeklenip VTYS dışına çıkarılan verinin şifrelenmesi. Her iki durum için de çeşitli algoritma ve yöntemler bulunur ancak

yedekleme konusunda değinildiği gibi çok önemli olan bir husus şifreleme verisinin güvenliğidir. İnceleme sırasında ilk önce kurumun veri şifreleme gereksinimleri (en önemlisi yasal zeminde) kontrol edilmeli, buna göre şifreleme yapılıp yapılmadığı ve şifreleme verisinin güvenliğinin nasıl sağlandığı incelenmelidir. Kurumda durağan verinin şifrelenmesi VTYS'den başlayabilir ya da sadece yedeklere uygulanmış olabilir, bu ayrıma dikkat edilmeli ve gerekçelendirilmelidir.

- Yedekleme: Veri tabanı yönetim sistemlerinin ayrılmaz bir bileşeni de yedekleme sistemidir. Yedeklemesi yapılmayan veri tabanı düşünülemeyeceği gibi, yedeklerin geri dönüşü de maalesef garanti edilemez. Bu yüzden kurumların hem kendilerine uygun bir yedekleme çizelgesi oluşturması hem de yedekten geri dönüş testlerini periyodik olarak gerçekleştirmesi gerekir.

Yedekleme çizelgesi oluşturulurken öncelikli kısıt iş tarafının gereksinimleridir. Ancak iş tarafının gereksinimi de rasyonelleştirilmelidir. Çünkü yedekleme türü, sıklığı ve bu yapının işlerliği aynı zamanda maliyeti de doğrudan etkiler. Burada bir denge söz konusudur ve bunu sağlayabilmek için ilk önce bir iş sürekliliği çalışması yapmak gerekir. Bu çalışmanın adımlarından biri de iş etki analizi olacaktır ve özellikli bu çalışma sonrasında iş birimlerinin kesinti ve kayıplara tahammülü ortaya çıkacaktır. Buradaki tahammülden kasıt, hem kurumların müşterilerine verdikleri hizmet hem de çeşitli yasal zorunluluklardır. Veri tabanı yedekleme politikası; maliyet, yasal çerçeve, çalışılan sektör, müşteri haklarını içeren karmaşık bir konudur, dolayısıyla geliştirilirken hem teknik hem de iş birimlerinin olaya dahlini gerektirir ve sonunda mutlaka ilgili yönetim kademelerince onaylanmalıdır.

Veri tabanı yedeklerinin (diğer tür yedeklerle birlikte) güvenli hale getirilmesi de ayrı bir husustur. Veri tabanı sisteminin güvenliği sağlanmış olabilir ancak veri yedekleri veri tabanının dışında saklanacaktır. Öyleyse bunun güvenliği üzerinde ayrıca durulmalıdır. En güvenli yöntemlerden biri, veri yedeklerinin şifreli saklanmasıdır ki bu konu da beraberinde şifreleme verisinin güvenliği ve yedekliliği konusunu akla getirir. Çünkü şifrelenmiş veri (veri tabanı üzerinde veya yedekleme sisteminde/disk üzerinde) şifreleme verisi olmadan kesinlikle erişilemez durumdadır. Yedekleme politikasında/yönergesinde bu konunun etraflıca ele alınması gerekir. Şifreleme verisi ve bunun yedeği çok sınırlı erişime sahip olmalı ama asla erişilemez hale gelmemelidir. Ayrıca işi şansa bırakmamak için de şifreleme verisi önceden belirli zamanlarda değiştirilmelidir.

- İz (log) kayıtları: Günümüzde iz kayıtlarının alınması ve güvenli saklanması birçok durumda yasal zorunluluk haline gelmiştir. Kurumda ilk önce bu konudaki yasal gereksinim öğrenilmeli ve buna cevaben kurumun yaklaşımı incelenmelidir. VTYS kapsamında bir iz kayıt envanteri olmalı ve iz kayıtlarının nasıl alındığı, nasıl güvenli saklandığı, kimlerin erişim yetkisi olduğu, nasıl imha edildiği incelenmelidir.

İz kayıtları söz konusu olduğunda dikkate alınması gereken bazı hususlar:

- İz kayıtlarına erişim izinleri ve erişim kayıtları. Bunların güvenli saklanması ve gözden geçirilmesi.
- İz kaydı envanteri. İş birimleri veya yasal gereksinimden dolayı takibi yapılan işlemler- örneğin kişisel veriye erişimler.
- İz kayıtları yönetiminde yapılan değişiklikler.
- İz kayıtlarının nereye gönderildiği, nasıl saklandığı, nasıl yedeklendiği ve bütünlüğünün nasıl sağlandığı.

Veri Ambarı

Veri ambarı (Data Warehouse, DW), anlamlı iş iç görüleri sağlamak için çeşitli kaynaklardan veri toplama ve analiz uygulamasıdır. Bir veri ambarı, genellikle heterojen kaynaklardan gelen iş verilerini birleştirmek ve analiz etmek için kullanılır. Veri ambarı, veri analizi ve raporlama için oluşturulmuş iş zekâsı (Bussiness Intelligence-BI) sisteminin çekirdeğini oluşturmaktadır.

Verilerin stratejik kullanımına yardımcı olan teknolojilerin ve bileşenlerin bir karışımıdır. Bir işletmede büyük miktarda bilginin analiz edilmesi ve bir çıkarım yapılması amacıyla kullanılır. Verileri bilgiye dönüştürme ve fark yaratacak şekilde zamanında kullanıcılara sunma sürecidir.

Veri ambarı, işletmenin operasyonel veri tabanından ayrı olarak tutulur. Ancak veri ambarı bir ürün değil, bir ortamdır. Geleneksel operasyonel veri deposunda erişilmesi veya sunulması zor olan güncel ve geçmiş karar destek bilgilerini kullanıcılara sağlayan bir bilgi sisteminin mimari yapısıdır.

Bir veri ambarı, geleneksel bir veri tabanında çok uzun sürede çalıştırılacak sorguların ve raporların yanıt süresini azaltmaya yardımcı olabilecek yeni bir tasarım sağlamaktadır.

1.1.6.4. Veri Modelleri

Veri modelleme, veri kaynakları ve kullanıldığı yapılar arasındaki bağlantıların görsel bir temsilini oluşturma sürecini ifade etmektedir. Bilgi sistemlerinde kullanılan ve depolanan veri türlerinin, bu veri türleri arasındaki ilişkilerin, verilerin gruplama ve organize edilme yollarının, biçimlerinin ve niteliklerinin gösterilmesi amaçlanmaktadır. En genel anlamda yapılandırılmış (structured) ve yapılandırılmamış (unstructured) veriler olarak iki grupta toplanmaktadır.

Veri modelleri iş ihtiyaçları çerçevesinde oluşturulmalıdır. Kurallar ve gereksinimler, yeni bir sistemin tasarımına dâhil edilebilmeleri veya mevcut bir sistemin yenilemesinde kullanılabilmeleri için iş tarafından gelen geri bildirimlerle önceden tanımlanır. Veriler çeşitli soyutlama seviyelerinde modellenebilir. Süreç, paydaşlardan ve son kullanıcılardan iş gereksinimleri hakkında bilgi toplayarak başlamalıdır. Bu bilgiler, daha sonra somut bir veri tabanı tasarımı formüle etmek için veri yapılarına çevrilir. Bir veri modeli; bir yol haritası, bir mimari plan veya neyin tasarlandığının daha derinden anlaşılmasını kolaylaştıran herhangi bir şemaya benzetilebilir.

Veri modellemede çeşitli standartlar veya teknikler kullanılabilir. Veri modelleri, değişen iş ihtiyaçları ile gelişen ve yaşayan belgeler olup iş süreçlerinin desteklenmesinde önemli bir rol oynamaktadır. Veri modelleri tedarikçiler, iş ortakları, denetçiler gibi üçüncü partilerle paylaşılabilir.

Bir veri modeli, veri öğelerini organize eden ve bunların birbirleriyle ve gerçek dünya ile nasıl ilişkili olduklarını standart bir şekilde ortaya koyan soyut bir modeldir.

Veri modellemenin faydaları

Veri modelleme, işletmede bir veri tabanında veya veri ambarındaki veriler arasındaki ilişkilerin görüntülemesini ve anlamlandırılmasını kolaylaştırmaktadır. Ek olarak aşağıdaki faydaları bulunmaktadır:

- Yazılım ve veri tabanı geliştirmedeki hataların azaltılması,
- Kuruluş genelinde dokümantasyon ve sistem tasarımında tutarlılığın artırılması,
- Uygulama ve veri tabanı performansının iyileştirilmesi,
- Kuruluş genelinde veri eşlemenin kolaylaştırılması,
- Geliştiriciler ve iş zekâsı ekipleri arasındaki iletişimin geliştirilmesi,
- Kavramsal, mantıksal ve fiziksel düzeylerde veri tabanı tasarım sürecinin kolaylaştırılması ve hızlandırılması.

Veri modeli türleri

Herhangi bir tasarım süreci gibi, veri tabanı ve bilgi sistemi tasarımı da yüksek bir soyutlama düzeyinde başlar ve giderek daha somut hale gelir. Veri modelleri genel olarak soyutlama derecelerine

göre değişen üç kategoriye ayrılabilir. Süreç kavramsal bir modelle başlayacak, mantıksal bir modele doğru ilerleyecek ve fiziksel bir modelle sonuçlanacaktır. Her bir veri modeli türü aşağıda daha ayrıntılı olarak tartışılmaktadır:

Kavramsal veri modelleri: Sistemin neyi içereceğine, nasıl organize edileceğine ve hangi iş kurallarının dâhil olduğuna dair büyük bir resim sunarlar. Kavramsal modeller genellikle ilk proje gereksinimlerini toplama sürecinin bir parçası olarak oluşturulur. Tipik olarak varlık sınıflarını, özelliklerini ve kısıtlamalarını, aralarındaki ilişkileri, ilgili güvenlik ve veri bütünlüğü gereksinimlerini içerirler. Herhangi bir gösterim genellikle basittir.

Mantıksal veri modelleri: Daha az soyutturlar ve incelenen alandaki kavramlar ve ilişkiler hakkında daha fazla ayrıntı sağlarlar. Mevcut veri modelleme sistemlerinden biri izlenir. Bunlar, veri türleri ve bunlara karşılık gelen uzunluklar gibi veri özniteliklerini belirtir ve varlıklar arasındaki ilişkileri gösterir. Mantıksal veri modelleri herhangi bir teknik sistem gereksinimi belirtmez. Mantıksal veri modelleri, oldukça prosedürel uygulama ortamlarında veya veri ambarı tasarımı veya raporlama sistemi geliştirme gibi doğası gereği veri odaklı projeler için faydalı olabilir.

Fiziksel veri modelleri: Verilerin bir veri tabanında fiziksel olarak nasıl depolanacağına dair bir şema sağlarlar. Bu nedenle en az soyut olanlardır. Varlıklar arasındaki ilişkileri gösteren ilişkisel tablolar ve bu ilişkileri sürdürmek için kullanılacak anahtarlar dâhil, ilişkisel bir veri tabanı olarak uygulanabilecek nihai bir tasarım sunarlar. Fiziksel veri modelleri, performans ayarlama dâhil olmak üzere veri tabanı yönetim sistemine özgü özellikleri içerebilir.

Veri Modelleme Süreci

Farklı veri modelleme tekniklerinin farklı kuralları vardır. Genel bir veri modelleme süreci şu şekilde ifade edilebilir:

- Varlıkların tanımlanması: Veri modelleme süreci, modellenecek veri setinde temsil edilen olayların veya kavramların tanımlanmasıyla başlar. Her varlık tutarlı ve mantıksal olarak diğerlerinden ayrı olmalıdır.

- Her varlığın temel özelliklerinin tanımlanması: Her varlık türü ve nitelik adı verilen bir veya daha fazla benzersiz özelliğe sahip olduğu için diğerlerinden ayırt edilebilir. Örneğin "müşteri" olarak adlandırılan bir varlık ad, soyad, telefon numarası gibi niteliklere sahip olabilirken, "adres" adlı bir varlık bir sokak adı ve numarası, bir şehir, ülke ve posta kodu içerebilir. .

- Varlıklar arasındaki ilişkilerin tanımlanması: Bir sonraki aşamada varlıklar arası ilişkiler belirlenir. Yukarıdaki örnekte, her müşteri bir adreste "yaşamaktadır". Bu model, "siparişler" adı verilen bir varlığı içerecek şekilde genişletilirse, her sipariş aynı zamanda bir adrese sevk edilecek ve bu adrese faturalandırılacaktır. Bu ilişkiler genellikle birleşik modelleme dili (Unified Modelling Language) aracılığıyla belgelenir.

- Özniteliklerin varlıklarla tamamen eşleştirilmesi: Bu, modelin işletmenin verileri nasıl kullanacağını yansıtmasını sağlayacaktır. Birkaç resmi veri modelleme modeli yaygın olarak kullanılmaktadır. Nesne yönelimli geliştiriciler genellikle analiz kalıpları veya tasarım kalıpları uygularken, diğer iş alanlarından gelen paydaşlar başka kalıplara yönelebilir.

- Anahtarların gerektiği gibi atanması ve normalleştirme derecesine karar verilmesi: Normalleştirme, anahtar olarak adlandırılan tanımlayıcıların, verileri tekrar etmeden aralarındaki ilişkileri temsil etmek için veri gruplarına atandığı veri modellerini (ve veri tabanlarını) düzenlemek için bir tekniktir. Örneğin, müşterilerin her birine bir anahtar atanmışsa, bu anahtar, müşteri adları tablosunda bu bilgileri tekrarlamak zorunda kalmadan hem adreslerine hem de sipariş geçmişlerine bağlanabilir. Normalleştirme, bir veri tabanının gerektireceği depolama alanı miktarını azaltma eğilimindedir, ancak performansı sorgulamanın maliyeti olabilir.

- Veri modelinin sonlandırılarak doğrulanması: Veri modelleme, iş ihtiyaçları değiştikçe tekrarlanması ve iyileştirilmesi gereken yinelemeli bir süreçtir.

1.1.7. Sistem ve Kullanıcı Arayüzleri ve Ara Katmanlar

Arayüzler, başka bir veya birden çok sistemle birlikte çalışmak üzere tasarlanmış uygulama ve sistemlerin uçlarındaki fonksiyonel ve fiziksel bağlantılardır. İletişim arayüzleri, sinyal arayüzleri, hizmet arayüzleri, veri arayüzleri, donanım arayüzleri, yazılım arayüzleri ve uygulama programı arayüzleri dâhil olmak üzere birçok arayüz türü bulunmaktadır. Arayüzler, günümüz sistemlerinin coğrafi olarak dağılmış ve bağımsız olarak geliştirilmiş diğer sistemlerle birbirine bağlı hale gelen karmaşık doğasını destekleyen kritik unsurlardır. Birlikte çalışabilirlik sağlarlar. Girdi ve çıktılardan oluşurlar. Dış arayüzlere bağımlı olunması sebebiyle, geleneksel konfigürasyon yönetimi sürecinin ötesinde, bunların nasıl tasarlandıklarına, yönetildiklerine ve yayımlandıklarına özel bir dikkat gösterilmesi gerekmektedir.

İnsanların etkileşimde olduğu yapılara kullanıcı arayüzleri denmekteyken sistem arayüzleri, iki veya daha çok donanım, yazılım ve/veya uygulama programının birbiriyle etkileşim içinde olduğu yapıları tarif etmektedir. Bir yazılımın veri çıktısının otomatik olarak, insan müdahalesi olmaksızın diğerine girdi olarak gönderildiği yerler de mevcuttur. Genel olarak sistemlerde veri akışları üç başlığa ayrılabilir:

- Sistemden sisteme:

Sistemden sisteme arayüzler, verilerin iki sistem arasında dâhili veya harici olarak aktarılmasıyla oluşmaktadır. Veriler ayrıca, veri ambarı gibi özel araçlara da aktarılabilir. Büyük veri ve veri madenciliği gibi son dönemde yaygınlık kazanan analiz yöntemleri, istihbarat ve içgörü elde etmek için bir veri havuzundan analitik bir araca veri aktarımının giderek yaygınlaşmasını sağlamıştır.

- Ortaktan ortağa:

İki iş ortağının üzerinde anlaşmaya varılan sistemler arasında sürekli olarak veri ilettiği arayüz tipidir.

- Kişiden kişiye:

Bu tür iletim genellikle fark edilmesi ve yönetimi en zor olan iletim türüdür. Bir e-postaya veri dosyası eklemek ve göndermek kadar kolay olabilirler. Bu iletim yöntemlerinin izlenmesi, yönetilmesi, güvenliğinin sağlanması ve kontrol edilmesi diğerlerine kıyasla daha zor gerçekleştirilmektedir.

Ara Katman Yazılımları

Bir tür otomatikleştirilmiş arayüz olan ara katman yazılımı, iki ayrı uygulamayı birbirine bağlayan özel bir yazılım türüdür. "Yapıştırıcı" olarak hizmet eder ve iki uygulama arasında veri aktarımına izin verir. Ara katman, uygulama katmanı ve işletim sistemi (OS) katmanı arasında yer alan, bu iki bileşen arasında bir iletişim kanalı ve veri akışı sağlamak için altyapı unsuru olarak çalışan bir yazılım çözümü olarak tarif edilmektedir.

Kurumun kendi içinde geliştirilebileceği gibi piyasada hazır olarak satılan ara katman yazılımları da kullanılabilmektedir.

Sistem Arayüzleri İlgili Riskler

Kuruluşlar, büyüdükçe ve bilgi sistemleri karmaşıklaştıkça yazılım altyapısının da izlenmesini ve yönetilmesini sağlamak için merkezi olarak uygulanacak bir yöntem benimsemelidir. Aynı zamanda düzenlemelere uyum, denetim ve kontrol çalışmalarına bilgi sağlanması için arayüzler ve veri akışları dokümante edilmeli ve denetim izlerinin tutulmasına önem verilmelidir.

Kuruluşların ve bilgi sistemleri denetçilerinin sistem arayüzleri üzerinden alınan verilerin bütünlüğüne, tamlığına ve doğruluğuna güvenebilmesi gerekmektedir. Bir arayüzün hatalı çalışması, yönetim raporlarının ve finansal raporlamanın kuruluş ve alınan kararlar üzerinde önemli olumsuz etkileri olmasına yol açabilir. Kurumsal itibar üzerindeki bir etkinin ötesinde, küçük bir hata bile idari ve yasal yaptırımlara neden olabilmektedir.

Sistem Arayüzleri İle İlgili Güvenlik Sorunları / Önlemleri

Sistem arayüzleri üzerinden aktarılan verilerin güvenliğini sağlamanın başlıca amacı, kaynak sistemden alınacak verilerin alıcı sisteme indirilen ve kaydedilenlerle aynı olmasını sağlamaktır. Verilerin, aktarım boyunca korunarak güvenliğinin sağlanması gerekir. Ek olarak, müdahale, kötü amaçlı faaliyet, hata veya diğer yollarla verilere yetkisiz erişim yapılmasını önlemek de gerekir.

Sistem arayüzlerinin bulunmaması veya manuel aktarım yönteminin kullanılması da verilerin güvenliğini etkileyebilir. Otomatize edilen sistemlerin kullanımı, doğru ve beklendiği şekilde çalıştıklarına güvence verilebildiği ölçüde, bilgi sistemleri denetimi bakış açısıyla da önerilmektedir.

Sistem Arayüzlerinin Değerlendirilmesi

Sistem arayüzleri değerlendirilirken, işletmenin kurumsal ihtiyaçları ve amaçları doğrultusunda, dâhili veya harici tüm sistem arayüzlerinin ve veri aktarımlarının izlenmesini ve yönetilmesini sağlayan bir yöntemin veya programın kullanıldığına emin olunmalıdır. Böyle bir yöntem veya program sayesinde aşağıdaki hususlar kontrol edilebilmelidir:

- Dosya gönderilip alınırken e-posta ve güvenli e-posta kullanılması,
- Düzenli veri aktarımlarını otomatik olarak planlanması,
- Verilerin otomatik olarak şifrelenmesi, çözülmesi ve elektronik olarak imzalanabilmesi,
- Birden çok dosya aktarım mekanizmasının yönetilmesi,
- Çeşitli protokollerin bir arada kullanılması,
- Veri dosyalarının sıkıştırabilir ve tekrar açılabilir olması,
- Ortak veri tabanı sunucularına bağlanılabilmesi,
- Aktarılan verilerin özelliklerinin analiz edilerek izlenmesi ve raporlanması,
- Gerekli düzenleyici yasalara ve yükümlülüklere uyumun sağlanması,
- Kesintiler yaşanması durumunda geri dönüş gerçekleştirilebildiğinin test edilmesi,
- Veri aktarımlarının otomatikleştirilmesi için arka plandaki uygulamalarla entegre edilmesi.

Veri akışı sırasında verilerin korunduğuna güvence verebilmek için kuruluşun her kullanım için uygun şifreleme yöntemi kullandığı teyit edilmelidir. Siber saldırı, yetkisiz erişim veya müdahale riskinin yüksek olduğu değerlendirilmiş ise şifreleme gereklidir. Ayrıca aktarımda, güçlü erişim ve kimlik doğrulama kontrolleri zorlanabilmekte ve veri dosyaları parola korumalı olabilmektedir. Verinin asıl alıcısının amaçlanan alıcı olmasını sağlayan inkâr edilemezlik kontrollerinin uygulanması da önerilmektedir. Verilerin alıcı sisteme kaydedildikten sonra otomatik olarak bütünlük kontrolleri gerçekleştiren yazılımların kullanımı da değerlendirilmelidir.

Sistem arayüzleri ve ara katmanlarının faaliyetleri ile denetim izi kayıtlarının ilişkilendirilebileceğinden emin olmak için, kuruluşun veri gönderip göndermediği, ne zaman gönderdiği, ne zaman alındığı, hangi veri yapısının (örn. xls, csv, txt, xml, vb.) kullanıldığı, verilerin nasıl gönderildiği ve verileri kimin aldığı bilgisi yakalanmalıdır. Özellikle verilerin internete bağlı birden fazla bilgisayarla temas ettiği ve siber olaylara daha fazla maruz kalabileceği harici bir sisteme aktarıldığı durumlarda iletim esnasında loglar mutlaka alınmalı ve izlenmelidir.

1.1.8. Son Kullanıcı Bilgi İşlemi (End user computing-EUC)

Son kullanıcılar, başkaları tarafından programlanan, kurulan, bakım ve destek hizmeti verilen iş uygulamalarına erişen kişilerdir. Son kullanıcı bilgi işlemi ise özel bir programlama veya teknik bilgisi olmayan bir kullanıcının çeşitli yazılım ürünlerini kullanarak kendi uygulamalarını veya bilgi sistemlerini tasarlama ve uygulama becerisini ifade etmektedir. Böyle bir durumda genellikle, son kullanıcılarla bilgi sistemleri birimi arasında bağlantıyı ve iletişimi sağlayan bir destek yöneticisi/ yardım masası fonksiyonu bulunmaktadır.

Gölge bilgi işlem olarak da bilinen son kullanıcı bilgi işleminin avantajlarından biri, kullanıcıların uygulamaları hızla oluşturup dağıtabilmeleridir. Bu model kuruluşların daha esnek olmalarını ve değişen pazarları, düzenlemeleri ve tüketici çıkarlarını daha hızlı karşılamalarını sağlamaktadır.

Bu çalışma modelinin yarattığı bazı riskler de bulunmaktadır; aşağıda bunlar kısaca açıklanmıştır:

- Geliştirilen çözümler, değişiklik yönetimine tabi olmayabilir, bu nedenle gerekli tasarım ve testler gerçekleştirilmeden kullanılabilir ve sürüm farklılıkları mevcut olabilir, hatalı kodlar ve/veya veriler içerebilir, yanlış sonuçlar verebilir, kurumun ve endüstrinin genel kabul görmüş güvenlik prensiplerini karşılamayabilir, uygun şekilde yedeklenmeyebilir, kesinti ve kayıplara sebep olabilir, sisteme erişimi yetkilendirmek için güvenli bir mekanizma işletilmeyebilir,
- Kullanıcıların kimliğinin doğrulanması için güvenli bir mekanizma işletilmeyebilir,
- Denetim izi kayıtlarının tutulmasında sorun yaşanabilir hatta hiç tutulmayabilir, çözümler buna uygun geliştirilmeyebilir,
- Geliştirilen çözümler şifrelenmemiş veya başka koruma önlemlerine tabi olmayan hassas veriler içerebilir.
- Genellikle son kullanıcı bilgi işlemi uygulamalarının işletme için yarattığı risk çok yüksek olmamakla birlikte mevcut riskler tanımlanmalıdır. Bu modelde geliştirilen uygulamaların envanteri bulunmalı ve yeterince diğer uygulamalarla aynı kontrollere tabi tutulmalıdır. Kuruluşların son kullanıcı bilgi işleme modelini yönetmesi ve kontrol etmesi gerekmektedir.
- İşletmede son kullanıcı bilgi işlem modelinin kullanılmasına izin verilmeden önce bu durum üst yönetimce değerlendirilmeli ve risk analizi yapılmalıdır. Modelin kullanımına karar verilirse gerekli politika ve prosedürler geliştirilmeli, duyurulmalı ve takip edilmelidir. Bu politika ve prosedürler asgari olarak:
  - Kullanıcıların kendi bilgisayarlarında yerel yönetici haklarına sahip olmasının engellenmesini, bilgisayar ve sunucularda çalıştırılabilecek uygulama ve servislerin beyaz liste veya kara liste yöntemlerinden biriyle kısıtlanmasını,
  - Uzaktan çalışmanın yaygınlaşmasıyla giderek kullanımı artan şahsi bilgisayar ve mobil cihazlardan işletme sistemlerine erişimin kontrollü sağlanması ve bunların işletme güvenlik politikalarına uyumunun garanti edilmesini,
  - Bu modelde geliştirilen çözümlerin ve kullanılan/üretilen verinin mutlaka envanterinin tutulması ve sınıflandırılmasını

sağlamalıdır.

1.1.9. Denetimde Kullanılan Bilgiler

Bir BS denetçisi, denetim esnasında bilgi sistemlerinden temin edilen verilerin doğruluğu, bütünlüğü ve erişilebilirliği ile ilgili kanıt görmelidir. Bu nedenle sistemden elde edilen ve denetim esnasında tespit edilen verilerin doğruluğuna dair kanıt elde edilmelidir.

Otomatik kontroller genellikle manuel kontrollere göre tercih edilmekle birlikte, gönderilen verilerin bir raporunu çalıştırarak ve bunu alınan verilerle karşılaştırarak manuel mutabakat da gerçekleştirilebilir. Bu kontrol verilerdeki maddi farklılıkları tespit edebilecek bir kişi tarafından yapılmalıdır.

Kuruluş tarafından üretilen ve bilgi sistemleri denetimi kapsamına girip denetim kanıtı olarak kullanılan bilgiler yaygın olarak iki grupta toplanmaktadır:

- **Kontrollerde Kullanılan Bilgiler (IUC)**

İşletme tarafından üretilen ve işletmenin ilgili kontrolleri işletirken kullandığı bilgilere kontrolde kullanılan bilgiler (IUC) adı verilmektedir.

BS Denetçisi tarafından IUC verilerinin güvenilir olup olmadığının tespit edilmesi gerekmektedir. Bir kontrolün, başka bir kontrol sonucunda üretilen bilgileri (örneğin veriler veya bir rapor) kullanması durumunda, kullandığı bilgilerin doğruluğu ve güvenirliği önemlidir.

Bunu sağlamak için, verinin çekildiği kaynak (veri tabanı, raporlama uygulaması, veri ambarı vb.), verinin temininde kullanılan parametreler (tarih, tutar aralığı, kullanıcı rolü vb.), raporun arkasında çalışan sorguların mantığı/doğruluğu gibi kriterler göz önünde bulundurulmalıdır.

İşletme tarafından bir kontrolün işletilmesinde kullanılan bilgiler, üçüncü taraflardan da elde edilebilir. Bu durumda da denetim planının bir parçası olarak üçüncü taraflardan elde edilen bu bilgilerin yeterince güvenilir olup olmadığının değerlendirilmesi gerekmektedir.

- **İşletme tarafından üretilen bilgiler (IPE)**

İşletme tarafından üretilen bilgiler (IPE), risk değerlendirme prosedürlerini, işletmenin kendi kontrolünde de kullanılmayan ilgili kontrollerin işleyiş etkinliğinin testlerini veya doğrulama prosedürlerini uygularken denetim kanıtı olarak kullanılan bilgilerdir. Bilgilerin doğruluğuna ilişkin güvence verilirken IUC başlığında anlatılan yöntemler izlenmektedir.

Bu kapsama giren bilgilere örnek olarak, personel listesi, denetim dönemi değişiklik listesi, işten ayrılan kullanıcı kontrolü için sistemden çekilen kullanıcı listesi verilebilir.

Değerlendirme Soruları

Soru 1: Aşağıdaki tanımlarından hangisi yanlıştır?

A) IPE: Risk değerlendirme prosedürlerini, işletmenin kendi kontrolünde kullanılmayan ilgili kontrollerin işleyiş etkinliğinin testlerini veya doğrulama prosedürlerini uygularken denetim kanıtı olarak kullanılan bilgiler

B) MAO: Maximum Acceptable/Tolerable Outages (Maksimum tolere edilebilir kesinti)

C) IUC: İşletme tarafından üretilen ve işletmenin ilgili kontrolleri gerçekleştirirken kullandığı bilgilere, kontrolde kullanılan bilgiler

D) Arayüz: Diğer sistemlerle birlikte çalışmak üzere tasarlanmış BT sistemlerinin uçlarındaki fonksiyonel ve fiziksel bağlantılardır.

E) Otomatik Kontrol: Bir yazılımın veri çıktısının otomatik olarak, insan müdahalesi olmaksızın diğerine girdi olarak gönderilmesi

Cevap: E

Soru 2: Aşağıdakilerden hangisi USB kullanımının içerdiği risklerden değildir?

A) Virüsler ve diğer kötü amaçlı yazılımlar

B) Veri hırsızlığı

C) Pilinin bitmesi

D) Gizlilik Kaybı

E) İzinsiz paylaşım

Cevap: C

Soru 3: Hipervizörler için aşağıda sayılan kontrollerden hangisi sanallaştırma teknolojisinin getirdiği riskler arasında yer almaktadır?

A) Aynı sunucuda bulunan farklı güvenlik seviyelerindeki iş yükleri

B) Sanallaştırma yazılımına yetkisiz erişim

C) Çevrimdışı ve atıl VM'lerin güvenliği

D) Kaynak kullanımı

E) Hepsi

Cevap: E

Soru 4: Aşağıdakilerden hangisi işletim sistemleri kapsamında BS Denetçilerinin gözden geçirmesi gereken unsurlardan değildir?

A) Windows sistem seçenekleri ve parametrelerinde gerçekleştirilmiş değişiklikleri gözden geçirmelidir

B) Denetim durumunu korumak için kullanılan kontrol seçenekleri için tüm işletim sistemlerindeki sistem yapılandırma dizinlerini / dosyalarını gözden geçirmelidir.

C) Yazılımsal zafiyetlerin varlığı veya sistemlerin en son güvenlik yamalarıyla yapılandırılmasının sağlanıp sağlanmadığı kontrol edilmelidir.

D) İşletim sisteminin sanal sunucuda mı fiziksel sunucuda mı çalıştığını kontrol etmelidir.

E) UNIX tabanlı işletim sistemlerinde çekirdek (root) işlemleri, sistem başlatma, ağ dosya paylaşımı ve diğer uzak hizmetler ile ilgili kritik sistem yapılandırma dosyaları ve dizinleri uygun şekilde korunmalı ve doğruluk açısından kontrol edilmelidir.

Cevap: D

Soru 5: Veri Yönetişimi aşağıdaki unsurlardan hangisini içermemektedir?

A) Veri kalitesi stratejisi tanımlanması

B) Hassas verilerin kontrol olmaksızın kurum dışına e-posta ile atılabilmesi

C) Veri yedekleme ve geri dönüş sürecinin yönetilmesi

D) İş süreçlerinde kullanılan terimlerin tutarlı bir sözlüğü oluşturulması ve sürdürülmesi

E) Veri kalitesi değerlendirme yaklaşımının uygulanması

Cevap: B

1.2. Bilgi Sistemleri Altyapısı Teknolojileri

Gelişen teknolojilerle iş süreçlerinin daha verimli hale getirilmesi, zamanında ve doğru kararların alınması, gelecek planlarının veriye dayandırılarak daha gerçekçi yapılabilmesi, risklerin azaltılması ve fırsatların yakalanması, müşterilere çok daha iyi bir deneyim sunulması ve tedarik zincirinin daha iyi yönetilerek maliyetin düşürülmesi mümkündür. Böylece işletmelerin kârlılığı, sürdürülebilirliği, değer üretmesi ve iş hedeflerine ulaşması sağlanacaktır. Bunu yaparken yalnızca mevcut iş süreçlerine en son teknolojilerin entegre edilmesi değil (yani sadece "digitalization" değil), yeni olanakların ışığında iş süreçlerinin, ürün ve hizmetlerin yeniden tasarlanması, hatta yeni ürün ve hizmetler geliştirilmesi şansı bulunmaktadır. Dijital dönüşüm (digital transformation) adı verilen bu süreç ancak yeni teknolojilerin kullanımıyla gerçeğe dönüşebilir.

Yeni nesil teknolojilerden en önemlileri aşağıda daha detaylı olarak açıklanmaktadır:

1.2.1. Bulut Bilişim

Bulut bilişim, minimum yönetim veya servis sağlayıcı etkileşimi ile hızlı bir şekilde sağlanabilen ve serbest bırakılabilen, yapılandırılabilir bilgi işlem kaynaklarına (örneğin ağlar, sunucular, depolama ortamları, uygulamalar ve hizmetler) ortak bir havuzdan ve her yerden isteğe bağlı erişimi sağlayan bir modeldir. Daha basit bir ifadeyle teknolojik kaynakların paylaşımı ve kullanımı için yeni bir işletim modelidir.[5]

Bulut altyapısı, bulut bilişimin beş temel özelliğini sağlayan donanım ve yazılım koleksiyonudur. Bulut alt yapısı, hem fiziksel bir katman hem de bir soyutlama katmanı içerir. Fiziksel katman, sağlanan bulut hizmetlerini desteklemek için gerekli olan donanım kaynaklarından oluşur ve genellikle sunucu, depolama ve ağ bileşenlerini içerir. Soyutlama katmanı ise, temel bulut özelliklerini gösteren fiziksel katman boyunca dağıtılan yazılımdan oluşmaktadır. Kavramsal olarak soyutlama katmanı, fiziksel katmanın üzerinde yer almaktadır.

Bulut bilişim, beş temel özellik, üç hizmet modeli ve dört dağıtım modelinden oluşur.

1.2.1.1. Temel Özellikler

İsteğe bağlı self-servis: Bir tüketici, bulut hizmetlerine (sunucu veya depolama ortamı gibi) insan etkileşimi gerektirmeden, gerektiğinde otomatik olarak tek taraflı erişebilir.

Geniş ağ erişimi: Bulut hizmetlerine heterojen platformlar (örneğin cep telefonları, tabletler, dizüstü bilgisayarlar ve iş istasyonları) tarafından standart mekanizmalar aracılığıyla erişilebilir.

Kaynak havuzu: Bulut hizmeti sağlayıcısının bilgi işlem kaynakları, dinamik olarak atanan ve tüketici talebine göre yeniden atanan farklı fiziksel ve sanal kaynaklarla, çok kiracılı bir model kullanarak birden çok tüketiciye hizmet vermek için bir havuzda toplanmaktadır. Tüketicinin sağlanan kaynakların tam konumu üzerinde genellikle kontrolü veya bilgisi olmaz, ancak kaynakların konumunu daha yüksek bir soyutlama düzeyinde (örn. ülke, şehir veya veri merkezi) bilebilir, böylece konumdan bağımsız çalışabilir. Kaynak örnekleri arasında depolama, işlem, bellek ve ağ bant genişliği yer almaktadır.

Hızlı esneklik: Bulut hizmetleri taleple orantılı olarak hızlı bir şekilde otomatik artırılabilir, azaltılabilir veya serbest bırakılabilir. Tüketiciye mevcut yetenekler genellikle sınırsız gibi görünür ve herhangi bir zamanda herhangi bir miktarda tahsis edilebilir.

Ölçülü hizmet: Bulut sistemleri, hizmet türüne (örn. depolama, işleme, bant genişliği ve aktif kullanıcı hesapları) uygun bir soyutlama düzeyinde bir ölçüm yeteneğinden yararlanarak kaynak kullanımını otomatik olarak kontrol ve optimize etmektedir. Kaynak kullanımı izlenebilmekte, kontrol edilebilmekte ve raporlanabilmekte, kullanılan hizmetin hem sağlayıcısı hem de tüketicisi için şeffaflık sağlanmaktadır.

[5] https://cloudsecurityalliance.org/download/security-guidance-v4/

Eğer alınan hizmet yukarıdaki özellikleri taşımıyorsa sadece bir dış kaynak kullanımıdır ama bulut bilişim değildir. Bulut bilişim aslında dış kaynaktan hizmet alımının bir alt türü olarak görülebilir, dolayısıyla 1020 numaralı "*Bilgi Sistemleri Yönetimi ve Denetimi*" adındaki çalışma notunda yer alan dış kaynak yönetimi ile ilgili hususlar kıyasen burada da göz önüne alınmalıdır. Ancak bulut bilişimin dış kaynak kullanımına göre daha karakteristik özellikleri olduğu unutulmamalıdır.

1.2.1.2. Hizmet Modelleri

Hizmet Olarak Yazılım (Software as-a service-SaaS)

Bu modelde tüketiciye sağlanan yetenek, hizmet sağlayıcının bulut altyapısı üzerinde çalışan uygulamalarıdır. Uygulamalara, bir web tarayıcısı veya bir program arabirimi aracılığıyla çeşitli istemci cihazlarından erişilebilir. Tüketici, sınırlı olan kullanıcıya özel uygulama yapılandırma ayarları istisnası dışında, ağ, sunucular, işletim sistemleri, depolama ve hatta bireysel uygulama yetenekleri dâhil olmak üzere temel bulut altyapısını yönetemez veya kontrol edemez.

Hizmet Olarak Platform (Platform as-a service-PaaS)

Bu modelde tüketiciye sağlanan yetenek, servis sağlayıcı tarafından desteklenen programlama dilleri, kitaplıklar, hizmetler ve araçlar kullanılarak tüketici tarafından oluşturulan veya edinilen uygulamaların bulut altyapısında kullanımıdır. Tüketici; ağ, sunucular, işletim sistemleri veya depolama dâhil olmak üzere temel bulut altyapısını yönetemez veya kontrol edemez, ancak konuşlandırılmış uygulamalar ve muhtemelen uygulama barındırma ortamı için yapılandırma ayarları üzerinde kontrole sahiptir.

Hizmet Olarak Altyapı (Infrastructure-as-a service-IaaS)

Bu modelde ise tüketiciye sağlanan yetenek, tüketicinin işletim sistemleri ve uygulamaları içerebilen isteğe bağlı yazılımları dağıtabileceği ve çalıştırabileceği işleme, depolama, ağ ve diğer temel bilgi işlem kaynaklarıdır. Tüketici, temel bulut altyapısını yönetemez veya kontrol edemez, ancak işletim sistemleri, depolama ve konuşlandırılmış uygulamalar üzerinde kontrole sahiptir ve muhtemelen belirli ağ bileşenleri (örn. ana bilgisayar güvenlik duvarları) üzerinde sınırlı kontrole sahiptir.

1.2.1.3. Dağıtım Modelleri

Özel Bulut

Bulut altyapısı, birden çok tüketiciden oluşan tek bir kuruluş (örn. iş birimleri) tarafından özel kullanım için sağlanır. Kuruluşa, üçüncü bir tarafa veya bunların bir birleşimine ait olabilir, yönetilebilir ve işletilebilir ve tesis içinde veya dışında var olabilir.

Topluluk Bulutu

Bulut altyapısı, ortak endişeleri olan (örn. görev, güvenlik gereksinimleri, politika ve uyumluluk hususları) kuruluşlardan belirli bir tüketici topluluğu tarafından özel kullanım için sağlanmaktadır. Topluluktaki bir veya daha fazla kuruluşa, üçüncü bir tarafa veya bunların bir birleşimine ait olabilir, yönetilebilir ve işletilebilir ve tesis içinde veya dışında var olabilir.

Halka Açık (public) Bulut

Bulut altyapısı, genel halk tarafından açık kullanım için sağlanır. Bir işletme, akademik veya devlet kuruluşu veya bunların bir birleşimi tarafından sahiplenilebilir, yönetilebilir ve işletilebilir. Bulut, sağlayıcısının tesislerinde bulunmaktadır.

Melez (Hibrit) Bulut

Bulut altyapısı, veri ve uygulama taşınabilirliğini sağlayan standartlaştırılmış veya tescilli teknolojiler ile birbirine bağlanan iki veya daha fazla farklı bulut altyapısının (özel, topluluk veya genel) bir bileşimidir

Denetçi, bulut platformlarının doğru oluşturulduğunu ve bu platformların işleyişinin doğru şekilde devam ettiğini değerlendirmelidir. Dağıtımlara (deployment) ilişkin denetimler, güvence seviyelerinin nasıl sağlandığını ve bulut dağıtım yönetiminin[6] nasıl yapıldığını tespit ederek yapılabilir:

- Güvence seviyelerinin sağlanması
- Geleceğe yönelik bulut dağıtımlarının yönetilmesi [7]

Bulut Bilişimin Avantajları

Yukarıda yer alan bulut bilişimin temel özelliklerinden de anlaşılacağı gibi bulut bilişim kabaca aşağıdaki konularda hizmet alan tarafa büyük avantaj sağlayabilir:

- Maliyet kazancı: Bulut hizmeti sunan firmalar tamamen bu işe odaklandıkları ve büyük oldukları için ölçek ekonomisi sebebiyle bir işletmenin sıfırdan bilgi sistemi kurmasından daha ucuza gelebilir. İşletmeler de kendi işlerine odaklanabilirler.
- Hız: Kurumlar bilgi sistemlerini sıfırdan kendileri geliştirmek isteseler belki aylara yayılacak süreler, bulut hizmetlerinin kullanımıyla günlere düşebilir.
- Ölçeklenebilirlik: İhtiyaç kalmayan hizmetlerin iptali. Kaynaklara sadece ihtiyaç olduğunda sahip olmak, sadece "kullanıldığı kadarını" ödemek işletmelere büyük bir esneklik sağlamaktadır.

Bulut Yönetişimi [8]

BT yönetişim çerçevesi içinde bulut yönetişim çerçevesi bulunmaktadır. Bir kurumsal yönetişim politikası, bir kuruluşun risk toleransını tanımlarken ve bir BT yönetişim politikası doğru paydaşların belirlenmesi ve kontrol çerçevesinin ayarlanması ile ilgilenirken, bir bulut yönetişim politikası bu kriterleri gerçek politika için bir temel olarak kullanmaktadır.

Bulut yönetişiminin bir parçası olarak kuruluşlar; değerlendirme yolları, minimum güvenlik gereksinimleri, uyulması gereken düzenlemeler, standartlar ve kontrol listeleri dâhil olmak üzere bulut yönetişimi ilkelerini de tanımlamalıdır.

Bir işletmede bulut kullanımı değerlendirilirken göz önünde bulundurulması gereken konular aşağıda daha detaylı açıklanmıştır:

Bulut Politikası[9]

Bir bulut denetimine başlamak için ilk yapılması gereken, işletmenin bulut politikasını kontrol etmektir. Bulut politikası, buluta geçiş sürecini tanımlar, ilgili tüm aşamaları ve paydaşları belirler, buluta geçişle ilişkili riskleri ve tehditleri tanımlar ve bu riskleri yönetmek için önlemleri uygulamaya koyar. Kapsanması gereken bulut riskleri için iyi bir temel referans, Bulut Güvenliği İttifakı'nın (Cloud Security Alliance, CSA) En İyi Tehditler Çalışma Grubu tarafından periyodik olarak yayınlanan bulut bilişime yönelik en önemli tehditler raporudur.

1.2.1.4. Bulut Bilişim Güvenliği

Bulut bilişim güvenliği, bulut hizmet sağlayıcısı tarafından sağlanan altyapı ve diğer hizmetlerin ve bulutta saklanan verinin güvenliğidir. Bulut hizmetlerinde güvenlik konusu hem hizmet verenin hem de hizmet alanın sorumluluğuna girer. Bulut sistemlerinde hizmet alanın yetki/sorumluluğu, bulut hizmet modeline ve bulut dağıtım modeline göre değişebilir[10].

Bulut bilişimde korunacak iki ana faktör veri ve altyapı sürekliliğidir.

[6] https://cloudsecurityalliance.org/blog/2021/04/06/what-an-auditor-should-know-about-cloud-computing-part-1/
[7] https://cloudsecurityalliance.org/blog/2021/04/06/what-an-auditor-should-know-about-cloud-computing-part-1/
[8] https://cloudsecurityalliance.org/blog/2021/04/06/what-an-auditor-should-know-about-cloud-computing-part-1/
[9] https://cloudsecurityalliance.org/blog/2021/04/27/what-an-auditor-should-know-about-cloud-computing-part-3/
[10] https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security

Veri koruması: Verinin dinlenmede (data at rest) ve dolaşımda (data at motion) iken korunmasıdır. Dinlenmedeki verinin koruması depolama sistemine, dolaşımdaki verinin korunması ise ağ hizmetlerine karşılık gelir ve her iki durumda da en iyi koruma şifrelemedir. Şifreleme, verinin çalınsa bile korumasının devam etmesi anlamına gelir-şifreleme verisi olmadan çözmek imkânsızdır (şifreleme verisinin güvenli saklandığı, güvenli bir algoritma seçildiği varsayımı ile).

Teorik olarak bulutta saklanan veri "dünyayı dolaşır" ve daima internet üzerinden erişilebilir durumdadır. Veri koruması aynı zamanda donanım arızalarından ileri gelebilecek veri kaybına karşı da güvence sağlamalıdır. Çünkü bu durum verinin erişilebilirliğini etkiler.

Bulut bilişime karşı bazı kurumlarca geliştirilen en büyük endişe nedeni, bulut bilişiminin doğası gereği veri lokasyonunun hizmet alanın tasarrufunda olmamasıdır. Bu durum, günümüzde özellikle kişisel verinin lokasyonunu temel alan bazı yasal düzenlemelerde sorun olarak karşımıza çıkabilmektedir. Bu gibi durumlarda bulut hizmeti verenlerin bazı hizmetlerinde farklılaşma yaptıklarını görüyoruz.

Altyapı sürekliliğinden kasıt ise, bulut altyapı hizmetlerini durduracak veya performansını düşürecek siber saldırılardan sistemin korunmasıdır. Ayrıca altyapı hizmetlerinin, gerçekleşmiş bir saldırının etkilerini azaltacak veya sınırlandıracak yetenekte olması da gerekir. Bulut hizmet sağlayıcıları açısından düşünülürse, her bir müşteri (kurum), bulut hizmet sağlayıcısının sistemine açılan bir zafiyet kapısıdır. Bir müşterinin dikkatsizliği diğer müşterilerin sistemlerinin etkilenmesine de sebep olabilir.

Bulut hizmeti kullanan kurumlarda bulutta sunulan sistemler kurumun kendi sistemleri veya en azından kendi kullanıcı donanımı ile etkileşim içindedir. Bu yüzden erişim yönetimi pratiklerinin hem bulutta konuşlanan veri ve hizmetler için, hem de kurumdaki (on premise) donanım ve hizmetler için dikkatlice uygulanması gerekir.

Bulut hizmetlerine erişen her kurum cihazının (ve varsa kullanıcı cihazlarının) güvenli hale getirilmesi gerekir. Veri yedeği sadece bulutta olmamalı veya en azından sadece bir tek bulutta olmamalıdır.

Buluta erişimde public wifi kullanılmamalı, VPN tercih edilmelidir.

1.2.1.5. Hizmet Sağlayıcı Değerlendirmeleri/Bulut Bilişim Denetimi

Bulut bilişimle ilgili denetim yaparken bulut hizmeti veren kurumun sahip olduğu sertifika ve standartlar önemlidir. Bulut sağlayıcılarını değerlendirirken standartlar, en iyi uygulamalar ve kontrol listelerinin bir karışımı kullanılmaktadır. Sağlayıcıları değerlendirmek için piyasadaki birincil araçlardan biri, güvenlik kontrollerini belgelemek için bir standart haline gelen CSA'nın Consensus Assessment Initiative Questionnaire adlı dokümanıdır (CAIQ). Bulut sağlayıcıları, güvenlik duruşlarını detaylandırmak için CAIQ'yu kullanırken, bulut tüketicileri de sağlayıcı kontrollerini ve olgunluğunu değerlendirmek için CAIQ'yu kullanır.

- **Bulut Kontrol Matrisi (CCM)** - Birden fazla yasa, yönetmelik ve standarttan gelen gereksinimleri tek bir kontrol çerçevesinde birleştiren CSA çerçevesi.

- **CSA GDPR Davranış Kuralları** - Sağlayıcıların sunduğu veri koruma düzeyi için şeffaf yönergeler sağlayan, GDPR (General Data Protection Directive Genel-Avrupa Birliği Veri Koruma Yönetmeliği)-uyumluluğu için en iyi uygulama belgesi.

Destek hizmeti veren firmalar hakkında hazırlanan başka rapor türleri de bulunmaktadır. Bulut hizmeti veren kurumun bu veya benzeri bir denetim raporuna/sertifikaya sahip olup olmadığı sorgulanmalıdır.

Bulut hizmeti alınması, alınan hizmetin/ürünün sahip olduğu riskleri ortadan kaldırmaz, tıpkı dış kaynaktan hizmet alımında olduğu gibi. Denetim sürecinde bu konu akılda tutulmalıdır. Ayrıca bulut hizmeti alınması sebebiyle denetçi, normalde hizmete/ürüne elde edebileceği erişim haklarını da –genelde- alamaz. Bu konuda imzalanan hizmet anlaşmasının önemi büyüktür. Anlaşmalarda hizmet alan firma tarafından "denetim hakkının (right to audit)" alınmasının önemi de burada devreye girer. Ancak

maalesef hizmet sağlayıcılar güçlendikçe ve yaygınlaştıkça anlaşmalarda böyle bir hakkın hizmet alan tarafa verilmesi nadir görülmektedir. Bu konuda daha detaylı bir değerlendirme 1020 numaralı "*Bilgi Sistemleri Yönetimi ve Denetimi*" adlı çalışma notunda bulunmaktadır.

Hizmet alan tarafın denetim hakkını alamadığı durumlarda en önemli konu yukarıda da bahsedilen çeşitli denetim raporları ya da standartlara ait sertifikaların hizmet veren tarafından sunulabilmesidir. Firmadan bu tür raporları talep etmek için de sözleşme aşamasında bu hususun akılda tutulmuş olması gerekir.

Bu arada, hizmet veren de kendi bünyesinde dış kaynak kullanımı yapabilir. Varsa böyle alanların tespit edilmesi ve sorumlu durumda olan hizmet sağlayıcının kendi alt yüklenicisinden nasıl bir güvence aldığının öğrenilmesi ve bununla ilgili belgelerin gözden geçirilmesi önemlidir. Bu, hizmet sağlayıcı firmanın kendi hizmet sağlayıcılarıyla olan ilişkisinin niteliğine (ve ciddiyetine) dair bir izlenim verir.

Buraya kadar anlatılanları şöyle özetleyebiliriz: İşletmede herhangi bir modelde bulut bilişim kullanılacaksa firmanın seçimi, yapılacak sözleşmenin içeriği ve firmanın denetimi önemlidir. Firmanın seçimi aşamasında birtakım güvence raporlarına/standartlara ilişkin sertifikalara sahip olması kriterlerden biri olursa minimum bir yetkinlik seviyesi en baştan sağlanmış olur. Sözleşme aşamasında denetim hakkının dile getirilmesi, bu söz konusu olamıyorsa diğer güvence sağlama yöntemleri konusunda hizmet sağlayıcıyla nasıl etkileşim kurulabileceğinin belirlenmesi gerekir. Bu noktada güvence raporlarının/üçüncü taraf denetim raporlarının istenmesi ve incelenmesi, bunların güncelliğine ilişkin gereksinimler, kim tarafından yapıldığı, bu raporlara ilişkin alınan aksiyonlar hakkında bilgi elde etme hakkı gibi hususlar akılda tutulmalıdır.

Bulut bilişim incelemesinde dikkate alınması gereken diğer bir konu ise işletmenin verisinin (eğer bulutta veri saklanacaksa), diğer hizmet alanların verisinden nasıl ayrıldığıdır. Bu konuda ülke veya sektör çapında yasal gereksinimler de olabilir. Tüm bunlar göz önüne alınarak incelenir. Hizmet sağlayıcının kendisinde saklanan veriyi korumak için şifreleme yapıp yapmadığı, anahtar yönetimi ve veri sınıflandırması konularına dikkat edilmelidir. Ayrıca hizmet sağlayıcının işletme verisine erişim kontrolleri, siber saldırılara karşı alınan teknik ve idari kontroller ile bunların yönetimiyle ilgili süreçler de göz önüne alınması gereken noktalardır.

Bunun dışında, bulut bilişim sağlayıcısında uygulanan kimlik yönetimi, ihlal yönetimi, veri saklama ve imha süreci, felaket kurtarma süreçleri incelenmelidir. Hizmet sağlayıcıdan istenebilecek periyodik ve periyodik olmayan raporlar konusu üzerinde durulmalıdır. Özellikle hizmet sağlayıcının yasal düzenlemelere nasıl uyum sağladığı ve bu konuda nasıl bir güvence verdiği de önemlidir.

1.2.2. Büyük Veri

Dijitalleşme insan kapasitesiyle analiz edilemeyen verinin anlamlı hale getirilmesini sağlarken, geçmiş verinin saklanabilmesi, işlemci teknolojisinde yaşanan gelişmeler ve bulut bilişimle kurumlar kendi tarihinden geleceğe bakma şansına sahip olmaya başlamışlardır.

İnternet ve sosyal medyadan elde edilen büyük verinin işlenmesi, tüketiciye yönelik sektörlerde daha önce görülmemiş bir pazarlama, satış ve müşteri analitiği üretme şansını doğurmaktadır. Muhasebe sistemlerindeki entegrasyonlar ve dijitalleşme, tedarik zincirlerinin büyük veriye dayalı şekilde analiz edilebilmesi gibi konularda raporlama kabiliyetlerinin veri görselleştirmesiyle birleşmesi kurumların mali durumlarını doğru şekilde tahlil ederek ileriye dönük tahminler ve planlar yapmaları, önemli kararlar alırken veriden faydalanabilmeleri için oldukça etkilidir.

Büyük veri (Big data), adından da anlaşılabileceği gibi büyük miktarda veridir. Ancak o kadar büyüktür ki alışılagelen veri yönetimi araçlarıyla inceleme yapmaya elverişli değildir, iyi bir performans gösteremez. Ancak değeri de buradan gelmektedir, kurumlara normal yollarla elde edilemeyecek bilgi sağlarlar. Büyük veri, sadece geleneksel anlamda üretilen ve yayılan bilgiden –örneğin bir forma girilen bilgiler- oluşmaz. Tanım olarak her türlü sensörden, araçtan gelen her tür veriyi içine alır –örneğin sosyal medya, IoT, işitsel-görsel veri, pdf, e-posta vb. Sadece saklanması değil fakat özellikle de işlenmesi için özel teknolojiler gerektirir.

Elimizdeki verinin "büyük veri" kategorisine girip girmediğini anlamak için aşağıda verilen üç kritere bakabiliriz: (3V's)

- Hacim (Volume): Çok fazla miktarda veri.

- Hız (Velocity): Verinin çok hızlı üretilmesi, ele geçmesi ve anlamlandırılması gerekliliği. Geleneksel olarak kurumsal uygulamalarda üretilen veri miktarından çok daha fazlası kastedilmektedir. Örneğin sosyal medya üzerindeki yeni içerik üretiminin hızını düşünün.

- Çeşitlilik (Variety): Mümkün olduğunca çok kaynaktan gelen yapılandırılmamış veri. Yapılandırılmış veriden kasıt, geleneksel veri tabanlarında saklanan, belirli bir formatı, büyüklüğü, tipi olan veridir. Yapılandırılmamış verinin ise, önceden tanımlanmış bir formatı, uzunluğu, alabileceği değer kümesi yoktur. Günümüzde yapılandırılmış verinin, toplam veri büyüklüğünün sadece %5'ini oluşturduğu tahmin edilmektedir.

Büyük Verinin Gelişimi

İnternetin hayatımıza girmesiyle kurumların yönetmek zorunda oldukları veri miktarı çok büyük miktarda artmaktadır. Artan veri miktarı, geleneksel olarak ilişkisel veri tabanlarında saklanan verinin verimli şekilde analiz edilebilmesi sorununu ortaya çıkarmış olup bu amaçla veri ambarı (Data Warehouse, DW) sistemleri geliştirilmiştir. Veri ambarı, büyük miktarda verinin analizi için özel tasarlanmış veri tabanlarıdır.

Zamanla daha da artan ve yapılandırılmamış olarak da sınıflandırılan verinin analizi için yeni modeller gerekmiş ve bu yönde çalışmalarla ortaya farklı yazılım çerçeveleri ve dosya sistemleri çıkmıştır. Örneğin Hadoop, büyük verinin birden çok makine üzerinde saklanması ve bu şekilde paralel olarak analiz edilmesini sağlar. Paralel saklama ve işletim, kurumlara hız ve verimlilik artışı getirir. Bu gelişmelerle birlikte ortaya çıkan bir diğer teknoloji de Spark'dır. Spark, büyük verinin analizi için geliştirilmiş bir araç olup özelliği veriyi ana bellek üzerinde analiz etmesidir ki bu da hız artışı sağlar. Bu ve benzer birçok teknoloji beraber kullanılarak kurumsal kapasitenin artırılmasına olanak sağlar.

Büyük verinin kullanımındaki zorluklardan biri büyük miktarda depolama ihtiyacıdır. Bulut teknolojilerinin gelişimi bu konuda kurumlara daha esnek ve ekonomik çözümler sağlamaktadır.

İşin içine büyük miktarda yapılandırılmamış verinin girmesiyle veri gölü (data lake) kavramı ortaya çıkmıştır. Bu aslında bir veri deposudur, özelliği aynı anda hem yapılandırılmış hem de yapılandırılmamış veriyi saklamasıdır. Yapılandırılmamış veriyi saklaması bakımından veri ambarından ayrışır. Veri gölüne her kaynaktan yapılandırılmamış veri aktarılabilir, verinin önceden temizlenmesi, ayrıştırılması, yapılandırılması gerekmez. Bu şekilde kurumlar verilerine çok farklı analiz ve sorgular yapabilir ve işleri için iç görü sağlayabilirler.

Bu noktada ortaya data platform (veri platformu) çıkmaktadır. Veri platformu, kurumlara yapılandırılmış verileri için klasik ilişkisel veri tabanı ve veri ambarı çözümlerini kullanma, yapılandırılmamış ve veri gölünde tutulan verileri için de diğer çözümleri kullanma şansını vermektedir. Veri platformları veri tekrarını önler ve kurumların tüm veri setini bir platformda tutmalarını ve yönetmelerini sağlar.

Veri platformlarının üzerine uygulanan büyük veri ve yapay zekâ uygulamaları ise kurumların sahip oldukları veri üzerinde daha önceleri edinilmesi mümkün olmayan anlamları ve ilişkileri görmesini sağlar.

Büyük Verinin Kullanımı

Geleneksel anlamda kullanılan veri tabanlarından elde edilen raporlamalar geçmiş veriye dayalıdır. Ancak günümüzde kurumlar işlerini daha iyi planlayabilmek için özellikle sosyal medyada üretilen gerçek zamanlı verinin analizine ihtiyaç duyarlar.

Tahmin analizi ile geçmiş veri ve güncel veri birlikte analiz edilir ve geleceğe yönelik tahmin yapılır, risk ve fırsatlar belirlenmeye çalışılır.

Büyük verinin analizi, 3V karakteristiğindeki verinin kendi içindeki örüntüleri, ilişkileri, korelasyonları bulmak amacıyla yapılır. Büyük verinin analizi, kurumların daha önceden kullanamadıkları büyük miktarda veriyi anlamlandırarak daha iyi ve daha hızlı karar almalarını sağlar.

Büyük verinin finansal piyasalarda en önemli kullanım alanlarını şu şekilde sıralayabiliriz:

- Algoritmik alım satım işlemleri,
- Yatırımların geri dönüşünün daha iyi tahmini,
- Piyasa trendlerinin analizi,
- Risk yönetimi ve hileli işlemlerin tespiti.

Kurumda büyük veri konusunda yapılan çalışmalarda özellikle verinin büyüdüğü noktalar kontrol altında olmalıdır. Yeni eklemeler, mevcut verinin sınıfını, riskini, güvenliğini, kalitesini etkileyebilir. Bunların dikkate alındığından ve gerekli eylemlerin gerçekleştirildiğinden emin olunmalıdır. Veri ne kadar büyürse gizlilik riskinin de artacağı akılda tutulmalıdır.

Bunun dışında kurumun BS stratejisi ile büyük veri projeleri arasındaki ilişki araştırılmalıdır. Böyle büyük projelerin mutlaka BS stratejisiyle bağlantısı olmalıdır. Ayrıca kurumun bu konuda çalışacak yeterli insan kaynağı olup olmadığı, ekipteki kişilerin yetkinliğinin göz önüne alınıp alınmadığı da değerlendirilmelidir.

Diğer yandan, geleneksel sistem geliştirme ve işletim süreçlerinde yürürlükte olan süreçlerin (veri sınıflandırması ve buna ilişkin kontroller, yedekleme/kurtarma süreçleri, erişim yönetimi, ayrıcalık yönetimi süreçleri gibi) büyük veri çalışmaları kapsamında da işletiliyor olması gerekir. Farklı ve yeni bir teknoloji olması sebebiyle bu çalışmalar kontrollerden bağımsız olmamalıdır ancak mevcut kontrollerde konuya özel değişiklikler yapılabilir.

1.2.3. Nesnelerin İnterneti (IoT)

Artan dünya nüfusu ve talep, üretim ihtiyacını ve doğru kapasite kullanımını zorlarken Covid salgını ile yaşanan karantina süreci, üretim süreçlerinin olabildiğince insansızlaştırılması konusunda bir fikir birliği doğurdu. Bu durum, Endüstri 4.0'ın ve bununla birlikte Nesnelerin internetinin (IoT) yaygınlaşacağını ve bu konuya olan talebin artacağını göstermektedir. Makinelerin daha akıllı hale gelmesi, birbiriyle konuşabilmeye başlamasını sağlayan sensör teknolojisi ve büyük verinin kullanımıyla üretim süreçleri daha şeffaf hale gelirken kestirimci bakım teknolojisiyle oluşacak hata ve bozulmalar önceden tahmin edilerek hem üretimdeki kesintiler azaltılabilmekte hem de tamir ve bakım maliyetlerinde düşüş sağlanmaktadır.

Nesnelerin interneti (IoT) cihazları; tıbbi cihazlar, arabalar, insansız hava araçları, basit algılayıcılar (sensörler) ve daha fazlası gibi çok çeşitli geleneksel olmayan cihazları temsil etmektedir. Bu benzersiz cihazlar, sınırlı boyut ve doğuştan gelen güvenlik eksikliği nedeniyle geleneksel güvenlik kontrolleri ve metodolojileri ile güvenliklerini zorlaştıran bir güvenlik sorunu oluşturmaktadır. Birçok cihazı Mirai botnet gibi saldırılara karşı savunmasız hale getiren bu faktörlerin bir birleşimidir.[11]

IoT'nin Güvenlik Riskleri

Nesnelerin interneti, tüketici, iş ve endüstriyel süreçleri ve uygulamaları hızla dönüştürmektedir. BS denetçisinin denetim planı içerisinde dikkat etmesi gereken IoT ürün güvenliği için en önemli konular:

- Tüketicilere ait veri güvenliği kapsamında kişisel ve özel nitelikli kişisel verilerin bu ortamlarda bulunmasının sınırlandırılması,
- Yapılan işe ait verilerin güvenliğinin sağlanması ve hassas bilgilerin açığa çıkmasını önleyecek önlemler alınması,
- DDoS saldırılarına karşı IoT ürünlerinde önlemlerin alınması

[11] CSA, https://cloudsecurityalliance.org/research/working-groups/internet-of-things/

• Siber ya da fiziksel saldırılar sonucunda sistemlerin tehlikeye girmesinden kaynaklanan hasar veya zarara karşı korunması[12].

1.2.4. Yapay Zekâ

Yapay zekâ (artificial intelligence, AI), insana özgü muhakeme yeteneğiyle donatılmış bilgisayar sistemi olarak tarif edilebilir. Bu şekilde geliştirilmiş bir sistemin, tıpkı bir insan gibi (ancak çok daha hızlı biçimde), eldeki veriyi (büyük miktarda veri) kullanarak akıl yürütmesi, anlam çıkarması, genelleme yapması, "öğrenmesi" beklenir.

Makine öğrenmesi, derin öğrenme, pekiştirmeli öğrenme gibi birçok alt başlığı olan yapay zekâ, günlük hayatımızın içinde de yer alan öneri sistemleri ve arama motorları, cep telefonlarındaki kişisel asistanlar, otonom araçlar gibi uygulamaların altında yatan teknolojinin genel ismidir. Büyük veriyle beslenen yapay sinir ağı modellerinin çeşitli ihtiyaçlar için özelleştirilmesiyle çalışan yapay zekâ, finans sektöründe suistimal tespiti, yatırım tavsiyesi verilmesi, üretimde hatalı çıkan mal tespiti, sağlık alanında hastalıkların teşhisi, hava ve iklim olaylarının tahmini, yüz tanımayla kimlik tespiti gibi sayısız alanda kullanılabilir. Teknolojinin kendisiyle birlikte kullanım alanları da hızla artmaktadır.

Kurumlarda geleneksel iş gücünün yanında çalışanların yapay zekâyla desteklenmesi, daha üst düzeyde verimliliğin kapılarını açacaktır. Bunun için iş yerindeki insan-makine etkileşimi en baştan ele alınarak hangi işlerin, nerede, kimin tarafından yapılacağı yeniden düşünülmelidir.

İşletmeler yapay zekâ stratejilerini belirlerken öncelikle daha küçük ve özelleşmiş projelerle denemeler yapmalı, kendi insan kaynağını ve bilgi birikimini oluşturduktan sonra başarılı örnekleri işletmenin tümüne yaygınlaştırmalıdır.

Makine öğrenmesi (machine learning, ML) kısaca büyük veri üzerinde analiz yapan, örüntüleri bulan ve bu sayede geleceği daha iyi tahmin edebilen, daha iyi karar alabilen sistemlerdir. Veri ne kadar büyük ve veri kalitesi ne kadar iyi olursa daha iyi kararlar alınır. Makine öğrenmesi algoritmalarının kullandıkları veri miktarı (ve veri kalitesi) arttıkça daha iyi çıkarımlar yapması ve daha iyi sonuçlar üretmesi beklenir. Günümüzde büyük veri işleme teknolojilerinin artmasıyla yapay zekâ uygulamaları da artmaktadır.

1.2.4.1. Yapay Zekâ ve Siber Güvenlik

Siber güvenlik, üç ana alandan oluşan bilgi güvenliğinin daha odaklı alanıdır. Daha geniş anlamda:

Gizlilik: Çoğunlukla kişisel, hassas ve gizli olanlar da dâhil olmak üzere verilerin mahremiyetini ilgilendirmektedir.

Bütünlük: Dosyaların, veri tabanlarının ve kaynak kodların doğruluğunu ve tamlığını sağlar.

Kullanılabilirlik: Sistemlerin aktif olarak çalışmasını ve gerektiğinde uygulamaların ve verilerin kullanıma hazır olmasını sağlar.

Saldırganlar, BS kontrollerindeki eksikliklerden ve sistem güvenlik açıklarından yararlanmayı amaçlar. Siber güvenliğin amacı, kritik veri ve varlıklara yönelik saldırıları önlemek, bilgi sistemlerini daha dayanıklı hale getirmek, herhangi bir ihlal olup olmadığını tespit etmek ve zamanında düzeltici önlem almaktır. Yaygın siber güvenlik saldırıları; dağıtılmış hizmet reddi (DDos), kaba kuvvet saldırısı (brute force attack), kimlik avı saldırılarıdır.

Saldırılara karşı koruma sağlamak için üstesinden gelinmesi gereken dört ana sorun vardır:

• Web sunucusu günlükleri, uygulama günlükleri, ağ paketleri, IoT sensör verileri, iş istasyonları, API çağrıları vb. gibi ağ etkinliğinin ve veri kaynaklarının ölçeği muazzam bir düzeyde artmaktadır. Kendi aralarında bunun manuel olarak veya kural tabanlı güvenlik duvarı ve saldırı tespit sistemi (intrusion detection system-IDS) çözümleri ile izlenemeyeceği karmaşık ilişkilere sahiptirler.

[12] CSA, https://cloudsecurityalliance.org/research/working-groups/internet-of-things/

• Gizli verilerin sızmasını durdurmak açısından e-postaların ve belgelerin içeriğini anlamak çok önemlidir ve geleneksel metin eşleştirme ile çalışan Veri Kaybı Önleme (Data Loss Prevention - DLP) çözümleri içeriğin bağlamını değerlendiremez.

• Kesinlik ve doğruluk elde etmek çok zordur. Geleneksel güvenlik açığı yönetimi hizmeti (VMS) ve güvenlik olayı analizi (SIEM) çözümleri birçok yanlış pozitif ve yanlış negatif üretir, web güvenlik duvarı/proxy URL engelleme listeleri manuel olarak güncellenir ve kimlik avı saldırılarına açık bırakılır.

• Hız da, herhangi bir güvenlik olayının tespit edilmesinde çok önemlidir. Zamanında müdahale edilmezse, tespit edilmiş olsa bile güvenlik ihlali ve veri sızıntısı yaşanmış olabilir.

1.2.4.2. Yapay Zekânın Bilgi Varlıklarının Korunmasındaki Rolü

Kural tabanlı algoritmalar, muazzam verileri yönetmek ve bunlardan anlamlı sonuçlar çıkarmak için yetersiz hale geldikçe, derin öğrenme ve makine öğrenimi kullanılmaktadır. Derin öğrenme, gerçek zamanlı algılama ve tahmin yapar. Akıllı sistemler ya da uygulamalar, kullanıcı oturum açma kalıplarını ve anormallikleri tanımlayabilir ve binlerce satırlık kodu analiz edebilir, yazılım mühendislerinin yazdığı zayıflıkları belirleyebilir. Ayrıca, test için orijinal veriler paylaşılmak istenmediğinde, Markov zincirleri, Boltzmann makineleri, GAN algoritmaları tarafından sentetik veriler üretilebilir.

Ölçek sorununu çözmek ve olayları bulmak için yapay zekâdan yararlanan bir saldırı tespit sistemi (IDS) kullanılmalıdır. Kuralları ve kalıpları aramak yerine, bir tahmin modeli, her paketin ne zaman yakalandığı, kaynak ve hedef IP adresi ve paketin port numarası gibi gerekli özellikleri belirlemelidir.

Geleneksel olanlarla birlikte bağlam eşleştirme yaklaşımıyla çalışan akıllı veri sızıntısı önleme (data loss prevention-DLP) sistemleri kullanılarak bağlam sorunu aşılabilir. Akıllı DLP için derin öğrenme modeli, biri korunması gereken kelime ve kelime öbekleri, diğeri korumaya ihtiyaç duymayan iki farklı veri kümesinde eğitilmelidir. Ayrıca model, kelime gömme tekniği kullanılarak dilin anlamsal ilişkileri ile beslenmelidir. Yapay zekâ tabanlı DLP, bir belgeye bir hassasiyet seviyesi atar ve buna izin verilip verilmeyeceğine veya engellenip engellenmeyeceğine karar verir.

Yapay zekâ, manuel listelere ve veri tabanlarına güvenmek yerine gerçek zamanlı keşif yoluyla kesinlik ve doğruluk sorununun çözülmesine yardımcı olabilir. Örneğin, kimlik avı saldırılarının olasılığını azaltmak için elle tutulan URL engelleme listeleri yerine bir model dağıtılabilir. Model bazı özellikleri kullanabilir, bir web sitesinin gerçekliğini belirleyebilir.

Hız sorununa cevap verebilmek için öngörülebilirlik modelleri devreye alınabilir ve proaktif aksiyonlar alınabilir. Yapay zekâ tabanlı IDS, henüz bir imzası bile olmayan kötü amaçlı yazılımları tespit edebilir. Eyleme geçirilebilir önerilerde bulunabilir ve bağımsız olarak düzeltici eylemde bulunabilirler.

1.2.4.3. Yapay Zekâ ve Finansal Piyasalar

Uluslararası Menkul Kıymetler Komisyonları Örgütü (IOSCO) tarafından yayınlanan bir danışma raporuna göre, aracı kurum ve varlık yöneticileri, yapay zekâ ve makine öğrenmesi teknolojilerini, mevcut iş süreçlerini güçlendirmek, verimi artırmak ve genellikle insan gücü ile karar alma süreçlerini desteklemek amacıyla kullanmaktadır. Söz konusu raporda, yapay zekâ ve makine öğrenmesi sistemlerinin hem kullanım alanlarından ve potansiyel risklerinden bahsedilmiş, hem de bu risklerin üstesinden gelebilmek için bazı tedbirler önerilmiştir:[13]

[13] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD658.pdf

1.2.4.3.1. Kullanım Alanları

- Danışmanlık

Bu alanda Robo-danışmanlık (robo-advisor) çözümleri karşımıza çıkmaktadır. Bunlar genellikle kural bazlı çalışmakla birlikte makine öğrenmesi ile çalışan ve tahmin yapabilen türleri de bulunmaktadır. Bu çözümler genelde insan gücünün (müşteri temsilcisi/danışmanı) kararlarını desteklemek amacıyla veya yapılan önerilerin insan gücü tarafından gözden geçirilmesi şeklinde kullanılmaktadır.

- Risk yönetimi

Aracı kurumların makine öğrenmesi bazlı araçları risk yönetiminde erken uyarı amacıyla kullandıkları görülmektedir. Kurum çalışanlarının e-postalarını makine öğrenmesi araçlarıyla izleyen kurumlar olduğu da rapor edilmiştir. Ayrıca varlık/portföy yöneticilerinin makine öğrenmesi sistemlerini risk yönetimi ve uyum süreçlerinde kullandıkları örnekler mevcuttur.

- Müşteri tanımlama ve gözetim

Makine öğrenmesine dayalı araçların aracı kurumların müşteri tanıma/kabul, hileli işlem tespiti, kara para aklama ve siber saldırıları izleme süreçlerinde kullanıldığı rapor edilmiştir. Sahte fotoğraflı kimliklerin tanınmasında bu sistemler kullanılabilir. Ayrıca muhtemel kara para aklama, terörist faaliyetlerin tespitinde de bu araçların kullandığı görülmektedir.

- Algoritmik alım satım

Birçok aracı kurumun müşterilerine algoritmik alım satım (trading) için çeşitli araçlar sunduğu rapor edilmiştir.

- Varlık/Portföy yönetimi.

Aracı kurumların ve portföy yöneticilerinin alım satım kararlarına yardımcı olması için makine öğrenmesi temelli sistemleri bir süredir kullandıkları bilinmektedir. Ancak daha rekabetçi olabilmek amacıyla benzer sistemlerin varlık fiyatlandırması/tahmini için de kullanılmaya başlandığı rapor edilmiştir. Bu sistemler yeni finansal ürünlerin fiyatlandırılmasında da kullanılabilir.

1.2.4.3.2. Potansiyel Riskler ve Tedbirler

- Yönetişim ve gözetim

Yapay zekâ ve makine öğrenmesine dayalı geliştirme ve işletim süreçleri kurumun geleneksel yazılım geliştirme süreçleriyle birlikte değerlendirilmemelidir. Yeni teknolojiler olduğu için kendine özel riskleri vardır ve buna göre yeni yönetişim süreçleri oluşturulmalı veya mevcut süreçler uyarlanmalıdır.

- Algoritma geliştirme, test ve gözetim

Yapay zekâ ve makine öğrenmesi çözümlerini kendi bünyelerinde geliştirecek kurumların sağlam bir yazılım geliştirme sürecinin olması gereklidir. Diğer yandan, geleneksel uygulamaların aksine bu çözümlerde sisteme giren veri miktarı arttıkça ve çeşitlendikçe sistemin ürettiği sonuçlarda beklenmeyen değişiklikler, farklılaşmalar olabilir. Bu yüzden bu sistemler üretim ortamına geçtikten sonra bile gözetim altında tutulmalı ve amacına göre çalışmaya devam ettiği garanti edilmelidir.

- Veri kalitesi

Yapay zekâ ve makine öğrenmesi sistemlerinin çıktılarının performansı bu uygulamaların dayanak aldığı verinin (büyük veri) kalitesiyle doğrudan ilişkilidir. Veri seti içinde özellikle ön yargı (bias) faktörünün varlığı önemlidir çünkü böyle bir verinin işlenmesi sonucunda alınan kararlar/çıktılar da ön yargı taşıyacaktır. Verinin algoritmalara girişinden önce "temizlenmesi" gerekir ki bu süreç de

ayrıca kendi içinde bir ön yargı taşıyabilir, sanıldığının aksine ön yargı istenmeden de oluşabilir. Yapay zekâ ve makine öğrenmesi uygulamalarında veri kalitesinin üzerinde önemle durmak gerekir. Bu konu etik açıdan da önemlidir.

- Şeffaflık ve açıklanabilirlik

Yapay zekâ ve makine öğrenmesi çözümlerini kullanan kurumlar, müşterilerine ne amaçla bunları kullandıklarını ve doğabilecek riskleri açıklamalıdır.

- Dış kaynak kullanımı

Yapay zekâ ve makine öğrenmesi çözümlerini geliştirmek veya kullanmak için dış kaynaktan yararlanılabilir. Özellikle nispeten küçük kurumlar bu yola başvurabilir. Hem ürün geliştirme hem de veri saklama için dış kaynaktan hizmet alınabilir. Bu durumda dış kaynaktan hizmet alma konusundaki risklere de ayrıca dikkat etmek gerekecektir.

- Etik çerçeve

Yapay zekâ ve makine öğrenmesi sistemlerinde veri kalitesinin öneminden bahsedilmişti. IOSCO Fintech Network çalışmaları sonucunda da Robo-Advisor çözümleri (makine öğrenmesi algoritmaları kullananlar), sermaye piyasalarında önemli etik sorunlara yol açabilecek AI/ML çözümü olarak belirlenmiş ve bu konuda aşağıdaki hususların üzerinde durulmuştur:

- Yatırımcının çıkarı ve piyasanın bütünlüğünün korunması.
- Zarar vermeme ilkesi. Verilen önerilerin yorumlanabilmesi.
- Son karar mercii olarak insan gücünün kullanılması.
- Sistemlerin ürettiği sonuçlar ve kararlardan kurumun üst yönetiminde sorumlu kişilerin olması ve bu kişilerin kullanılan sistemi anlaması.
- Sistemlerden çıkan sonuçların rasyonalize edilebilmesi.

Güvenlik

Derin öğrenme ve makine öğreniminin içsel sınırlamaları olduğunu hatırlamak akıllıca olacaktır. Yapay zekâ uygulamasının/modelinin kendisi, eğitim özniteliklerine (özellikler), eğitim için kullanılan verilere ve algoritmanın kendisine müdahale etme gibi saldırılara açıktır. Ortak sorunları çözerek siber güvenliğin verimliliğini ve etkinliğini artırma olanaklarını araştırırken yeni sorunların olasılığını her zaman aklımızda tutmalıyız.

1.2.5. Robotik Süreç Otomasyonu

Tekrara dayalı ve sıkça karar vermeyi gerektirmeyen rutin işlerin bilgisayarlara yaptırılması anlamına gelen robotik süreç otomasyonuyla çalışanlar daha üretken olabileceği alanlara vakit ayırırken tekrarlı işler daha çabuk ve minimum hatayla yapılabilmektedir.

Yenilemesi gelen sigorta poliçesinin kesilmesi, her gün gelen faturaların üzerindeki bilgilerin excel dosyalarına alınarak vergi beyannamesi oluşturulması, gün içinde oluşmuş sipariş bilgilerinin e-postayla yüzlerce bayiye gönderilmesi, ödeme listesiyle muhasebe kaleminin mutabakatının yapılması, işten çıkan kullanıcı hesaplarının kurum bilgi sistemlerinden silinmesi gibi birçok konuda robotik süreç otomasyonundan faydalanılabilir. Ayrıca kurumlar için önemi giderek artan iç kontrol ortamının otomatize edilmesinde de kullanımı giderek yaygınlaşmaktadır.

1.2.6. Blok Zincir-Dağıtık Defter Teknolojisi

Blok zincir; sistemi değiştirmeyi, ele geçirmeyi veya hile yapmayı zorlaştıracak veya imkânsız hale getirecek şekilde veri/bilgi kaydetmek için geliştirilmiş bir bilgi teknolojisi olup altyapısı "Dağıtık Defter Teknolojisi (Distributed Ledger Technology, DLT) olarak bilinen kavrama dayanmaktadır.

Blok zincir, veri güvenliğini özellikle de verilerin değiştirilemezliğini sağlayan ve bunu merkezi bir otoriteye ihtiyaç duymadan, birbiriyle eş statüde taraflar arasında mutabakata vararak gerçekleştiren bir teknolojidir. Blok zincir teknolojileri farklı türde uygulanabilir. Tamamen özel, genel ve karma blok zincirler oluşturulabilir. İhtiyaçlara ve düzenleyici gereksinimlerine uymaları için işlem (transaction) gerçekleştirme, anlaşmazlık çözümü için mutabakat mekanizmaları ve yönetişim modeli seçilebilir. Blok zincir yıkıcı/dönüştürücü bir teknolojidir.

1.2.6.1. Temel Kavramlar

Bir blok zinciri, tek bir merkezden doğmayıp İnternet üzerinde bir ağda bilgisayarlar (node, düğüm) boyunca çoğaltılan ve dağıtılan bir veri tabanıdır. Zincirin en küçük yapı taşı *blok* olarak adlandırılır. Zincirdeki her blok belirli bir boyuttadır ve bir dizi veri/işlem içerir. Sistemde gerçekleşen işlemler (veya oluşan veriler) hemen bir bloğa yazılmaz. Çeşitli kontrollerden geçtikten sonra bir bloğu dolduracak boyuta ulaştığında belirli bir mekanizmaya göre yeni bir blok haline getirilir ve zincirin sonuna eklenir. Sistemdeki her düğüm blokların tümüne sahip olabilir ya da bunları görebilir. Temeli DLT teknolojisine dayanır dedik, bu durumda her bir bloğu defterin bir sayfası olarak düşünebiliriz.

Blok zinciri alışageldiğimiz veri tabanlarından (örn: bir kurum tarafından işletilen ilişkisel bir veri tabanı) ayıran bazı özellikleri şöyle sayabiliriz:

- Belli bir kurum tarafından yönetilmemesi ve saklanmaması,
- Herkese açık olması, isteyen herkesin bir düğüm olarak sistemde saklanan tüm veriyi kendi bilgisayarına indirebilmesi, okuyabilmesi, doğruluğunu kontrol edebilmesi,
- Herkesin yeni blok yaratım sürecine katılabilmesi yani sistemin ortaklaşa işletilmesi,
- Sisteme eklenen blokların (verinin) sonradan sadece okunabilmesi, bloklar üzerinde değiştirme ve silme yapılamaması,
- Sistemin bir güven kurumuna/otoritesine gerek kalmadan işletilmesi, sisteme olan güvenin kriptografik yöntemler ve mutabakat protokolleriyle sağlanması,
- Sistemdeki hiçbir düğümün bir diğerine güvenmemesi, ancak bloklar üzerinde herkesin mutabık olması,
- Sistemdeki tüm blokların (verinin) birden çok düğümde saklanıyor olması (tüm veri tabanının belki yüzlerce, binlerce kopyasının olması).

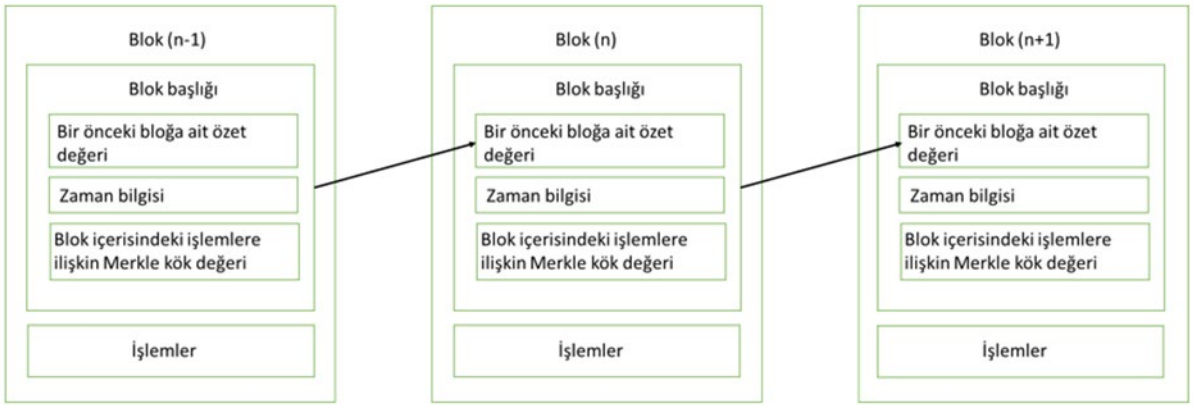
Blok zincirde genellikle bir değer veya değer üzerinde yapılan işlemler tutulur. Burada kaydı tutulan herhangi bir şey olabilir: Para (kripto para biriminde olduğu gibi), varlık sahipliği (menkul veya gayrimenkul), kod parçacığı (akıllı sözleşmelerde olduğu gibi). Blok zincir ile bahse konu değerin hem güvenli saklanması, hem de bununla ilgili, buna yönelik işlemlerin güvenli şekilde yapılması sağlanır.

Bir blok zincir ağının temel unsurlarını aşağıdaki gibi sayabiliriz:

- Sistemin temeli: Blok zincirin kendi gerçekleştirimi (kaynak kodu), bunu geliştiren yazılımcılar, ağın protokolüne karar vericiler, bunların testlerini yapanlar.
- Düğüm (node): Blok zincir ağı üzerindeki her bir bilgisayara düğüm (node) denir. Her düğüm üzerinde zincirin bütünü veya büyük bir bölümü bulunmaktadır ve oluşan bu ağ eşlerin ağıdır (peer-to-peer network, P2P). Bu ağda bir yönetici ya da kontrol mercii yoktur. Blok zincirin merkeziyetsiz olarak ifade edilmesindeki sebep budur. Bir blok zincirde düğümlerin görevleri/rolleri farklı olabilir, bu blok zincirin yönetişimine (kural ve protokollerine) bağlıdır. Kısa bir sınıflandırma şöyledir (daha detaylı sınıflandırmalar da mevcuttur):

- Tam düğüm (full node): Blok zincirin ilk bloğundan itibaren bütün bir kopyasını tutar. Blok zincirin güvenle çalışmasında belirleyici bir rol oynar, yeni blokları onaylar. Gerektiğinde tüm zinciri ilk bloğa kadar doğrulayabilir. Tüm blokların zincirin protokollerine uyduğundan emin olur.
- Hafif düğüm (light node): Blok zincirin tüm kopyasını değil daha küçük bir bölümünü tutar (genelde blok başlıklarını). Çalışmaları daha hızlıdır ancak tam düğümlerin çalışmasına bağımlıdırlar.
- Madenci düğüm (miner node): Madenci düğümler yeni blokların yaratılmasından sorumludurlar. Yarattıkları yeni blokları ağa yayıp tam düğümlerden onay beklerler. Mutabakat protokolüne bağlı olarak pahalı ve özelleştirilmiş donanıma sahiptirler.
- Süper düğüm (süper node): Bazı tam düğümler süper düğüm olarak adlandırılırlar. Dünyadaki her saat diliminde yer alırlar. Tüm düğümlerin zincirin en doğru sürümüne erişmelerinin garantisidir.

- İşlem (transaction): Bir blok zincir üzerinde gerçekleştirilen atomik veri parçasıdır. Bir transfer emri veya akıllı sözleşme çağrısı olabilir. Blok zincir türüne göre içerdiği veri türü ve boyutu değişebilir.
- Dağıtık defter/veri tabanı: İşlemleri/kayıtları (yapılan işlem ve tutulan kayıt her ne ise) içeren bloklar (veri tabanı) ağ üzerinde düğümlere yayılmıştır (birden çok kopya halinde).
- Mutabakat/uzlaşı protokolü: Zincire yeni bir blok eklemek için kullanılan yöntemdir. Birden çok yöntem mevcut olup bir blok zincir ağının en önemli bileşeni olarak görülebilir. Zincirin çalışma hızını belirler. Zorluğu (hızı belirleyen faktör) artırılıp azaltılabilir. Bazı protokoller çok fazla elektrik tüketimi nedeniyle eleştiri almaktadır.
- Kriptoloji: Blok zincir ağlarını güvenli kılan unsur kriptolojidir. Blok zincirlerde kriptolojinin kullanımı basitçe şu şekilde özetlenebilir (*konu hakkında daha detaylı bilgi için "1023-Bilgi Sistemleri Güvenliği" çalışma notuna bakılabilir*):
  - Bütünlük: Zincire eklenen blokların değişmezliğini/bütünlüğünü sağlamak amacıyla özetleme (hashing) fonksiyonu kullanılır. Kabaca her blok, bir önceki bloğun özet değerini taşır, böylece her blok bir önceki bloğa "zincirlenmiş" olur.
  - Elektronik (dijital) imza: Bloğa eklenmesi istenen her işlem (transaction), işlemi yapan tarafından gizli anahtar ile imzalanır. Bu şekilde ilgili işlemi hangi hesabın yaptığı hakkında inkâr edilemez bir kanıt oluşur. Bu durum aynı zamanda kimlik tanıma süreci olarak da kullanılır (gerçek dünya kimliklerinden bağımsız).
- Kullanıcılar: Blok zincir üzerinde işlem yapanlar, varlık transfer edenler, akıllı sözleşmelerden (*açıklanacaktır*) hizmet alanlar.
- Cüzdanlar: Blok zincir üzerinde işlem yapmak için gereken anahtar ve adresleri tutan uygulama veya donanımlar (*açıklanacaktır*).
- Kripto varlıklar: Blok zincirin kendi doğal (native) para birimi (coin) veya token, NFT gibi diğer kripto varlıklar.



Şekil 6: Blok zincirin temel gösterimi

Bir blok içinde saklanan veriler blok zincirinin türüne bağlıdır. Örneğin, bir Bitcoin bloğu gönderici, alıcı, aktarılacak bitcoin sayısı hakkında bilgiler içerir. İlk blok kök (genesis) blok olarak adlandırılmaktadır. Her bloğun kendine özgü bir parmak izi olarak düşünülebilecek bir özet değeri (hash) vardır. Bir bloğu ve tüm içeriğini tanımlar ve tıpkı bir parmak izi gibi her zaman benzersizdir. Yeni bir blok oluşturulduğunda blok içindeki herhangi bir değişiklik özet değerin değişmesine neden olacaktır. Bu nedenle özet değer, bloklardaki değişiklikleri tespit etmek için çok kullanışlıdır. Bir bloğun parmak izi değişirse, aynı blok olarak kalmaz.

Mutabakat Protokolleri

Mutabakat (consensus-uzlaşı) protokolleri, blok zincirde kontrolden geçmiş ve bekleyen işlemlerin bir bloğa yazılması ve zincire eklenmesi işleminde kullanılır ve blok zincirin en önemli unsurlarından biridir. Dağıtık ağlarda tüm katılımcıların ortak bir karara varmasını sağlayan protokollerdir. Birden çok mutabakat protokolü olup her birinin avantaj ve dezavantajları bulunmaktadır. Blok üretme işlemi blok zincir terminolojisinde "madencilik (mining)" olarak ifade edilmektedir. En çok kullanılan iki protokol aşağıda verilmiştir:

- **Çalışma Kanıtı (Proof Of Work, PoW)**

Çalışma kanıtı, istenmeyen e-postalar göndermek veya hizmet reddi saldırıları başlatmak gibi bilgi işlem gücünün anlamsız veya kötü niyetli kullanımlarını caydırmak için önemsiz olmayan ancak uygulanabilir miktarda çaba gerektiren bir sistemi tanımlamaktadır. Kavram SHA-256 karma algoritmasını kullanmaktadır.

2009 yılında piyasaya sürülmesinin ardından Bitcoin, çalışma kanıtı fikrinin yaygın olarak benimsenen ilk uygulaması olmuştur. Çalışma kanıtı, diğer birçok kripto para biriminin de temelini oluştururken güvenli ve merkezi olmayan fikir birliğine izin vermektedir.

Yöntem bir matematik probleminin çözümü sayesinde bir blok üretmek için kullanılmakta olup blok oluşturmak isteyen düğümlerin belli bir işlem (hash) gücünde özel donanımlara sahip olması gerekir. Günümüzde bu donanımlar çok pahalı olduğundan artık her düğüm bireysel olarak madencilik yapmamakta, madenci havuzlarına katılmaktadır. Madenciliğin belli bir ekonomik değeri vardır, bireyler bu amaçla bu işe girmektedir. Örneğin Bitcoin madenciliğinde blok üretiminden belirli bir miktar Bitcoin elde edilir. Bu ekonomik fayda dünyada madenci sayısını artırmakta, ancak madenci sayısı arttıkça da elde edilen ekonomik değer azalmaktadır.

Bu protokolde çalışan bir sistemde madenci kabaca, "*nonce*" adı verilen bir sayıyı yeni oluşturulacak bloğun içeriğiyle birlikte özetleme fonksiyonuna tabi tutacak, elde edilen değer hedef değer ile uyumlu değilse bu işlemi (nonce değerini değiştirip) tekrar yapacaktır ta ki hedef değer bulunana kadar. Burada yapılan iş aslında basit (özetleme fonksiyonu) olup zorluk bunu belki milyonlarca kez tekrar etme işidir. Bir anlamda bu bir kaba-kuvvet saldırısı gibidir, bir sayı tahmin etme problemidir. Hedef değer elde edildikten sonra madenci bunu blok zincir ağında yayınlar, taraflar bloğun

doğruluğunu kontrol eder, doğru kabul edilen blok zincire eklenir. Kaç düğüm tarafından doğrulama yapılacağı uygulamaya göre değişebilir. Madenciler blok onaylamasında görev alamaz.

Çalışma kanıtı mutabakatının olumsuz yanları; maliyetli olması (milyonlarca kez özetleme fonksiyonunu çalıştıracak hızlı donanım gerektirmesi), çok fazla elektrik enerjisi tüketmesi, zaman alması ve bu yüzden ağda gerçekleştirilen işlemlerin yavaş sonuçlanması ile ağdaki işlem gücünün %51'ini ele geçiren grubun zincirin bütünlüğünü bozma ihtimalinin[14] olması olarak özetlenebilir.

- **Hisse Kanıtı (Proof Of Stake, PoS)**

Çalışma kanıtı protokolünün en büyük dezavantajlarından biri olarak görülen elektrik tüketiminin önüne geçebilmek amacıyla Hisse Kanıtı protokolü kullanılmaya başlanmıştır. Örnek vermek gerekirse Bitcoin ağı çalışma kanıtı protokolünü kullanmakta iken Ethereum 2.0 ağı ise hisse kanıtı protokolünü benimsemiştir. PoW protokolündeki madenci kavramı burada yerini onaylayıcı (validator) kavramına bırakmıştır ancak madenci veya onaylayıcı olarak adlandırılsın ağdaki fonksiyonları aynıdır, yeni blok yaratırlar.

Hisse kanıtında yeni blok oluşturma sürecinde yüksek bir donanım yatırımı gerekmez ve süreçte yüksek enerji tüketimi olmaz. Onaylayıcılar sahip oldukları kripto varlık miktarı doğrultusunda blok oluşturma sürecinde yer alırlar. Blok oluşturmak isteyenler belli bir miktar varlığı sistemde kilitler (bu varlık kullanılamaz duruma gelir), bu arada çeşitli yöntemlerle bir sonraki bloğu oluşturacak düğüm seçilir (farklı seçim yöntemleri mevcuttur), blok üretilir, diğer onaylayıcılar bu bloğu doğrularsa blok, zincire eklenir ve bloğu üreten kişi belli bir ekonomik değer kazanır.

Bu protokolde blok üretimi işlem gücü/donanım sahipliğinden varlık/sermaye sahipliğine geçmiştir. Bu sistemde de çok büyük varlıkla sistemi domine etme tehlikesi mevcuttur ve buna karşı çeşitli kurallar/yaklaşımlar benimsenmektedir. Sistemde kötü niyetli davranan onaylayıcıların hisselerine el koyulabilir.

Hisse kanıtı protokolünün en önemli avantajları arasında madenci olmak için çok büyük yatırım gerektirmemesi, elektrik tüketiminin normal sınırlarda olması ve çalışma kanıtına göre daha hızlı çalışmasıdır.

1.2.6.2. Blok Zincirde Kriptolojinin Kullanımı

Blok zincirler ve kripto varlıklar kriptografik yöntemlerle yaratılır ve işletilir. Bu yöntemlerin en önemli bileşeni ise anahtar (key) dediğimiz bir yapıdır. Anahtar, sayı veya rakamlardan oluşan, bilgisayarda bir dosyada veya bir kağıda yazılarak saklanan bilgidir. Kriptolojide bir metni anlaşılmaz bir hale dönüştürmeye (coding) veya anlaşılmaz hale dönüştürülmüş bir metni tekrar orijinal haline dönüştürmeye (encoding) yarar. Türleri ve kullanım alanları çok geniş ve çeşitlidir. Blok zincir uygulamalarında asitmetrik anahtarlama kullanılır. Asitmetrik anahtarlamada bir anahtar çifti bulunur: özel (private) ve genel (açık, public) anahtar. (*Bu konuda detaylı bilgi SPL 1023 numaralı "Bilgi Sistemleri Güvenliği" çalışma notunda yer almaktadır*). Kabaca özel ve genel anahtar bir çift halindedir. Genel anahtar herkes tarafından bilinebilir, genel anahtardan özel anahtar elde edilemez ancak genel anahtar belli bir algoritma ile özel anahtardan elde edilir. Özel anahtar sadece sahibinde olacağından (olması gerektiğinden) bu anahtarla yapılan şifrelemenin, gönderimin, herhangi bir eylemin sahibince yapıldığı genel anahtarla ispatlanabilir[15].

Blok zincirlerin popüler oluşu kripto varlık transferleri ile başlamıştır. Bu yüzden varlık transferi ile örnek verebiliriz (*ancak her blok zincirin aynı kurallar ve protokollerle çalışmayacağı akılda tutulmalıdır, farklı zincirlerde farklı yöntemler ve algoritmalar kullanılabilir)*: Blok zincirdeki her işlem (transaction) (örn. bir varlığın başka bir kişiye gönderilmesi), işlemi gerçekleştiren tarafından (gönderen) özel anahtarla imzalanır. Böylece bir kişinin sahip olduğu kripto varlıklar sadece o kişi tarafından harcanabilir (varlığın sahipliği kanıtlanmış olur). Genel anahtarlar ise alıcıyı tanımlar. Yani varlık transferinin zincir üzerinde nereye (kime) yapılacağını belirtir. Fakat genel anahtarlar herkes tarafından bilinebileceğinden, bir genel anahtara yapılan gönderimin sahibinin kim olduğu da yine

[14] https://www.geeksforgeeks.org/blockchain-proof-of-work-pow/
[15] https://www.infosecinstitute.com/resources/cryptography/blockchain-and-asymmetric-cryptography/, 30 Haziran 2024

gönderim yapılan genel anahtara karşılık gelen özel anahtarla ispatlanabilir. Anahtar çiftlerinden bahsetmişken bir de adres kavramına değinmek yerinde olur. Adres olarak ifade ettiğimiz kavram aslında cüzdan adresleridir. Genel anahtar ile cüzdan adresinin aynı şey olduğu düşünülür ancak bu her zaman doğru değildir. Adresler, ilişkili olduğu genel anahtardan belirli algoritmalar aracılığıyla üretilir. Son tahlilde şöyle bir özet yapabiliriz: Özel anahtar kişinin varlık sahipliğini kanıtlar, kişiye harcama yetkisi verir. Genel anahtar cüzdan sahipliğini (bir transferde alıcı taraf olunduğunu) kanıtlar, cüzdan adresi ise alıcının banka hesap numarasıdır, alıcıya yapılacak gönderim bu numaraya yapılır.

Bazı blok zincir uygulamalarında adres yerine alıcının sadece genel anahtarına da varlık transferi yapılabilir ancak genel bir uygulama pratiği olarak kişiler her kripto varlık transferi için farklı adres kullanırlar böylece toplam varlık bakiyelerinin zincirde açığa çıkmasını önlemiş olurlar, çünkü blok zincirler üzerinde yapılan işlemler (dolayısıyla adresler veya genel anahtarlar) herkes tarafından görülebilir. Adreslerin bir kullanım nedeni budur. Diğer bir nedeni adreslerin boyut olarak genel anahtardan kısa olması böylece işlem (transaction) bilgilerinin daha az yer tutmasıdır. Fakat belki de geleceğe yönelik en önemli neden şudur: Kuantum bilgisayarların anahtar oluşturma algoritmalarını kırabileceği, böylece ele geçirilen özel anahtarlar ile kripto varlıkların çalınabileceği düşünülmektedir. Bu noktada adres kullanımının nedeni genel anahtarı da özel anahtar gibi gizli tutmaktır.

Günümüzün finansal dünyasında birçok işlem için merkezi/otorite kurumlara ihtiyaç vardır. Bu kurumlar çok basitçe tarafların kimliğini belirler, yapılan işlemlerin geçerliliğini onaylar ve tüm işlemleri güvenli bir şekilde saklar. Blok zincir üzerinde gerçekleştirilen işlemlerde bu sayılan fonksiyonları kim yerine getirir? Çünkü blok zincirin temel fikri merkeziyetsiz olması yani klasik finansal güven kurumlarına ihtiyaç duyulmamasıdır demiştik. İşte müşteri tanıma, işlemlerin geçerliliği ve güvenliği fonksiyonları blok zincirde kriptolojik işlemler ile özel olarak da asimetrik şifrelemeyle gerçekleşir. Yani blok zincirin güvenliği kriptolojiye dayanır.

Müşteri tanıma kısmına bir parantez açmak gerekir: Burada müşteri tanıma, bildiğimiz anlamda (know your customer, KYC) müşteri tanıma değildir, aksine blok zincirin çıkış noktasında işlem yapanların gizli olması fikri yatar. Blok zincir uygulamalarında müşteri olarak elimizde müşterinin işlem adresi/açık anahtarı vardır, gerçek dünyadaki kimliğini (çok özelleşmiş bazı durumlar/uygulamalar haricinde) bilemeyiz. Blok zincir uygulamalarında müşteri tanıma, müşterinin yaptığı işlemi kendi özel anahtarı ile imzalaması, zincire yayılan bu işlemin de müşterinin açık anahtarı ile tüm taraflarca doğrulanabilmesidir. Yani işlemi, iddia eden kişinin yaptığı doğrulanmış olur. Bu anlamda kriptoloji, blok zincirde işlem sahiplerinin anonim kalmasını ve işlemlerin düğümler tarafından doğrulanabilmesini sağlar.

Kriptolojinin bir diğer uygulaması olan özetleme fonksiyonu (hash, hashing) ise blok zincirin değiştirilemez, tahrif edilemez olmasını sağlar. Bu sayede normalde finansal bir otorite/güven kurumu tarafından gerçek/doğru olduğu kabul edilen işlem listesinin tutulmasına gerek kalmaz, zincirdeki işlemler zaten değiştirilemez. Özetleme fonksiyonu hem bir blok içindeki işlemlerin değiştirilemez olmasını sağlar, hem de blokları değiştirilemez şekilde birbirine bağlar.

1.2.6.3. Blok Zincir Dünyasında Bazı Tanımlar

1.2.6.3.1. Kripto Varlıklar

Kripto varlık, Sermaye Piyasası Kanunu'nda şu şekilde ifade edilmiştir:

"*Dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak elektronik olarak oluşturulup saklanabilen, dijital ağlar üzerinden dağıtımı yapılan ve değer veya hak ifade edebilen gayri maddi varlıklar.*"

Kripto varlıklar bir dağıtık defter gerçekleştirimi olan blok zincir ağları üzerinde üretilir ve bu ağ üzerinde "*yaşarlar*". Kriptolojik teknikler kullanılarak üretilir ve korunurlar. Bildiğimiz anlamda fiziksel bir varlık değildir. En bilinen türleri bugün artık çok aşina olduğumuz "coin"ve "token"lardır. Bu iki kavramın arasındaki farkı anlamak için kısa tanımlarına bakabiliriz:

Coin, bir blok zincirin doğal (native) para birimidir. Her zincir üzerinde bir tane coin üretilir. Kendi mutabakat mekanizmaları vardır. Buna en bilinen örnek olarak bitcoin ağı üzerindeki BTC,

ethereum ağı üzerindeki ETH verilebilir. BTC bitcoin blok zinciri, ETH ise ethereum blok zinciri üzerinde üretilir ve harcanır. Ortaya çıkış amaçları bir ödeme/takas aracı olmaktır ancak popülerlikleri sebebiyle yatırım amacıyla da alınıp satılabilirler.

Token ise, mevcut bir blok zincir üzerinde çalıştırılan akıllı sözleşme marifetiyle üretilir, doğrudan blok zincir üzerinde değildir, araya bir katman girmiş gibi düşünülebilir. Doğal (native) bir kripto para birimi değildir. Bir zincir üzerinde sayısız token üretilebilir. Altyapıdaki blok zincirin mutabakat mekanizmasına güvenir. Genelde bir ürün/hizmet üzerinde bir hakkı temsil ederler veya bir firma/proje için fon toplamak üzere üretilir ve dolaşıma sokulur. İlk dolaşıma çıkması ilerleyen bölümlerde açıklanan Initial Coin Offering (ICO) süreci ile gerçekleşir, sonrasında borsalarda alınıp satılabilir. Farklı türde token'lar farklı işlevsellikler taşır, yani bir token üretildiği akıllı sözleşmenin mantığına göre davranış gösterir. Token sayesinde, bir fiziksel veya dijital varlık blok zincir üzerinde temsil edilir, alınıp satılır, işlemlere taraf olabilir.

Yeni bir kripto para birimi (coin) üretmek için yeni bir blok zincir ağı kurmak gerekir, ancak tokenlar mevcut (genelde ethereum) blok zincirler üzerinde üretilirler. Özet olarak kripto varlıkları aşağıdaki gibi sınıflandırılabiliriz:

- Kripto para birimleri (coin): Kripto varlıkların hayatımıza girişi bunlar sayesinde olmuştur. Merkezi otoriteler tarafından yönetilmezler. Her coin'in kendi blok zinciri vardır. Üretildikleri zincir üzerinde işlem ücretleri bunlar ile ödenir (örneğin Ethereum ağında tüm işlem ücretleri Eth ile ödenir, çünkü bu ağın para birimi budur).

- Token (jeton): Yukarıda anlatıldığı gibi birer akıllı sözleşme uygulamasıdır ve farklı işlevsellikler sunarlar. Mevcut token türleri kabaca aşağıda verilmiştir, ancak bu liste değişime açıktır, farklı bir token fikri olan bir kişi bunu akıllı sözleşme olarak programlayabilir ve dolaşıma çıkarabilir:

  - Utility (hizmet) token: Bir şirketin/kurumun ürünlerine/hizmetlerine erişim, kullanım veya indirim hakkı verirler.

  - Security (menkul kıymet) token: Bir ürün/hizmet üreten firma tarafından (genelde startup) yatırımcılardan fon toplamak amacıyla geliştirilir. Karşılığında token sahiplerine firma üzerinde söz hakkı, pay sahipliği verebilir. Bir yatırım türü olarak düşünülebilir.

  - Non Fungible Token (Nitelikli Fikri Tapu, NFT): Yukarıda bahsedilenlerden biraz daha farklı olarak benzersiz dijital varlıkları ve bunların sahipliğini temsil ederler. Bir dijital sanat eseri, bilgisayar oyunlarındaki öğeler, fikri mülkiyet hakkı olabilir. Bu varlıkların sahipliği ve gerçekliği (authenticity) üretildikleri blok zincir üzerinde takip edilir.

  - Real world assets token (gerçek dünya varlıkları, RWA): Gerçek dünyadaki fiziksel varlıkların (gayrimenkul, emtia vb.) bir blok zincir üzerindeki dijitalleştirilmiş karşılığıdır (tokenization). Bu şekilde blok zincir üzerinde işlem görebilirler.

  - Governance (yönetişim) token: Sahiplerinin bir platformun yönetiminde söz sahibi olmasını sağlarlar. Merkezi olmayan özerk kuruluşlar (Decentralized Autonomous Organization, DAO) içinde kullanılırlar. Genelde üyelerin hepsinin token'ı vardır ama fazla token demek yönetimde daha fazla söz sahibi olmak demektir.

  - Stable coin: Her ne kadar ilk kripto paralar asıl olarak alternatif bir ödeme/takas aracı olarak ortaya çıktıysa da günümüzdeki yüksek fiyat oynaklığı bunları ödeme aracı olarak elverişsiz kılmaktadır. Stablecoin'lerin değeri ise belli bir para birimine/finansal araca (örneğin emtia) belirli bir oranda bağlanmıştır. Bu yüzden ödeme aracı olarak daha rahat kullanılabilirler. Örneğin 1 Tether=1 Amerikan Dolarıdır.

- Altcoin: Açılımı alternative coin olup Bitcoin'in kazandığı popülarite sonrası oluşturulmuşlardır. Altcoin, Bitcoin dışındaki tüm kripto varlıkları ifade eder.

Kripto varlıkların bazı temel özellikleri aşağıdaki gibidir:

- Belli bir otorite (örneğin merkez bankaları) tarafından üretilmezler ve kontrol edilmezler. Bu yüzden "merkeziyetsiz" olarak adlandırılırlar. Diğer yandan merkez bankaları kendi ülkelerinin itibari (fiat) para birimi bazında kripto para birimi üretebilirler, ancak bunlar merkeziyetsiz değildir.

- Tamamen kriptolojik teknikler kullanılarak blok zincir veya dağıtılmış defter (distributed ledger) altyapıları üzerinde yaratılır, transfer edilir ve izlenirler.

- Ödeme, yatırım, takas, hak kullanımı gibi amaçlar için kullanılabileceği gibi maalesef (merkeziyetsizlik ve anonimlik özelliklerinden ötürü) yasa dışı ürün ve hizmetlerin alım satımı, dolandırıcılık ve kara para aklama gibi faaliyetlerde de kullanılabilir.

- Kripto para birimlerinin çoğunluğunun değeri arz/talep dengesiyle serbest olarak belirlenir. Fiyatlamalarda çok aşırı oynaklık olabilir.

- Üretimi, ödeme aracı olarak kullanımı, alım satımı veya kişiler/kurumlar arasındaki transferi, blok zincir altyapılarının fonksiyonları ile gerçekleşir. Mülkiyetleri hakkındaki tek değişmez kaynak da yine blok zincirdir.

- Yatırım aracı olarak kripto varlık borsalarında (platformlarda) alım satımı yapılabilir. Borsalar merkeziyetsiz veya merkezi olabilir.

1.2.6.3.2. Akıllı Sözleşmeler (Smart Contracts)

Akıllı sözleşmeler, blok zincir ağında çalışan uygulamalardır. Belirli koşullar gerçekleştiğinde dış müdahaleye gerek kalmadan çalışmak üzere tasarlanmışlardır. Akıllı sözleşmelerin belirli bir platformda yazılması daha sonra da çalışması planlanan blok zincire yüklenmesi gerekir. Blok zincirlerde genelde veri/değer tuttuğumuzu belirtmiştik. Akıllı sözleşmelerde ise blokta program/kod tutulur. Sözleşme koşulları doğrudan koda yazılmıştır. Sözleşmeler kendi içinde veri veya kripto varlık da tutabilirler. Ayrıca dış dünya ile iletişim kurabilir, dış dünyadan veri alabilirler. Başka akıllı sözleşmeler ile de etkileşime girebilirler.

Akıllı sözleşmeler ilk defa ethereum blok zincir uygulamasıyla ortaya çıkmıştır. Bir akıllı sözleşmeyi zincire yüklemek ve daha sonra buradan bir hizmeti (servisi, fonksiyonu) çağırmak için belli bir miktarda ücret (eth) ödenir. Akıllı sözleşmede, tıpkı kâğıt üzerindeki bir sözleşmeye benzer şekilde birden çok taraf olmalıdır ve bu taraflar sözleşme şartlarını kabul etmiş olmalıdır. Bundan sonra programlanan ve bir blok zincire yüklenen sözleşme, hükümler için gerekli şartlar sağlandığında otonom olarak (akıllı) çalışacaktır. Örnek olarak bir arabayı satın alan ve satan taraflar için bankaya arabanın bedeli yatırıldığında sahiplik bilgisinin otomatik olarak parayı gönderen tarafa geçmesi gibi. Burada alıcı ve satıcı arasında başka bir güven kurumuna gerek kalmayacaktır. Ayrıca taraflar gerçekleşen kayıtları/işlemleri görebilecek ancak değiştiremeyecektir. Akıllı sözleşmeler konusunda, blok zincire yüklenen programın/kodun doğruluğu çok önemlidir. Burada hem kodun doğru çalışmayıp taraflara zarar verebilmesi hem de bir yazılım olduğundan siber saldırıya uğraması riski bulunmaktadır.

1.2.6.3.3. Airdrop

Airdrop temelde bir pazarlama girişimidir. Genelde blok zincir bazlı ürün/hizmet sunmayı tasarlayan startup firmalar tarafından gerçekleştirilir. Firma kendini/ürün ve hizmetini tanıtmak için bedelsiz veya çok küçük, sembolik bir bedel/işlem karşılığı (yeni müşteriler bulma, sosyal medya üzerinde beğeni gibi) kripto varlık (token) dağıtır[16]. Avantajları ve dezavantajları olabilir. Sahiplerine belirli bir üründe/hizmette öncelik verebilir. Ancak esas amaç dolandırıcılık da olabilir, kullanıcıların cüzdanlarından anahtarları çalınabilir veya sadece işe yaramayan, değersiz bir kripto varlık olarak da kalabilir.

[16] https://www.investopedia.com/terms/a/airdrop-cryptocurrency.asp, 1 Temmuz 2024.

1.2.6.3.4. İlk Kripto Varlık Arzı/İlk Satışı (Initial Coin Offering, ICO)

İlk kripto varlık arzı olarak Türkçeye çevirebileceğimiz ICO faaliyeti ise, bir girişime/projeye fon sağlamak amacıyla yeni üretilen bir kripto varlığın, popüler kripto paralar veya itibari paralar cinsinden satışa çıkarılmasıdır. Burada alıcıyı yatırım yapmaya sevk eden esas dürtü, geliştirilecek yeni kripto varlığın değerinin artması, alım satımından para kazanılması ve girişimci tarafından geliştirilecek ürün/hizmette imtiyazlar elde edilmesidir. Yöntemin ismi, ilk halka arz (initial public offering, IPO) terimine benzetilse de alınan kripto para, ihraç eden şirkette pay sahipliği hakkı vermeyebilir. Bir kitle fonlama türü olarak düşünülebilir. Ancak yapılan araştırmalarda, ICO yapan girişimlerin yarıya yakınının ömrünün ortalama dört ay olduğu belirtilmiştir[17]. Dolayısıyla belli bir yasal çerçeve ile düzenlenmeyen ICO faaliyeti yatırımcıların zarara uğramasına sebebiyet verebilmektedir. Çin ve Güney Kore'de ICO yasaklanmış olup, bazı ülkelerde düzenleyiciler bu konuda yatırımcılara uyarı yapmaktadırlar[18].

Günümüzde başarılı airdrop veya ICO girişimleri olduysa da maalesef birçok dolandırıcılık olayı airdrop veya ICO kisvesi altında işletilmiştir.

1.2.6.3.5. Köprü (Bridge) Uygulamaları

Normalde blok zincirlerin her biri dışarıya kapalı olarak çalışırlar. Gelinen noktada çeşitli ihtiyaçları karşılamak için iki blok zinciri birbirine bağlayan köprü uygulamaları geliştirilmiştir. Bunlar da akıllı sözleşme olarak çalışır ve blok zincirler arası varlık transferi yapmaya yararlar.

1.2.6.3.6. Kâhin (Oracle) Uygulamaları

Blok zincirler normalde dış dünyaya kapalı olarak işletilirler demiştik. Ancak gittikçe sofistikleşen blok zincir uygulamaları dış dünyadan bilgi alışverişine ihtiyaç duymaktadır. Bu amaçla kâhin uygulamaları geliştirilmiştir. Bunlar da birer akıllı sözleşmedir, ancak blok zincire dışardan açılan bir kapı olarak düşünülürse güvenilir olmaları gerektiği aşikârdır çünkü birer saldırı aracı veya istismar noktası olabilirler.

1.2.6.3.7. Kripto Varlık Platformları (Borsaları)

Kripto varlıkların alınıp satıldığı (itibari para birimleri veya başka bir kripto varlık karşılığında) organize platformlardır. Sermaye Piyasası Kanunu'nda "*platform*" olarak ifade edilmiş olup şu şekilde tanımlanmıştır:

"Kripto varlık alım satım, ilk satış ya da dağıtım, takas, transfer, bunların gerektirdiği saklama ve belirlenebilecek diğer işlemlerin bir veya daha fazlasının gerçekleştirildiği kuruluşlar".

Burada kripto varlık alım satımının motivasyonu yukarıda da belirtildiği gibi genelde kripto varlıkların değerlerindeki artış veya azalıştan fayda sağlamaktır. Bir kripto varlık borsası piyasa yapıcı (market maker) olabileceği gibi sadece alım-satım eşleme platformu olarak da çalışabilir. Platformların tabi oldukları mevzuat sundukları işlevleri önemli ölçüde etkileyebilir.

Kripto varlık platformlarının temel özellikleri aşağıdaki gibi özetlenebilir (*platformların tabi oldukları düzenlemeler çerçevesinde çalışma şekillerinin değişebileceği akılda tutulmalıdır*):

- Her platform her kripto varlığın alım satımını desteklemeyebilir. Hangi varlıkların alınıp satılabileceği ve karşılığının nasıl kabul edileceği platformun iş modeline ve/veya düzenleyici otoritelere göre değişebilir.

- Platformlar merkeziyetsiz (decentralized exchange, DEX) veya merkezi (centralized exchange, CEX) olabilir. Yukarıda verilen tanım merkezi borsaları ifade eder. Çünkü müşterinin karşısında alım satım hizmetini sunan, destek sağlayan bir kurum (merkez) vardır.

- Merkeziyetsiz borsalar alım-satım sırasında doğrudan blok zincirle iletişime geçerler. Bu durum borsanın daha yavaş işlemesine neden olur ancak her işlem doğrudan blok zincire işlenir. Burada

[17] https://en.wikipedia.org/wiki/Initial_coin_offering#cite_note-halfdie
[18] https://www.coindesk.com/learn/what-is-an-ico/

aslında alım satım doğrudan taraflar arasında yapılır, işlemler merkezi bir kurum üzerinden geçmez ya da onaylanmaz. Merkeziyetsiz olarak ifade edilen budur. Merkeziyetsiz borsalar, merkeziyetsiz finans (Decentralized Finance, DeFi) ekosisteminin önemli bir parçasıdır, birer merkeziyetsiz uygulamadır (decentralized application, dApp) ve yapılan işlemler akıllı sözleşmeler tarafından gerçekleştirilir.

- Merkezi borsalar her alım satımda blok zincirle iletişime geçmezler çünkü bu yavaşlık yaratır. Bu yüzden zincir dışı çalışırlar. Genelde kendi havuzlarından alım satımı karşılar ve sahiplik için kendi içlerinde bir liste tutarlar.

- Merkezi borsalarda müşteri genelde blok zincirle iletişime geçmez, ancak aldığı kripto varlığı borsa dışına çıkarmak istediğinde blok zincirle iletişim kurulur.

- Bazı platformlar blok zincirde bir düğüm işletebilir.

- Merkezi kripto varlık platformları aslında bildiğimiz menkul kıymet borsalarına çok benzer bir mantıkla çalışır. Kripto varlık alım satımı yapmak isteyen kişi ilk önce bir platform seçmelidir. Daha sonra burada kendine bir hesap açtıracak, işlemleri onaylandıktan sonra alım satıma başlayabilecektir.

- Platformlar, alım satım gerçekleştirmenin yanında müşterilere bir dizi işlev de sunarlar, bunların belki de en önemlisi saklama işlemidir (custody). Bu işlev, müşterilerin cüzdanlarının özel anahtarlarının borsa bünyesinde saklanmasıdır. Saklama hizmeti platformlar dışındaki kuruluşlarca da yapılabilir.

- Bazı borsalar müşteriye karşı kendi namına (hesabına) alım satım yapabilirler ki bu durumda piyasa yapıcı (market maker) olarak adlandırılırlar. Bazı borsalar da sadece müşterilerden gelen emirlerin birbirleriyle eşleştirilmesine aracılık ederler.

- Merkeziyetsiz borsalarla çalışmak biraz daha teknik bilgi gerektirmekte olup, belli bir düzenlemeye tabi olmamaları nedeniyle de çok daha risklidir. Bu yüzden bazı merkeziyetsiz borsalarda çok fazla alım-satım talebi oluşmamakta yani sığ bir piyasa meydana gelmektedir. Bu durum da fiyatların müşteriler için çok avantajlı olmaması sonucunu doğurur. Genel olarak bir borsada ne kadar fazla müşteri varsa o oranda likit bir borsa oluşur.

- Merkezi borsalar her şeyden önce kuruldukları ülkede çeşitli kurumlarca düzenlenen kuruluşlardır. Birden çok yasal düzenlemeye tabidirler, bu yüzden daha güvenilir olarak kabul edilirler.

- Merkezi borsalar hem kripto varlık hem de kullanıcılara ait bilgi barındırdığı için içeriden ve dışarıdan siber saldırılara karşı bir hedeftir.

1.2.6.3.8. Cüzdanlar

Kripto varlıkları borsada alıp satarken, borsa dışı bir araçla kripto varlık harcarken veya transfer ederken aslında kripto varlığa hiç "dokunmayız". Kripto varlık daima ait olduğu blok zincir üzerinde durur. Benzer şekilde borsalar da kripto varlığa dokunamaz, onların kripto varlıkları da blok zincir üzerindedir. Peki, bu varlıklara sahip olduğumuzu nasıl kanıtlarız? Veya bunları nasıl harcarız? Bu soru bizi Cüzdan (wallet) kavramına getirir.

Kripto varlıklarla işlem yapmak isteyen herkesin bu kavrama aşina olması gerekir. Cüzdanlar kripto varlığın kendisini değil, blok zincirde kripto varlığa erişmek için kullanılan özel anahtarı tutarlar. Bir bakıma banka kartlarına da benzetebiliriz. Banka kartı da aslında paranın kendisi değildir, bankadaki paraya erişmemizi sağlar. Cüzdanlar hakkında en temel bilgi, cüzdanın asla kripto varlığın kendisini tutmamasıdır. Kripto varlık daima blok zincir üzerindedir. Blok zincir üzerindeki varlığın alınıp satılması, transfer edilmesi sadece özel anahtar aracılığı ile yapılır. Özel anahtar, bireyin kripto varlık üzerindeki mülkiyet hakkını gösterir, ayrıca bu özel anahtar merkezi bir otorite tarafından verilmediği, gerçek dünyada belirli bir kimliğe bağlanmadığı için de özel anahtar kimdeyse buna bağlı kripto varlık da onundur. İşte kripto varlıklarla uğraşmanın (almanın, satmanın, kullanmanın) en önemli zorluklarından biri de budur, özel anahtarın saklanması. Özel anahtarı cüzdanda saklarız. Cüzdanlar birkaç türe ayrılabilir, farklı işlevler sunabilir. Genel kabul görmüş sınıflandırma aşağıdaki şekildedir:

- **Soğuk (cold) cüzdan**: Soğuk cüzdan, özel anahtar(lar)ı İnternet bağlantısı olmayacak (çevrimdışı, offline) şekilde tutan yapı olup genelde bir donanımsal cihazdır (USB gibi). En önemli özelliği İnternete bağlı olmamasıdır ki bu şekilde İnternet bazlı birçok saldırı/çalma girişimine bağışıktır. Soğuk cüzdanın en önemli güvenlik riski kaybolması veya çalınmasıdır. Yukarıda anahtarların belli bir otorite tarafından verilmediğini belirtmiştik. Çalınma veya kaybolma durumunda cüzdan sahibinin başvurabileceği, kaybını telafi edebileceği bir merci veya yöntem yoktur.

- **Sıcak (hot) cüzdan**: Sıcak cüzdan aslında bir bilgisayar uygulamasıdır, dolayısıyla bir cihaz üzerinde çalışır (bilgisayar, akıllı telefon, tablet gibi) ve daima İnternete bağlı veya bağlanabilir durumdadır yani sürekli işlem yapmaya hazır durumdadırlar. Bu durum da sıcak cüzdanları siber güvenlik konusunda saldırıya/hırsızlığa karşı savunmasız kılar. Burada sıcak cüzdanın (uygulamanın) güvenliği ve kullanan kişinin maruz kalabileceği riskleri bilmesi önemlidir.

Güvenlik risklerinden bahsedince akla neden sıcak cüzdan kullanalım sorusu gelebilir. Buna cevap olarak sahip olunan kripto varlığı kullanmak (harcamak, transfer etmek) için sıcak cüzdana ihtiyacımız olduğunu söyleyebiliriz. Sıcak cüzdan sadece özel anahtarı saklamak için kullanılmaz, sahip olduğu (uygulamaya göre değişebilir) işlevlerle/ara yüzlerle kullanıcının blok zincire bağlanmasını ve orada işlem yapabilmesini sağlar. Yani özel anahtarımızı güvenli saklamak için soğuk cüzdan kullansak bile kripto varlıkla işlem yapabilmek için sıcak cüzdana ihtiyacımız vardır. Kısaca soğuk cüzdanlar kripto varlıkları uzun süreli saklamak için güvenli bir çözümdür. Kurumsal kullanıcılar için de soğuk cüzdan kullanımı daha doğru bir yaklaşımdır. Bunun yanı sıra, sıcak cüzdanların ve bunları kullandığımız donanımların güncel ve güvenli sürümlerini kullanmak da önemlidir.

- **Ilık (warm) cüzdan**: Bunlar da aslında birer sıcak cüzdandır ancak daha güvenli tasarlanmışlardır. Kontrollü olarak çalışan sıcak cüzdanlar denebilir. Bunların bazıları bir donanımla beraber gelirler ve hem sıcak hem de soğuk cüzdan işlevi görürler, işlem sırasında bir yazılım ara yüzü ile sıcak cüzdan özelliği gösterirler. Sıcak cüzdanın kullanım kolaylığını ve soğuk cüzdanın güvenlik özelliklerini birleştirmek için geliştirilmiştir.

Cüzdanlara ilişkin farklı bir sınıflandırma ise aşağıdaki gibidir:

- **Yazılımsal cüzdan (software wallet):** Bu tip cüzdanlar genellikle ya bir donanım üzerine kurularak (bilgisayar, telefon, tablet) veya bulut hizmeti üzerinden kullanılır. Bu cüzdanların cüzdan adresleri oluşturma, blok zincir ile iletişime geçip işlem yapma, bakiye görüntüleme, DeFi hizmetlerine erişme gibi işlevsellikleri bulunur. Sıcak cüzdan özelliği gösterirler, bu yüzden siber saldırılara açıktır.

- **Donanımsal cüzdan (hardware wallet):** Bunlar USB veya benzeri bir donanım olarak gelirler. Soğuk cüzdan sınıfına girerler bu yüzden siber saldırılara karşı dayanıklıdır ancak donanım arızası veya çalınma riski mevcuttur.

- **Akıllı sözleşme temelli cüzdanlar:** Bu cüzdan tipi akıllı sözleşme olarak programlanmıştır, kripto varlıklar sözleşme adresinde tutulur. Kripto varlık üzerindeki işlemler akıllı sözleşmenin fonksiyonları aracılığı ile yapılır. Bir tek özel anahtarla korunan sıcak cüzdanlara göre daha güvenlidir. Bunlar aslen bir akıllı sözleşme olduğu için farklı işlevsellikler de taşır:
    - Otomatik ödeme/transfer: Belirli koşullar oluştuğunda ödeme veya transfer işlemlerinin gerçekleştirilmesi.
    - Çoklu imza işlemleri: Birden fazla tarafın onayını gerektiren işlemler.
    - Zaman bazlı işlemler: Belirli bir zaman aralığında yapılacak işlemler.

- **Hiyerarşik Deterministik (HD) cüzdanlar**[19]**:** HD cüzdanlar geliştirilmeden önce tüm cüzdanlar aslında ND (non deterministic) cüzdan tipindeydi. Yani her bir kripto varlık hesabı (veya

[19] https://learnmeabitcoin.com/technical/keys/hd-wallets/#:~:text=So%20basically%2C%20an%20HD%20Wallet,and%20stored%20private%20keys%20individually, Temmuz 2024

işlemi) için ayrı anahtar çiftleri (veya adresler) kullanılmaktaydı ve bu çiftler birbiriyle ilişkili değildi, hepsi ayrı ayrı muhafaza edilmeliydi. Çok fazla farklı hesaba sahip olan veya çok fazla işlem yapan kişiler için yönetim zorluğu ortaya çıkıyordu.

HD cüzdan tipinde ise, cüzdan içindeki tüm genel ve özel anahtar çiftleri bir master anahtar çiftinden üretilir (extended public key (XPUB) ve extended private key (XPRIV). Teorik olarak bu master anahtar çifti ile milyonlarca anahtar çifti hiyerarşik olarak üretilebilir.

Ayrıca bu cüzdanın kullanımı için master anahtar çiftinin hatırlanmasına da gerek yoktur, HD cüzdan uygulamaları anımsatıcı cümle/tohum cümlesi (mnemonic phrase/seed phrase) kullanırlar. Anımsatıcı cümle genelde rastgele 12-24 kelimeden oluşur ve HD cüzdanı kullanmak için bilinmesi/hatırlanması (ya da çaldırılmaması) gereken tek bilgi budur. Günümüzde neredeyse tüm cüzdanlar HD cüzdan tipindedir.

- **Kağıt cüzdan:** Kağıt cüzdanlar, anahtarların ve bazı durumlarda bunların barkodlarının veya kare kodlarının basılı olduğu kağıt parçalarıdır. Bir cüzdan uygulaması ile basılırlar, bu uygulama basım sonrası anahtarları ağdan temizler. Bu işlem sonrası bu kâğıt cüzdanlar birer soğuk cüzdan haline gelir. Kâğıt cüzdanlar elbette fiziksel hasara ve çalınmaya karşı dayanıksızdır. Üretildiği, basıldığı ve işlem için kullanıldığı uygulamaların ve basım için kullanılan yazıcıların güvenliği de çok önemlidir. Bu cüzdanlar sonradan işlem için kullanılırken yine bir uygulama ile üzerindeki kodların okunması gerekecektir.

- **Çok Taraflı Hesaplama Cüzdanı (MPC) ve Çoklu İmza Cüzdanı (Multisig):** Birey olarak sanal varlıklarımızı harcarken bir özel anahtara ihtiyaç duyarız ve bunu cüzdanımızda saklarız, bunlar yukarıdaki bölümde anlatıldı. Elbette bir kişi birden çok özel anahtara sahip olabilir ve her harcamasını farklı bir anahtarla yapabilir ancak her bir işlemde sadece bir anahtar ve anahtarın bütününü kullanır. Zaten işlemi de tek başına yapmaktadır. Kendisi karar verir ve işlemi gerçekleştirir.

Ancak bir kurum/firma kripto varlık alacak, bununla işlem yapacaksa özel anahtar kimde olacak ve kullanmaya kim yetkili olacaktır? Kurum burada tüm yetkiyi bir kişiye vermek istemeyebilir, bir kişinin kötü niyetli davranarak kurumu zarara uğratmasını istemeyebilir. Burada bireysel kullanımdan daha farklı bir risk vardır. Bu riskin yönetilebilmesi için yine kriptoloji yardıma koşar:

MPC (Multi Party Computation) Protokolü[20]: Bu protokolde bir özel anahtar birden çok parçaya ayrılır (sharding) ve her parça bir tarafa/kişiye verilir. Bu durumda kurumun sahip olduğu kripto varlıklar üzerinde tasarruf yapabilmesi için anahtarın parçalarının dağıtıldığı kişilerin bir araya gelmesi (bir protokol/uygulama aracılığıyla) gerekir. Kimse tek başına varlıklar üzerinde bir işlem yapamaz. Yetki (ve risk) dağıtılmıştır. Bu protokolde bir işlemin onaylanması için belli sayıda anahtar parçasının bir araya gelmesi (yani anahtar parçalarını tutan kişilerin onayı) gerekir. Anahtar parçalarının tümünün (parçalara sahip tüm kişilerin) bir araya gelmesi gerekmez.

Multi Signature Protokolü: Bu protokolde ise, bir işlemin onaylanması için birden çok imzaya ihtiyaç vardır. Doğal olarak tek bir imza ile onaylanan işlemlere göre daha güvenlidir. Bu protokolde toplamda M imza (taraf) vardır ve bir işlemin onaylanması genelde N imza (taraf onayı) ile gerçekleşir (M>N). MPC'de olduğu gibi bir özel anahtar parçalara bölünmez, ancak ortada birden çok özel anahtar bulunur.

MPC veya Multi Sig protokolünü kullanan cüzdan uygulamaları bulunmaktadır. Kişi ve kurumlar kendi risk algılarına göre bunlar arasından seçim yapabilirler.

[20] https://digitalprivacy.ieee.org/publications/topics/what-is-multiparty-computation, 2 Temmuz 2024.

1.2.6.4. Blok Zincir Ağ Türleri

Blok zincir uygulamaları ilk önce herkese açık/herhangi bir izin gerektirmeyen yapılar olarak tasarlanıp işletilmeye başladıysa da zaman içinde bu yapıda bazı farklılaşmalara gidilmiştir[21]. Belirli bir blok zincire katılmadan önce yapının dikkatlice incelenmesi gerekir çünkü aynı türde olduğu söylenen zincirler arasında bile ufak gerçekleştirim farklılıkları oluşabilir. Yine de mevcut durumda aşağıdaki gibi bir sınıflandırma yapmak mümkündür.

- Herkese açık (public) ağlar

Bu zincir katılım izni gerektirmez, herkes katılabilir. Blok zincir ağlarının ilk ortaya çıkış modeli budur (örn: Bitcoin). Katılımcılar hem tüm defteri görebilir hem de blok üretebilir (madencilik). Avantajı herhangi bir kurumun kontrolünde olmaması (gerçek merkeziyetsizlik) olup en önemli dezavantajı da büyüklüğü sebebiyle performans düşüklüğüdür (işlemlerin tamamlanması, zincire blok eklenmesi).

- Özel (private)/izinli blok zincir ağları

Bu şekilde bir zinciri genelde bir kurum/organizasyon işletmekte olup katılmak için işleticiden izin alınması gerekir. Avantajı kurumun zincire katılacak düğümleri seçebilmesi ve yetkilendirebilmesidir. Sadece okuma izni verilebildiği gibi yeni blok üretimi izni de verilebilir. Dezavantajı ise, gerçek merkeziyetsizliğin olmamasıdır.

- Hibrit blok zincir ağları

Bu tür bir blok zincir, hem herkese açık (public) hem de özel (private) blok zincirin özelliklerini taşır. Bu tür blok zincirde ağa kabul edilmek için zinciri işleten kurumdan izin almak gerekir. Kabul edilenler hem blok verisini okuyabilir hem de yeni blok üretimine katılabilir. Bu tür ağlarda düğümlerin kimliği diğer düğümlerden gizlenir.

Bu türün herkese açık olan kısmı ise, işleten kurumun istediği blokları bir public zincire ekleyebilmesi veya public tarafından blok verisinin doğrulanabilmesidir.

Kurum kuralları değiştirebilir. Public tarafa neleri açacağını kendi belirleyebilir. Ağa katılım izne bağlı olduğundan bu ağlarda %51 atağı yapılamaz.

- Konsorsiyum blok zincir ağları

Hibrit blok zincirin birden çok kurum tarafından ortaklaşa işletilen türüdür.

1.2.6.5. Blok Zincir Kullanımının Avantajları

Esneklik: Blok zincirleri genellikle kopyalanmış bir mimaridir. Zincir, sisteme karşı büyük bir saldırı olması durumunda çoğu düğüm tarafından işletilmeye devam eder. Özellikle büyük zincirlerde tek hata noktası (single point of failure) ihtimali yoktur.

Zaman tasarrufu: Finans endüstrisinde blok zinciri; uzun bir doğrulama, ödeme ve tasfiye sürecine ihtiyaç duymadığından, işlemlerin daha hızlı çözülmesine izin verebilir. Çünkü paylaşılan defter, üzerinde anlaşmaya varılan verilerin tek sürümüdür. Tüm taraflarca ortaklaşa kullanılabilir. Ancak burada, blok zincir ağının kendi içindeki işlem sonuçlandırma süreleri dikkate alınmalıdır.

Güvenilirlik: Blok zincir, ilgili tarafların kimliklerini onaylar ve doğrular. Bu, çift kayıtları kaldırır, hata oranını düşürür ve işlemleri hızlandırır.

İşlemlerin değişmezliği/bütünlüğü: İşlemleri kronolojik sıraya göre kaydeden blok zincir, zincire eklenen blokların içeriğinin değişmezliğini onaylar, yani zincire yeni bir blok eklendiğinde artık bu blok kaldırılamaz veya değiştirilemez.

[21] https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology#:~:text=There%20are%20four%20main%20types,consortium%20blockchains%20and%20hybrid%20blockchains

Dolandırıcılığı önleme: Paylaşılan bilgi ve fikir birliği kavramları, dolandırıcılık veya zimmete para geçirme nedeniyle olası kayıpları önler. Lojistik tabanlı endüstrilerde, bir izleme mekanizması olarak blok zincir maliyetleri azaltmak için hareket eder.

Güvenlik: Geleneksel bir veri tabanına saldırmak, belirli bir hedefi düşürmektir. Dağıtılmış defter teknolojisinin yardımıyla, her bir taraf (düğüm), orijinal zincirin bir kopyasını tutar, böylece sistem çalışır durumda kalır- çok sayıda düğüm düşse bile.

Şeffaflık: Herkese açık blok zincirlerinde yapılan işlemler/oluşturulan kayıtlar herkes tarafından görülebilir.

İşbirliği: Tarafların, üçüncü tarafların aracılık etmesine gerek kalmadan doğrudan birbirleriyle işlem yapmalarına olanak tanır.

Merkezi Olmayan: Her düğümün işlemleri nasıl onayladığı ve zincire eklediği konusunda standart kurallar vardır. Böylece, işlemlerin/kayıtların doğruluğunu ve geçerliğini garanti edecek üçüncü taraflara ihtiyaç yoktur.

Gizlilik: Bir blok zincirde işlem yapan kişilerin kimlikleri açık değildir. Kimlikler bir sayı dizisiyle ifade edilir, bunları gerçek kişilerle eşleştirmek zordur. Ancak blok zincir ağındaki işlemler ile İnternet üzerinde gerçekleştirilen diğer işlemlerin çeşitli analiz yöntemleri ile birleştirilip gerçek kimliklerin belirlendiği durumlar rapor edilmektedir. Diğer yandan kripto varlık alım satımı yapılan platformların işleticileri, burada işlem yapan kişilerin gerçek kimliklerine vakıftır.

1.2.6.6. Blok Zincirin Yaygın Kullanım Alanları

Blok zincirin günümüzdeki yaygın kullanım alanlarına aşağıdaki örnekler verilebilir:

- Finans: Kripto varlıklar (crypto assets), ödemeler ve havale, finansal araçların alım satım işlemleri ve sahipliğine ilişkin kayıtlar, bunlar sayesinde elde edilen hakların kaydı, izlenmesi ve işletimi, müşteri tanıma süreçleri (Know Your Customer-KYC).
- Sağlık: Veri yönetimi, dijital sağlık kayıtlarının güvenli paylaşımı, dijital sağlık cüzdanı.
- Bilim ve Sanat: NFT, süper bilgi işlem, kalabalık analizi, P2P kaynakları, dijital zihin uyumu hizmetleri.
- Nesnelerin İnterneti: Tarım ve drone sensör ağları, akıllı ev ağları, entegre akıllı şehirler, akıllı ev sensörleri, otonom araçlar, kişiselleştirilmiş robotlar, robotik bileşen, kişiselleştirilmiş drone'lar, dijital asistanlar.
- Kamu sektörü: Tapu ve arsa-arazi kayıtları, araç kayıtları, işletme lisansları, mevzuatlar, suç kayıtları, pasaportlar, doğum ve ölüm belgeleri, oy kullanım belgeleri, oylama ve oylama kayıtları, sağlık ve güvenlik denetimleri, izinler ve ruhsatlar, adli tıp ve mahkeme kayıtları.
- Yarı kamusal kayıtlar: Unvanlar, dereceler, sertifikalar, diplomalar, sağlık kayıtları, ticari kayıtlar vb.
- Özel Kayıtlar: Sözleşmeler, imzalar, emanetler, vergi makbuzları, noterlik hizmetleri ve çıktıları.
- Transferler için belgelerin/sözleşmelerin ve mülkiyet kanıtlarının dijitalleştirilmesi, kayıt ve tanımlama, tele-avukat hizmeti, IP kaydı ve değişimi, vergi makbuzları, noterlik hizmeti ve belge kaydı.
- Soyut Varlıklar: Rezervasyonlar, patentler, telif hakları, yazılım lisanları, müzik/film/kitap lisanları, domain (alan) adları, dijital kimlikler
- Marketler: Faturalandırma, izleme ve veri aktarımı, tedarik zinciri ağında kota yönetimi.

Sermaye Piyasaları Muhtemel Kullanım Alanları[22]:

- Takas: Alım satımın takasının yapılması için ilgili tüm taraflarca erişilebilir bir blok zincir uygulamasında, üçüncü taraflarca mutabakata gerek olmadan takas faaliyeti gerçekleştirilebilir.
- Finansal araçların arzı: Finansal kurumlar, amaca özel geliştirilmiş bir blok zincir uygulamasıyla yeni finansal araçları arz edebilir ve arz edilen araçların burada alım satımı yapılabilir.
- Ödeme/para transferi: Bir güven kurumuna ihtiyaç duyulmadan para transferleri eşler arasında gerçekleşebilir.
- Kimlik tanıma: Bu amaçla kurulmuş bir blok zincirde, kişilerin kimlikleri bir kez kaydedildikten sonra yetkili taraflarca sorgulanabilir, müşteri tanıma (KYC) süreçleri daha verimli işleyebilir.
- Kurumlar tarafından faiz ve temettü ödemeleri akıllı sözleşmelerce yapılabilir.
- Raporlama ve uyum: Blok zincirin en önemli özelliğinin değiştirilemezlik olması sebebiyle, buradaki veri doğrudan denetim kanıtı olarak kullanılabilir, buna ek olarak denetleyici kurumlar sisteme katılarak gerçek zamanlı denetim yapabilirler.

1.2.6.7. Blok Zincir Teknolojisinin Sınırları

Daha yüksek maliyetler: Düğümler, arz ve talep ilkesine göre çalışan bir işletmede işlemleri tamamlamak için daha yüksek ödüller arar.

Daha yavaş işlemler: Düğümler, daha yüksek ödüllü işlemlere öncelik verir, işlem birikimleri oluşur.

Daha küçük defter: Potansiyel olarak değişmezliği, fikir birliğini vb. etkileyebilecek blok zincirin tam bir kopyası mümkün değildir.

İşlem maliyetleri, ağ hızı: Bitcoin'in işlem maliyeti, ilk birkaç yıl "neredeyse ücretsiz" olarak lanse edildikten sonra oldukça yüksektir.

Hata riski: İnsan faktörü olduğu sürece her zaman hata riski vardır. Bir blok zincirinin bir veri tabanı görevi görmesi durumunda, gelen tüm verilerin yüksek kalitede olması gerekir. Ancak, insan müdahalesi hatayı hızla çözebilir.

Müsrif: Blok zincirini çalıştıran her düğüm, blok zinciri boyunca fikir birliğini sürdürmek zorundadır. Bu, çok düşük kesinti süresi sunar ve blok zincirinde depolanan verileri sonsuza kadar değiştirilemez hale getirir. Bununla birlikte, tüm bunlar israftır çünkü her düğüm bir fikir birliğine varmak için bir görevi tekrarlar.

1.2.6.8. Blok Zincir Uygulamalarında Karşılaşılabilecek Zorluklar[23]

- Farkındalık eksikliği: Blok zincirin yeni bir teknoloji uygulaması olmasından hareketle, neler yapılabileceği ve ne gibi kazanımların ihtimal dâhilinde olduğu birçok ortamda henüz tartışma aşamasındadır.
- Projenin doğru seçilememesi: Her kurumun kendi blok zincir projesini geliştirmesi mevcut sistemin sadece farklı bir sürümüdür (elbette bu durum bir tür egzersiz olarak da kabul edilebilir). Blok zincir yöntemi için uygun olan proje karakteristikleri[24] şöyle gruplanmıştır:
    - Birden çok tarafın işin içinde olması.

[22] https://www.wipro.com/capital-markets/blockchain-in-capital-markets/
[23] https://www.techtarget.com/searchcio/tip/5-challenges-with-blockchain-adoption-and-how-to-avoid-them)
https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-key-challenges.pdf
https://www.forbes.com/sites/bernardmarr/2023/04/14/the-5-biggest-problems-with-blockchain-technology-everyone-must-know-about/?sh=3984e91c55d2
[24] https://webcase.studio/does-your-project-need-blockchain/

- Tarafların birbirine güveninin olmaması.
- Merkezi kurumlara gereksinimin kaldırılmak istenmesi.
- Veri bütünlüğü noktasında yüksek güvenlik gereksinimi.

• Kurum kültürü: Merkeziyetsizliğe geçiş bir anlayış değişikliğidir ve belli bir zaman alır.

• Maliyet: Geliştirme ve bakım maliyetleri, yetkin ve yeterli iş gücüne ulaşımdaki zorluklar.

• Yasal çerçeve: Hukuki altyapının hazır olmaması, güven problemleri.

• Yatırımın geri dönüşü: Kısa sürede maliyet avantajının ortaya çıkarılamaması.

• Farklı blok zincirler arası birlikte çalışabilirlik unsurunun henüz olmaması.

• Performans: Blok zincirlerde mutabakat mekanizması sebebiyle işlem hızı (özellikle işlem sayısı arttıkça ve zincir büyüdükçe) yavaşlayabilir.

• Enerji tüketimi: Yaygın kullanılan mutabakat mekanizması işlem gücüne dayanmakta ve çok fazla elektrik tüketmektedir. Elektrik tüketimine dayalı olmayan mutabakat mekanizmaları da mevcuttur. Enerji tüketimini azaltmak amacıyla bazı girişimler bulunmaktadır.

• Siber saldırılar: Blok zincir teknolojisi değişmezlik ve bir ölçüde anonimlik sağlamakla birlikte siber saldırılara ve hırsızlığa karşı bağışık değildir.

1.2.6.9. Blok Zincir İle İlgili Güvenlik Riskleri

Herhangi bir karmaşık teknoloji gibi çoğu blok zincir sistemi de yeni güvenlik sorunlarından mustariptir. Bulut Güvenliği Derneği (CSA), blok zincir teknolojisinde birçoğu şu anda tam olarak anlaşılmamış veya belgelenmemiş olan yaklaşık 200 zayıflık ve güvenlik açığından oluşan bir taslak listeye sahiptir. Bu zayıflıkları sınıflandırmakta ve duyurmaktadır (CWE, https://cwe.mitre.org gibi).

Bir BS denetçisi, kuruluşlarda bu teknolojiyi denetlerken güvenlik risklerinin analiz edildiğinden ve risklerin yönetilmesine ilişkin ilgili kontrollerin tanımlandığından emin olmalıdır[25].

Blok zincirlerin tasarımı gereği değiştirilmeye ve tek hata noktası olarak çökmeye dayanıklı olduğu ifade edilmiş olmasına rağmen, yine de siber saldırıların tümüne karşı bağışıklıkları yoktur. Aşağıda verilen iki örnek olay durumun ciddiyetini ortaya koymaktadır[26]:

• 2016 yılında kripto para alım satım platformu olarak faaliyet gösteren ve Hong Kong'da yerleşik bulunan "Bitfinx" adlı şirketteki kullanıcıların hesabından yaklaşık 120.000 adet Bitcoin çalındığı bildirilmiştir.

• 2019 yılında Güney Kore'de yerleşik bulunan ve yine bir kripto para alım satım platformu olarak faaliyet gösteren "Bithumb" adlı şirketin 13 milyon Amerikan Doları değerinde kripto varlığının çalındığı belirtilmiştir.

Blok zincir ağlarına yapılan siber saldırılarda aşağıdaki yöntemler öne çıkmaktadır:

• Oltalama (Pishing) Saldırısı: Bir sosyal mühendislik saldırısı türü olan bu yöntemde saldırganlar, kripto varlık sahiplerine yasal/güvenilir bir kurumdan geldiği izlenimi veren e-postalar göndermekte ve kişilerin kimlik bilgileri ile kripto varlıklarını sakladıkları cüzdanların anahtar verilerini ele geçirmektedirler. Bu bilgiye sahip olduktan sonra kurbanın sahip olduğu kripto varlıklar rahatlıkla çalınabilir.

• Routing Saldırısı: Bu saldırı türü İnternet Servis Sağlayıcıları düzeyinde gerçekleştirilmektedir. Kabaca, blok zincir ağındaki bazı düğümlerin ISS üzerinden ağa katılımları belli bir süre geciktirilir, böylece ağ adeta birkaç parçaya bölünür ve bu zaman süresince erişimi engellenen düğümlerde yaratılan yeni blokların geçersiz kabul edilmesine sebep olunur. Geçersiz sayılan bloklar

[25] https://cloudsecurityalliance.org/research/working-groups/blockchain/
[26] https://www.ibm.com/topics/blockchain-security

da ilgili düğümlerin gelirini azaltacak, ayrıca blok içinde bekleyen işlemlerin de geçersiz olmasına sebebiyet verecektir.

• Sybil Saldırısı: Bu saldırı türünde bir saldırgan, bir blok zincir ağında farklı kullanıcı hesaplarıyla birden çok düğüme sahip olup gerçek düğümlerin yaptıkları işleri reddedebilir, blok yaratım sürecini baltalayabilir.

• %51 Saldırısı: Daha önce belirtildiği gibi, blok zincirdeki bloklar kronolojik olarak ve bir önceki bloğun özet değeriyle birbirine bağlıdır. Saldırganların bir bloğu değiştirebilmesi ve sistemin bu şekilde çalışmaya devam edebilmesi için, değiştirilmek istenen bloktan sonraki tüm blokların da değiştirilmesi gerekecektir. Çünkü değiştirilen bloğun özet değeri de değişir ve kendisinden sonra gelen tüm blokların geçerliliği bozulmuş olur. Bu durumda sonradan gelen her bloğun özet değeri yeniden hesaplanmalı ve tekrar zincire eklenmelidir. Bunun başarılı olabilmesi için ağdaki düğümlerin en az %51'inin ele geçirilmesi gerekir ancak bu durum çok büyük bir işlem gücü ve hassas bir zamanlama gerektirir. Çok büyük zincirlerde (örn: Bitcoin, Ethererum gibi) bu saldırının ekonomik olarak fayda sağlamayacağı ifade edilmektedir. Ancak küçük zincirlerde bu saldırının gerçekleştirilebileceği kabul edilir. Diğer yandan, özel blok zincirlerin bu saldırı türüne bağışıklığı vardır. Bu saldırı türü blok zincir ağının kendisine yapılan bir saldırıdır.

• Eclipse Saldırısı: Blok zincirin mutabakat protokolünü hedef alır. Bir veya birçok blok zincir düğümünü diğer düğümlerden habersiz hale getirmeye çalışır. Böylece mutabakat mekanizmasını bozabilir, blok zincir ağını parçalara ayırabilir, hizmette kesintiye, çift harcama saldırılarına ve kaynak israfına yol açabilir. Bu saldırı türü de blok zincir ağının kendisine yapılan bir saldırıdır

• Timejack Saldırısı: Bitcoin gibi bazı blok zincirlerinde düğümler komşu düğümlerden öğrendikleri zaman bilgisinin ortalamasını alarak saatlerini ayarlarlar. Saldırganlar, bir düğümün komşuları ile haberleşmesini aksatarak (örneğin Eclipse saldırısı ile) zaman bilgisini manipüle edebilirler. Böylece bu düğüm, ağda üretilen legal blokları zaman bilgilerinin hatalı olduğunu düşünerek kabul etmeyecektir. Daha sonra saldırgan bu düğüme gönderilecek işlemlerle çifte harcama gibi çeşitli saldırılar yapabilir.

• Race saldırısı: Burada saldırgan bir kripto varlık üzerinde bir gönderim işlemi (örn. bir satıcıya) ile bununla çelişen ikinci bir işlemi arka arkaya ağa gönderir. Eğer çeşitli mekanizmalarla ikinci işlem ilk işlemden önce onaylanırsa ilk gönderim işlemi geçersiz olur. Eğer satıcı dikkatli değilse mağdur olur (bir alıcı kendisine gönderilen varlıkların blok zincire işlenmiş olmasını kontrol etmelidir). Bu saldırı türü blok zincir altyapısını hedef almaz, ancak blok zincir işlevleri ile dolandırıcılık yapılmış olur.

• Finney saldırısı: Race saldırısına benzer, ancak burada saldırganın kendisi madencidir, mağdur aleyhine yapmış olduğu ters işlemi içeren bloğu üretir ve ilk işlemi geçersiz kılar. Burada mağdurun dikkatli davranıp kendi adına gelen gönderimin gerçekten bloğa yazılıp yazılmadığını kontrol etmemesi saldırıyı etkisiz kılacaktır.

• Diğer: Yukarıda bahsedilenler dışında cüzdanlara saldırı, kripto varlık platformlarına veya kripto varlık hizmet sağlayıcılarına saldırı, zararlı yazılımların kullanımı, akıllı sözleşmelere yapılan saldırılar, akıllı sözleşmelere dışardan veri sağlayan uygulamaları (oracle) bozmak suretiyle akıllı sözleşmelerin yanlış çalışmasına sebebiyet vermek, akıllı sözleşme kodlarının bilinçli şekilde zarar verici şekilde yazılması, akıllı sözleşmelere yönelik hizmet dışı bırakma saldırıları gibi çok çeşitli ve sayıları her gün artan saldırı türleri bulunmaktadır.

1.2.6.10. Blok Zincir Uygulamalarının Denetimi

Blok zincir görece yeni bir teknoloji/uygulama alanı olmasına rağmen özellikle borsalar yoluyla çok fazla parasal değerin değiş tokuş edildiği ve siber saldırılara da gayet açık bir alan olduğu için denetimi önemli ancak zordur. Denetimde her şeyden önce bir kapsam ve hedef belirlenmesi ve buna göre yol alınması önemlidir. Genelde denetimlerde ilk önce güvenlik akla gelmelidir ve sistemin güvenlik riskleri ortaya çıkarılmalıdır. Denetimde en azından aşağıdaki konular değerlendirilmelidir.

- Sistemin amacı, tarafları, bileşenleri, veri akışı. Sistemin tam olarak ne yaptığının anlaşılması.
- Sistemin yönetimine ilişkin üst düzey politika ve prosedürler. Sistemin tasarımının ve işletiminin doğru şekilde dokümante edilip edilmediği, kontrol değişikliklerinin kayda alınıp alınmadığı ve alınan kararlara uyulup uyulmadığının tespiti.
- Blok zincirin mimarisi ve türü (herkese açık, izinli gibi).
- Risk yönetimi.
- Erişim denetimi. Özellikle herkese açık olmayan ağlarda ağa kabul prosedürleri.
- Akıllı sözleşme denetimi. Akıllı sözleşmelerin güvenlik, doğruluk ve performans açısından incelenmesi ve değerlendirilmesi.
- Sistem ve ağ güvenliğinin denetimi.
- Mutabakat protokolleri.
- Anahtar yönetimi.
- Üçüncü tarafların güvenilirliği. Kâhin ve köprü uygulamalarının denetimi.
- Blok zincir uygulamaları ile diğer bilgi sistemlerinin iletişimi, ara yüzleri.
- Sistem geliştirme ve değişim yönetimi süreçleri.
- Kod gözden geçirme ve sızma testleri.
- Siber olaylara müdahale yönetimi.
- İş ve bilgi sistemleri sürekliliği.
- İnsan kaynakları süreçleri.

Değerlendirme Soruları

Soru 1: Aşağıdakilerden hangisi Bulut Bilişimin avantajları arasında yer almamaktadır?

A) Fiziksel sunucunun kendi fiziki kontrolünde bulunmaması

B) Geniş ağ erişimi

C) İsteğe balı self-servis

D) Hızlı esneklik

E) Ölçülü hizmet

Cevap: A

Soru 2: Blokzincirin yaygın kullanım alanlarından biri değildir?

A) Dijital para birimi

B) NFT

C) Dijital sağlık cüzdanı

D) Görüntü işleme

E) Akıllı sözleşmeler

Cevap: D

Soru 3: Yapay zekâ ve Siber Güvenlik alanında aşağıdakilerden hangisi yanlıştır?

A) Yapay zekâ algoritmaları, toplanan denetim izlerinden anlamlı sonuçları çıkartılmasını sağlamaktadır.

B) Yapay zekâ tabanlı bir DLP, bir belgeye bir hassasiyet seviyesi atayıp buna izin verilip verilmeyeceğine veya engellenip engelleneceğine karar vermektedir.

C) Yapay zekâ uygulamasının/modelinin kendisi, eğitim özniteliklerine (özellikler), eğitim için kullanılan verilerle sınırlıdır ve algoritmanın kendisine müdahale etme gibi saldırılara açıktır.

D) Siber güvenliğin amacı, kritik veri ve varlıklara yönelik saldırıları önlemek, bilgi sistemlerini daha dayanıklı hale getirmek ve herhangi bir ihlal olup olmadığını tespit etmek ve zamanında düzeltici önlem almaktır.

E) Kimlik avı saldırılarının olasılığını azaltmak için URL engelleme listelerine dayanmaktadır.

Cevap: E

Soru 4: Robotik Süreç Otomasyonunun kullanım alanlarındandır?

A) İşten çıkan kullanıcı hesaplarının kurum bilgi sistemlerinden silinmesi

B) Vergi beyannamesi oluşturulması,

C) Sipariş bilgilerinin e-postayla yüzlerce bayiye gönderilmesi,

D) İç kontrol ortamlarının otomatize edilmesi

E) Hepsi

Cevap: E

Soru 5: Aşağıdakilerden hangisi Blokzincir teknolojisinin sınırlarına/dezavantajlarına örnek verilemez?

A) İşlem maliyetleri

B) Merkeziyetsiz olması

C) Daha yavaş işlemler

D) Hata riski

E) Daha yüksek maliyetler

Cevap: B

2. BİLGİ SİSTEMLERİ OPERASYONLARI

Gartner bilgi sistemleri operasyonlarını; müşterilere/kullanıcılara doğru hizmeti, doğru kalitede ve rekabetçi bir bütçeyle sunmak için BS hizmet yönetimiyle ilgili çalışanlar ve yönetim süreçlerinin bütünü olarak ifade etmektedir. BS operasyon pratiklerinin amacı; kurumun iç ve dış kullanıcılarının bilgi teknolojisi konusunda desteklenmesi ve kurumda bilgi teknolojisine dayalı çözümlerin/süreçlerin başarılı bir şekilde işletimi ve sürdürülmesidir.

Operasyon yönetimi, bir kurumun tüm bilgi teknolojisi altyapısının yönetimidir. Diğer bir ifadeyle operasyon yönetimi aslında hizmetlerin teknik gerçekleştirimidir. Hizmet yönetiminden daha geniş bir perspektifi vardır.

BS birimlerinde kullanıcıya sunulan her bir hizmetin arkasında işleyen çok fazla süreç, mekanizma bulunmaktadır. Yani bir anlamda sunulan hizmetler buzdağının görünen kısmıdır. BS birimi, kullanıcılara görünenden çok daha fazlasıdır. Operasyon Yönetimi kurumun tüm BS altyapısının düzgün bir şekilde, sorunsuz çalışmasını sağlayan tüm iş ve işlemlerin tasarlanması, işletilmesi ve gözlenmesidir. Aslında operasyon yönetimi bir bakıma görünmezdir-işler yolunda gittiği sürece…

Hizmet ise, bir kurumun iç ve dış personelinin/kullanıcılarının/müşterilerinin/iş ortaklarının, kendi iş hedeflerini gerçekleştirirken kullandıkları her tür araç, program, mekanizmadır. Bilgi teknolojisi hizmetleri bir kurumda günlük çarkların dönmesini ve stratejik hedeflere ulaşılmasını sağlayan hizmetlerdir. Hizmet sunumunda aksama doğal olarak iş akışlarının aksamasına, durmasına, gecikmesine sebep olur. Bu yüzden hizmetlerin "yönetilmesi" gerekir. Önemli bir diğer bir husus da hizmetlerin tek seferlik olmadığıdır. Hizmetlerin tasarımı ve sunumunda bu hususlar akılda tutulmalıdır.

2.1. Hizmet Yönetimi

Hizmet Yönetimi, bilgi sistemleri hizmetlerinin; çalışanlar, müşteriler ya da çözüm ortakları tarafından belirtilen ihtiyaçları ve işletmenin iş hedeflerini karşılayacak şekilde uygulanması, sağlanması, yönetilmesiyle ilgili süreçler ve bu süreçlere bağlı uygulamalar bütünüdür. Sunulan hizmetlerin çalışan/müşteri algısına göre sürekli iyileştirilmesini sağlamak amacıyla kullanılır.

Hizmet Yönetimi ile hizmet kalitesinin arttırılması ve sürekli iyileştirilmesi, bilgi sistemleri yeteneklerinin net olarak görülebilmesi, mevcut yapıların/hizmetlerin farkında olunması, kullanıcı memnuniyetinin sağlanması, kaynakların etkin yönetilmesi, problem ya da olayların gözden geçirilmesi ve geçmiş deneyimlerden ders çıkarılması amaçlanır. BS operasyon faaliyetlerinin odağında doğru hizmeti, istenen kalitede ve bütçe sınırları dâhilinde, verimli bir biçimde sunmak yer alır. Hizmet sunumun genellikle aşağıdaki özellikleri taşıması beklenir:

- Süreklilik: Hizmetlerin istenen kalitede ve sürekli sağlanması gerekir. Bu konuda sürprizlere yer olmamalıdır.

- Çeviklik: Yeni ihtiyaç duyulan hizmetlerin hızlıca geliştirilmesi, aksi durumda kurum rekabet edemez hale gelebilir.

- Kapasite: Hizmetin kabul edilebilir ölçüm değerleri içerisinde sunulmasıdır. Bu noktada hem mevcut teknoloji, hem maliyet unsurları hem de hizmetin kullanıcılarının beklentileri işin içine girer.

- Maliyet: Hizmetin sürdürülebilmesi ya da işletmeye faydasının dokunabilmesi hususu bütçe sınırlamasına uyulduğu sürece geçerlidir.

- İyileştirme: Teknolojinin, ekonominin, iş gereksinimlerinin sabit olmadığı bir dünyada, hizmetlerin değişmez biçimde sunulması beklenemez. Elbette bir iyileştirme yapabilmek için önce ölçüm yapılması gerekir ki bu konuda ölçümü yapılacak hususlar hizmetin temel kriterleridir (hizmet seviyesi). Ölçümden önce de bu kriterlerin belirlenmesi gerekecektir.

Hizmet yönetimi daha çok müşteri/kullanıcı odaklıdır. Hizmet yönetimi genelleyici bir ifadedir, belli bir standardı ya da yönetim çerçevesini işaret etmez. BS birimi bulunan her kurumda bir şekilde hizmet yönetimi yapılıyordur ancak kalitesi düşük olabilir. Hizmet yönetiminde genellikle müşteriye/kullanıcıya dönük hizmetler kastedilir. Ayrıca hizmet yönetimi sadece donanımsal tabanlı işler/hizmetler olarak düşünülmemelidir, kullanıcılara/müşterilere sunulan her türlü yazılım, uygulama da birer hizmettir-bir işe yarıyordur, öyleyse uygun şekilde yönetilmelidir. Burada yazılımın kullanıcının karşısına gelmeden önceki geliştirme aşamaları hizmet yönetiminin dışında düşünülebilir.

Hizmet ve operasyon yönetiminde genel kabul görmüş en iyi uygulama örneklerine uyulabileceği gibi belli bir standardın/çerçevenin izlenmesi de faydalı olabilir. Bu konuda en kabul görmüş çerçevelerden biri ITIL olup 1020 numaralı "*Bilgi Sistemleri Yönetimi ve Denetimi"* adlı çalışma notunda detaylı bir şekilde anlatılmıştır.

Burada hizmet yönetimi konusunda çok popüler bir yönetim çerçevesi olan ITIL tarafından geliştirilen iki kavramdan bahsetmek uygun olacaktır:

- **Hizmet kataloğu (service catalog):** Bir işletmede kullanıcılara/müşterilere sunulan bilgi teknolojisi hizmetlerinin envanteridir. Her işletmede BS birimi birtakım hizmetler sunar ancak bunun bir envanter şeklinde somutlaştırılması hizmet yönetimi felsefesine geçişin bir sonucudur diyebiliriz. Bu şekilde hem BS biriminin işletmedeki rolü ve iş tarafı için yaptıkları daha görünür hale gelir, hem de BS biriminin sunduğu hizmetleri daha iyi yönetmesi mümkün olur. Hizmet kataloğunun en önemli özelliği, sadece cari durumda sunulan hizmetleri içermesidir. Hizmet kataloğunun kategorizasyonu aynı zamanda hizmet masası pratiklerini de kolaylaştırıcı bir unsurdur.

- **Hizmet portföyü:** BS birimi tarafından cari durumda sunulan, geçmişte sunulmuş ancak artık sunulmayan (üretim ortamında olmayan) ve gelecekte sunulması planlanan (geliştirme sürecinde olan) tüm hizmetlerin kataloğudur. Bir anlamda BS biriminin yaptıkları ve yapacaklarının bir envanteri gibi düşünebiliriz.

Etkin ve verimli bir hizmet sunumu/yönetimi yapmak isteyen işletmelerin hizmet kataloğunu oluşturması elzemdir. Ancak hizmet portföyünün oluşturulması bu anlamda bir zorunluluk taşımasa da hizmet sunumu pratiklerini iyileştirmek isteyen ve hizmet sunumu konusunda belli bir olgunluğa gelmiş işletmeler için gereklidir.

Hizmet portföyü, bir anlamda kurumsal hafızaya da hizmet eder. Bunun yanında gelecekte sunulması planlanan hizmetlerin görünür olması kullanıcılara bir perspektif sunar, kullanıcıların bu hizmetlere ilişkin ilgisini canlı tutar, bunlar hakkında etkileşimi artırır.

- **Hizmet kategorileri:** Hizmet kataloğunda kategorizasyona gidilmesi hem kullanıcı hem de BS birimleri tarafı için işleri kolaylaştırır. Genelde kategoriler (işletmeden işletmeye değişmekle beraber)- kabaca şu şekilde listelenebilir:
    - Yazılım (gerek kurum için geliştirilen özellikli iş uygulamaları, gerekse de ofis yazılımları)
    - Donanım (yazıcı, bilgisayar, telefon…)
    - E-posta
    - İnternet
    - Yedekleme/Kurtarma

Bu veya benzer şekilde bir kategorizasyon işletmedeki yardım masası işlevinin etkinliğini ve verimliliğini artırır. Hangi alanlarda problemlerin yoğunlaştığı, hata ve taleplerin çözüm süresi gibi unsurlar ölçülebilir.

Hizmet kataloğu ve kategoriler oluştururken, hizmetin işletmenin kendi kaynaklarıyla mı yoksa dış kaynak kullanımı yoluyla mı gerçekleştirildiğinin önemi yoktur-tüm hizmetler burada yer almalıdır. Ancak bu bilginin de bir şekilde katalogda muhafaza edilmesi gerekir.

Hizmet yönetiminde önemli bir husus da şudur: Hizmet seviyesini BS değil, iş tarafı belirler. Ancak elbetteki bu belirleme de bir rasyonalite içermelidir: hizmet seviyeleri iş hedefleri doğrultusunda belirlenir ki buradan yine işletmenin stratejisi ve iş hedeflerine geliyoruz.

2.1.1. Hizmet Masası

Hizmet Masası; tüm olayları, sorunları ve istekleri yönetirken tek iletişim noktası (single point of contact-SPOC) görevi görür. Problem raporlarının oluşturulmasını, olayların zamanında çözülmesini ve ilgililerine uyarı gönderilmesini, ilerlemelerin takip edilmesini ve aynı zamanda problemlerin kaynağının belirlenmesini ve uygun düzeltici faaliyetler ile önlemler alınmasını sağlar.

Hem acil sorunu çözmekle hem de daha geniş bağlamda kullanıcıların ihtiyaçlarının tam olarak karşılandığından emin olmak için sunulan hizmetlerin kalitesini ve performansını geliştirmekten sorumludur.

Hizmet masası sistemi, olaylara en uygun hizmet seviyesi anlaşmaları uygulamasında ve son kullanıcılarla öncelikler hakkında iletişim kurmaya da yardımcı olur. Olay yönetimi işlemi ilgili otomasyonlarla etkinleştirildiğinde hizmet masası ekibinin hizmet seviyesi anlaşmalarının uyumluluğunu kontrol etmesini sağlar ve bir hizmet seviyesi anlaşması ihlali ihtimali ortaya çıktığında ilgili ekiplere bildirimler göndererek ihlallerin önüne geçilmesini sağlar.

BS birimlerinde kronolojik olarak ilk önce yardım masası (help desk) birimleri ortaya çıkmış, ITIL tarafından BS hizmetleri kavramı dolaşıma sunulunca da hizmet masası kavramı öne çıkmıştır. Günümüzde yardım masasını, hizmet masasının alt kümesi olarak, "olay yönetimi" süreci altında düşünebiliriz. Yardım masası, hizmet yönetimi yaklaşımının olgunlaşmadığı, küçük ölçekli kurumlarda daha yaygındır. Özellikle nispeten küçük işletmelerde kullanıcılara destek verilirken pratikte en çok karşılaşılan iki problem şudur:

- Kullanıcıların, sorunların çözümü için genelde BS personeliyle doğrudan kişisel temasa geçmesi, hiçbir şekilde belli bir telefon hattı, e-posta hesabı veya uygulama kullanmaya ikna edilememesi,
- Hizmet masasında (veya küçük işletmelerde yardım masasında) görevli personelin yapılan işlemleri kayıt altına almaya ikna edilememesi.

Bu iki sorun aşağıdaki problemlere sebep olur:

- Ne kadar sorun çıktığının belirlenememesi
- Sorunların kategorizasyonunun yapılamaması
- Hangi donanımın, yazılımın, uygulamanın ne kadar sorun çıkardığı ve sorunların kök sebebinin belirlenememesi
- Sorunların önceliklendirilememesi
- Sorunların çözümü için gereken süre ve maliyet
- BS biriminde kimin, hangi sorun üzerinde ne kadar zaman harcadığı
- Eğitim ihtiyacı (hem iş, hem de BS tarafında, özellikle sık karşılaşılan sorunlar hakkında)
- Geliştirilen çözümler hakkında bir bilgi havuzu oluşamaması, benzer sorunların farklı şekillerde çözülmesi ya da çözümlerin birbiriyle çatışması (özellikle uygulama bazlı sorunlarda). Kişiye özel çözümlerin oluşturulması (hem iş tarafı, hem de BS tarafında).
- Kurumsal hafızanın oluşamaması.

2.1.1.1. Hizmet Masası Araçları

Olayların zamanında çözülmesi, problem raporlarının başlatılması, ağ, sistem ve uygulamalar ile ilgili bilgi sahibi olmak, teknik destek sağlamak gibi görevlerin yönetilmesini sağlayan araçlardır.

• Yanıt Süresi Raporları: Kullanıcı tarafından girilen komutların ana sistem tarafından cevaplanması için geçen süreyi tanımlar. Cevap süresi uzun ise, CPU kapasitesi, bant genişliği kullanımı gibi olası nedenler araştırılmalıdır. Çözümler analiz edilerek önlem ve iyileştirmeler yapılmalıdır.

• Kesinti Raporları: Haberleşme hatlarının ve sistemlerinin kullanılabilirliğinin takip edilmesi için kullanılır. Güç arızaları, aşırı trafik yükü, operatör hataları, diğer anormal durumlardan dolayı yaşanan kesintilerin raporu tutulur. Kesinti süresi çok fazlaysa BS yönetimi tarafından haberleşme hatlarında değişiklik, yedek güç kaynağı, erişim kontrollerinde iyileştirme, güvenilir bir iletişim bağlantısı gibi çözümler alınabilir.

• Yardım Masası Raporları: BS kullanımı sırasında meydana gelen sorunların çözümü için yetkili uzmanlar tarafından hazırlanır. Rapor içerisinde problemlerin ve çözümlerinin tarihçesi yer alır.

• Çevrimiçi Monitörler: Veri iletimlerini ve oluşan hataları kontrol eder. Ağ monitörleri bilgilerin gerçek zamanlı görüntülenmesini sağlar.

• Ağ analizörleri: Kullanılan protokoller, trafik hacmi analizi, donanım hataları, yazılım sorunları, problemler ve çözümlerinin yer aldığı araçlardır.

• Basit Ağ Yönetimi Protokolü (SNMP): Ağdaki değişkenleri inceler, yapılandırmaları yönetir, performans ve güvenlik unsurları hakkında bilgi toplar.

2.1.2. Talep Yönetimi

Şirket ihtiyaçlarının belirlenmesi için iş birimleri ile çalışma yapılır. Yapılan çalışmalar ile kullanıcıların beklentilerine göre ihtiyaçların neler olduğunu belirlemek ve belirlenen konularda verilecek hizmetlere ait maliyet, kalite ve kapasite planlarının yapılması amaçlanmaktadır. Yeni hizmet talebi gibi konular talep yönetimi içerisinde değerlendirilmelidir.

Talep yönetimi, iç ya da dış müşteriden gelen isteğin, talep ya da proje olarak değerlendirilmesine olanak sağlar. Bu ayrım sayesinde, isteklerin niteliklerine göre değerlendirilmesi ve önceliklendirmesi yapılır. Eğer talep kategorisinde ise, hizmet masası üzerinden önceden tanımlanmış süreçlere göre yönetilir ve izlenir. Proje kategorisinde yer alacaksa, proje yönetim süreçleri çerçevesinde takip edilir.

Değerlendirmeye alınan tüm talep ve projeler ilgili birimlere aktarılır. Yapılan ve planlanan işlemler düzenli olarak kontrol edilmeli ve raporlanmalıdır. Aksayan durumlara müdahale edilmelidir. Tamamlanan talepler de gözden geçirilmeli, rapora eklenmeli ve performans değerlendirmeleri yapılmalıdır. Değerlendirme kriterleri içerisine, müşteri memnuniyeti (birimler ya da müşteriler), zamana uyum, maliyet ve kalite gibi faktörler eklenebilir.

2.1.3. Olay Yönetimi

Olay yönetimi, BS hizmet yönetiminin alanlarından biridir. Olay yönetimi sürecinin ilk amacı, hizmet kesintilerini en aza indirmek, mümkünse engellemek, en kısa sürede normal bir hizmet operasyonunu geri yüklemek ve üzerinde anlaşılmış hizmet seviyesi sözleşmeleri (Servis Level Agreement-SLA) içinde hizmetlerin sürekliliğini sağlamaktır. Arıza, hata, sorun, çalışmama gibi kavramlar olay olarak tanımlanabilir.

Olay yönetimi yaşam döngüsü, son kullanıcının bir sorun bildirmesiyle başlar ve bir hizmet masası çalışanının o sorunu çözmesiyle sonuçlanır. Olay yönetimi yaşam döngüsünün diğer adımları olayın kategorileştirilmesi, önceliklendirilmesi ve ilgililerinin atanmasıdır. Aciliyet ve etkiye göre olayların önceliğini belirleyebilmek için parametreler belirlenir. Parametrelere göre bir olay kategorize edildiğinde ve önceliklendirildiğinde ilgililer olayı tanımlar. Sorunu tanımladıktan sonra ilgili, son kullanıcıya son kullanıcının doğrulayabileceği bir çözüm sunar.

Olay yönetimi süreci otomasyonlarla etkinleştirildiğinde hizmet masası ekibinin SLA uyumluluğunu kontrol etmesini sağlar ve bir SLA ihlali yaklaştığında uzman teknik destek gruplarına bildirimler gönderir; bildirimleri alan ilgililer de olay için geçerli otomatik iletimleri yapılandırarak SLA ihlallerini iletme seçeneğine sahiptir.

2.1.3.1. Olay Çözümünün Beş Adımı

Olay yönetimi çözüm süreci beş standart adımdan oluşur. Bu adımlar, bir olayın çözümü sırasında her durumun değerlendirilmesini sağlar ve ekiplerin olaylara etkili bir şekilde yanıt vermesine yardımcı olur. Bu beş adım ile gelen olayların sıralanması, aynı zamanda sorunla ilgili en uygun ekiplere yönlendirilmesi sağlanır. Olay kategorizasyonu, hizmet masası sistemine olaylara en uygun hizmet seviyesini uygulamasında ve son kullanıcılarla belirlenen öncelikler hakkında iletişim kurmaya da yardımcı olur. Bir olay kategorize edildiğinde ve önceliklendirildiğinde uzman ekipler olayı tanılayabilir ve son kullanıcıya bir çözüm sağlayabilir.

1) Olay Tanımlama, İz (log) Kaydı ve Sınıflandırma

Olaylar; kullanıcı raporları, çözüm analizleri veya manuel tanımlama yoluyla kayıt altına alınır. Kayıt altına alınan olaylar için araştırma ve sınıflandırma yapılır. Sınıflandırma, olayların nasıl ele alınması gerektiğini belirlemek ve müdahale kaynaklarına öncelik vermek için önemlidir. Kayıt içerisinde; tarih/saat, açıklama, olayı kaydeden ile ilgili bilgi ve detaylı açıklama, olaya atanan ekip, mevcut durum ve alınan karar/onay gibi detaylar yer alır.

2) Olay Bildirimi ve Eskalasyon

Olay ile ilgili uyarılar gerçekleştirilir, olaylar küçükse ayrıntılar loga kaydedilebilir veya resmi bir uyarı olmadan bildirimler gönderilebilir. Sorun iletme, bir olaya atanan kişi ve müdahale prosedürlerinden kimin sorumlu olduğuna bağlıdır.

3) Araştırma ve Teşhis

Olayla ilgili görevler atandıktan sonra olayın türü, nedeni ve olası çözümleri araştırılır. Olay teşhis edildikten sonra, uygun düzeltme adımları belirlenir. Gerekli ise yedekten geri dönüş gibi süreçler kontrol edilir ve uygulamaya hazır hale getirilir. Eğer olay büyükse ya da çözülemezse bir üst merciye taşınması (eskalasyon) sağlanır.

4) Çözüm ve Kurtarma

Çözüm ve kurtarma, sorunların temel nedenlerinin ortadan kaldırılmasını ve sistemlerin tam çalışır halde geri yüklenmesini içerir.

5) Olay Kapatma

Olayların kapatılması ve müdahale sırasında yapılan işlemlerin değerlendirilmesini içerir. Bu değerlendirme gelecekteki olayları önlemeye ve iyileştirme alanlarının belirlenmesine yardımcı olur.

Olay kapatma adımı, ekiplere, yönetime veya kullanıcılara olay ve çözümü ile ilgili rapor veya geçmişe dönük bilgi sağlamayı da içerir. Aynı zamanda tüm işlemlerin kayıt altına alınarak kurumsal hafıza oluşturulmasına destek olunur.

2.1.3.2. Olay Yönetiminde Roller ve Sorumluluklar

1) Son kullanıcı/kullanıcı/talep eden

Genellikle hizmette bir sorundan bahseden paydaştır ve olay yönetimi işlemini başlatmak için bir olay kaydı oluşturur.

- Yeni bir olay isteği oluşturmak için hizmet masasına başvurur.
- Var olan bir isteği izler.
- Gerekli tüm bilgileri uzman ekibe net bir şekilde iletir.
- Hizmetin geri geldiğini ve olayın tamamlandığını paylaşır.
- Olay çözümünden sonra geri besleme döngüsünü tamamlamak için anketleri yanıtlar.

2) Katman 1 Hizmet Masası

Talep veya olay kaydı oluşturmak için ilk başvuru noktasıdır. Katman 1 hizmet masası genellikle parola sıfırlamaları, Wi-Fi sorunları gibi bir BS ortamında oluşabilecek en genel sorunlarla ilgilidir.

- Kategori, aciliyet ve öncelik gibi parametrelerle gelen tüm olay isteklerini geliş zamanına göre kaydeder.
- Uzman ekibe kayıtları verir.
- Hizmeti geri yüklemek için olayı analiz eder ve çözülmemiş olayları Katman 2 hizmet masasına iletir.
- Talep edenlerden gerekli tüm bilgileri toplar ve onlara düzenli olarak isteklerinin durumu hakkında güncellemeler gönderir.
- Talep edenler için başvuru noktası görevi görür ve gerekirse Katman 2 hizmet masası ve talep edenler arasında koordinasyonu sağlar.
- Çözümü son kullanıcıyla doğrular ve geri bildirim toplar.

3) Katman 2 Hizmet Masası

Hizmet masası olay yönetimi ile ilgili ileri bilgiye sahip uzman ekipten oluşur. Genellikle daha karmaşık olayların çözümünde görev alırlar.

- Olay tanımlarını yapar.
- Olayı çözmek için izlenen adımları belgeler ve bilgi tabanına ekleme yapar.
- Bir olay, bir sorun olduğunda tanımlar ve olay kaydını sorun kaydına dönüştürür.
- Olay çözülürse çözümü son kullanıcıyla onaylar.
- Olay çözülmezse Katman 3 hizmet masasına iletir.
- Olay çözülmezse, altında yatan sorunu veya varsa dış tedarikçileri tanımlamaları için olayı BS sorun yönetimi ekibine iletir.
- Konuyla ilgili uzmanlık sağlar.

4) Katman 3 (ve üstü) Hizmet Masası

Genellikle BS altyapısında belirli etki alanlarında ileri bilgiye sahip çalışanlardan oluşur. Örneğin, donanım bakımı ve çok kritik alanlarda sunucu destek uzmanlığı.

5) Olay Yöneticisi

İşlemin etkilerini izleyerek iyileştirmeler öneren ve diğer sorumluluklarla birlikte işlemin izlenmesini sağlayan roldür.

- Tüm büyük olaylar için başvuru noktası görevi görür.
- Olay yönetimi sürecindeki tüm etkinlikleri planlar.
- Tüm kayıtlar için doğru adımların izlenmesini sağlar ve sapmaları düzeltir.
- Çalışmaları koordine eder ve olay sorumlusu ile iletişim kurar.
- Hizmet seviyesi anlaşmalarının uyumluluğunu sağlar.
- İncelenmesi gereken olayları tanımlar ve inceleme işlemi yapar.

6) Olay Sorumlusu

Kuruluşun yararına en iyi şekilde hizmet etmesini sağlamak için işlemi analiz eder, değiştirir ve iyileştirir.

- Olay yönetiminin tüm işlemleri için sorumluluğa sahiptir.
- Anahtar performans göstergelerini (key performance indicators-KPI) tanımlar ve bunları kritik başarı etmenlerine (critical success factors-CSF) uyarlar.
- Anahtar performans göstergelerini inceler ve işletmenin hedeflerini ve kritik başarı etmenlerini karşılamasını sağlar.
- İşlemleri tasarlar, belgeler, inceler ve iyileştirir.
- İlkeler, roller, teknoloji ve olay yönetimi işleminin incelenmesi ve iyileştirilmesi konusunda diğer açılardan sürekli hizmet iyileştirmesi (continual service improvement-CSI) yapar ve dokümante eder.
- Endüstrinin en iyi uygulamaları hakkında bilgi sahibi olur, sürekli araştırır ve bunları olay yönetim işlemine uygular.

Olay yönetimi ile:

- Rapor edilen tüm BS olayları merkezi bir veri tabanına/sisteme kaydedilir.
- BS olayları; öncelik, aciliyet, etki ve kaynaklanan birim gibi parametrelere göre otomatik olarak kategorize edilebilir ve sınıflandırılabilir.
- Uygun hizmet seviyesi anlaşmalarının olay kayıtlarıyla ilişkilendirilmesine olanak sağlanır.
- Kayıtların inceleme için uzman ekiplere veya destek gruplarına atanması sağlanır.
- Olayların çözümleri ve geçici çözümleri tanımlanır.
- Daha sonra başvurmak için çözümler bilgi tabanına kaydedilir.
- Olayların etkin bir şekilde ele alınması için kavrayış ve analiz sağlayan yaratıcı canlı panolar ve yardım masası verilerinden oluşturulan raporlar sağlanır.

Anormal Koşulların Tespiti (Güvenlik olayları dışında)

Yazılımın, donanımın ve birbiriyle olan ilişkilerinin karışık yapısı nedeniyle anormal durumların tespit edilmesi, tespit edilen anormal durumlara ait manuel veya otomatik belgelerin oluşturulması gerekir.

Kayıt altına alınabilecek hata türleri; uygulama hataları, donanım hataları, operatör hataları, sistem hataları, haberleşme ve ağ hataları olabilir. Hata türleri ile hata tarihi, hata açıklaması, hata kodu, hata çözümü açıklaması, kaynağı, eskalasyon tarihi ve saati, kayıtları saklayan personele ait isim, kaydı kapatan kişiye ait isim, hata çözümlemesinden sorumlu bölüm, probleme ait çözümün durumu, çözüme ilişkin detaylı bilgi içermelidir.

Oluşturulan kayıtlarda değişiklik yapma hakkı kısıtlanmalı ve tüm güncellemeler izlenebilir olmalıdır. Görevler ayrılığı ilkesince, hata kaydını açan personel ile kaydı kapatan ya da koruyan kişi birbirinden farklı olmalıdır.

Olay ve problem yönetiminin uygun şekilde sürdürülmesinin, izlenmesinin ve hataların zamanında ele alınmasının takibi sağlanmalıdır. Çözülmemiş problemlerin daha üst seviye bir BS yönetimine eskale edilmesi ve buna yönelik prosedürlerin oluşturulması, güncellemesi sağlanmalıdır. Süresiz olarak çözümsüz kalan problemler kabul edilebilir değildir ve böyle bir durumunun en büyük riski iş operasyonlarının kesintiye uğramasına neden olmasıdır. Bu nedenle problem eskalasyon prosedürlerinin iyi belirlenmesi ve uygulanması önemlidir. Bu prosedürlerin içeriğinde; hangi tip

problemlerle hangi personeller ilgilenmekte ve iletişim bilgileri, acil çözüm gerektiren problem türleri, normal çalışma saatlerine kadar bekleyebilecek problem türleri gibi bilgiler olmalıdır.

Problemler, zamanında ve etkin çözülmesini sağlamak için uygun kişi/kişilere iletilmelidir.

BS Denetçisinin, problemlerin zamanında çözüldüğünü ve problemi çözüme ulaştıran kişinin doğru ve yetkin olduğunu kontrol etmesi gerekir. Bunun için problem kayıtları ile ilgili her türlü belge ve bilgiyi incelemelidir.

2.1.4. Problem Yönetimi

Bir BS hizmetindeki olayların nedenlerinin belirlenmesi, benzer olan birkaç olayın derinlemesine analizinin yapılarak araştırılması ve çözülmesi sürecidir. Problem yönetimi, olayların tekrarlanmasını önlemeye veya gerçekleşecek olayların işletmeye olan etkisini en aza indirmeye çalışır.

Aynı sorunlu olayın birden çok defa tekrarlanması ya da birçok kullanıcının işini etkileyen olaylar problem tanımı içerisinde yer alabilir.

Problem yönetimi, bir olayın altında yatan nedenleri belirleyip anlamak ve bu temel nedeni ortadan kaldırmak için en iyi yöntemi belirler. Nedenleri belirlemek için; balık kılçığı/Ishikawa sebep-sonuç diyagramları ve yinelemeli soru tekniği olan 5 Neden kullanılabilir.

Kök nedenleri ve geçici çözümleri saptanmış problemler Bilinen Arıza (Known Error) olarak tanımlanır.

Bu süreç içinde bulunan geçici çözümler gerçek problemle ilişkilendirilir ve sorunun kaynağı, çıkabilecek hatalar daha net görülür. Ortaya çıkan hatanın yol açtığı problemleri, kalıcı bir çözüm bulununcaya kadar gidermek veya hafifletmek üzere, önceden tanımlanmış önlemler Geçici Çözüm (Work around) olarak uygulanabilir. Servislerde ortaya çıkan hatalar ve Bilinen Arıza'lar, ilgili ekiplerin erişimine açık olarak problem veri tabanında kayıt altına alınır.

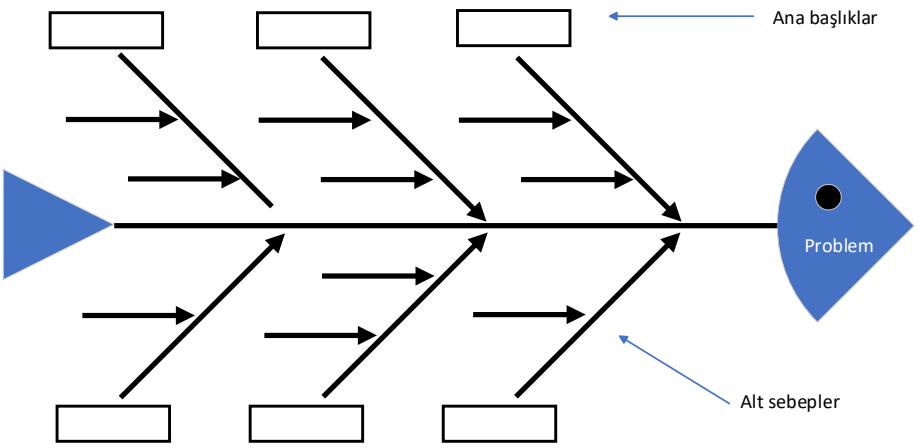
Böylece daha sonra karşılaşılacak problemlere müdahale ve çözüm süreci hızlanır. Problem Yönetimi, Olay Yönetiminden tamamen farklıdır. Problem Yönetimi prensip olarak, kökte yatan sorunların tespitini ve ortadan kaldırılmasını hedeflerken Olay Yönetimi, mümkün olan en az iş kaybı ile sistemi mümkün olduğu kadar kısa bir sürede normal çalışma düzenine getirmeyi hedefler. Aradaki fark şu şekilde de açıklanabilir: Olay yönetimi gerçek zamanlı bir aktivitedir ve gerçekleşen olayın etkisini azaltmaya ve etkilenen hizmetleri en kısa zamanda eski haline geri döndürmeye odaklanır. Problem yönetimi ise, gerçek zamanlı bir aktivite değildir. Olaylara sebep olabilecek veya olmuş olan kök sebeplerle ilgilenir, bunları kalıcı olarak çözmeye veya bir daha ortaya çıkmasını engellemeye odaklanır. Problemler önceden yakalanabilir veya olaylar önlenebilir. Bu zaten problem yönetiminin asıl amacı olup bu kapsamda BS gözetim ve gözden geçirme aktiviteleri çok değerlidir.

Problem Yönetimi sürecinde, vakaların sayısını ve önem derecesini azaltmayı hedefleyen çalışmalar ile 1. seviye ve 2. seviye destek ekiplerinin ulaşıp kullanabilmesi için rapor ve dokümantasyon hazırlanması sağlanır. Proaktif bir problem yönetimi süreci, problemleri daha sorunlar oluşmadan çözmeyi hedefleyen aktivitelerde bulunur.

Problem yönetim sürecinin girdileri; Olay Yönetiminden gelen olay ayrıntıları ya da tanımlı çözüm çalışması, Konfigürasyon Yönetimi Veri tabanından gelen konfigürasyon ayrıntıları olabilir.

Balık Kılçığı (Ishikawa) Diyagramı

Sebep-Sonuç analizi olarak da adlandırılmaktadır. Bir etki veya problemin birçok olası sebebini bulmak için kullanılır. Problemin kaynağını belirlemek için belirlenen ana başlıklar omurgadan oklar çıkarılarak yazılır. Alt sebepler de ana ok çevresinde alt dallara ayrılarak not alınır. Görsellik sayesinde problemi oluşturan olası nedenlerin toplu olarak görülüp problem kaynağının daha hızlı bulunmasına yardımcı olur.



5 Neden Analizi

5 kez "neden" sorusunu sorarak problemlerin nedenlerini geriye dönük inceleyen, problemin temel sebeplerini anlamak için kullanılan yöntemdir. Bu yöntem balık kılçığı diyagramı (sebep-sonuç) ile yakından ilişkilidir. Problemin farklı nedenleri arasındaki bağlantının fark edilmesini ve temel nedenlerinin bulunmasını sağlar.

2.1.4.1. Problem Yönetimi Raporlarının İncelenmesi

Problem yönetimi raporları incelenirken denetim yaklaşımı ile yapılmalıdır. Bu kapsamda;

1. BS operasyon personeli ile görüşülmelidir. Bu görüşme esnasında, operasyonun amacına ve yetkisine uygun olarak BS operasyon personelinin problemleri zamanında kayıt altına alıp almadığı, analizlerinin yeterliliği, çözüm ve dokümante edilmiş prosedürlerin durumu kontrol edilmelidir.

2. BS birimi tarafından kullanılan prosedürler ve operasyon belgeleri kontrol edilmelidir. Bu kontroller esnasında herhangi bir sorunu işlemek, kayıt altına almak, değerlendirmek, çözmek ya da eskale etmek için kullanılan prosedürlerin uygunluğu, çevrimiçi işlem performansları ile ilgili kayıtların nasıl toplanacağı ve tutulacağı ile ilgili dokümante edilen verilerin ve analizlerin yeterliliği sorgulanmalıdır.

3. Performans kayıtları, bekleyen hata günlük kayıtları, yardım masası çağrı günlükleri incelenmelidir. Bu incelemelerde; işleme sırasında sorun meydana gelmiş mi, gecikme yaşanmış mı, eğer yaşandıysa nedenleri kayıt altına alınmış mı, önemli ve tekrar eden olayların kök nedenlerinin incelenmesi sağlanmış mı ve önlemler yeterli mi, sorunlara zamanında müdahale edilmiş mi ve BS yönetimine rapor edilmeyen tekrarlanan sorunlar var mı gibi detaylara bakılmalıdır.

2.1.5. Değişiklik, Sürüm ve Yama Yönetimi

2.1.5.1. Değişiklik Yönetimi

ITIL'a göre değişiklik yönetimi, standart veya sistematik şekilde bir kuruluşun BS altyapısını değiştirme işlemidir.

Değişiklik yönetimi, hizmetler üzerinde doğrudan ya da dolaylı etki yaratabilecek herhangi bir şeyin eklenmesi, değiştirilmesi veya kaldırılması sırasında başlangıçtan kapanışa kadar riskleri en aza indirme hedefiyle takip etme, yönetme ve hızlıca hayata geçirme sürecidir. Donanım değiştirilirken, mevcut uygulamalarda yeni sürüm yüklerken veya yükseltirken, yazılım yaması kurarken ve ağ aygıtları yapılandırılırken kullanılır.

Değişiklik Yönetimi, gerçekleşen değişimin en hızlı ve sorunsuz bir şekilde gerçekleşmesini ve hayata geçmesi süreçlerini içermektedir. Değişimler; uygulama değişiklikleri, sistem geçişi, yeni donanım değişiklikleri ve benzeri durumlar olabilir.

BS birimlerinde değişim gereksinimleri farklı kaynaklardan ileri gelebilir: en basitinden hataları/aksaklıkları düzeltmek için değişim yapılır, kullanıcılar veya müşterilerden gelen yeni talepleri karşılamak için değişim yapılır, çalışılan sektöre ait veya sadece bilgi sistemlerine ait yasal mevzuatın değişmesi de bir değişim zorunluluğu doğurabildiği gibi, hiçbir dış uyaran olmadan, sadece BS içinde gözetim ve değerlendirme faaliyetleri sonucunda da değişim gereksinimleri ortaya çıkabilir.

Değişimin amacı bir fayda sağlamaktır ancak maalesef her değişim kendi içinde belirli bir risk de barındırır. Amacımız değişimin riskini en azda, getireceği faydayı da en çokta tutabilmektir. Bu da değişimin çalakalem değil, belirli bir yöntem dâhilinde yapılmasını gerektirir.

Kuruluşlarda değişiklik yönetimi; değişiklik kayıtlarının hizmet masası uygulamalarında oluşturulması ile başlar. Zorunlu alanlardan oluşan form doldurulur. Roller kullanılarak değişiklik sorumlulukları farklı paydaşlara aktarılabilir. Tüm değişikliklerin planlanması ile devam edilir. Bu aşamada değişiklik planları paydaşlara net olarak iletilmelidir. İletilen değişikliklerin acil, standart ya da normal değişiklik olmasına ve ilgili paydaşlara göre onaylarının alınması ile devam edilmelidir. Uygulama aşamasında onaylar alındıktan sonra görevler oluşturularak ya da proje kapsamında ele alınarak gerekli değişiklikler uygulanmalıdır. Sonraki adım olan gözden geçirmede, uygulama tamamlandıktan sonra değişiklik kaydı kapatılmadan tüm sorunların düzeltildiğinden emin olunmalıdır. Gözden geçirmeler ile süreç kontrol edilmelidir. Tüm adımlar tamamlandıktan sonra başarılı, başarısız ya da tamamlanmadı şeklinde kayıt kapatılmalıdır.

Tipik olarak BT değişiklikleri, tanımlanan BT sorununu düzeltmek için, tekrarlanan olaylara yol açan hatalı bir varlığı değiştirmek için veya büyük bir olayın çözümünün bir parçası olarak BT sorun yönetimi işlemlerinden sonra başlatılır. BT yönetiminin amacı BT arızalarını minimuma indirmek ve hizmetleri en kısa sürede geri yüklemektir. Bazı durumlarda değişiklik uygulamaları, geçici hizmet kesintileri veya hizmetin kullanılamaması gibi çoğu küçük olmak üzere olaylara neden olabilir. Değişiklik uygulaması ve beklenen olay veya hizmetin kullanılamaması konusunda son kullanıcılar bilgilendirilerek bu tür olayların etkisi minimuma indirilebilir. Bir değişikliğin neden olduğu büyük olay durumunda, değişiklik yönetimi ekipleri normale dönmek için anında değişikliği geri alabilirler.

Değişiklik Yönetiminin uygulanması ile alt yapıda meydana gelen bütün değişikliklerin kaydının tutulması, standardize edilmiş metotlar ve prosedürlere bağlı kalınarak verimli ve hızlı şekilde gerçekleştirilmesi, değişiklerden kaynaklanan olayların ve servis kesintilerinin engellenmesi sağlanır. Aynı zamanda değişikliklerin değerlendirilmesi, onaylanması, gerçekleştirilmesi ve gözden geçirilmesinin takibi sağlanmış olur.

Değişiklik yönetimi süreçleri ve prosedürleri aşağıdaki hususları sağlar:

- Değişikliklerin gerçekleşme zamanının izlenmesi ve tüm ilgili personele duyurulması,
- Sistem, operasyonlar ve program dokümantasyonlarının açık bir şekilde tanımlanmış, güncel ve belirlenen standartlara uygun olması,

- Değişikliklerin öncelik ve risk faktörleri göz önüne alınarak planlanması, gerekli durumlarda geri alma planının oluşturulması ve uygulanması,
- Yasal ve uyumluluk hususlarının dikkate alınması,
- Sistem ve test sonuçlarının ilgili kişiler tarafından gözden geçirilmesi, aynı zamanda test edilen işlerin yetkili kişi tarafından yeterli test edilip edilmesinin kontrol edilmesi,
- İzinsiz değişiklik sayısının tespit edilmesi ve kontrol altına alınması,
- Altyapı ve süreçlerin sürekli iyileştirilmesi.

Yapılarına göre değişiklikler birbirinden farklı gerekliliklere sahip olabilir. Bazı değişikliklerin mümkün olduğunca kısa süre içinde uygulanması gerekir, bazıları kuruluşun üst düzeylerinden onay gerektirir ve bazıları da haftalık olarak uygulanan normal değişikliklerdir. Değişim sürecinin çok uzayıp işleri yavaşlatması engellenmelidir. Bu yüzden tüm değişikliklere aynı şekilde cevap verilmez, kategorileştirilir ve süreç içinde bu kategorilere göre birtakım "kısayollar" tasarlanabilir.

1) Standart değişiklikler

Etkisi düşük, bilinen ve önceden onaylanmış değişikliklerdir. İlk uygulandıklarında risk değerlendirmesi yapılır ve izin gerektirir, değişiklik değiştirilmediği sürece daha sonraki uygulamalar için izin ve risk değerlendirme adımı atlanır.

2) Normal değişiklikler

Değişiklik gerçekleştirilmeden önce planlanmalı, risk değerlendirmesinden geçmeli ve onaylanmalıdır. Normal değişiklikler hem küçük hem de yüksek etkili ve öncelikli değişiklikleri içerir. Değişikliğin uygulanmasında risklerin değerlendirilmesi ve onay süreci her defasında işletilir.

3) Acil değişiklikler

Acil değişiklikler yüksek etkili ve önceliklidir. İş operasyonlarını etkiler bu nedenle kesintilere neden olabilir. Hizmetlerin mümkün olan en kısa süre içinde çalışır ve etkin hale getirilebilmesi için hızlandırılmış değerlendirme, onay ve uygulama süreçlerinden geçmeleri gerekir. Birincil sunucu arızası, veri merkezi kesintisi, güvenlik zaafı için acil yama gibi durumlar acil değişikliklere örnek verilebilir.

Kurumda değişiklik yönetimi yapılmazsa veya dokümante edilmiş süreçlere uyulmazsa aşağıdaki sorunlar ortaya çıkabilir:

- Değişimin başarısız olması, üründe/hizmette beklenen kazanımın elde edilmemesi,
- Değişim sürecinde öngörülemeyen hataların yaşanması, bunun bilgi kaybına, gizlilik kaybına, erişim kaybına, iş süreçlerinde aksamaya sebep olması, işletmenin maddi/manevi kaybı,
- Başarısız olan değişimlerde eski (değişim başlamadan önceki) duruma dönülememesi, bu şekilde iş/operasyon kaybı yaşanması, işletmenin maddi/manevi kaybı,
- Değişimlerin başarılı ama çok maliyetli olması,
- Değişimlerin bazı istenmeyen sonuçlarının (yan etkileri diyelim) hemen değil, belki aylar sonra ortaya çıkması, bu süreçte oluşan tahribatın ayrıca araştırılması ve düzeltilmesi gerekliliği.

Değişim sürecinde kayıt altına alınması gereken bilgiler genel olarak aşağıdaki gibi listelenebilir:

- Değişimin kaynağı, sebebi, getireceği fayda/kazanım, önceliği
- Değişimin riski
- Etkilenen sistem/uygulama/alt yapı elemanı
- Kapsamı, etkilenen kullanıcı/müşteri sayısı, etkilenecek iş süreçleri

- Değişimin sınıfı
- Değişimin planlanan zamanı
- Değişimi yapacak ekip
- Değişime ilişkin ilgili tarafların onayı
- Tahmini süre ve maliyet
- Geri dönüş planı

2.1.5.2. Sürüm Yönetimi

Büyük ölçekte ve etkide yapılacak yazılım güncellemeleri ve geniş çaplı donanım değişikliklerini yöneten süreçler sürüm yönetimi içerisinde tanımlanır. Çeşitli sorun düzeltmeleri ve geliştirmelerden oluşur.

Bazı durumlarda küçük düzeltmeler başka sorunları tetikleyebilir. Test edilmiş büyük sürümlerde bu durumlar ile karşılaşılmayabilir. Test süresi, kısaltmalar nedeniyle delta adı verilen kısmi sürümlerde uygulanabilir. Delta sürüm, en son yapılan sürümden o ana kadarki değişiklikleri içerir.

Sürüm yönetimi, bir ya da daha fazla sayıdaki değişikliği gerçek ortama sunmak, dağıtmak ve izlemek gibi faaliyetlerinin planlanması ve gerçekleştirilmesi için hizmet sağlayıcının ve pek çok tedarikçinin faaliyetlerini ve işini koordine eder.

Tüm donanım ve yazılım sürüm değişiklikleri sırasında önceki sürümlerin yedeklenerek ilgili kütüphanelerde tutulması, BT altyapısındaki yazılımlara ait yeni sürümlerin donanımlarla uyumluluğunun takip edilmesi, yasal ve uyumlu yazılımların kullanıldığının garantilenmesi sürüm yönetiminin uygulanması ile amaçlanmıştır. Sürümler kontrol edilmelidir. Eğer herhangi bir sorun ile karşılaşılırsa önceki duruma geri getirilmelidir.

Yazılım paketleri oluşturulurken en çok değişiklik yapılan süreç geliştirme sürecidir. Hem yerel ortamda hem de sürekli tüme varım ortamında yazılım paketleri oluşturularak denemelerin yapılması sağlanır. Böylece değişiklikler ile ilgili gidişat izlenir. Bu sırada oluşturulan paketlere anlık paket (snapshot) denir.

Geliştirme sürecinin tamamlanması ile ara sürümler oluşturarak test ve onaya sunulur. Bunlara ek olarak sürüm adayları (release candidates) vardır. Sürüm adaylarından bir tanesi test edilip onaylandıktan sonra sürüm olur. Bu paketlerin adımlardan geçerek bir sürüm haline gelme sürecine eser terfisi (artifact promotion) veya sürüm aşamalandırma (release staging) denir.

Kuruluşlar, bir DevOps modelini benimseyerek daha hızlı çıkış süreleri kazanır. Bununla birlikte, üretime daha hızlı dağıtımlarla kapsamlı bir risk yönetimi stratejisine ihtiyaç vardır. Sürüm yönetimi; DevOps süreç denetimleri, gereksinimlerin standartlaştırılması ve yönetişim ilkeleri aracılığıyla risk yönetimi sürecine yardımcı olur.

Sürüm yönetiminin öncelikli amaçları:

- Yeni sürümün tasarlanması, gerekli değişikliklerin yapılması, test edilmesi ve hizmetin ürün olarak sunulmasının planlandığı günde hazır olmasını sağlamak,
- Yeni ya da güncellenmiş servisin, daha önceden belirlenmiş servis gereksinimlerini karşılayıp karşılamadığını kontrol etmek,
- Geçiş döneminde ve sonrasında öngörülemeyen etkiyi en azda tutmak,
- Yeni ya da güncellenmiş servis hakkında kullanıcılar, müşteriler ve yetkili personel için dokümantasyon ve eğitim verilmesi gibi konuları denetlemek.

Sürüm Yöneticisinin rol ve sorumlulukları:

Yapıların ve uygulamaların artması karmaşıklığın artmasına neden olur ve geliştirme aşamalarını koordine etmek kritik öneme sahip hale gelir. Sürüm yöneticisinin rolü, kuruluş genelinde

sürümlerin verimli bir şekilde planlanmasını, koordinasyonunu ve yönetimini sağlamaktır. Bununla birlikte:

- BS yayın takvimini oluşturur, çeşitli BS yöneticileriyle çalışarak koordinasyonu sağlar,
- Uygulama sürümlerinin zamanında ve bütçe dâhilinde teslim edildiğinden emin olmak için ilerlemeyi izler,
- Riskleri yönetir ve sürümün kapsamını, kalitesini ve zamanlamasını etkileyen sorunları çözmek için takip eder, aksiyon alır ya da alınmasını sağlar,
- İlerleme hakkında yönetime bilgi verir,
- Yazılım sürümlerini diğer uygulamalar ile entegre etmek ve dağıtmak için komut dosyaları ve otomasyon araçları araştırır.

Sürüm yönetimi, kuruluşların son kullanıcı veya iş işlevlerinde minimum kesinti ile yazılımı zamanında dağıtmalarını sağlar.

Sürekli Test

Test, sürüm yönetimi sürecindeki aşamalardan biridir. Ancak yazılım oluşturmanın daha etkin ve doğru olabilmesi için her aşamada sürekli testler yapılmalıdır.

Geliştirme sırasında yazılan birim testlerine ek olarak, yeni eklenen özelliklerin birbirleriyle doğru bir şekilde etkileşime girmesini sağlamak için entegrasyon testleri yapılır. Yapılan test çeşitleri aşağıdaki gibi açıklanabilir:

1. Regresyon Testi: Yeni eklenen özelliğin veya kodun mevcut herhangi bir işlevi bozup bozmadığını kontrol eder.

2. Performans Optimizasyon Testleri: Genellikle web uygulamasının ortalama yüklenme süresini, erişilebilirliğini ve arama motoru optimizasyonunu kontrol etmek için yapılır.

3. Yük Testi: Spesifik iş yükleri altında sistem performansını, spesifikasyon limitlerine yakın seviyelerde ölçen bir performans testi yöntemidir. Kullanıcı veya işlem sayısı arttıkça uygulamanın yanıt süresi ve kullanılabilirlik açısından ne kadar iyi performans gösterdiğini değerlendirmeye yardımcı olur.

4. Fonksiyonel Test: Yazılımın fonksiyonel analize uygunluğunun kontrolüdür. Testin amacı, sistem analizinde belirtildiği gibi yazılım bileşenlerinin birbiriyle doğru olarak entegre edilmesidir. Ürünün kullanıcı ihtiyacını karşılayıp karşılamadığını görmek için kritiktir. Test yürütme sürecinde, beraber yazılan fonksiyonel gereksinim maddelerinin de onayları alınmış olur. Fonksiyonel testlerde genellikle yazılımın harici davranışları, girdi ve çıktılar dikkate alınır.

5. Kullanıcı Kabul Testi: Proje ekibi tarafından yürütülen testlerin başarılı olarak sonuçlanması halinde, Proje Teknik Lideri tarafından kullanıcı kabul testine çıkılabileceğinin onayı verilir. Kullanıcı kabul testi aşamasına gelen projelerde testi yapacak proje sahibi ve proje paydaşlarına ilgili bilgilendirme Proje Yöneticisi tarafından yapılır.

Test öncesi senaryolar ve kullanılacak verilerle ilgili hazırlık yapılmalıdır. Senaryolar için belirli bir şablon kullanılır ve sonucu olumlu/olumsuz (pass/fail) olarak gösterilir.

Kullanıcıya test senaryoları gönderilerek senaryolar için onay alınmalıdır. Test edecek kullanıcı test kanıtlarını kayıt altına almalıdır. Tespit edilen hatalar var ise önceliklendirilerek çözüm sağlanır ve tekrar test edilir.

Kullanıcı kabul testinin sonuçlanması sonrasında ilgili paydaşlardan kullanıcı kabul onayı alınır.

Ek olarak bir grup kullanıcı, uygulamayı beta testi aşaması olarak bilinen aşamada test eder ve geri bildirimde bulunur. Kuruluş, bu geri bildirimi kullanarak ürünü gerçek ortamda kullanıma sunmadan önce iyileştirebilir.

2.1.5.3. Yama Yönetimi

Yama (patch) yönetimi, programlama kodunun daha yüksek verimlilikle çalışabilir olmasını sağlamak, değişik tipteki kod değişikliklerini tanımlamak ve test etmek için uygun yöntemler üzerine kuruludur ve güvenlik açıklarına karşı korumak, yüksek performansta çalışmasını sağlamak için yazılımlara ve sürücülere güncellemeler yükleme işlemidir. Yapılan güncellemeler; kuruluş içerisinde üretkenliği destekler, cihaz yönetim ve onarım maliyetlerini düşürmeye, yasaları, yönetmelikleri ve uyumluluk standartlarını yerine getirmeye yardımcı olur.

Belirli bir sisteme uygulanan yamalar veya tüm kod değişiklikleri hakkında sürüm ve içerik bilgisi tutulmalıdır. Yapılan değişiklik ya da yamanın doğruluğundan emin olmak için önceki test verileri ile karşılaştırma yapılabilmelidir. Kod değişiklikleri/yamalar tamamlandıktan sonra son kullanıcı erişimine açıldığında da test yapma işlemi devam etmelidir. Bu işleme devam edilmesinin nedeni, değişiklik ile simülasyonlar sırasında görülemeyen sorunların, canlı ortama çıkmadan önce farklı bir göz tarafından tekrar değerlendirilmesi ve gerçek zamanlı ortamda ne kadar verimli işlediğinin takip edilmesidir.

Yama yönetimi görevleri; mevcut yamalar ile ilgili güncel bilgileri koruma, belirli sistemler için hangi yamaların uygun olduğuna karar verme, düzeltme eklentilerinin doğru olduğundan emin olma, kurulduktan sonra sistemlerin test edilmesi ve tüm işlemlerin belgelendirilmesi gibi faaliyetleri içerir.

Yama işlemleri sırasında; öncelikle veri yedeklemesinin yapılmış olmasına, yamanın benzer sistemlerde test edilmesine, mümkünse mesai saati dışında yapılmasına, kesinti olacaksa kesinti zamanı ve ne kadar süreceği ile ilgili bilgilendirme yapılmasına, herhangi bir aksi durumda yedekten dönüşlerin yapılabilir halde bulundurulmasına dikkat edilmelidir. Yapılan işlemler otomatik güncelleştirme ya da merkezi dağıtım şeklinde yapılabilir.

1. Otomatik Güncelleştirme: Windows, Linux gibi kişisel sistemlerin daha sık güncellenmesi gerekmektedir. Ancak her makinanın tek tek yama alması gereksiz bant genişliği harcanması ve yeterince hızlı olmaması gibi bazı sorunlara neden olabilir.

2. Merkezi Dağıtım: Kurumsal ağ yapılarında, yamalar merkezi bir makinaya çekilir ve buradan diğer makinalara dağıtılması sağlanır. Böylece hangi cihazlarda yama yapıldığının takibi sağlanabilir. Active Directory kullanılan ortamlarda, sistemlerin etki alanı yöneticisi (domain) üzerinde kurulu Smart Update Services ile otomatik güncelleme alması sağlanabilir.

2.1.5.4. Konfigürasyon Yönetimi

Konfigürasyon (yapılandırma) yönetimi, verilen servislerle ilgili ve takip edilmek istenen her parçayı kayıt altına alma yönetimidir. Bu sayede; BT altyapısının maliyet ve işletim takibinin sağlanması, diğer süreçlerin kullanacağı bilgi kaynağının sağlanması, bileşenlerin birbiriyle olan ilişkilerinin kayıt altına alınarak olay ve problem etkilerinin tespit edilmesi sağlanır.

Konfigürasyon yönetim sisteminde tutulan bilgilerin eksiksiz olduğunun ve değişikliğin yetkili kişiler tarafından yapıldığının kontrol edilmesi gerekmektedir. Bu nedenle, BT varlıklarını ve konfigürasyonlarını etkili yönetebilmek ve takibini sağlayabilmek için değişiklik ve sürüm yönetimi ile birlikte planlanmalıdır.

Ağ konfigürasyon yöneticisi, ağ cihazları ve konfigürasyonlarının tüm yaşam döngüsünü yönetmeye yardımcı olur. Karmaşık ağ faaliyetlerini otomatik hale getirir, yedeklemeleri planlar, kullanıcı faaliyetlerini izler ve ayrıntılı raporlar oluşturur.

Konfigürasyon yönetimi için kullanılan uygulamalar, belirli kullanıcıları belirli cihazlarla ilişkilendirmeyi sağlayan kullanıcı odaklı yönetimi destekler. Bu işlevsellik, en önemli uygulamaların her zaman kullanıcının her cihazında kullanılabilir olmasını sağlar. Kullanıcı yeni bir bilgisayar kullanmaya başladığında konfigürasyon yönetimi oturum açmadan önce uygulamaları cihaza otomatik olarak yükleyebilme çözümü sunar.

- Konfigürasyon Yönetim Sistemi Değişiklik Politikası

Konfigürasyon yönetim sisteminin yapısını ve içeriğini değiştirmeye kimin yetkili olduğunu tanımlayan kural setlerini içerir.

- Konfigürasyon Yönetimi Denetim Raporu

Konfigürasyon yönetim sisteminde bulunan kayıtlar ile gerçekte kurulu konfigürasyon öğeleri arasındaki farkları gösteren rapordur.

Konfigürasyon Yönetimi Veri Tabanı (Configuration Management Database- CMDB)

Bir kuruluşun BT hizmetlerinde kullanılan donanım ve yazılım bileşenleri ile bu bileşenler arasındaki ilişkilerle ilgili tüm bilgileri içeren bir veri tabanıdır. CMDB, konfigürasyon verilerinin ve bu verilerin istenen herhangi bir perspektiften incelenmesini sağlar.

Bilgi sisteminin bileşenleri, yapılandırma öğeleri (Configuration Item - CI) olarak isimlendirilir. Yapılandırma yönetimi süreçleri, yapılandırma öğeleri ve bunlarda yapılan değişiklikleri kapsamlı ve sistematik bir şekilde belirlemeyi, kontrol etmeyi ve izlemeyi sağlar.

ITIL spesifikasyonlarına göre, Konfigürasyon Yönetimi'nin (Configuration Management-CM) dört ana görevi vardır:

- Konfigürasyon yönetimi veri tabanı içerisinde yer alacak yapılandırma öğelerinin tanımlanması (discovery),
- Sadece yetkili kişiler tarafından değiştirilebilmesi için kontrol verilerinin oluşturulması(security),
- Yapılandırma öğelerine ait mevcut durumunun kaydedilmesinin ve güncel tutulmasının sağlanması (reporting),
- Verilerin doğruluğundan emin olmak için sürekli denetlenmesi (audit).

Konfigürasyon yönetimi veri tabanı yapılandırma öğeleri arasındaki ilişkiler (bağımlılıklar) hakkında ayrıntılı bilgi sağlar. Örneğin bir kesinti olması durumunda, BS birimi, kimin veya hangi sistemlerin etkileneceğini yapılandırma öğeleri verileriyle anlayabilir. Ayrıca gereksiz BS kaynaklarını ve bunlara bağlı maliyetleri ortadan kaldırarak BS liderlerinin kurum içinde tasarruf etme yollarını tespit etmelerini sağlayabilir.

Ağ Konfigürasyonu Yönetimi (Network Configuration Management)

Ağ Konfigürasyonu Yönetimi, ağdaki her cihazın kullanım ömrü boyunca takip edildiği bir süreçtir. Cihaz bulma, envanter bakımı, uyumluluk izleme, kullanıcı etkinliği izleme, arıza giderme, konfigürasyon yedekleme ve değişiklik işlemlerini kapsar.

- Ağ cihazı bulma

Mevcut cihazlar envantere eklenir. Envanter, cihazın seri numaraları, arayüz detayları, port konfigürasyonları ve donanım bilgileri gibi cihaz bilgileri hakkında ayrıntılı bir görünüm sağlar. Bu sayede denetim raporlarının oluşturulması ve takibine faydalı olur.

- Konfigürasyon yedekleme

Hatalı bir değişiklik, hatalı bir güncelleme, ağ kesintisi, güvenlik ihlali gibi sorunlar ile karşılaşılması durumunda kullanılmak üzere ağ yedeklerinin oluşturulması sağlanmalıdır. Böylece bir hata/arıza durumunda güvenilir bir sürümle geri yüklenerek iş sürekliliği sağlanır.

- Konfigürasyon değişiklik yönetimi

Konfigürasyon değişikliklerinin daha kolay tanımlanması için kullanıcı kaydı tutulmalıdır. Ne zaman ve hangi kullanıcı tarafından ne tür bir değişiklik yapıldığına dair bilgi içerir. Problem ile karşılaşılması durumunda geri dönüş ya da yapılan işlemlerin kontrol edilmesini sağlar.

- Karmaşık ağ işlemlerini yürütme

Ağ Konfigürasyon Yönetimi birçok ağ işleminin aynı anda yürütülmesini sağlar. Örneğin parola değişikliğini tüm cihazlarda ayrı ayrı yapmak yerine, konfigürasyon araçları kullanarak tüm cihazlarda merkezi olarak yürütülmesi sağlanır.

2.1.5.5. Hizmet Seviyesi Anlaşmaları (SLA) ve İş Birimleriyle Mutabakat (OLA)

Şirkete hizmet sağlayan birbirinden farklı özelliklere sahip süreçlerin birbiriyle olan ilişkilerinde, müşteri memnuniyetini korumak ve geliştirmek için takip ve ölçülebilir hedefler belirlenir. Bu hedefler, şirketlerin dışarıdan aldığı veya şirket içi vermiş olduğu hizmetlerin kalitesini ölçebilmeye ve yapılan hizmet (servis) anlaşmalarının tutarlılığının kontrol edilmesine olanak tanır.

Hizmet Seviyesi Anlaşması, hizmet sağlayıcı (tedarikçi) ile son kullanıcı (müşteri) arasında beklenen hizmet düzeyini belirleyen bir sözleşmedir. Hizmet seviyesi anlaşmaları (Service Level Agreement) bir görevin veya projenin sonucunun kararlaştırılan nitelikte, sürede ve beklenen kalite seviyesinde tamamlanmasını sağlamak için oluşturulmaktadır. Aynı zamanda sunulan ürün ya da hizmet ile müşteri beklentilerinin arasındaki bağlantıyı korumaya yardımcı olur.

Hizmet seviyesi anlaşmaları, öncelikler, sorumluluklar ve garantiler dâhil olmak üzere verilen tüm hizmetlerin kapsamı, minimum veya hedeflenen seviyelere dair ölçülebilir hizmetleri, yasal olarak bağlılıkları, müşteri görev ve sorumlulukları, sözleşme fesih şartları, felaket kurtarma prosedürleri gibi bilgileri içerir. Bakım ve onarım anlaşmaları da bu hizmetler arasına dâhil edilebilir. Hizmet seviyeleri donanım ve yazılım performans hedeflerini (kullanıcı yanıt süreleri ve donanım erişilebilirliği vb.) içerecek şekilde tanımlanmalıdır. Finansal performans ölçümleri, insan kaynakları ölçümleri, personel işten ayrılma süresi vb. gibi kriterler de eklenebilir. BS denetçisi, mevcut farklı ölçüm kriterlerinin farkında olmalıdır ve bunların kapsamlı olduğundan, risk, güvenlik, kontrol ölçümleri ile verimlilik ve etkinlik ölçüm kriterlerini içerdiğinden emin olmalıdır.

BS hizmetlerinin özellikleri hizmet seviyesi anlaşmalarının tanımlarında kullanılır. Bu özelliklerde; doğruluk, bütünlük, zamanlılık ve güvenlik ilkelerine dikkat edilmelidir. BS çalışanı tarafından sağlanan hizmetlerin verimliliğini ve etkilerini takip edebilmek için kullanılan bazı araçlar vardır. Bu araçlar;

- **İstisna raporları:** Başarılı tamamlanmayan veya başka bir şekilde çalışmayan tüm uygulamaları tanımlar. İstisnaların çok olması, iş gereksinimlerinin yeteri kadar anlaşılamaması, uygulamalarda kötü tasarım, test ve geliştirme, yetersiz kullanım talimatları, yetersiz operasyon desteği, eğitim ve performans izlemede yetersiz olunması, görevlerin yetersiz olması, yetersiz kapasite yönetimi gibi durumlardan kaynaklanabilir.

- **Sistem ve uygulama günlüğü:** Tüm sistem sorunlarını tanımlamak için çeşitli sistemlerden ve uygulamalardan oluşturulan günlükler düzenli olarak gözden geçirilmelidir. Anormal ya da problemli durum ve uygulamalarla ilgili günlüklerde kayıt olacağı için kök nedenlerinin tespit edilmesine kolaylık sağlar. Ancak günlüklerin boyutu ve karmaşıklığı nedeniyle manuel kontrol etmek oldukça zordur. Sistem günlüklerini analiz ederek rapor oluşturabilen araçlar kullanılabilir. Bu araçları denetçi, hassas verilere sadece onaylı programların erişmesini ve yetkili BT çalışanı tarafından erişim sağlanmasını, veri dosyalarını ve veri kütüphanelerini değiştirebilen yardımcı yazılım programlarının yalnızca yetkili amaçlar için kullanıldığını, onaylanan yazılımların sadece gerekli durumlarda çalıştığını ve veri dosyalarında güvenliğin sağlandığını test etmek için kullanabilir.

- **Operatör problem raporları:** Bu raporlar manueldir ve bilgisayar işlemleri sorunlarını ve çözümlerini kaydetmek için kullanılır. Operatör müdahalelerini, bu müdahalelerin uygun olup olmadığını veya operatörlere verilen eğitimin yeterliliğini tespit etmek için BS yönetimi tarafından düzenli olarak gözden geçirilmelidir.

- **Operatör çalışma çizelgeleri:** İnsan kaynakları planlamasına yardımcı olmak için manuel hazırlanan dokümandır. Uygun personelin uygun operasyonel destek için planlanmasına kolaylık sağlar. BS yönetiminin, son kullanıcıların hizmet gereksinimlerinin karşılanacağından emin olmasını sağlar.

OLA (Operational Level Agreement), müşteriyle SLA (Service Level Agreement) anlaşması yapmış bir kurumun iç destek grupları (operasyon grupları) arasındaki anlaşmadır. Anlaşma, her bir iç destek grubunun beklenen kalitede ve zamanda hizmetlerin sunulması için diğer destek gruplarına karşı sorumluluklarını tanımlamaktadır. Aynı zamanda teknik detayları içerir. OLA'nın amacı, çeşitli destek ekipleri tarafından gerçekleştirilen destekleyici faaliyetlerin SLA'da beklenen standartları karşılamasına yardımcı olmaktır.

SLA ve OLA arasındaki fark esas olarak odaklarına bağlıdır. SLA, anlaşmanın hizmet kısmına odaklanmaktadır. OLA, bakım ve diğer hizmetler ile ilgili teknik bir anlaşmadır.

- **Hizmet Seviyelerinin İzlenmesi**

BS operasyonlarının amaçlarına ulaşılmasını sağlamak için, tanımlanmış hizmet seviyeleri düzenli olarak izlenmeli ve müşteriler ve şirketin diğer paydaşları üzerindeki etkileri gözden geçirilmelidir. Hizmet sevilerinin izlenmesi, şirket tarafından müşterilerine sunulan hizmette dış kaynak kullanımı mevcut ise çok daha kritik önem taşır. Hizmet sunumlarında dış kaynak kullanımı olan şirketlerde BS denetçisi, üçüncü taraf iletişim ve takip gibi konulardaki yöntemin ve kontrollerin düzgün tasarlandığını, etkin çalışıldığını ve güvence altına alındığını belirleyebilmelidir. Anketler, yerinde ziyaretler ve üçüncü taraf güvence raporları gibi farklı kontrol teknikleri kullanılabilir.

- **Hizmet Seviyeleri ve Kurumsal Mimari**

Hizmet sunumunun sürekliliği ve düzgün çalışmasında kurumsal mimarinin tanımlanması ve uygulanması etkilidir. Erişilebilirlik ve kurtarma seçeneklerini değerlendirirken, sunulan hizmetlerdeki operasyonel gereksinimler ile hedeflerin karşılanmasındaki uyuma katkı sağlar.

2.1.5.6. Kaynak Yönetimi

Kaynak yönetimi, kaynakların bir görev için yeterli ve verimli olmasını sağlama sürecidir. Kaynaklar, bir işletme veya kuruluşun işletme operasyonları oluşturma veya sürdürme sürecinde kullanılan her şeyi içerebilir. İnsan, zaman, finansman ve teknoloji gibi gereklilikler kaynak kavramı için örnek verilebilir.

Belirli bir proje için gerekli olan bazı kaynaklar şirket içinde bulunmayabilir, bu nedenle üçüncü taraf kaynaklardan elde edilebilir. Bunlara danışmanlar, dış kaynak firmaları ve ödeme sistemi sağlayıcıları örnek verilebilir.

Kaynak yönetimi, gereksiz kullanımı engeller ve üretkenliği optimize ederek verimli ve etkili olmayı sağlar. Etkili bir kaynak yönetimi planı, öngörülemeyen engellerden kaçınılmasını sağlar. Bir projeye başlamadan önce mevcut olan kaynakları doğru bir şekilde anlayarak potansiyel problem önceden tespit edilebilir.

Başarısız projeler, işlerin nerede yanlış gittiğini hızlı bir şekilde belirlemek için kaynak yönetimi yazılımı ile analiz edilebilir. Proje yöneticisinin proje için ihtiyaç duyulan insan kaynaklarını verimli kullanmak ve bu kaynakları güvence altına almak için çalıştığı gibi, proje için ihtiyaç duyulan fiziksel kaynakları güvence altına almak için de çalışması gerekir.

Kaynak yönetimi planında, proje ekibi üyelerinin projeye nasıl dâhil edileceği ve projeden ne şartlarda ayrılabileceği ayrıntılarıyla anlatılır. Bu plan aynı zamanda proje kaynaklarına ne kadarlık bir süre için ihtiyaç duyulacağını da tanımladığı gibi, aktivite kaynaklarının nasıl tahmin edileceğine dair rehberlik görevi de görür.

2.1.5.7. Yığın (batch) İşler

Bilgisayar bilimlerinde, belirli bir zamanda yapılması planlanan, çoğunlukla kullanıcı etkileşimi gerektirmeyen işlerin biriktirilmesidir. Yığın işlem, bilgisayar sistemlerinin daha verimli kullanılmalarını sağlayarak, iş başına düşen sistem giderlerini azaltmayı amaçlamaktadır.

Örneğin, sistemin yedeği mesai saati sonrasında, birden fazla bilgisayara bağlanılarak alınacak ve oluşan yedek dosyaları sunucuya kaydedilecektir. Bunun için bir yığın iş (batch process) hazırlanarak sistemde saklanır. Beklenen zaman geldiğinde bu iş otomatik olarak çalışır ve sistemin yedeğini alır.

Çeşitli işletim sistemlerinde kullanımları farklıdır. Örneğin Windows işletim sisteminde bulunan zamanlanmış görevler (scheduled tasks) vasıtasıyla istenilen zamanda bir işin çalışması mümkündür. Daha eskiden DOS işletim sisteminde ".bat" uzantılı dosyalar da batch file (yığın dosya) olarak literatürde geçmekteydi. Bu dosyalarda çalışacak olan komutlar arka arkaya sıralanmakta ve sırayla çalıştırılmaktaydı. Bu dosyaların en başında "autoexec.bat" dosyası gelir. İşletim sisteminin özel dosyalarından olan bu dosya ilk açılışta okunan ve sistem açılınca yapılması istenen özel işlerin sıralandığı dosyadır. Windows işletim sistemiyle birlikte gelen "başlangıç (startup)" grubunda bulunan işler buna benzetilebilir.

Unix (veya linux) işletim sisteminde ise örneğin "at" komutu ile istenilen zamanda çalışmak üzere bir iş tanımlanabilir.

Değerlendirme Soruları

Soru 1: Olayların sınıflandırılması olay yönetimi sürecine nasıl yardımcı olur?

A) Olaya atanan önceliği belirler.

B) Sorunların temel nedenlerinin ortadan kaldırılmasını sağlar.

C) Kayıtları, inceleme için doğru uzman ekiplere veya destek gruplarına atamayı sağlar.

D) Uygun SLA'ların BT olay kayıtlarıyla ilişkilendirilmesine olanak sağlar.

E) Olayların çözümlerini ve geçici çözümlerini tanımlar.

Cevap: C

Soru 2: Hizmet masası uygulamasının temel amacı nedir?

A) Olayların çözümü ve taleplerin yönetimi için kayıtların alınması.

B) Hizmet performansları için hedeflerin belirlenmesi.

C) Risklerin değerlendirilmesi için değişiklik sayılarını arttırmak.

D) Sürüm yönetimi kayıtlarının tutulması.

E) Olayların nedenlerini belirleyerek olasılığını ve etkisini azaltmak.

Cevap: A

Soru 3: Kuruluşlarda herkesin sorumluluğunda olan uygulama hangisidir?

A) Değişiklik Yönetimi

B) Sürekli İyileştirme

C) Problem Yönetimi

D) Sürüm Yönetimi

E) Olay Yönetimi

Cevap: B

Soru 4: Hizmet seviyesi anlaşmalarına (SLA) neler dahil edilmelidir?

A) Öncelikler, sorumluluklar ve garantiler dâhil olmak üzere verilen tüm hizmetlerin kapsamı

B) Net olarak tanılanmış hizmet sonuçları

C) Kaynakların verimliliği

D) Hizmet bileşenlerinin teknik açıklamaları

E) Sistemlere ait ölçüm sonuçları

Cevap: A

Soru 5: Olay Yönetimi için BT hizmet masası araçlarını kullanmanın yararı nedir?

A) Karışık olayların otomatik olarak çözülmesini ve kapatılmasını sağlar.

B) Hizmet sağlayıcının ihtiyaçları ile tedarikçi sözleşmelerinin uyumlu olmasını sağlar.

C) Olayların SLA sürelerine uygun zamanda çözülmesini sağlar.

D) Risk ve fırsatların tespit edilmesini sağlar.

E) Olayların bilinen hatalar ile eşleşmesini sağlar.

Cevap: E

Soru 6: Hangi uygulama ile kullanıcılar için tek bir iletişim noktası sağlanır?

A) Yama Yönetimi

B) Değişiklik Yönetimi

C) Hizmet Masası

D) Talep Yönetimi

E) Olay Yönetimi

Cevap: C

Soru 7: Aşağıdakilerden hangisi standart değişiklik tanımıdır?

A) İlk uygulandıklarında risk değerlendirmesi yapılır ve izin gerektirir, değişiklik değiştirilmediği sürece daha sonraki uygulamalar için izin ve risk değerlendirme yapılmayan değişikliklerdir.

B) Değişikliğin uygulanmasında risklerin değerlendirilmesi ve onay süreci her defasında işletilen değişikliklerdir.

C) Güvenlik zafiyetini önlemek için yapılan acil değişikliklerdir.

D) Hızlandırılmış değerlendirme, onay ve uygulama süreçlerinden geçirilen değişikliklerdir.

E) Sürekli iyileştirme kapsamında değerlendirilen, yetkilendirilen ve planlanan değişikliklerdir.

Cevap: A

Soru 8: Aşağıdaki değişiklik yetkisi tanımlarından hangisi doğrudur?

A) Değişiklik türlerinin hepsinde yetki aranmaksızın yapılabilir.

B) Her türlü değişiklikleri yetkilendirmek için tek bir değişiklik yetkisi atanmalıdır.

C) Normal değişiklikler önceden yetkilendirilir ve değişiklik yetkisine ihtiyaç duyulmaz.

D) Acil değişiklikler bir değişiklik yetkilisinden izin alınmadan uygulanabilir.

E) Her değişiklik türü için değişiklik yetkisi atanmalıdır.

Cevap: E

2.2. Gözetim, Kapasite ve Performans Yönetimi

2.2.1. Yedekleme ve Yedekten Geri Dönme

Yedekleme ve felaketten kurtarma kavramları bilgi sistemlerinde sıkça birbiriyle karıştırılır. Bilgi sistemlerinde "felaket", her türlü doğal afet (sel, deprem, kasırga), insan faktörleri (hırsızlık, sabotaj), donanım veya çevresel faktörler (veri kaybı yaratan teknik problemler ya da yangın gibi olaylar) nedeni ile çalışma sürecinin kesintiye uğraması veya veri kaybı yaşanması olarak nitelenir. Yedekleme ise verilerin fazladan bir kopyasını (veya birden çok kopyasını) alma işlemidir. Veriler korumak için yedeklenir, öte yandan felaketten kurtarma, bir kesintiden sonra uygulamalara, verilere ve BT kaynaklarına erişimi hızlı bir şekilde yeniden sağlamaktır. Veriler, herhangi bir işletme için faaliyetlerini sürdürmede temel bir varlık olduğundan yedekleme, depolama ve potansiyel geri yükleme gibi süreçler işletmeler için kritik süreçlerdir. Bu süreçler işletmenin risk iştahına göre belirlenebileceği gibi düzenlemelerden de kaynaklanabilir.

Yedekleme çeşitleri şu şekilde sıralanabilir:

- **Tam Yedekleme (Full Backup):** Yedekleme işlemi için yapılandırılan verilerin bütün bir kopyasının alınmasıdır.
- **Artımlı Yedekleme (Incremental Backup):** Daha önce yapılan yedeklemeden sonraki değişmiş olan verilerin yedeklenmesidir.
- **Diferansiyel Yedekleme (Differential Backup):** En son yapılan tam yedeklemeden sonra değişen verilerin yedeklenmesidir.
- **Sentetik Yedekleme (Synthetic Backup):** Bu yedekleme türünde öncelikle tam yedekleme alınıp bir yere depolandıktan sonra ardından artımlı yedekleme alınır. Daha sonra tam ve artımlı yedeklemeler birleştirilir.
- **Ayna Yedeklemesi (Mirror Backup):** Tam yedeğin bir kopyasının başka bir yere alınarak yedeklenmesidir.
- **Sürekli Yedekleme (Continuous Backup):** Veri gerçek zamanlı ve sürekli olarak izlenir. Değişiklik olması durumunda veri hemen yedeklenir.

2.2.1.1. Veri Yedekleme Teknolojileri

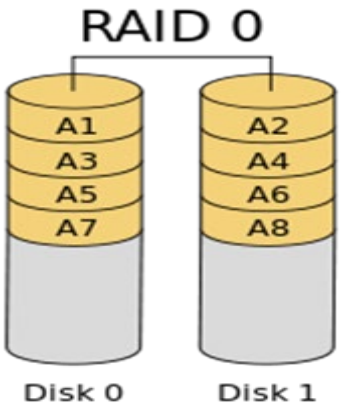
Yedekli bağımsız diskler dizisi (Redundant array of independent disks-RAID), performans iyileştirme, depolama kapasitesini genişletme, hata toleransı veya tüm yetenekleri aynı anda kullanmak amacıyla fiziksel sürücüleri bir veya daha fazla mantıksal birimde birleştirmek için kullanılan bir veri depolama sanallaştırma teknolojisidir. RAID yapıları yazılımsal RAID ve donanımsal RAID olmak üzere ikiye ayrılmaktadır. Donanımsal RAID, yazılımsal RAID'e göre daha performanslı olduğundan dolayı daha çok tercih sebebidir.

RAID Seviyeleri

Veriler, gereksinim duyulan yedekleme ve performans düzeyine bağlı olarak, RAID seviyeleri olarak adlandırılan birkaç yoldan biri seçilerek sürücüler arasında dağıtılır. Toplamda 11 farklı RAID seviyesi bulunmaktadır. Yaygın olarak kullanılanlar aşağıda verilmiştir:

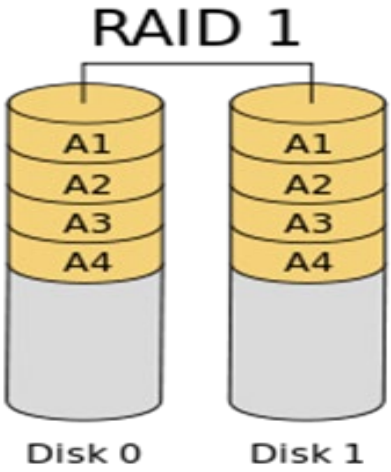
RAID 0 (Stripe Set):

Bu RAID seviyesi için en az 2 disk kullanılır. 32 diske kadar çıkılabilir. Veriler disklere dağıtılarak yazılır. Bu sayede yazma ve okuma hızı oldukça iyidir. Ayrıca parity–eşlik biti yazılmaması da performans artışında etkendir. Disklerin toplam alanı kullanılabilir.



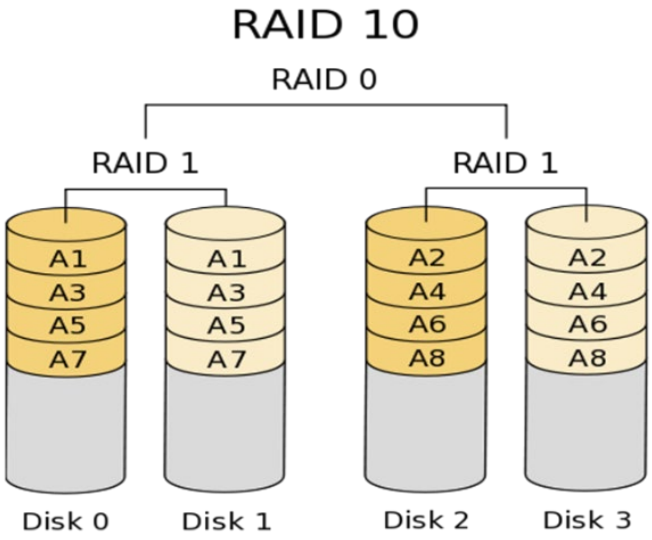
RAID 1 (Mirror):

Bu RAID seviyesi için 2 disk kullanılır. Veriler bir diske yazılır, kopyası birebir olarak diğer diske de yazılır. Okuma hızı yazma hızına oranla iyidir. Tek bir diske göre okuma ve yazma hızı daha iyidir.



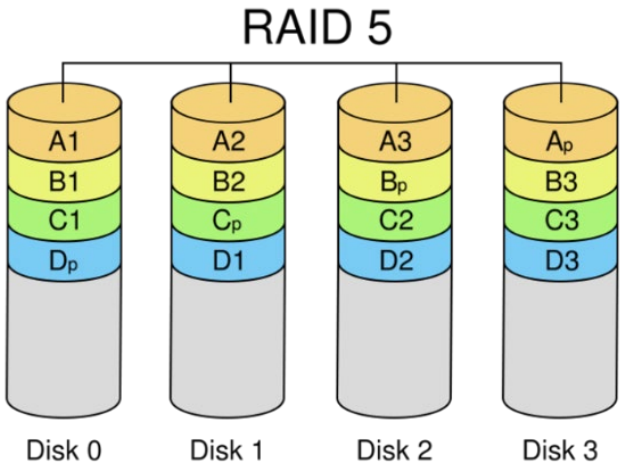
RAID 10:

Bu RAID seviyesi için en az 4 disk kullanılır. 32 diske kadar çıkarılabilir. RAID 0'da olduğu gibi veriler disklere dağıtılarak yazılır. Dağıtılan verilerin kopyası RAID 1'de olduğu gibi diğer diske yazılır.



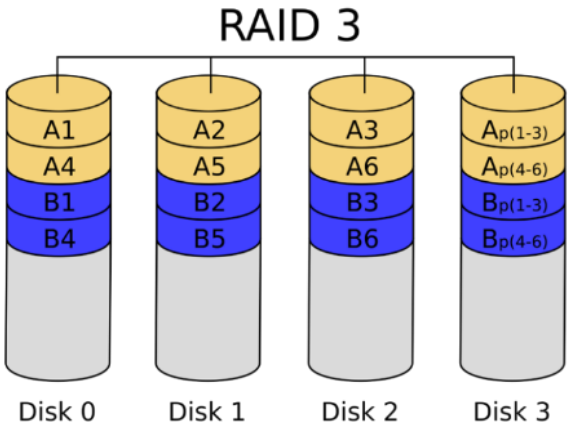
RAID 5 (Stripe Set with Parity):

En çok kullanılan RAID türüdür. Bu RAID seviyesi için en az 3 disk kullanılır. 16 ya da RAID kartına bağlı olarak 32 diske kadar çıkarılabilir. Veriler disklere dağıtılarak yazılır. Aynı yazım sırasında verinin bir diskte hataya düşmesi durumunda verinin kurtarılması için bir kopyası, verinin yazılmadığı diğer diske yazılır. Bu şekilde performans sağlanır. Bu veriye parite – eş veri denir.



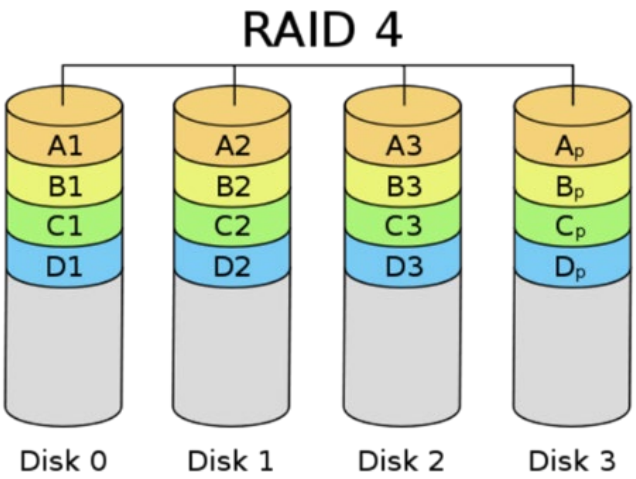
RAID 3:

Bu RAID seviyesi için en az 3 disk gerekir. Veriler disklere RAID 0'da olduğu gibi dağıtılarak yazılır. Yazılan veriler byte-level yani byte seviyesinde, kısaca daha küçük parçalar kullanılarak yazılır. Yazılan verilerin parity-eş verileri atanmış bir disk üzerine yazılır. Yüksek yazma ve okuma hızı oranına sahiptir. Bir diskin bozulması durumunda genel olarak performans çok etkilenmez.



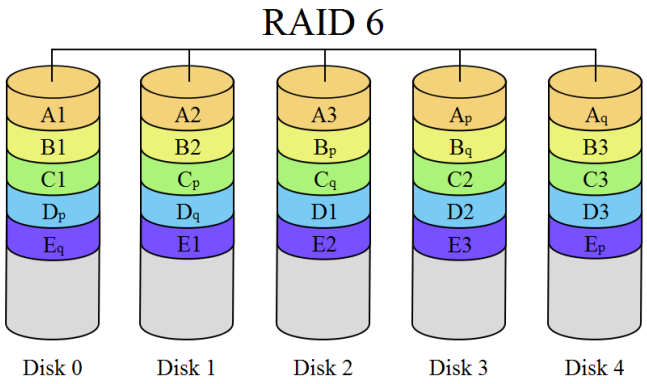
RAID 4:

Bu RAID seviyesi için en az 3 disk gerekir. Veriler disklere RAID 0 da olduğu gibi dağıtılarak yazılır. Yazılan veriler, RAID 3 ten farklı olarak daha büyük parçalı block-level yani veri blokları şeklinde yazılır. Yazılan verilerin parity-eş verileri atanmış bir disk üzerine yazılır. Yüksek okuma hızı oranına sahiptir.



RAID 6 (Dual Distributed Parity):

Bu RAID seviyesi için en az 4 disk gerekir. Bu yapı RAID5 gibi dağıtılmış pariteler kullanır. RAID 5'ten farkı, iki ayrı parite bilgisi kullanarak iki diski tolere etmesidir. RAID 6 oldukça yüksek oranda hata toleransı sunar ve birden fazla diskte eş zamanlı olarak ortaya çıkabilecek hataları ya da arızaları karşılayarak sistemin kararlı bir şekilde çalışmaya devam etmesini sağlar. Okuma hızı çok iyidir, ancak yazma hızı çift parite kullanıldığından RAID 5'e göre daha kötüdür.



2.2.1.2. Dâhili Depolama Türleri

Doğrudan Bağlı Depolama (Direct Access Storage-DAS): Genellikle aralarında bir ağ olmadan bir sunucuya veya iş istasyonuna bir ana bilgisayar veri yolu adaptörü aracılığıyla doğrudan bağlanan bir veri depolama cihazından (bir veya birkaç sabit disk sürücüsü) oluşan düşük maliyetli bir depolama sistemidir.

Ağa Bağlı Depolama (Network Attached Storage-NAS): Bir ağa bağlı olan ve atanmış bir ağ adresi aracılığıyla erişilen özel bir depolama cihazıdır. NAS tabanlı sistemler, birden çok bilgisayarda veri depolamayı kolaylaştırmak için kullanılır, yani bilgiye ağdaki herhangi bir makineden veya internet üzerinden erişilebilir.

Depolama Alan Ağı (Storage Area Network-SAN): Sunucular ve depolama cihazları arasında blok düzeyinde veri aktarımı sağlayan özel, yüksek performanslı bir depolama sistemidir. NAS tabanlı depolamaların esnekliği ve güvenilirliği ile DAS hızlarında dosya paylaşımı sunar.

Yedekleme teknolojileri farklı olsa bile ikincil bir depolama aygıtı kullanılabilir. Bu ikincil depolama ortamları taşınabilir medyalar (teyp, CD – DVD) veya yerel ya da uzak disklerdir. Uzak depolama sistemlerinin yerleri ve sayısı verinin erişilebilirlik ihtiyacına ve işletmenin risk iştahına göre belirlenir. Alınan yedeklerin sınıflandırılmaları ve bakımları manuel ya da yedekleme çözümleri ile otomatik yapılır. Veri miktarı arttıkça yedekleme sürecinin manuel yürütülmesi operasyonel risklerin de doğmasına neden olur, bu nedenle işletmeler süreç ilerledikçe entegre yedekleme ve kurtarma çözümlerinin konumlandırılmasını düşünebilir.

Herhangi bir olağanüstü durum gerçekleştiğinde ya da verinin gün içinde canlı sistemden bağımsız bir eşleniğine ihtiyaç duyulduğunda yedekleme sistemleri verinin yedek kopyasının tutulduğu tek yerdir. Bu verilerin bütünlüğünü garanti etmek için hem fiziksel hem de mantıksal veriler üzerinde katı kontroller uygulamak gerekir. Bu verilere (yerinde ya da taşıma halinde) izinsiz erişim, kayıp ya da bütünlüğünün bozulması işletmenin geleceğini riske atabilir.

Veri yedeklerinin tutulduğu alanlar ve veriler üzerinde uygulanan kontroller aşağıdakileri içerir:

- Yedeklerin tutulduğu ortamlara fiziksel erişimi güvenli hale getirerek sadece yetkili personelin erişmesini sağlamak,
- Yedekleri aktarım esnasında ve sonrasında şifreleyerek gizliliğini sağlamak,
- Yedeklerin tutulduğu ortamların çevresel risklere karşı güvenliğini temin etmek,

- Asıl veri ile yedek verinin tutulduğu bölgelerin coğrafi yedekliliği de sağladığından emin olmak,
- Yedek verilerin belirlenen saklama süreleri içerisinde muhafaza edildiğini garanti etmek,
- Belirtilen saklama süreleri boyunca yedek verinin sürüm ve konum bilgilerini içeren envanter kaydının ve sonrasında envanter dışına çıkartılma sürecinin işletildiğini garanti etmek,
- Varsa düzenlemeler kapsamında talep edilen gerekliliklerin de sağlandığını garanti etmek.

2.2.1.3. Yedekleme Teknolojisi Seçimi

İşletmeler yedekleme teknolojisini ve yedeklenecek medyaları aşağıdaki kriterlere göre seçmelidir:

- **Standartlaştırma –** İşletmeler iştirak yapılarında ya da çok lokasyonlu olabilir. Mevcut yapı değerlendirildiğinde içeride kullanılan en iyi çözüm tüm alt işletmeler ya da lokasyonlarda da standart olarak kullanılabilir ya da seçilecek yeni bir teknoloji mevcut iştirak ve lokasyonlar için de uygulanacak şekilde standartlaşmaya gidilebilir. Böyle durumlarda standartlaşmanın getireceği olumlu etkilerin yanında daha fazla destek ve maliyetlerde artış gibi olumsuz etkileri de olabilir.
- **Kapasite –** Verinin sürekliliğini sağlamak için mevcut kapasitenin en az iki katı kadar saklama alanına ihtiyaç duyulmasıdır. İşletmeler veri büyüdükçe verinin tekilleştirilmesi ve yedekleme sıklıklarının yeniden düzenlenmesi gibi iyileştirmelere yönelir.
- **Hız –** Yedekleme yapılan sistemin işlevi (örneğin veri tabanları) ya da verinin kabul edilebilir kesinti süresi dikkate alınır.
- **Maliyet –** Yedekleme sistemleri, lisans ve disk ihtiyaçları, replikasyon hatları, personel maliyetleri göz önüne alınır.

2.2.1.4. Yedekleme İşlemleri

Hem veri hem de uygulama dosyaları, tanımlanan kurtarma noktası hedefi (RPO) değerine göre periyodik olarak yedeklenmelidir. Yedeklemenin planlanacağı zaman, verinin değişim sıklığına ya da uygulamanın yapılandırmasının değiştiği durumlara göre belirlenir. Periyodik yedeklemelerin planlanması genellikle entegre yedekleme sistemi ile kolayca gerçekleştirilir. Bu tür otomatize araçlar kullanmak manuel süreçlerde karşılaşılacak olası operatör hatalarını engelleyerek hatalı/eksik yedekleme riskini azaltır.

Verinin Yedekleme Sıklığının Belirlenmesi

Veri ve uygulamaların yedeklenmesi, verinin sürekliliği ve işletmenin devamı için hayati önemdedir. Yedekleme zamanlarının belirlenmesi için aşağıdaki hususlar dikkate alınır:

- Her uygulama için yedekleme döngüsü ve saklama süresi, ayrı ayrı uygulama bazında tanımlanan RPO değerine göre belirlenmelidir.
- Yedekleme döngüsünün herhangi bir anında hata olabileceği öngörülmelidir.
- Uygulama dosyalarının yedekleri canlı sistemin sürümlerini takip etmelidir.
- Yedekleme, işletmenin risk iştahına göre alternatif zamanları da içerebilir.

Yedekten Geri Dönme

Veriyi geri döndürme için çeşitli yaklaşımlar olmasına rağmen en çok rağbet edilen yöntemlerden birisi Büyükbaba – Baba – Oğul yöntemi olarak adlandırılmaktadır. Bu yöntemde bir hafta boyunca günlük yedeklemeler (Oğul) yapılır. Hafta sonu alınan son yedekleme o haftanın yedeği olur (Baba). Daha önce günlük alınan yedek, ikinci hafta içinde yedeklemede kullanılır. Ayın sonunda alınan haftalık yedek de o ayın yedeği olarak tutulur (Büyükbaba). Yıl sonunda nihai alınan aylık yedekle de yıl yedeği olur.

	PAZARTESİ	SALI	ÇARŞAMBA	PERŞEMBE	CUMA
H1	O	O	O	O	B
H2	O	O	O	O	B
H3	O	O	O	O	B
H4	O	O	O	O	BB

O	Oğul
B	Baba
BB	Büyükbaba

Alınan yedeklerin doğruluğunu ve bütünlüğünü test etmek için belirli dönemlerde yedekten geri dönüş testleri planlanmalıdır. Tüm testler ön test, test ve son test raporlarıyla tam olarak belgelenmelidir. Yedekten geri dönüş testlerinde verinin rotasyonuna da mutlaka dikkat edilmelidir. Örneğin 1. haftanın yedeğinin geri dönüş testinde kullanılabilmesi için ay sonunda alınacak yedeğin güvenli bir şekilde alındığının garanti edilmesi beklenmelidir.

2.2.2. Sürekli İyileştirme

Sürekli iyileştirme, bir sürecin zamanını ve maliyetini minimize ederken istikrarını maksimize etmeye yönelik yapılan faaliyetler bütünüdür. Sürekli iyileştirme bir program olarak algılanmamalıdır. Çünkü programların bir başlangıç ve bitiş zamanları bulunur. Bu durum oluşturulmak istenen değişim ile doğrudan çatışmaktadır.

Planla-Uygula-Kontrol Et-Önlem Al (PUKÖ) Döngüsü

Sürekli iyileştirme faaliyetlerinde çeşitli tekniklerden yararlanılır, bunlardan biri de PUKÖ(PDCA) döngüsüdür. PUKÖ kısaltması; Planla, Uygula, Kontrol et ve Önlem al sözcüklerinin baş harflerinden oluşur.

PUKÖ Döngüsü, Walter Shewhart tarafından "sürekli iyileştirme" çalışmaları için 1939 yılında yazmış olduğu "*Statistical Method From the Viewpoint of Quality Control*" isimli kitabında belirtilmiştir. Daha sonra Edwards Deming döngüde bazı değişiklikler yapmış ve modeli günümüzdeki PUKÖ Döngüsü haline getirmiştir.

Deming'in kalite yönetim çemberi, aşağıdaki adımlara bağlı kalınarak sunulan uygun kalite seviyeleriyle sürekli iyileştirme sistemini önermiştir.

Planla: Bu aşama çözülmesi gereken problemin analiz edildiği aşamadır. Sırasıyla şu adımlar uygulanır;

- Problem tanımlanır.
- Hedefler belirlenir.
- Kullanılacak yöntemler seçilir.
- Şu soru tekrar tekrar sorulur ve eksiksiz bir cevap verilmesi beklenir: "Bu problem neden ortaya çıktı?"
- Kimin hangi işi hangi kaynakla, ne zaman yapacağı belirlenir.

Uygula: Bu aşama, bir önceki adımda planlanan faaliyetlerin gerçekleştirildiği, yapılan planların hayata geçirildiği aşamadır.

- Yöntemler uygulamaya alınır ve gerçekleştirilir.
- Değişiklikler yapılır.
- Mükemmel olması için fazladan çaba sarf etmeye gerek yoktur. Daha pratik olarak neler yapılabileceği araştırılmalıdır.
- Sonuçlar değerlendirilip kaydedilir.

Kontrol Et: Döngünün en önemli aşamalarından biridir. Bu aşamadan sonra eylemlerin gelişip gelişmediği görülecektir.

- Standartlara uyulup uyulmadığı kontrol edilir.

- Nelerin çalışıp nelerin çalışmadığı kontrol edilir.
- Ve her adımda 'Neden?' sorusu sorulur.
- Alınan cevaplara göre, tanımlanmış olan yöntemde geliştirmeler yapılır.

Önlem Al: Döngünün son aşamasıdır. Bu aşamanın sonunda döngüye yeniden başlanılması önerilir ve böylelikle sürekli ve kesintisiz iyileştirme sağlanmış olur.

- İşler planlandığı gibiyse devam edilir.
- Herhangi bir sorun varsa bunları engellemek için harekete geçilir.
- Çalışma sistemi geliştirilir.
- Çalışan çözümler tekrar edilir.

Sürekli iyileştirme sürecinde planlanan faaliyetlerin gerçekten ölçülebilir iyileştirmeler üretip üretmediğini kontrol etmek amacıyla çeşitli yöntemler ve teknikler bulunmaktadır. Bunlar:

- **Uygulamanın gözden geçirilmesi:** İyileştirmelerin arzulanan etkileri üretip üretmediği değerlendirilir.
- **Değerlendirme:** Bir süreç ya da organizasyonun performansı, hizmet seviyesi anlaşması ya da olgunluk standardı gibi bir performans standardıyla karşılaştırır.
- **Kıyaslama:** Özel bir değerlendirme tipidir. Organizasyon süreçlerini yaygın biçimde "en iyi uygulama" olarak kabul edilen aynı tip uygulamaların ya da süreçlerin performansıyla kıyaslar.
- **Boşluk analizi:** Organizasyonun şu anda nerede olduğunu ve olmak istediği yerle arasındaki boşluğun büyüklüğünü belirler.
- **Dengelenmiş skor kartı (balanced scorecard):** Organizasyonel performans üzerine dört farklı bakış açısı içerir. Müşteri, süreçler, büyüme ve öğrenme, finansal değerler.
- **Swot analizi:** Bir organizasyonun ya da bileşenin güçlü yönlerini ve zayıflıklarını, fırsatlarını ve tehditlerini değerlendiren analizdir.
- **Rummler-branche-swim-lane diyagramı:** Süreçler, organizasyonlar ya da birimler arasındaki ilişkileri, sorumluluk hakları ile görselleştirir.

2.2.3. Kapasite Yönetimi

Kapasite Yönetimi'nin amacı, BS altyapısının mevcut durumunu ve gelecekte oluşacak ihtiyaçları karşılayacak şekilde gereksinim analizi yapılması ve BS hizmetlerinin kapasitesini etkin maliyetler içerisinde kullanmaktır. ITIL'e göre, kapasite yönetiminin kilit faaliyetleri aşağıdaki gibidir:

- **Performans İzleme:** Performans ölçümleri, eşikler, işlem hacmi.
- **Ayarlama:** Mevcut kaynakları optimize etmek.
- **Planlama:** İşletme faaliyetlerine paralel olarak altyapı gereksinimlerini tanımlamak için kapasite yönetimi yapmak.
- **Politika tanımlama:** Sistem operasyonlarının tespiti ve kısıtlamaları tanımlama.
- **Talep Yönetimi:** Mevcut ve gelecekte ortaya çıkacak kaynak taleplerini anlamak. Kapasite yönetimi BS hizmet sunumu potansiyelini anlamakla ilgili bir durumdur. Bu nedenle yeni teknolojilere geçiş için öncelikle mevcut sunulan hizmetin işin gerektirdiği kapasiteye sahip olup olmadığı, maliyet etkin ve optimum kullanım prensiplerinin işletilmiş olması gibi politikaların işletmelerde kabul gördüğünü unutmamak gerekir. İlk hedef mutlaka mevcut kaynaklardan en etkin şekilde yararlanıldığını garanti etmek olmalıdır.

Kapasite Yönetiminin işlem adımları aşağıdaki gibidir:

- **Talep Yönetimi:** BS altyapısı kapasitesinin işletmenin ortaya çıkan talepleriyle maliyet açısından en etkili biçimde ve zamanında eşleşmesini sağlamak BS ekiplerinin sorumluluğundadır. Kapasite Yönetimi belki finans yönetimi ile kaynak talebini de etkileyebilir. Kapasite Yönetimi her zaman maliyete karşılık kapasite dengesini tutturmaya çalışır. Örneğin:

  - Satın alınan işletme kapasitesinin, sadece işletmenin ihtiyaçları bakımından değil aynı zamanda o kaynakların en verimli biçimde kullanılması ve talebe karşılık arz edilmesi ihtiyacı bakımından da maliyet açısından haklı çıkarılabilir olmasını sağlama ihtiyacı,

  - Kullanılabilir işletme gücü arzının işletmenin hem şimdiki hem de ileride bu konuda göstereceği talebe uygun olmasını sağlamak. Belirli bir kaynağa olan talebi yönetmek ya da etkilemek de gerekli olabilir.

- **Talebi İzlemek:** BS hizmetlerinin ve onu destekleyen altyapı bileşenlerinin performansının ve işlem hacminin tutarlı ve devam eden bir temelde izlenmesi ve rapor edilmesidir.

- **Ayarlama:** Mevcut kaynakların en verimli biçimde kullanılması için gerekli ayarlama faaliyetlerinin yerine getirilmesidir.

- **Analiz Etme:** Mevcut BS kaynaklarına olan talebi anlamak için performans yönetimi, kaynak yönetimi, iş yükü yönetimi, talep yönetimi gibi süreçlerden girdi alınması, gelecekte ortaya çıkacak gereklilik için tahminde bulunulmasıdır.

- **Yeni Hizmetler:** BS hizmet tedarikçilerinin hizmet seviyesi anlaşmalarında tanımlanan kalitede hizmet sunmasını sağlamak için yıllık kapasite planının icra edilmesidir.

Şu ana kadar yapılan anlatımdan Kapasite Yönetiminin, içerisinde çeşitli faaliyetler olan ve çok sayıda alt süreçten oluştuğu anlaşılmaktadır. Kapasite Yönetim Sürecinin alt süreçleri aşağıdaki gibidir:

- **İş Kapasite Yönetimi:** Bu alt süreç, BS hizmetleri için gelecekte ortaya çıkacak iş gereksinimlerinin zamanında göz önünde bulundurulmasını, planlanmasını ve uygulanmasını sağlamaktadır. İyi bir zamanlamayla gelecekte ortaya çıkacak gereklilikleri tahmin etmek ve modellemek için, mevcut kaynak kullanımı verisi analiz edilir. Gelecekte ortaya çıkacak gereksinimler ise yeni hizmetlere ve mevcut sistemlerde ihtiyaç duyulan iyileştirmelere ya da büyüme trendlerine göre belirlenir. Bu tür stratejik kararlarda mutlaka tüm birimlerin faaliyetlerine göre ihtiyaçlarını analiz etmek elzemdir.

- **Hizmet Kapasite Yönetimi:** Bu alt sürecin ana odağı, son kullanıcıların günlük faaliyetlerini icra etmek için kullandıkları canlı, operasyonel BS hizmetlerinin performansının yönetilmesidir. Bu alt süreç tek tek alt yapı bileşenlerinden çok uçtan uca hizmetlere odaklanır. BS burada, tek tek altyapı bileşenlerini incelemeden önce işletme ihtiyaçlarını belirlemek için hizmete bir bütün olarak bakmak zorundadır. Hizmet Kapasite Yönetimi sürecinde BT ekipleri bu tür stratejik kararları iş birimleri ile almak zorundadır.

- **Kaynak Kapasite Yönetimi:** Bu alt sürecin odak noktası ise BS altyapısının tek tek bileşenlerinin yönetimidir. Bu en temel geleneksel BS bakış açısıdır ve belirli bir hizmeti destekleyen bütün BS bileşenlerinin yakından izlenmesinden, ölçülmesinden ve hizmet kapasitesi gerekliliklerini iyileştirmek için sürekli olarak uygulamalar yapılmasından sorumludur. Yine, yapısal ve yukarıdan aşağıya bir Kapasite Yönetimi yaklaşımı daha iyi bir iş uyumunu garanti eder ve kapasite yatırımlarının önceliklendirilmesinin işletmenin ihtiyaçlarına dayanmasını sağlar.

Farklı disiplinlere ait olsalar bile her tür sürecin gözden geçirilmesi ile ilgili analizin öncelikle mevcut durumun analiz edilmesi ile başladığını unutmamak gerekir.

Kapasite Yönetiminin Süreçlerini detaylandırmak gerekirse:

Talebi İzleme

Talebi izleme, kullanıcıların kapasite taleplerini desteklemek için mevcut kapasite konusunda şu anda nerede olduğumuzu anlamakla ilgilidir. Kapasite talep seviyelerini izlemek, bize kaç

kullanıcının kaynaklarımızı nasıl etkilediği hakkında bilgi verebilir. Böylece BS ortamına sürülecek yeni hizmetlerin nasıl destekleneceğini ve Hizmet Seviyesi Anlaşmalarının nasıl etkileneceği ile ilgili gerçekçi tahminlerde bulunulabilir. Talep izleme faaliyetlerini yürütmek önemlidir çünkü işletmeye etkili kararlar alınması ile ilgili yardımcı olabileceğimiz verileri toplamamızı sağlar.

Donanım ve yazılım kaynaklarının en uygun biçimde kullanılmasını, kararlaştırılmış hizmet seviyelerine ulaşılabilmesini ve iş hacimlerinin beklendiği gibi olmasını sağlamak için her bir kaynağın ve hizmetin kullanımı sürekli olarak izlenir. Kapasite Yönetiminin izleme faaliyetlerinde aşağıdakiler izlenebilir:

- CPU ve bellek kullanımı
- I/O oranları
- Aygıt kullanımı
- Depolama kullanımı
- İşlem oranı
- Paket kaybı
- Cevap süresi
- Bant genişliği kullanımı

İzlenen veri, örneğin CPU; kullanımı ya da işlem yanıt sürelerini içerebilir ancak kapasitenin yönetilmesi (işlem hacmi) etrafında toplanan bilgiyle performansı izlemek için gerekli veri arasında (yanıt süresi) fark olduğunu unutmamak gerekir. İş kararları her ikisinin de anlaşılması ile alınır.

Analiz Etme

Mevcut talebin izlenmesinden toplanan verinin, normal kullanımın ya da hizmet seviyesi ya da referans alınacak bilgilerin oluşturulabileceği eğilimlerin analiz edilmesidir.

Kapasite Yönetimi için bazı kilit ölçütler aşağıdaki gibidir:

- İş yükü ya da uygulamaya göre işlem sayısı
- Nispi kaynak kullanımı
- Saniyede minimum / maksimum işlem sayısı
- Online yanıtlama süresi ve eğilimleri
- Kullanım istatistikleri
- İşletmeninin kullanım eğilimleri
- İşlemci ve I/O kullanım eğilimleri
- Ağ kullanım eğilimleri
- İş yükü eğilimleri ve tahminleri
- Büyüme tahminleri

Bu verilerin analiz edilmesi, eğilimlerin ortaya çıkmasına olanak sağlar. ITIL Problem Yönetimi sürecinden gelen neyin "normal" kabul edilmesi gerektiğini anlamamızı sağlar ve "normal" den her türlü sapmayı karşılaştırmak için bir referans görevi görür. Beklenen kullanım seviyelerinden, eşiklerden ya da yanıtlama sürelerinden her türlü sapma anında tespit edilebilir ve buna göre aksiyon alınır. Kapasitenin izlenmesinin ve analizin en katma değerli yanı, gelecekteki davranışları tahmin edebilmede kullanılmasıdır. Teknoloji, gelecekteki kaynak kullanımını tahmin ederek ve fiili iş büyümesini tahmini büyümeyle karşılaştırıp izleyerek yardımcı olabilir. Analiz edilen bilgiyle, performansı iyileştirmek ya da sistem kaynaklarını daha verimli kullanmak üzere kararlar alınabilir.

Performansı İzleme

Hizmet Seviyesi Anlaşmaları genellikle beklenen yanıtlama sürelerini, özellikle de kullanıcının hizmetin geri yüklenmesi, eskalasyon ve çözümleme için beklediği yanıtlama sürelerini referans aldığından Hizmet Seviyesi Yönetimi sürecinin çıktıları kullanılır. Performansı izlemek içinse destekleyici izleme yazılımları, ağ izleme sistemleri gibi birden fazla katman için çözümler kullanılabilir.

Tahmin Etme

Tahmin faaliyetleri işletmenin gelecekteki büyümeyi öngörmesine ve buna göre kapasite planlaması yapmasına imkân verir. Bu, teknolojiye bağlı olarak çeşitli şekillerde yapılabilir. Örneğin bir işletme bir hizmetin web tabanlı kullanıcılarının sayısını iki katına çıkartmaya karar verdiğinde mevcut veri ve büyüme biçimlerine dayanan yeni kullanım oranlarıyla ilişkili maliyetleri çıkartabilir. Kapasite ile ilgili tahmin, kaynakların artırılması gerektiği sonucunu veriyorsa bu artık BS bütçe döngüsüne bir girdi haline gelir. Beklenen hizmet seviyelerinin izlenmesi ve analiz edilmesi, kapasite planlaması sadece mevcut duruma bakılarak yapılmaz. Kullanılabilecek tahmin teknikleri aşağıdaki gibidir:

- Ayarlama: İzlenen verinin analizi, sistem kaynağının daha etkin kullanılması ya da belirli bir hizmetin performansının artırılması için ayarlanabilecek yapılandırma ayarlarının tespit edilmesidir.

- Uygulama: İzleme, analiz ve ayarlama faaliyetleriyle tespit edilmiş olan her türlü değişikliğin canlı ortama alınmasıdır.

- Kapasite Yönetim Verisinin Saklanması: Diğer süreç ve alt süreçlerde iş, hizmet, teknik, finansal ve kullanım verilerinin belli süreler saklanmasıdır.

- Modelleme: BS hizmetlerinin belirli bir iş hacmi ve çeşitliliği altında davranışlarının öngörülmesidir.

- Uygulama Büyüklüğü: Uygulama büyüklüğünün birincil amacı, kendisi için gerekli olan hizmet seviyelerini karşılaştırmak amacıyla önerilen bir uygulama değişikliğinin ya da yeni bir uygulamayı desteklemek için gerekli olan kaynağın tahmin edilmesidir.

Satın Alma

Kapasite Yönetimi işletmeye, hangi bileşenlerin yükseltileceği ve gelecekte ortaya çıkacak kapasite gereksinimlerini desteklemek için yeni donanımın ne zaman alınacağı gibi finansal kararları almak için ihtiyaç duyduğu bilgiyi sağlar. BS önerilen çözümlerin maliyetlerini elde eder ve işletme bu bilgiye dayanarak "satın almaya ya da almamaya" karar verir.

Yük Testi

Bütün uygulamalar eşzamanlı ve "tam yük" olarak belirlenen işlem seviyesinde çalıştığında işlerin kesintiye uğramadan devam etmesini sağlamak için yürütülen faaliyettir.

Ayarlama

Yeni hizmetler devreye alındıktan sonra ya da mevcut hizmetlerde kullanılan sistemlere belli dönemlerde yapılan optimizasyon çalışmasıdır.

2.2.3.1. Kapasite Yönetiminin Faydaları

Kapasite Yönetimi sürecinin ana hedefi, kullanıcılara/müşterilere kararlaştırılmış seviyelerde hizmet sağlamak için yeterli BS kapasitesinin var olduğunun garanti edilmesidir. Kapasite Yönetiminin faydaları aşağıdakileri içerir:

- Doğru zamanda doğru şeylere para harcanması,
- Var olan sistemlerin bütçe içerisinde verimli bir şekilde kullanılması,
- Olayları ve problemleri azaltmak için sistemlerin proaktif bir şekilde yönetilmesi,
- Artan müşteri tahmini yapılması,

- Tahmin etme becerisinin gelişmesi.

2.2.3.2. Kapasite Yönetiminde Karşılaşılabilecek Problemler

- İşletmede resmi olmayan ya da olgunlaşmamış hizmet yönetim süreçlerinin varlığı ve bunların çıktılarının Kapasite Yönetiminin temel girdileri olması,
- Temelde Kapasite Yöneticisi gibi ayrı bir rol tarafından yürütülmesi tavsiye edilen sürecin kadro eksikliği gibi organizasyonel dinamikler nedeniyle sahipsiz kalması,
- Süreç sahibi tayin edilse bile o kişinin amacına ulaşabilmesi için uygun yetki ve izin seviyelerine sahip olmaması (Kapasite Yönetimi tüm seviyelerde BS süreçleri için tasarlanır),
- Süreci destekleyecek doğru uzmanlık ya da teknolojinin seçilmemesi,
- Mevcut kapasite seviyelerinin baştan "iyi" kabul edilmesi ile sürecin gerekçelerinin kalmaması,
- Kapsam tanımının doğru yapılamaması. Çok büyük kapsam belirlemek süreci işlemez hale getirebilir.

2.2.4. Kullanılabilirlik Yönetimi

Kullanılabilirlik Yönetiminin amacı, işletmenin amaçlarına ulaşmasına imkân sağlayan, maliyet açısından verimli ve tanımlanmış hizmet seviyesinde bir kullanılabilirlik sağlamaktır. Bu süreç; teknoloji, insan, kaynak planlama ve uygulamalar aracılığıyla sağlanabilir. Bu yönetim işletmeye aşağıdaki faydaları sağlar:

- Arıza süresi ve maliyetlerin azalması,
- Sistemlerin, işletmenin kullanılabilirlik hedefine göre yönetilmesi,
- İşletmenin çekirdek operasyonları için artan destek seviyesi,
- Bilgi sistemleri için tepkisel destek seviyesinde azalma.

Kullanılabilirlik Yönetiminin anahtar faaliyetleri:

- İzleme
- Etki hesaplama
- Analiz etme
- Esneklik ve güvenliği sağlama

Kullanılabilirlik Yönetimi, BS hizmetleri ve altyapı bileşenlerinin genel kullanılabilirliğini iyileştirmeyi, her türlü düzeltmeyi hızlıca tespit etmeyi ve aksiyon almayı hedefleyen proaktif bir kullanılabilirlik planı oluşturmalı ve bunu sürdürebilmelidir.

2.2.4.1. İzleme

Kullanılabilirlik Yönetimi, BS hizmet kullanılabilirliğinin o anki durumunu izleyerek başlar. Bu aşama; izlenmesi gereken altyapı ve bileşenlerin belirlenmesi, bir izleme planının oluşturulması ve uygun izleme araçlarının belirlenmesi ile devam eder. Bu aşamadaki temel görevler, aşağıda adı geçen temel altyapı kullanılabilirliği ölçülerinin toplanması ve izlenmesini içerir:

- **Kullanılabilirlik:** Belirli zaman dilimindeki toplam kesinti süresi.
- **Güvenilirlik:** Kesintinin süresi**.**
- **Sürdürülebilirlik:** Organizasyonun BS hizmetlerini çalışabilir durumda tutabilmesi.
- **Kullanışlılık:** Sürdürülebilirliğe benzer ancak harici sistemlerin izlenmesini de kapsar.

Kullanılabilirlik Yönetiminin izleme aşamasında Hizmet Yönetimi Anlaşmalarını doğrulayabilecek, sorun yaşanan alanları tespit edebilecek ve kullanılabilirliği iyileştirmek için öneriler sunabilecek şekilde, olabildiğince bilgiyi ölçmek kritiktir. İdeal bir BS Hizmet Yönetimi, süreç ortamının sürekli izlenmesini ve rapor edilmesini gerektirir.

2.2.4.2. Etki Hesaplama

En iyi donanımda bile operasyonel altyapı içinde normal hizmetlerden sapmalarla sonuçlanan sistem ve yazılım sorunları yaşanabilir. İzleme faaliyetlerinde kullanılabilirliği anlayıp ölçümleyebildiğimizde, bir sonraki adım her türlü kesintiyi BS hizmetleri ile uyumlu hale getirmek ve kesintinin etkisini kayıt altına almaktır. Kesinti ya da kullanılamamanın etkisi, kullanılabilirlik problemlerine neden olan altyapı bileşenlerini tespit etmemize imkân tanır ve fazladan maliyete, planlanmamış harcamaya ve tedarikçilerin faturalandırdığı ek maliyetlere maruz kalınabilecek yerleri anlamamıza yardım eder. Genelde Kullanılabilirlik Yönetimi içinde tedarikçilerin yönetilmesi gözden kaçabilir. Tedarikçi ilişkileri ilgili Hizmet Seviyesi Anlaşmalarını (SLA) mutlaka içermelidir çünkü hizmetin tam kullanılabilirliğinin yönetilmesi ve kullanılamamasının yarattığı etkinin anlaşılması bu değerler ile mümkün olabilir.

2.2.4.3. Analiz

İyileştirme yapılacak alanları tespit etmek ve değerlendirmek için o anki verinin tespit edilmesi, analizi ve yönetilmesi hayati önemdedir. BS organizasyonlarının geleneksel olarak bu tür analizler için ayrı kadroları bulunmaz ama mevcut kadrolar bu süreç için yeterli bilgi birikimine sahiptir. Yapısal bir analiz yaparken amaç, sağlanan hizmetler ve bileşenler hakkında uygun bilgiyle bir kullanılabilirlik matrisi oluşturmaktır.

Kullanılabilirlik matrisini oluşturmak için geniş bir yöntem ve teknoloji spektrumu mevcuttur:

- **Bileşen Başarısızlık Etki Analizi (CFIA):** Önemli bileşenlerin ve her hizmet içindeki rollerinin tespit edilmesinde kullanılabilir.
- **Hata Ağaç Analizi (FTA):** Başarısızlığa neden olan olaylar zincirinin tespit edilmesinde kullanılabilir.
- **CCTA Risk Analizi ve Yönetim Yöntemi (CRAMM):** BS hizmetlerini performans ve güvenlik ihlallerine karşı korumak amacıyla, doğrulanabilir karşı ölçümleri tespit etmek için gerekli araçları sağlar.
- **Hizmet Kesintisi Analizi (SOA):** Hataların nedenlerini tespit etmek, BS organizasyonlarının verimliliğini araştırmak ve iyileştirme önerileri (RFC) için kullanılan bir tekniktir. Bu çıktıları sağlayabilen organizasyonların belli bir hizmet seviyesi olgunluğunda olduğu kabulü bile yapılabilir.
- **Teknik Gözlem Mevki (TOP):** Rutin uygulamaların verdiği bilgi yetersiz olduğunda, kullanılabilirliğin tek bir yönünü araştırarak sadece bu işle ilgilenen BS uzmanları ile çalışmaya dayanır.

Bu yöntemler, müşteri ile kararlaştırılmış ilgili BS hizmeti için Hizmet Seviyesi Anlaşmasına dâhil edilecek hizmet kullanılabilirlik anlaşmalarında girdi olarak kullanılabilen ve önceden tanımlanmış ölçülere dayanarak yapılacak kullanılabilirlik hesaplamalarına girdi sağlayabilir.

2.2.4.4. Esneklik ve Güvenlik

Günümüzde, kullanıcılar BS hizmet kesintilerinden etkilenmeden önce hizmetteki değişimleri tespit eden ve sistemlerin esnek olmasını sağlayan araçlar ve en iyi uygulamalar mevcuttur. Kullanılabilirlik Yönetiminin amacı, sürdürülebilir hizmetleri desteklemek için güvenli bir ortam oluşturmak amacıyla izleme ve analizden gelen bilgiyi yukarı taşımaktır. Bunu yaparken güvenlik ve güvenilirliğin yakından ilişkili olduğunu anlamak önemlidir.

2.2.4.5. Çıktıların İyileştirilmesi

Başarılı bir Kullanılabilirlik Yönetimi, işletmenin kullanılabilirlik amaçlarının ve hizmet gerekliliğinin açıkça tanımlamasına bağlıdır. Kullanılabilirlik Yönetimi sürecinin optimize edilmesi ancak Hizmet Seviyesi Yönetimiyle entegrasyonu ile mümkündür. Kullanılabilirlik Yönetiminin optimize edilmesi Hizmet Seviyesi Anlaşmalarının kullanılabilirlik bileşenleriyle tanımlanmasını kapsamalıdır çünkü Hizmet Seviyesi Yönetimi, BS ve BS'nin müşterileri arasındaki ilişkiyi biçimlendirmeye hizmet edecek ve bu sayede BS hizmetlerinin kullanılabilirliğinin faydalarını ortaya koyacaktır.

2.2.4.6. Karşılaşılabilecek Problemler

Kullanılabilirlik Yönetiminde en yaygın bariyerler şunlardır:

- Algı: "Sistemlerin" kullanılabilirlik seviyesiyle "hizmetlerin" kullanılabilirlik seviyesi arasında bir fark vardır ve bu genellikle yanlış anlaşılır. Örneğin mail sisteminin kullanılabilirliğinin %98, işletim sisteminin kullanılabilirlik oranının %99 olduğu işletmeye raporlanabilir. Bununla birlikte "çıktı hizmetinin" kullanılabilirliği %80 ise işletmenin algısı BS'nin gerekli kullanılabilirlik seviyesini sağlayamadığı ve çıktı hizmetinin şirket dışından bir kaynağa yaptırılması şeklinde olabilir.

- Uygun kullanılabilirlik ölçümleri işletmeye sunulmalıdır ve bunlar sadece ham BS kullanılabilirlik verileri olmamalıdır.

- Özellikle Olay Yönetimi, Problem Yönetimi ve Değişiklik Yönetimi gibi disiplinler uygulandığında, Kullanılabilirlik Yönetiminin kayda değer bir iyileştirmeyi nasıl sağlayacağı daha büyük bir resme bakılmadan anlaşılamayabilir.

- Proje başlangıcında tespit edilen mevcut kullanılabilirlik seviyelerinin yönetim tarafından "kabul edilebilir" görülerek ilerleme sağlanamayabilir.

- BS personeli BS Kullanılabilirlik yönetimine direnç gösterebilir veya genel bir sorumlu rolü tayin edilemeyebilir.

Değerlendirme Soruları

Soru 1: Bir BS Denetçisinin yedekleme ve yedekten geri dönüşle ilgili sürecin denetiminde, aşağıdakilerin hangisi denetimin kapsamına girmez?

I - İşletmenin tabii olduğu regülasyonlar

II - İşletmenin risk kabulleri

III - Kullanılan RAID Seviyesi

IV - Cari dönemde sürece ait süreç çıktılar

A) Yalnız I

B) I ve II

C) Yalnız III

D) III ve IV

E) Hepsi

Cevap: C

Soru 2: Aşağıdakilerden hangisi, veri yedeklerinin tutulduğu alanlar ve veriler üzerinde uygulanan kontrollerden birisi değildir?

A) Verilerin gizliliğinin sağlanması

B) Verilerin tutulduğu yerlere ait fiziksel kontroller

C) Verilerin bütünlüğünü sağlanması

D) Yedeklerin belirtilen saklama sürelerinin içerisinde olması

E) Yedekten geri dönüş süreleri

Cevap: E

Soru 3: Bir BS Denetçisi, Kapasite Yönetim Sürecinin denetimi kapsamında işletmenin analiz sürecinde aşağıdaki hangi girdiler ile karşılaşabilir?

I - İşlemci ve I/O kullanım eğilimleri

II - İş yükü ya da uygulamaya göre işlem sayısı

III - Büyüme tahminleri

A) Yalnız I

B) Yalnız II

C) I ve III

D) II ve III

E) Hepsi

Cevap: E

Soru 4: Bir BS Denetçisi, Kullanılabilirlik Yönetim Sürecinin işletmede etkin olarak uygulandığını görmek için aşağıdaki çıktılardan hangisinden faydalanmaz?

A) Altyapı ve sistem bileşenlerinin izlenme istatistikleri

B) Hizmet kesinti analiz raporları

C) Hata ağaç analizleri

D) Tedarikçi SLA Raporları

E) Büyüme analiz raporu

Cevap: E

Soru 5: Bir BS Denetçisi, BS Operasyonları ile ilgili denetimde işletmenin yedekten geri dönüş testlerini her ayın 3. haftası rastgele sistemler üzerinde ilgili ayın ilk haftası alınan tam yedeği kullanarak düzenli olarak prosedürüne uygun gerçekleştirdiğini görmüştür. Bu süreçte nasıl bir tespit söz konusudur?

A) Yedeğin bütünlüğünün bozulması

B) Yedeğin rotasyonu nedeniyle riskli işlem yapılması

C) Yedeklemenin sırasının bozulması

D) Yedekleme sürecinin yetersizliği

E) Canlı sistem sürümünün değişmesi

Cevap: B

3. BİLGİ SİSTEMLERİ SÜREKLİLİĞİ

3.1. Bilgi Sistemleri Sürekliliği Kavramları

Bilgi, bir işletmenin en değerli varlığı olarak kabul edilir ve modern çağda işletmeler, işlerini bilgi sistemlerini kullanarak işlenen bilgiye dayalı olarak yürütürler. Bankacılık ve finans kuruluşları başta olmak üzere günümüzde değişik sektörlerde faaliyet gösteren birçok işletme, faaliyetlerini yürütebilmek için bilgi sistemlerinde üretilen veya işlenen sürekli bilgiye bağımlılık duymaktadır. İşletmelerin bağımlı olduğu bu bilgiler artık yalnızca işletmenin kendisi tarafından değil, müşterileri ve ortakları gibi paydaşlar tarafından da kullanılmaktadır. Bu paydaşlar, kurumsal bilgilere kesintisiz ve anında erişim bekler (McAnally, DiMartini, Hakun, Lindman & Parker, 2000). Bu nedenle bilgi, bir kuruluşun sürekliliği için kritik bir faktördür. Bir işletmenin rekabet üstünlüğünü korumasını sağlamak için, bilgilerin gizli, doğru ve sürekli erişilebilir durumda tutulması gerekir (ISO27001, 2013). İşletmelerin birçok kilit iş süreçleri bilgi teknolojileri altyapısına ve bu altyapıda işlenen bilgilere bağlı olduğundan, bir işletmenin bilgi sistemlerinin işler vaziyette bulunması kritik öneme sahiptir. Bu durumda bilgi sistemlerinin başarısızlığı veya kullanılamaması nedeniyle meydana gelen iş süreçlerindeki kesinti, işletmeler için diğer birçok etkinin yanı sıra, verimlilik, gelir, rekabet, imaj ve pazar payı kaybına neden olabilir. Kilit iş süreçlerini bilgi sistemleri olmadan yürütemeyen işletmelerin, bu tür kesintilerin yaşanması durumunda kritik iş süreçlerinin sürekliliğini sağlayacak bir esneklik oluşturabilmek için bilgi sistemlerini de kapsayan bir süreklilik planına sahip olmaları gerekir.

Bilgi sistemleri sürekliliği, bir işletmenin bilgi sistemleri süreçlerinin herhangi birinde kesinti olması durumunda, önceden belirlenmiş kabul edilebilir seviyede sürekliliğinin sağlanması için işletmenin bu kesintilere karşı müdahale planlama yetkinliği olarak tanımlanabilir. Esasında bilgi sistemleri sürekliliği bir işletmedeki bilgi sistemleri süreçlerinin tehdit altında olması dışında iş sürekliliği ile aynıdır. Bilgi sistemleri sürekliliği planına sahip olan işletmeler, hizmetlerinde daha az kesinti yaşayarak paydaşlarına daha iyi bir süreklilik sunarlar ve kritik iş süreçlerinin kesintiye uğramasını en aza indirirler.

İşletmenin bir bilgi sistemleri sürekliliği yönetim sistemi kurmasındaki amaçları arasında aşağıdakiler sayılabilir:

- Felaket sonrasında bilgi sistemleri hizmetlerinin kesintiye uğramasının riskini ve etkisini değerlendirmek,
- İşletme için kritik olan ve ek önleme tedbirleri gerektiren hizmetleri belirlemek,
- Bir kurtarma planı geliştirmek, test etmek ve sürdürmek,
- Bilgi sistemleri hizmetlerini geri yüklemek için kullanılacak yaklaşımı tanımlamak,
- Hizmetlerin geri yüklenmesi gereken süreleri tanımlamak,
- İşletmenin karşılaşabileceği afetlerin etkilerini önlemek, tespit etmek, bunlara hazırlanmak veya etkilerini azaltmak için gerekli önlemleri almak.

Yukarıda yer alan hususlara göre bilgi sistemleri sürekliliğinin amacı, bir felaketten (olaydan) sonra gerekli bilgi sistemleri altyapısının ve bilgi sistemleri hizmetinin en uygun zaman ve maliyet sınırları içinde geri yüklenebilmesini sağlayarak genel iş sürekliliği stratejisini desteklemek olarak özetlenebilir. Dolayısıyla bilgi sistemleri sürekliliği bir işletmenin genel iş sürekliliği stratejisinin önemli bir bileşeni olarak değerlendirilmelidir (CISA, 2017).

3.1.1. İş Sürekliliği Kavramları

İş sürekliliği, bir işletmenin kesintiye neden olan bir olayın ardından, ürün veya hizmetleri önceden belirlenmiş kabul edilebilir seviyelerde sunmaya devam etme yeteneği olarak tanımlanabilir. Bir başka deyişle, iş sürekliliği işletmenin kritik iş süreçlerinin devamlılığını sağlama veya kesinti olması durumunda bu süreçleri öngörülen kesinti süreleri içerisinde yeniden çalışır vaziyete getirme çalışmaları olarak ifade edilebilir. Tanımlardan da anlaşılacağı üzere, iş sürekliliği işletmenin bir

felakete etkin ve verimli bir şekilde müdahale edebilmesini ve kritik iş süreçlerinin her zamanki gibi devam edebilmesini sağlamayı içerir.

İş sürekliliği planı, bir işletmenin kritik iş süreçlerinin önceden belirlenmiş kabul edilebilir seviyelerde sürdürebilmesini sağlamak amacıyla, bir olay, kesinti veya felaket anında kullanılmak üzere geliştirilmiş politika ve prosedürlerden oluşmakta olup, bir işletmenin felaket anına hazırlıklı olmasını sağlamak için önlemler ve prosedürler geliştirmenin eksiksiz bir sürecidir.

İş sürekliliği yönetimi ise, iş sürekliliğini sağlama sürecidir ve bir işletmeyi, amaçlarına ulaşmasını engelleyebilecek felaketlerle veya yıkıcı olaylarla başa çıkmak için hazırlamakla ilgilidir. İşletmeler, faaliyetlerini kesintiye uğratan bir felaketle karşılaşmaları durumunda, hayatta kalabilmek için kritik olan iş süreçlerini belirlemeli ve bu kilit iş süreçlerini ayakta tutmalıdırlar (Cook, 2015). İş sürekliliği yönetimi, işletmelerde olası felaketlere hazırlıklı olmayı ve afet sonrasında kritik iş süreçlerini hedeflenen sürelerde ayağa kaldırabilme kabiliyetine sahip olmayı amaçlar (Eren, 2013:144). ISO 22301 İş Sürekliliği Standardı'na göre İş sürekliliği yönetimi, bir işletme için tehdit oluşturan unsurların işletmenin kritik iş süreçleri üzerindeki olası etkilerini belirleyen ve işletmenin verimlilik, gelir, rekabet, imaj ve pazar payı kayıplarını önlemeyi amaçlayan bütünsel bir yönetim süreci olarak tanımlanmıştır. Bu nedenle, iş sürekliliği yönetimi bir işletme için stratejik bir öneme sahip olup, işletme için başı ve sonu olan bir plan veya proje olarak görülmemeli, işletmenin kurum kültürünün bir parçası haline getirilmelidir.

İş sürekliliği yönetimi, işletmenin potansiyel kayıplarını azalttığından ve paydaşlarına süreklilik konusunda güvence verdiğinden, işletmenin paydaşları için de hayati önem taşımaktadır. Paydaşların bir işletmeden beklentisi, iş hedeflerinin kesintisiz bir şekilde sürdürülmesidir. Mevcut bir iş sürekliliği planı olan bir işletme, paydaşlara tehditleri ve kritik süreçleri analiz ettiğini ve beklenmedik durumlar için plan yaptığını garanti eder. İş sürekliliğine yüksek düzeyde bağlılık gösteren işletmeler, paydaşlar arasında güven oluşturur. Bu nedenle bir işletmenin iş sürekliliği planının olması, bir felaketle karşılaşıldığında bile işletmenin faaliyetlerini en az kayıpla devam ettirebileceğinin, potansiyel kayıplarını önlemek için mevcut bir plana sahip olduğunun güvencesini verir.

Bir işletmenin hem kendisi hem de paydaşları için, bir iş sürekliliği planına sahip olmanın görünmez faydaları da vardır. Örneğin:

- Bir felaket sonucunda yaşanabilecek potansiyel kayıplarını başarılı bir iş sürekliliği planı ile önleyebilen bir işletme, mevcut müşterilerinin yanı sıra yeni müşterilerinin gözünde de itibarını artırabilir.

- İş sürekliliği yönetim planı yapan işletmeler, günlük küçük ölçekli kesintilerde daha kolay aksiyon alabilir, riskleri değerlendirebilir ve bu risklere kolayca yanıt verebilir.

- Üçüncü bir taraf ile yapılan sözleşme gereği şart koşulan bir iş sürekliliği planına sahip olan işletmeler, bir kesintinin etkilerini azaltmanın ve sözleşme uyumluluğunu sağlamanın ötesinde, iş kesintileri nedeniyle ödeyecekleri iş kesintisi sigorta primlerini de azaltabilir.

Yukarıda sayılan hususlar işletmenin hem kendisi hem de paydaşları için bir iş sürekliliği planına sahip olmanın görünmez faydaları arasında sayılabilir.

3.1.2. İş Sürekliliği Standartları

TS ISO 22301 Standardı

İşletmelerde önceleri kriz yönetimi, risk yönetimi veya felaket yönetimi çerçevesinde kabul gören iş sürekliliği, yaşanan iş kesintilerinin engellenmesine yönelik olarak günümüzde daha geniş kapsamlı bir hale dönüşmüştür ve yapılan çalışmalar neticesinde International Organization for Standardization (ISO) örgütü tarafından 2012 yılında, bu alanda çalışan meslek kuruluşlarınca "ISO 22301 İş Sürekliliği Yönetimi Sistemleri-Gereksinimler" adı altında uluslararası bir standart yayımlanmıştır. Aynı standart 2013 Eylül ayında Türk Standartları Enstitüsü (TSE) tarafından Türkçeye çevrilerek TS ISO 22301:2013 numarasıyla Türk standardı olarak kabul edilmiştir. TS ISO 22301, işletmenin ihtiyaçları çerçevesinde iş sürekliliği yönetimi politikalarının ve hedeflerinin tesis edilmesinin önemine vurgu yapmaktadır. Bu standart; işlerin aksamasına sebep olabilecek bir olayın

ardından bir kuruluşun ürün veya hizmet sağlama kabiliyetinin önceden belirlenmiş kabul edilebilir seviyelerde devam etmesi, bir faaliyetin kesintiye uğraması sonucunda kuruluş faaliyetinin devam edebilmesinin temin edilebilmesi için süreçler, prosedürler, kararlar ve faaliyetler oluşturması, başka bir deyişle, kuruluşların krizlerden ve felaketlerden kaçınmasına yardımcı olmak için proaktif ve reaktif planlar yaparak bu gibi durumlar gerçekleştiğinde hızlı bir şekilde olağan duruma geri dönülebilmesini sağlamaya yardımcı olur.

ISO tarafından çıkarılan diğer standartlar gibi bu standart da bir işletmenin iş sürekliliği yönetim sisteminin planlanmasına, kurulmasına, gerçekleştirilmesine, işletilmesine, izlenmesine, gözden geçirilmesine, sürdürülmesine ve etkinliğinin sürekli olarak geliştirilmesine yönelik olarak Planla-Uygula-Kontrol et-Önlem al (PUKÖ) modelini uygulamaktadır. PUKÖ modeline göre iş sürekliliği yönetim sistemi için;

Planlama aşamasında, işletmenin genel politikaları ve amaçlarına uygun sonuçlara ulaşılması amacıyla iş sürekliliğinin iyileştirilmesi ile ilgili iş sürekliliği politikası, amaçları, hedefleri, kontrolleri, süreçleri ve prosedürleri belirlenir.

Uygulama aşamasında, iş sürekliliği politikası, kontrolleri, süreçleri ve prosedürleri gerçekleştirilir ve yürütülür.

Kontrol etme aşamasında, iş sürekliliği politikası ve amaçlarına karşılık sistemin performansı izlenir ve gözden geçirilir; sonuçlar gözden geçirilmek üzere işletme yönetimine rapor edilir; düzeltme ve iyileştirme için yapılacak işlemler belirlenerek bu konuda yetkilendirme yapılır.

Önlem alma aşamasında ise işletme yönetimi, yapacağı gözden geçirmenin sonuçlarına dayanarak ve iş sürekliliği yönetim sistemi kapsamının, iş sürekliliği politikasının ve amaçlarının yeniden değerlendirilmesi suretiyle düzeltici faaliyetler yaparak iş sürekliliği yönetim sistemini sürdürür ve iyileştirir.

Bilgi ve İlgili Teknoloji için Kontrol Hedefleri (COBIT)

Information Technology Governance Institute (ITGI) tarafından yayımlanan Bilgi ve İlgili Teknoloji için Kontrol Hedefleri (COBIT), bilgi teknolojileri yönetişimi için küresel olarak kabul edilen bir çerçeve dokümandır. Başarılı bir iş sürekliliği için kesinlikle gerekli olan bilgi sistemleri sürekliliği konusuna da değinen COBIT çerçevesinin Teslimat ve Destek (İng. Delivery and Support, DS) DS4 bölümü, kritik iş süreçlerine hizmet veren bilgi sistemleri hizmetlerindeki kesintilerin olasılığını ve iş süreçlerine etkisini en aza indirgemeyi amaçlamaktadır. Bu amaçla bilgi sistemleri süreklilik planlarının hazırlanması, eğitimlerinin verilmesini, testlerinin yapılmasını, süreklilik planlarının ve bilgilerin dış lokasyonlarda saklanmasını tavsiye etmektedir. DS4 bölümü içerisinde verilen 10 adet kontrol hedefi aşağıda yer almaktadır:

- DS4.1 BT Sürekliliği Çerçevesi (İng. IT Continuity Framework)
- DS4.2 BT Süreklilik Planları (İng. IT Continuity Plans)
- DS4.3 Kritik BT Kaynakları (İng. Critical IT Resources)
- DS4.4 BT Süreklilik Planı Bakımı (İng. Maintenance of the IT Continuity Plan)
- DS4.5 BT Süreklilik Planı Testi (İng. Testing of the IT Continuity Plan)
- DS4.6 BT Süreklilik Plan Eğitimi (İng. IT Continuity Plan Training)
- DS4.7 BT Süreklilik Planının Dağıtımı (İng. Distribution of the IT Continuity Plan)
- DS4.8 BT Hizmet Kurtarma ve Yeniden Başlatma (İng. IT Services Recovery and Resumption)
- DS4.9 Tesis Dışı Yedekleme (İng. Offsite Backup Storage)
- DS4.10 Kurtarma Sonrası Gözden Geçirme (İng. Post-resumption Review).

ITIL

Bilgi Teknolojileri Altyapı Kütüphanesi (İng. Information Technology Infrastructure Library) olarak adlandırılan ITIL, bilgi teknolojileri servislerini eksiksiz ve en iyi kalitede yönetmek üzere geliştirilmiş servis yönetim metodolojisidir. ITIL hizmet sunumunun önemli bir bileşeni olan BT Hizmet Sürekliliği Yönetimi (İng. Information Technology Service Continuity Management, ITSCM), felaketlerden kaynaklanan riski kabul edilebilir bir düzeye indirerek ve bilgi teknolojileri hizmetlerinin kurtarılması için planlama yaparak bilgi teknolojileri hizmet sağlayıcısının minimum hizmet düzeylerini sağlayabilmesini hedefler. ITSCM, iş sürekliliği yönetimini destekleyecek şekilde tasarlanır. Felaket düzeyindeki bir olaydan önce, olay sırasında ve sonrasında hizmet kullanılabilirliğini ve performansını mümkün olan en yüksek seviyelerde tutmak amacıyla olay önleme, tahmin ve yönetim için planlamaya odaklanır. ITSCM'nin amacı, bu olayların kaçınılmaz olarak meydana geldiği durumlar için etkin, standartlaştırılmış süreçleri devreye sokarak arıza süresini, maliyetleri ve olayların iş üzerindeki etkisini azaltmaktır.

3.1.3. Felaket Türleri ve İşletmeye Etkileri

Felaket, büyük hasar veya kayıplara neden olan ani, planlanmamış bir olaydır ve işletmenin kritik iş süreçlerinin belirsiz bir süre boyunca işletilememesine neden olan herhangi bir olay olarak görülebilir. Deprem, sel, hortum ve yangın gibi işletme merkezine veya işletmenin bulunduğu bölgeye büyük zararlar veren doğal afetler, işletmeler için bir felakete neden olabilir. Ancak önemli felaketler artık yalnızca doğal afetlerle sınırlı kalmamakta, terörist saldırıları, siber saldırılar, virüsler ve insan hataları gibi başka bir nedenden dolayı işletmeye sağlanamayan elektrik, telekomünikasyon, doğal gaz ve benzeri beklenen altyapı hizmetlerinin aksaması gibi olaylar sebebiyle de gerçekleşebilmektedir. Özellikle ABD'de yaşanan 11 Eylül saldırılarından sonra birçok işletmenin artık bilinmeyen birçok felaket türüyle karşı karşıya olduğu da unutulmamalıdır. Felaketleri üç ana kategoriye ayırmak mümkündür:

Doğal afetler, yeryüzündeki büyük ölçekli jeolojik veya meteorolojik değişikliklerin neden olduğu büyük olumsuz olaylardır. Bunlar şunları içerebilir: Çığlar, hortumlar, kuraklık, depremler, aşırı soğuk, aşırı ısı, seller, dolu, kasırgalar, böcek/hayvan vebaları, heyelanlar, kum fırtınaları, kasırgalar, tsunamiler, tayfunlar, volkanik patlamalar, orman yangınları.

İşletmelere zarar verebilecek ve iş sürekliliği stratejileri gerektiren bir diğer tehlike ise teknolojik afetlerdir. Teknolojik afetler, doğal olayların neden olduğu etkenler ile meydana gelen olay arasında bir neden sonuç ilişkisi kurulamayan, insanın faydalı yönde üretim yaptığı ve kullandığı teknolojinin yanlış, dikkatsiz veya kasti olarak kullanımından kaynaklanan afetler olarak nitelendirilmektedir (Ege, 1986: 5). Bu nedenle, her işletme, kayıpları azaltmak amacıyla kendi iç ve dış iş ortamında teknoloji kullanımını gözden geçirmek zorundadır. Teknolojik felaketlere, havacılık, deniz ve demiryolu kazaları, baraj arızaları, endüstriyel kirlilik, nükleer radyasyon, zehirli atık olayları örnek olarak verilebilir.

İşletmeler, kritik iş süreçlerini gerçekleştirmek için teknoloji kullanımına ek olarak insan etkileşimlerine de ihtiyaç duyar. İnsan etkileşimlerine bağımlı olan her işletme için, insan kaynaklı iş kesintileri ve afetler meydana gelebilir. İnsan kaynaklı afetler, ihmalkâr, kasıtlı ve suç teşkil eden insan davranışları ya da terörist saldırıları, hacker saldırıları, virüsler gibi insanlar tarafından tetiklenen olaylar sebebiyle de gerçekleşebilir.

Son birkaç yılda işletmelerin karşılaştığı yeni tehditler iş sürekliliği planının önemini daha da artırmıştır. Dünya genelinde geniş alanlara hızlı bir şekilde yayılma kabiliyeti bulunan ve insanlar arasında bulaşa sebep olan salgınlar olarak tanımlanabilen pandemiler de işletmelerin kritik iş süreçlerini kesintiye uğratabilmektedir. Nitekim birçok işletme son olarak Çin'de ortaya çıkan koronavirüsün pek çok ülkeye yayılmasının ardından ilan edilen Covid-19 pandemisi nedeniyle temel iş faaliyetlerini uzaktan çalışma veya sınırlı personelle, birkaç hafta veya ay boyunca çalışır durumda tutmayı planlamak zorunda kalmıştır. İşletmeler, pandemi döneminde devletlerin veya sağlık kuruluşlarının almış olduğu fiziksel mesafenin korunması, bir alanda toplanabilecek insan sayısına getirilen sınırlama, seyahat kısıtlamaları ve bazı sektörlerin kapatılması gibi önlemler nedeniyle çok ciddi zorluklarla karşılaşmıştır.

Dolayısıyla, iş sürekliliği planlaması yaparken doğal afetlerden, teknik aksaklıklardan, kötü niyetli eylemlerden veya terör olaylarından farklı olarak bir pandeminin etkisini, beklenen ölçek ve süre farkı nedeniyle belirlemek bir işletme için çok daha zordur.

Bu tür felaketlerden sonra, işletmeler, kritik iş süreçlerinin kesintiye uğraması nedeniyle meydana gelecek zararın nasıl finanse edileceği ve işletmeye verilen hasarla aynı anda nasıl başa çıkılacağı dâhil olmak üzere bir dizi zorlukla karşı karşıya kalır. Örneğin bir deprem, işletmenin iletişim hatları üzerinde yol açabileceği tahribatın yanı sıra en önemlisi, işletme yöneticilerinin, çalışanlarının veya tedarikçilerinin yaralanmasına veya ölmesine yol açabilir.

Büyük bir felaket yaşayan işletmeler için yaşanan olayın ekonomik veya fiziki sonuçlarından çok, bu olay neticesinde kamuoyunda oluşan olumsuz söylentiler daha maliyetli olabilir. İşletme faaliyetlerine zarar veren bu olumsuz söylentilerin gerçek olup olmadığından bağımsız olarak, bu durumun en kötü sonuçlarından biri, işletmeye karşı kamuoyunda ve piyasada oluşacak itibar kaybıdır. Böyle bir krize karşı işletmenin etkili bir iletişim stratejisinin olması, işletmenin itibarının daha da zarar görmesini önlemede çok önemli bir rol oynar. Bu nedenle, özellikle bankacılık, finans, havayolu, sağlık, ulaşım ve enerji gibi toplumu etkileyebilecek kapasiteye sahip olan işletmeler, kendi marka, imaj ve itibarlarına önemli ölçüde zarar verme potansiyeli olan bir felaketle başa çıkabilecek halkla ilişkiler protokolüne sahip olmalıdır.

3.1.4. Felaket Kurtarma ve İş Sürekliliği Kavramlarının Birbiriyle İlişkisi

İş sürekliliği ile anılan bir diğer önemli kavram ise felaket kurtarma kavramı olup, bu kavram iş sürekliliğinin bir parçasıdır ve bir olayın ani etkisi ile ilgilenir. İşletmeyi bir sunucu kesintisinden, güvenlik ihlalinden veya deprem, sel, yangın veya kasırga gibi doğal afetlerden kurtarma bu kategoriye girer. Felaket kurtarma, felaketin etkilerini olabildiğince çabuk durdurmayı ve hemen ardından müdahale etmeyi içerir. İşletmenin kritik iş süreçlerinin işlevsiz hale gelmesi durumunda, bu süreçlerin yeniden işler hale getirilmesi için yapılacak müdahaleleri belirler. Bilgi sistemleri açısından değerlendirildiğinde felaket kurtarma, bir felaket durumunda işletmenin kritik iş süreçlerine etki edecek bilgi sistemlerinin çalışır tutulmasını veya kısa sürede tekrar işler hale getirilmesini ve bilgi sistemleri varlıklarına minimum düzeyde zarar verilmesini amaçlayarak hızlı ve eksiksiz bir kurtarma sağlamayı hedefler. Bilgi sistemleri felaket kurtarma ile bilgi sistemleri altyapısını etkileyen tehditler analiz edilir. Örneğin, işletmenin kritik iş süreçlerinin gerçekleştirildiği birincil sistemler yerine geçici sistemlerin nereye kurulacağı, yedek sistemlerin veya parçaların nasıl temin edileceği, güvenliğin yeni bir yerde nasıl kurulacağı soruları bilgi sistemleri felaket kurtarma planının bir parçası olarak değerlendirilebilir.

Felaket kurtarma, dar bir şekilde bir felaketten sonra sistemlerin nasıl tekrar çevrimiçi hale getirileceğine odaklanırken, iş sürekliliği, işletmeleri büyük bir kriz karşısında bile ayakta tutacak ve faaliyet gösterecek proaktif bir süreç geliştirmeyi amaçlar. Buna göre, bir felaket kurtarma planı, veri korumasını sağlamak, sistemlerin zarar görmesini önlemek ve mümkün olan en kısa sürede kurtarmakla sınırlıdır; iş sürekliliği planı ise iş süreçleri, insan gücü, ortaklar ve tedarikçiler dâhil olmak üzere işin tüm yönlerini kapsayarak işletme genelinde bir tutum değişikliği yaratmaya ve tüm paydaş gruplarını dikkate almaya odaklanır. Özetlemek gerekirse, felaket kurtarma planı, bir işletmenin bir felakete nasıl müdahale etmesi gerektiğini belirlerken, iş sürekliliği planı, bir işletmenin bir felaket boyunca nasıl çalışmaya devam edebileceğini belirler.

3.1.5. İş Etki Analizi, Kritiklik Analizi ve Kurtarma Hedefleri

İş etki analizi, bir iş sürekliliği planı oluşturmanın en önemli adımıdır ve olası bir kesinti durumunda kesintinin işletmeye etkilerinin analiz edilmesi amacıyla, işletmenin temel ürün ve hizmetlerini sunması için gereken kritik kaynaklar da dâhil olmak üzere, işletmenin iş süreçlerini değerlendirmeye odaklanır. ISO, iş etki analizini işletmenin iş süreçlerini ve bir iş kesintisinin bunlar üzerindeki etkisini analiz etme süreci olarak tanımlamaktadır. Özetle iş etki analizi, işletmenin iş hedefleri için hangi süreçlerin kritik olduğunu ve bu süreçlerdeki bir kesintinin işletmeye potansiyel etkisini belirleme sürecidir. İş etki analizinin başarılı bir şekilde gerçekleştirilebilmesi için işletmenin kritik iş süreçleri ve bu süreçleri desteklemek için kullanılan bilgi sistemleri hakkında bilgi edinmesi gerekir. İş etki analizi, işletmenin üst yönetim desteği alınarak başlatılmalı ve sonuçları üst yönetim tarafından onaylanmalıdır.

İş etki analizi, işletmenin iş hedeflerini destekleyen kritik iş süreçlerini belirlemek ve anlamakla başlar. İşletmenin iş süreçlerinin kritikliği, önem düzeyi ve önceliği belirlenirken, bazı değerlendirme kriterleri kullanılabilir. Bu aşamada, işletmenin iş süreçlerinin belirli bir süre kesintiye uğraması durumunda söz konusu kesintilerin işletmeye etkileri belirlenir. Aşağıda, işletmelerin kritik iş süreçlerinde yaşanan kesintilerin işletmeye etkilerinden bazıları örnek olarak verilmiştir:

- İşletmenin iş süreçlerinin belirli bir süre kesintiye uğramasının cezai bir yaptırımının olup olmadığının değerlendirildiği yasal etki,

- İşletmenin iş süreçlerinin kesintiye uğraması nedeniyle belirli bir süre sunulamayan ürün veya hizmetlerin işletmede yaratacağı gelir kaybının değerlendirildiği finansal etki,

- İşletmenin iş süreçlerinde meydana gelen kesintilerin işletmenin; ortaklar, yatırımcılar, müşteriler ve tedarikçiler gibi paydaşları ile kamuoyu nezdindeki itibar ve imajında yol açacağı kaybın değerlendirildiği itibar etkisi,

- İşletmenin iş süreçlerinin kesintiye uğraması nedeniyle belirli bir süre sunulamayan ürün veya hizmetler nedeniyle müşterilerde oluşacak memnuniyetsizlik düzeyinin değerlendirildiği müşteri ilişkileri etkisi.

Yukarıda örnek olarak verilen işletmenin kritik iş süreçlerinde meydana gelen kesintilerin işletmeye potansiyel etkilerinin düzeyleri, işletmenin kendisi tarafından belirlenen herhangi bir ölçekte (örneğin kritik, hayati, önemli ve küçük) sınıflandırılır. Bu aşamada işletmenin iş süreçlerinin ve bu süreçlerle bağlantılı olan bilgi sistemlerine ilişkin bilgiler toplanır ve risk sıralaması belirlenir. Böylece, işletmeler, bir iş sürekliliği yönetim planı hazırlamanın makul bir maliyetini belirleyebilmek için, iş süreçlerini kesintiye uğratan olayların meydana gelme riskini değerlendirir. Bu şekilde bir risk tabanlı analiz süreci ile kritik süreç ve sistemlerin önceliklendirilmesi, işletmenin iş sürekliliğini sağlamak için bir kurtarma stratejisi geliştirmesine yardımcı olabilir. Bu aşama, işletmenin iş süreçlerinin potansiyel risklerine göre bir kritiklik derecesi belirleme süreci olarak ifade edilir ve kritiklik analizi olarak adlandırılır. Kritiklik analizi ile kritik olarak belirlenen her bir süreç ve sistem için birbiriyle bağımlılıkları, dış kaynak bağımlılığı, bilgi sistemleri bağımlılığı, personel ve diğer kaynak bağımlılıkları belirlenmesi konusundaki çalışmalar yapılır ve etki zaman dilimleri tahmin edilir. İşletme, kritiklik analizi ile iş süreçlerinin dayanabileceği maksimum kesinti süresi (İng. Maximum Tolerable Period of Disruption, MTPoD) ve bu süreçleri tekrar işler hale getirmeyi hedefleyeceği kurtarma süresi (İng. Recovery Time Object, RTO) ölçütlerini tahmin ederek kurtarma stratejisini oluşturur.

Maksimum Tahammül Edilebilir Kesinti Süresi (MTPoD), bir işletmenin meydana gelen bir kesinti nedeniyle kritik iş süreçlerinin ve bu süreçlerle bağlantılı olan bilgi sistemlerinin yokluğuna veya kullanılamamasına tahammül edebileceği maksimum süredir. Bu sürenin aşılması durumunda işletmenin ciddi boyutta olumsuz etkileneceği öngörülür. İşletme açısından bu olumsuz etkiler finansal ve yasal olabileceği gibi, işletmenin imajına ve müşteri ilişkilerine yönelik de olabilir. İşletmedeki farklı iş süreçlerinin farklı MTPoD değerleri vardır. Örneğin, bankacılık sektöründeki bir işletmenin ödeme sistemleri süreçleri faaliyet açısından kritik öneme sahip olarak değerlendirildiğinde, işletmenin ödeme sistemlerinde meydana gelecek bir kesintiye tahammül süresi minimum olacakken, aynı işletmenin işe alım süreçleri ve bu süreçlerle bağlantılı bilgi sistemlerinde meydana gelecek bir kesintiye dayanma süresi daha uzun olacaktır. Bir iş sürecinin kritikliği ile maksimum kesinti süresi arasında bir korelasyon vardır. Kritiklik ne kadar yüksekse, tahammül edilebilir kesinti süresinin o kadar kısa olması beklenir. MTPoD, kesintiye uğrayan süreç ve sistemleri kurtarma süresi (RTO) ile iş kurtarma süresi (İng. Work Recovery Time, WRT) olmak üzere iki unsurdan oluşur ve aşağıdaki gibi formüle edilebilir.

MTPoD = RTO + WRT

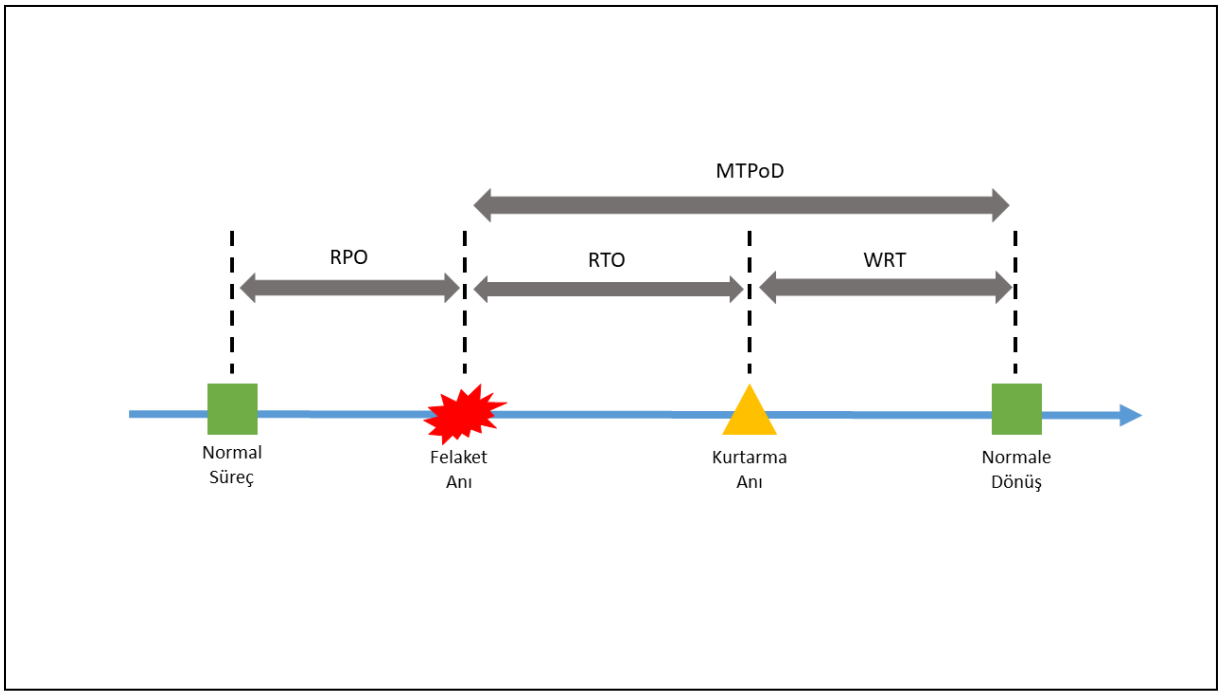
Kurtarma Süresi Hedefi (RTO), işletmenin kesintiye uğrayan kritik sistemlerinin tekrar kurtarılması için gerekli süredir. Bu aşamada, kritik sistemler tekrar çalışmaya başlar ancak işletmenin iş süreçlerini desteklemeye hazır değildir. RTO, işletmenin kritik iş süreçlerini tekrar hizmete almak için gereken maksimum kabul edilebilir sürenin ilk bileşenidir. İşletmenin kritik süreçlerinden biri kesintiye uğradığında, kurtarma süresi hedefinin gerçekleştirilebilmesi için bazı eylemler gerekebilir. Bu eylemleri gerçekleştirebilmek için işletmenin bazı maliyetlere katlanması gerekir. Bu nedenle kurtarma süresi ile kurtarmayı desteklemek için gereken maliyet arasında ters bir ilişki vardır. Yani, bir işletmenin

kritik bir süreci için hesaplanan RTO zaman açısından ne kadar kısa olursa, kurtarma maliyeti o kadar artar.

İş Kurtarma Süresi (WRT), Kurtarma süresi hedefi ile tekrardan çalışmaya başlayan kritik sistemleri ve veri bütünlüğünü doğrulamak için gerekli maksimum süredir. WRT, işletmenin kritik iş süreçlerini tekrar hizmete almak için gereken maksimum kabul edilebilir sürenin diğer bileşenidir.

Kurtarma Noktası Hedefi (RPO), özellikle veri yedekleme söz konusu olduğunda önemlidir. İşletmenin iş süreçlerinin kesintiye uğraması durumunda kabul edilebilir veri kaybına göre belirlenir. Verileri kurtarmak için kabul edilebilir olan en erken zaman noktasını gösterir. RPO, kesinti durumunda izin verilen veri kaybı miktarını etkin bir şekilde ölçer. Özetle, *"İşletme olarak ne kadarlık bir veri kaybına tahammül edilebilir?"* sorusunun cevabıdır.

Aşağıda yer alan şekil MTPoD, RTO, RPO ve WRT arasındaki ilişkiyi grafiksel olarak göstermektedir.



Şekil 7: Kritik kurtarma zamanı çerçeveleri arasındaki ilişki

Normal işlemler sırasında gerçekleştirilen son yedekleme ile verilerin mevcut durumu arasında genellikle bir boşluk vardır. Bazı işletmelerde bu süre dakika veya saat olabilirken, çoğu işletmede ise saatler veya günleri bulabilir. Bu zaman dilimi işletmenin kritik verilerinin yedeklemeleri arasındaki süredir ve çoğu işletmede kurtarma noktası hedefi (RPO) olarak belirlenir. İşletmede süreçlerin kullanılamaz hale geldiği nokta yani felaket anı işletmenin iş sürekliliği yönetim planlama faaliyetlerinin başlatıldığı noktadır. Buna göre işletmenin maksimum tahammül edilebilir kesinti süresi (MTPoD) kurtarma süresi hedefi (RTO) ile başlar. Bu zaman diliminde, işletmenin kritik iş süreçlerini destekleyen sistemler onarılır veya yeniden yapılandırılır. RTO, işletmenin kritik iş süreçlerini destekleyen sistemler tekrar hizmete alındığında ve güvenilir olan son yedekleme geri yüklendiğinde sona erer. MTPoD'un ikinci aşaması olan İş Kurtarma Süresi (WRT) daha sonra başlar. Bu zaman diliminde ise, işletmenin kritik iş süreçlerini destekleyen sistemler, genellikle yedeklemeler arasında çöktüğü için kaybedilen veriler ile bu sistemler hizmet dışıyken biriken iş yığınları otomatik veya manuel olarak tekrar sisteme dâhil edilir. Bu işlemler tamamlandıktan sonra işletme, artık felaket kurtarma planından çıkarak normal operasyonlarına kaldığı yerden devam edebilir.

Bir işletmenin iş süreçlerini etkileyen bilgi sistemlerine ilişkin hazırlanan iş etki analizi çalışmaları kapsamında kritik kurtarma zamanları aşağıda yer alan örneklerle detaylandırılmıştır:

"Bir sunucunun merkezi işlemci birimi veya belleği arızalanır, 2 saat içinde değiştirilir ve yeniden başlatılır. Hiçbir veri kaybolmaz. Bu işlem için hesaplanan RTO 2 saattir, RPO ise sıfırdır."

"Bir uygulamayı destekleyen depolama sistemi, tüm verilerin kaybolmasına neden olan bir donanım arızasından mustariptir. Veriler, her 6 saatte bir alınan başka bir sunucudaki anlık görüntüden kurtarılır. Bu durumda RPO 6 saattir."

"Bir uygulamanın veri tabanı bozuk ve kurtarılması gerekiyor. Yedekler günde iki kez alınır. RPO 12 saattir. Ancak, veri tabanındaki dizinleri yeniden oluşturmak, yani WRT 10 saat sürer, bu nedenle RTO 22–24 saate yakındır çünkü uygulama, dizinler kullanılabilir olana kadar hizmete döndürülemez."

Yukarıda yer alan hususları özetlemek gerekirse, bir iş sürekliliği planı oluşturabilmek için, işletmenin tüm iş süreçlerini tanımlayan, bunları kritiklik sırasına göre önceliklendiren, kritik olarak belirlenen her bir süreç ve sistem için birbiriyle bağımlılıkları, dış kaynak bağımlılığı, bilgi sistemleri bağımlılığı, personel ve diğer kaynak bağımlılıklarını analiz eden ve işletmenin kendisi tarafından belirlenmiş bir ölçek aracılığıyla bir kesintinin etkisini değerlendiren, kritik iş süreçleri için tahammül edilebilir maksimum kesinti sürelerini belirleyen bir iş etki analizi geliştirilmesi gerekmektedir.

3.1.6. Risk Değerlendirmesi

Risk, basit bir ifadeyle bir zarara uğrama tehlikesi veya zarar görme olasılığı olarak tanımlanabilir. ISO 30001'e göre ise risk, *"belirsizliğin hedefler üzerindeki etkisi"* olarak tanımlanmıştır. Dolayısıyla, risk bir şeyin olma olasılığı ile gerçekten olması durumunda ortaya çıkan etkinin birleşimi açısından değerlendirilmelidir. Nitekim birçok kaynakta da risk **"Risk = Olasılık x Etki"** olarak formüle edilir ve bu formülle sayısallaştırılır. Olasılık ve etki, her bir riskin seviyesini kabul edilebilir bir şekilde tanımlayabilen iki ana faktördür. Burada olasılık, bir olayın bir zaman dilimi içerisinde gerçekleşme durumunu ifade ederken, etki ise tehlikenin gerçekleşmesi durumunda hedeflere vereceği zararı ifade eder.

Riskin ölçülmesine ilişkin aşağıdakine benzer bir örnek verilebilir:

"Bir işletmenin üretimde kullandığı A ve B olmak üzere iki adet makinesinin olduğu kabul edilsin.

- A makinesinin 1 ay içinde arızalanma olasılığı 0,01 ve bu arızadan kaynaklı olarak işletmenin uğrayacağı kayıp 200.000 TL olsun. O halde, A makinesinin riski 0,01 x 200.000 TL = 2.000 olarak hesaplanır.

- B makinesinin 1 ay içinde arızalanma olasılığı 0,02 ve bu arızadan kaynaklı olarak işletmenin uğrayacağı kayıp 50.000 TL olsun. O halde, B makinesinin riski 0,02 x 50.000 TL = 1.000 olarak hesaplanır."

Riskler, genellikle tam olarak öngörülemezler ve bu nedenle bir belirsizlik içerirler. Risk, bir olayın gelecekte meydana gelme olasılığına bağlı olduğundan net olarak bilinmesi mümkün değildir. Bir olayın meydana gelme olasılığının hedefler üzerindeki etkisi zaman içinde değişebilir. Bu da riskin zamanla değişmesi anlamına gelir. Bir risk öngörüldüğü durumda, gerekli önlemler alınarak risk azaltılabilir veya tamamen önlenebilir. Buna göre riskin yönetilebilir bir olgu olduğu söylenebilir.

Bir işletmenin iş sürekliliği faaliyetlerinde üzerinde önemle durması gereken konulardan biri de risktir. Kurumsal bağlamda risk, genellikle işletmenin hedeflerinin gerçekleştirilmesini etkileyebilecek herhangi bir şey olarak tanımlanır. İşletmenin iş sürekliliği faaliyetlerinde dikkate alınması gereken bazı riskler, bunlarla sınırlı olmamakla birlikte aşağıda yer almaktadır:

Fiziksel risk; işletmenin kendisinin veya varlıklarından bir kısmının korunamaması riskidir.

Bilgi güvenliği riski; işletmenin elektronik ortamda ya da fiziksel olarak bünyesinde barındırdığı verilerin ve bilgilerin korunamaması riskidir.

Uyum riski; yasalara, mevzuata, iş kanununa, kurallara ve standartlara uyulmaması nedeniyle ortaya çıkan risktir.

İtibar riski; paydaşlar veya kamu tarafından işletmeye duyulan güvenin azalması ile ilgilidir.

Çalışan riski; yetişmiş personel gücünün varlığı ve elverişliliği ile ilgili risklerdir.

Çevresel riskler; çevre ve tabiatın zarar görmesine neden olacak risklerdir.

Biyolojik riskler; insan veya hayvan hastalıkları nedeniyle ortaya çıkan risklerdir.

Yukarıda sayılan riskler, işletmenin iş hedeflerine göre tek tek tanımlanan, meydana gelme olasılıkları ve işletmenin kritik iş süreçlerinde meydana getireceği olumsuz etkileri analiz edilen, eğer gerekirse, gerekli risk azaltma stratejileri uygulanan riskler olup, işletmenin iş sürekliliği faaliyetlerinin risk değerlendirme aşamasında detaylandırılır.

Risk değerlendirmesi, işletmenin iş sürekliliğinin amaçlarına ulaşmasına olumsuz etki eden ve kayba yol açan risklerin belirlenmesi ve bu risklerin yönetilmesi çalışmalarını içermektedir. Bir risk değerlendirmesi çalışmasının ana hedefi işletmeyi tehdit eden risklerin tanımlanması, analiz edilmesi, değerlendirilmesi ve işletmenin iş sürekliliği hedefleriyle orantılı risk tedavisi ve müdahale planlamasına hazırlıktır (ISO 22301, 2012). İşletmenin iş süreçlerinde herhangi bir kesinti yaşanmaması için yapılması gerekenlere ve atılması gereken adımlara odaklanır. İşletmenin iş süreçlerinin kesintiye uğramasına yol açabilecek koşulları ve durumları, bu koşul ve durumların meydana gelme olasılığını, bu süreçlere karşı insan, doğa, teknoloji vb. alanlardaki tehdit ve tehlikeleri belirleyerek bu kesintilerin nasıl önlenebileceğine yönelik çalışmaların yapıldığı bir süreçtir. Bu süreç, işletmenin faaliyetlerini tehdit eden bu risklerin olasılığını ve etkisini değerlendirmeyi ve bu kritik risklere karşı yanıt planları hazırlamayı içerir (Mahdevari, Shahriar ve Esfahanipour, 2014).

Risk değerlendirme aşamasında, iş süreçleri ve iş etki analizinin sonuçları olası felaket senaryoları ile teste tabi tutulur. Bu testlerin bazıları iş süreçlerinin başarılı olması için herhangi bir eylem gerektirmezken, bazıları ise önemli iş sürekliliği planlamasının geliştirilmesini ve kaynaklarla (finansal ve personel) desteklenmesini gerektirebilir.

İşletmeler, potansiyel olarak iş süreçlerini ve paydaşlarının beklentilerini karşılama yeteneklerini bozabilecek kapsamlı felaket senaryoları geliştirmelidir. Bu felaketler, daha önce de ifade edildiği gibi kötü niyetli faaliyetlerin yanı sıra doğal ve teknik felaketler de dâhil olmak üzere birçok biçimde olabilir. İşletmeler bir felaketi, felaketin doğasına değil, işletme üzerindeki etkisine odaklanarak analiz etmelidir. Örneğin, belirli tehdit senaryolarının etkileri, yalnızca belirli çalışma alanlarını, sistemleri, tesisleri (yani binaları) veya coğrafi alanları etkileyen iş kesintilerine indirgenebilir.

Ek olarak, iş kesintisinin büyüklüğü, pratik deneyimlere ve olası koşullara ve olaylara dayalı çok çeşitli felaket senaryolarını dikkate almalıdır. Felaket senaryoları kapsamlı değilse, iş sürekliliği planlaması çok basit olabilir ve iş süreçlerinin kesintilere karşı dayanıklılığını artırabilecek makul adımları atlayabilir. Felaket senaryoları, bir kesintinin etkisini ve tehdidin meydana gelme olasılığını dikkate almalıdır.

Tehditler, ortaya çıkma olasılığı yüksek ve işletme üzerinde etkisi düşük (örneğin kısa süreli elektrik kesintileri) veya meydana gelme olasılığı düşük ve işletme üzerinde etkisi yüksek (örneğin kasırga, terörizm) olabilir. Yüksek olasılıklı tehditler genellikle çok kapsamlı bir iş sürekliliği planlamasıyla desteklenir. Bununla birlikte, ele alınması en zor tehditler işletme üzerinde etkisi yüksek olan ancak gerçekleşme olasılığı düşük olan tehditlerdir. Bir risk değerlendirmesi kullanarak, iş sürekliliği planlaması daha esnek ve kapsamlı olabilir ve başlangıçta dikkate alınmayan belirli kesinti türlerine uyarlanabilir.

İş sürekliliği planlama sürecinin bu noktasında işletmelerin bir boşluk analizi (İng. gap analysis) yapması gerekir. Bu bağlamda boşluk analizi, bir kesinti durumunda işletmenin normal iş süreçlerini sürdürmek veya kurtarmak için ne tür planlara ihtiyacı olduğunun ve mevcut iş sürekliliği planının bunun ne kadarını sağladığının bir karşılaştırmasıdır. İkisi arasındaki fark, işletmenin iş sürekliliği planı geliştirmede ele alması gereken ek risk maruziyetini vurgular.

Belirli bir olayın meydana gelme olasılığını değerlendirirken işletmeler, tesislerin coğrafi konumunu ve doğal afetlere karşı duyarlılıklarını (örneğin bir taşkın ovasındaki konum) ve kritik altyapılara (örneğin güç kaynakları, nükleer santraller, havaalanları) yakınlığını dikkate almalıdır. Risk değerlendirmesi işletmenin tüm tesislerini içermelidir. Tesislerin yıkılması ve can kaybı gibi en kötü senaryolar düşünülmelidir. Bu aşamanın sonunda işletme, kritik iş süreçlerine öncelik vermiş ve çeşitli felaket senaryoları altında nasıl kesintiye uğrayabileceklerini tahmin etmiş olacaktır (PLUMB Ion, ZAMFIR Andreea, TUDOR Delia, Business Continuity Planning for Risk Reduction).

Risk değerlendirmesinin amaçları, iç ve dış tehditlerin belirlenmesi, bu tehditlerin önceliklendirilmesi ve bir eylem planının geliştirilmesi ile risk yönetimine bilgi verilmesidir. Bu hedeflere ulaşılmasını sağlayan süreç, en azından aşağıdaki faaliyetleri içerir:

(1) Seçilen süreçlere yönelik tehditlerin listelenmesi,

(2) Her tehdidin etkisinin tahmin edilmesi ve oluşma oranının belirlenmesi,

(3) Her tehdidin olasılığının belirlenmesi,

(4) Riskin önceki faaliyetlerden hesaplanması,

(5) Her bir tehdit için risk stratejisi seçilmesi (risk kabulü, risk transferi, riskten kaçınma, risk azaltma).

TS ISO 31000 Risk Yönetim Standardı'na göre ise risk değerlendirmesi (İng. risk assessment); risk tanımlama (İng. risk identification), risk analizi (İng. risk analysis) ve risk irdelemesi (İng. risk evaluation) aşamalarının genel sürecidir. Risk değerlendirmesi, paydaşların bilgi ve görüşlerinden yararlanılarak sistematik, yinelemeli ve işbirliği içinde yürütülmelidir. Gerektiğinde daha fazla araştırmayla desteklenen mevcut en iyi bilgileri kullanmalıdır (ISO 31000).

Risk Tanımlama, *"riskleri bulma, tanıma ve kaydetme süreci"* olarak tanımlanmaktadır (ISO 31010, 2009). Risk tanımlama, hangi risklerin işletmenin kritik iş süreçlerini etkileyerek iş sürekliliğini kesintiye uğratabileceğini belirler. Bu şekilde işletme, risk tanımlama süreci yoluyla işletmenin kritik iş süreçlerinde kesintiye neden olabilecek olaylar hakkında bilgi sahibi olur. Bir iş sürekliliği kapsamında yapılan risk değerlendirmesi aşamasında, risk tanımlamasının odak noktası işletmenin dayanıklılığıdır.

Risk tanımlama, işletmelerin coğrafi konumlarından piyasa değişkenlerine kadar birçok faktörün analiz edilmesini içerir. Risk tanımlama süreci, durumların çözümünü değil durumların saptanmasını kapsar. Risk tanımlama sürecine başlamadan önce işletmenin iş hedefleri, kritik iş süreçleri ve iş etki analizinin sonuçları hakkında bilgi sahibi olmak çok önemlidir. İşletme, etkin risk tanımlamasının önemli bir parçası olarak iç ve dış varlıklarını, tehdit ve tehlike türlerini, mevcut kontrolleri belirlemeli ve envanterini çıkarmalıdır. Risk tanımlama süreci, istenmeyen olayları, istenmeyen sonuçları, ortaya çıkan tehditleri ve ayrıca mevcut ve ortaya çıkan fırsatları tanımlamalıdır. Risk tanımlama süreci tek seferlik bir süreç olmaktan çok sürekli tekrarlanması gereken bir süreçtir. Riskleri tanımlamak için kullanılabilecek birçok farklı plan bulunmakta olup, Ward ve Chapman'a (2003) göre, riskleri tanımlarken bir belirsizlik perspektifi kullanmak en iyisidir.

Risk Analizi, risk olasılığı ve risk etkisinin ürünü olan risk derecelendirmesini değerlendirme ve belirleme sürecidir ve bu adımda her bir risk için, risk olasılığının ve etkisinin çarpımı olan ve o riskin seviyesi (yani değeri) olarak tanımlanan sayısal bir değer atanır. Risk analizi, belirsizliklerin, risk kaynaklarının, sonuçların, olasılıkların, olayların, senaryoların, kontrollerin ve bunların etkinliğinin ayrıntılı bir şekilde değerlendirilmesini içerir. Riskler tanımlandıktan sonra işletmenin, her bir riskin büyüklüğünü, meydana gelme olasılıklarına ve meydana gelmeleri durumunda kuruluş üzerindeki etkilerine göre ölçmesi gerekir. Bu, işletmenin iş sürekliliğine etki eden önemli risklerin belirlenmesine ve önceliklendirilmesine yardımcı olacaktır. İşletme için olası risklerin bir listesi oluşturulup belirlendikten sonra, her birini analiz etmek ve değerlendirmek gerekir. Riskleri analiz etmenin en yaygın yolu, her bir riski gerçekleşme olasılığı ve meydana gelmesinin sonuçlarına göre derecelendiren bir ölçek kullanmaktır.

Risk İrdelemesi, riskin önemini belirlemek için tahmini riski, verilen risk kriterleriyle karşılaştırmak için kullanılan süreçtir. Risklere yönelik ek eylemlerin nerede gerekli olduğunu belirlemek için risk analizinin sonuçlarını yerleşik risk kriterleriyle karşılaştırmayı içerir. Risk irdelemesi ile riskin tehdit edebileceği iş sürecinin işletme için önemi, işletmenin risk üzerindeki kontrolü, bu risk sebebiyle işletmede oluşacak potansiyel kayıplar dikkate alınır.

Riskleri tanımladıktan, analiz ettikten ve irdeledikten sonra, bunları öncelik sırasına göre sıralamak gerekir. Daha sonra işletmenin iş hedeflerini tehdit eden risklere karşılık hangi risk yanıt stratejisinin kullanılacağına karar verilmelidir.

Risk Yanıtı, işletmenin iş sürekliliği hedeflerini tehdit eden risklerin, risk yanıt stratejileri uygulanarak karşılanmasıdır. Bu kapsamda, işletmenin uygulayabileceği 4 farklı stratejiye aşağıda maddeler halinde yer verilmiştir.

- **Risk kabulü:** Bu strateji, işletmenin bir riskten kaynaklanan potansiyel kaybının, bu riskten kaçınmanın getireceği maliyet kadar büyük olmadığını kabul ettiği zaman veya işletmenin risk toleransı içinde ise uygulanır. Riskten kaynaklanan potansiyel kaybın yönetilebilir olduğu kabul edilir. Örnek olarak 1.000 TL'lik bir riskten kaçınmak için 1.000 TL veya daha fazla para harcamanın işletmeye hiçbir faydası yoktur. Bir riski hafifletmek için daha fazla maliyete katlanacağını öngören birçok işletme, bu riske cevap vermek yerine kabul etmeyi seçer. Riski kabul etme bilinçli veya bilinçsiz olabilir. Bilinçli olarak uygulandığında, risk algılanır ancak maliyet nedeniyle riski önlemek, azaltmak veya devretmek amacıyla olumlu önlemler alınmaz. Risk tanınmadığında ise, bilinçsizce kabul edilir ve işletme bu riski kabul ettiğinin farkında olmadan herhangi bir olumlu önlem almaz.

- **Riskten kaçınma:** Bu strateji, işletme için potansiyel bir kayba neden olabilecek bir riskin meydana geleceği kritik değeri yüksek olan sistemin veya sürecin tamamen ortadan kaldırılmasını içerir. Böylece potansiyel bir kayıp oluşturan herhangi bir riske maruz kalınmasına müsaade edilmez. Ne yazık ki bir riskten tamamen kaçınmak mümkün olmayabilir veya ancak aşırı önlemler alındığında bu mümkün olabilir. Örneğin, taşkın riski olan bir bölgede yer alan bir işletme, belirli bir düzeyde sel riskine maruz kalacaktır ve bu işletme riski azaltmak amacıyla pencere ve kapıları korumak için taşınabilir bariyerler yerleştirebilir, selin yönünü değiştirmek için çalışmalar yapabilir, elektrik kesintilerinin önüne geçmek de dâhil olmak üzere daha birçok adım atabilir. Ancak bunların hiçbiri, işletmenin maruz kalacağı potansiyel riski ortadan kaldırmaz. İşletme bu bölgeden taşınmadığı sürece sel riski devam edecektir.

- **Risk transferi:** Risk transferi, bir işletmenin karşılaştığı olumsuz bir sonuçtan kaynaklanan potansiyel zararın üçüncü bir tarafa kaydırıldığı veya üçüncü bir tarafla paylaşıldığı yaygın bir risk yönetimi tekniğidir. Üçüncü şahsın riski üstlenmesini tazmin etmek için işletme genellikle üçüncü şahsa periyodik ödemeler sağlar. En yaygın risk transferi türü, finansal riski karşılamak için bir sigorta şirketine prim ödemektir. Sigorta doğrudan hasar maliyetini, iş sürekliliği/kurtarma giderlerini ve arıza süresini telafi edebilir. Ancak kayıp müşterilerin veya müşteri memnuniyetsizliğinin dolaylı maliyetini karşılayamaz. Risk transferi yalnızca sigorta ile sınırlı değildir. Bir diğer türü ise sözleşmelerde yer alan tazminat maddesidir. Taraflar arasında yapılan sözleşmeler işletmenin potansiyel kayıplarının karşı taraftan tazmin edilmesini sağlayan maddeler içerebilir.

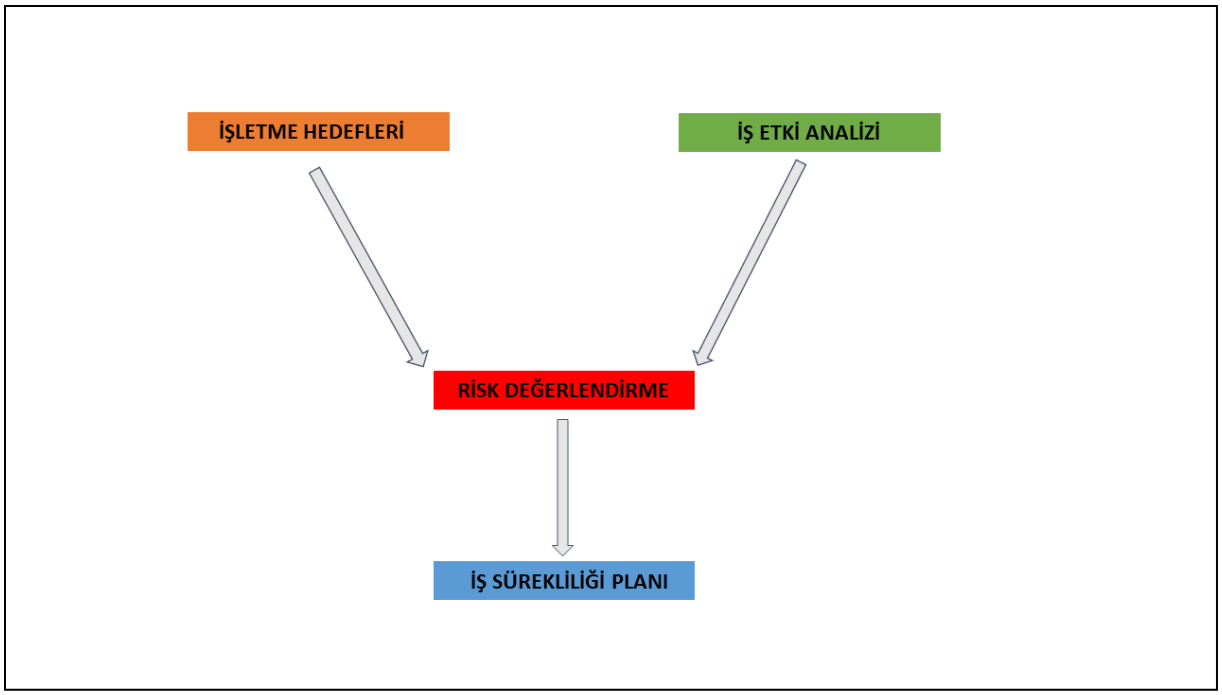
- **Riski azaltma:** Bir işletmenin kritik iş süreçlerinde veya sistemlerinde potansiyel bir kayba neden olabilecek bir riskin oluşturabileceği zararı hafifletmek için önleyici eylem planlarının uygulandığı bir stratejidir. Risk azaltma, bazı felaketlerin kaçınılmazlığına odaklanır ve bir tehdidin tamamen önlenemediği durumlarda kullanılır. Bir riskten kaçınmayı planlamak yerine, olumsuz ve potansiyel olarak uzun vadeli etkileri azaltmak için olay meydana gelmeden önce veya bir felaketin ardından atılabilecek adımlarla ilgilenir.

İşletmenin kritik iş süreçleri, uygulamaları, bilgi sistemi ve bilgi teknolojileri altyapısı bileşenleri arasında bağımlılıkların oluşturulması bir risk değerlendirmesi konusudur.

Risk değerlendirmesi, bilgi sistemleri bileşenlerinin işletme için önemini ve bu bileşenlere yönelik tehditleri ve güvenlik açıklarını belirledikten sonra, bileşenleri korumak için en uygun yöntemlerin oluşturulması amacıyla bir düzeltici eylem planı geliştirilebilir. İşletme, kritik iş süreçlerini etki eden bilgi sistemleri bileşenlerine yönelik tehditleri ortadan kaldırmak veya güvenlik açığını gidermek için bir risk yanıt stratejisi kullanır.

İş Etki Analizi ve Risk Değerlendirme İlişkisi

İş etki analizi ve risk değerlendirmesi, bir iş sürekliliği planında iki önemli adım olarak görülür. İş etki analizi genellikle bir risk değerlendirmesinden önce gerçekleşir. İş sürekliliği kapsamında yapılacak risk değerlendirme çalışmaları, iş etki analizi sonucunda belirlenen kapsam dâhilinde yürütülür. Bu sebeple iş etki analizinin çıktıları risk değerlendirmesinin en önemli girdisini oluşturur. Aşağıdaki şekil, risk değerlendirmesinin iş etki analizi ve işletmenin iş hedefleriyle ilişkisini anlatmaktadır.



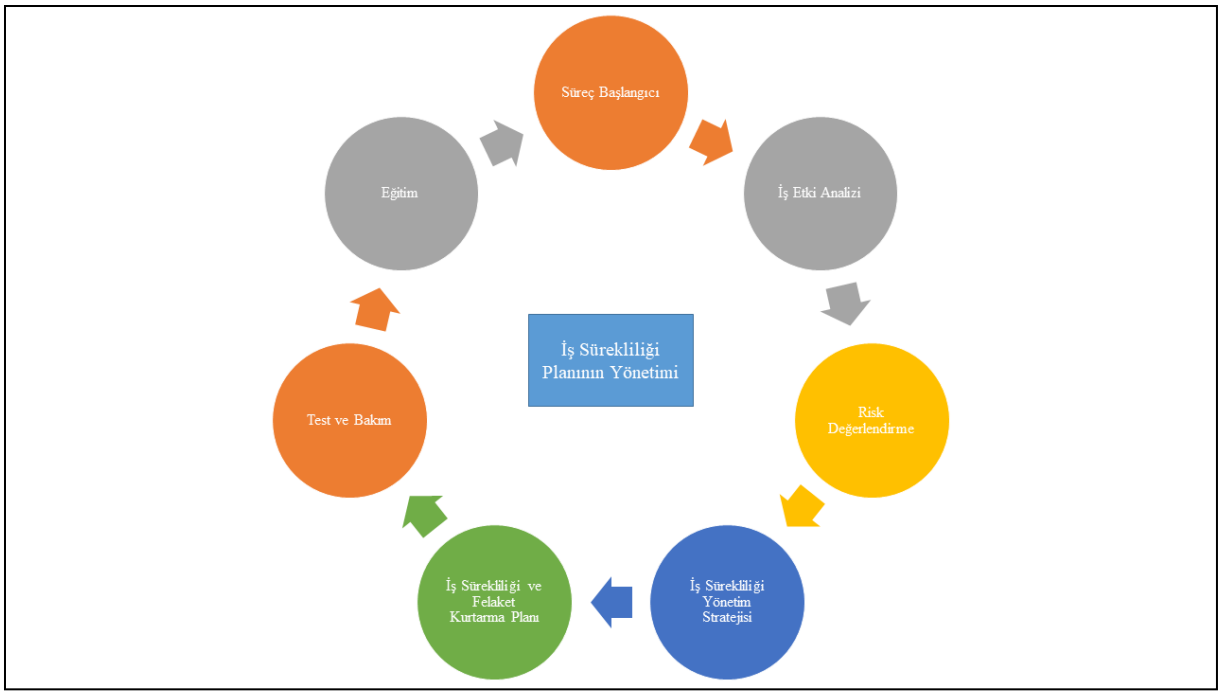
Şekil 8: İş Etki Analizi ve Risk Değerlendirme İlişkisi

Görülebileceği gibi, risk değerlendirme ve iş etki analizinin sonuçları, iş sürekliliği yönetim planı geliştirmek için birlikte kullanıldığından, risk değerlendirme ve iş etki analizi süreçlerinin birbirleriyle çok derin ilişkileri vardır. Başka bir deyişle, iş etki analizinin çıktıları (RPO, RTO, WRT ve MTPoD) risk değerlendirme sonuçlarıyla birlikte en uygun yanıtı hazırlamak için birlikte kullanılır. Ayrıca risk değerlendirme, işletmenin hedeflerini karşılamalı ve yöneticilerin hedeflerine ulaşmasına yardımcı olmalıdır (Torabi, Rezaei Soufi ve Sahebjamnia, 2014).

İş etki analizi, işletmenin kritik iş süreçlerindeki kesintinin etkilerine veya sonuçlarına odaklanır ve bir felaketle ilişkili finansal ve finansal olmayan maliyetleri ölçmeye çalışır. Risk değerlendirmesi ise işletmenin karşı karşıya kalabileceği potansiyel riskleri tanımlar. Kritik süreçleri kesintiye daha açık hale getiren zayıf noktalar gözden geçirilir. Risk değerlendirmesi aşamasında, bir tehlikenin işletmenin kritik iş süreçleri üzerinde önemli bir etkiye sahip olma olasılığını azaltmak için bir azaltma stratejisi geliştirilir. Ayrıca, iş etki analizi çıktıları çeşitli tehlike senaryolarına göre incelenir ve tehlike olasılığına ve ticari faaliyetlere olumsuz etki olasılığına dayalı olarak olası kesintilere öncelik verilir. İşletme, iş etki analizi sonuçlarına ve risk değerlendirmesi sonuçlarına tek bir bakış açısıyla bakarak, en kritik iş süreçlerinin neler olduğunu daha doğru bir şekilde anlayabilir. İş etki analizi ve risk değerlendirme sonuçlarını iş sürekliliği planlarına birlikte entegre eden işletme yönetimi, işletmenin iş hedeflerine kesintisiz bir şekilde ulaşmasına yardımcı olur. Bu hususlar, hem iş etki analizi hem de risk değerlendirmesi yapılmadan başarılı bir iş sürekliliği stratejisine sahip olmanın mümkün olmadığını açıkça ortaya koymaktadır.

3.2. Bilgi Sistemleri Süreklilik Planının Yönetimi

Bilgi sistemleri sürekliliğinin amacı, bir felaketten (olaydan) sonra gerekli bilgi sistemleri altyapısının ve bilgi sistemleri hizmetinin en uygun zaman ve maliyet sınırları içinde geri yüklenebilmesini sağlayarak genel iş sürekliliği stratejisini desteklemektir. Dolayısıyla bilgi sistemleri sürekliliği bir işletmenin genel iş sürekliliği stratejisinin önemli bir bileşeni olarak kabul edilmelidir. İş sürekliliği yönetim süreci bir yaşam döngüsü sürecidir. Başka bir deyişle, iş sürekliliği planlaması (ve olağanüstü durum kurtarma planlaması) tek seferlik bir olay veya faaliyet değildir. Sürekli olarak değişen iş koşullarına uyum sağlayan ve sürekli olarak gelişen felaketler için sürekli hazırlık ile sonuçlanan bir dizi faaliyettir. Aşağıda yer verilen şekilde iş sürekliliği yönetiminin adımlarına yer verilmiştir.



Şekil 9: İş Sürekliliği Planının Yönetimi

Yukarıdaki şekilde yer verildiği üzere, iş sürekliliği planının yönetimi ilk olarak, işletmede iş sürekliliği yönetimine ilişkin rollerin ve sorumlulukların belirlendiği, iş sürekliliği yönetim politikasının oluşturulduğu başlangıç adımı ile başlar. İkinci olarak, iş etki analizi ve risk değerlendirme aşamalarıyla devam eder. İş etki analizi ve risk değerlendirme sonuçlarından bir iş sürekliliği yönetim stratejisi belirlenir. Belirlenen politika ve prosedürler dikkate alınarak oluşturulan iş sürekliliği ve felaket kurtarma planı uygulamaya konulur. Bundan sonra, uygulamaya konulan iş sürekliliği ve felaket kurtarma planının performansını ve güvenilirliğini doğrulayan ve bu planın kurtarma hedeflerine uygun olup olmadığının değerlendirildiği test ve bakım adımı dönemsel olarak uygulanır. Devamında ise, işletmenin yönetim kurulu, üst düzey yönetimi, iş süreci sahipleri ve diğer personelleri; önemli iş sürekliliği kavramlarını, karşılıklı bağımlılıkları, kesinti etkilerini ve operasyonel esnekliği içeren bir sürekli eğitime tabi tutulmalıdır.

3.2.1. Organizasyon, Roller ve Sorumluluklar

İş sürekliliği yönetimi için işletmenin hangi kurumsal fonksiyonunun sorumluluk alması gerektiği sorusu önemlidir. İş sürekliliği yönetiminde işletmenin tüm kurumsal fonksiyonlarının ve üst düzey yönetiminin rol ve sorumluluklarının tanımlanması gerekir. Sağlam bir iş sürekliliği yönetim stratejisi, işletmenin yönetim kurulunun, üst düzey yönetici ekibinin, finans, muhasebe, bilgi teknolojileri ve diğer iş birimlerinin geniş katılımını gerektirir. Buna göre;

- İşletmenin yönetim kurulu, iş sürekliliği yönetim programının yürütülmesinde liderlik göstererek iş sürekliliği planının geliştirilmesine ve sürdürülmesine bağlılığın gösterilmesinde özel bir role sahiptir. Bu nedenle iş sürekliliği yönetiminin önemini ve yetersiz görülen iş sürekliliği yönetim stratejilerinin risklerini anlamalıdır. Bu kapsamda işletmenin iş sürekliliği planının yılda en az bir kez gözden geçirilmesi için gerekli aksiyonları almalıdır. İş sürekliliği yönetimi ile ilgili düzenleyici kuruluşlar tarafından yayımlanan yeni düzenlemelerden veya imzalanan sözleşmelerden kaynaklanan güncellemelere ilişkin işletmenin üst düzey yöneticilerinden konuyla ilgili gerekli aksiyonu almaları talep edilmelidir. Yönetim kurulu kararlarıyla iş sürekliliği yönetim stratejisinin stratejik hedeflerini onaylamalıdır. Bir felaket durumunda iş sürekliliği ile ilgili paydaşların nasıl bilgilendirileceği konusunda kararlar almalıdır. Bağımsız denetim faaliyetleri kapsamında iş sürekliliği yönetimi ile ilgili dokümantasyon ve süreçlerin gözden geçirilmesine yönelik denetim komitesini görevlendirmelidir.

- Üst düzey yönetici ekibi işletmenin iş sürekliliği yönetim uygulamaları ve yetersiz görülen iş sürekliliği yönetim stratejilerinin riskleri hakkında detaylı bilgilere sahip olmalı ve bu kapsamda

işletmenin iş sürekliliği yönetim stratejisinden ve iş sürekliliği planlarındaki önemli değişikliklerden yönetim kurulunu haberdar etmelidir. İş sürekliliği yönetiminin stratejik hedeflerini belirleme konusunda sorumluluk almalıdır. İş sürekliliği yönetim planlama çalışmalarında yapılan iş etki analizi, kritiklik analizi, risk değerlendirme aşamalarındaki sonuçları (RPO, RTO, WRT, MTPoD, risk yanıt stratejileri vs.) dönemsel olarak gözden geçirmeli ve onaylamalıdır. İş sürekliliği yönetiminin test, bakım ve eğitim çalışmalarının önemini desteklemeli ve bu konuda tüm çalışanları iş sürekliliğinin önemine inandırmalıdır. Ayrıca kilit iş sürekliliği yönetimi sorumluluklarına sahip olacak yöneticileri belirlemelidir.

- İş birimleri ise, iş sürekliliği yönetim uygulamaları hakkında sağlam bir çalışma bilgisine sahip olmalıdır. Bunun yanı sıra, kritik iş süreçlerinin tanımlanması aşamalarına katılım göstermelidir. Böylece işletmenin tüm birimlerinin katılımıyla hangi süreçlerin gerçekten kritik olduğu daha geniş bir bakış açısıyla değerlendirilir. Kendi sorumluluk alanları dâhilindeki kritik iş süreçlerinin iş etki analizi ve risk değerlendirme çalışmalarına katılmalıdır ve sorumluluk alanları dâhilindeki kritik iş süreçlerine ilişkin hazırlanan iş sürekliliği yönetim stratejilerinin oluşturulmasına katkıda bulunmalıdır. İş sürekliliği yönetimi test, bakım ve eğitim çalışmalarına katılımı desteklemeli ve müdahale stratejilerini test etmelidir.

3.2.2. İş Sürekliliği Yönetim Politikası

Bir iş sürekliliği yönetim politikası, iş sürekliliği yönetiminin işletme için ne olduğuna ve işletmenin iş sürekliliği yönetimi ile ilgili olarak nasıl hareket edeceğine ilişkin ilkeleri ana hatlarıyla belirten bir dokümandır. Bir işletmenin iş sürekliliği yönetimine yönelik amaçlarını, ilkelerini ve yaklaşımını belirler. İş sürekliliği yönetiminin nasıl gerçekleştirileceğini belirtmeden neyin başarılması veya ne sonuca ulaşılması gerektiğini belirtir. İş sürekliliği yönetim politikası, üst yönetime ve iş sürekliliği yönetimini yönlendirecek komiteye iş sürekliliği yönetim programında ve iş sürekliliği projelerinde önemli kararlar alırken direktif verir ve rehberlik eder. Politika, iş sürekliliği projesindeki kilit aşamaları, her aşama için ana faaliyetleri ve çıktıları belirler ancak her bir iş sürekliliği projesi için ayrıntılı faaliyetlerden ve görevlerden bahsetmez. İşletme yönetiminin iş sürekliliği yönetimi konusunda kararlı ve ciddi olduğu mesajını iletmeye ve bu mesajı güçlendirmeye yardımcı olur. Genel olarak bir iş sürekliliği yönetim politikası aşağıdaki temel unsurları içerir:

Politika bildirimi: İş sürekliliği yönetiminin işletme için ne anlama geldiğinin, iş sürekliliği yönetiminin işletme için öneminin ve işletmenin iş sürekliliği yönetimine ilişkin beklentilerinin yer aldığı bölümdür.

Kapsam: İş sürekliliği yönetiminin kapsamının belirtildiği bölümdür. Örneğin, işletmenin iş sürekliliği yönetimi tüm bölümleri, yan kuruluşları veya şubeleri kapsıyor mu? Dış hizmet sağlayıcıların, iş ortaklarının ve diğer paydaşların iş sürekliliği yönetimi için herhangi bir sorumluluğu bulunuyor mu?

İş sürekliliği yönetiminin amaçları: İş sürekliliği yönetiminin işletme için amaçlarının somutlaştırıldığı bölümdür. Örneğin, bir olaydan önce veya olay sırasında ve sonrasında nelerin başarılacağı, iş sürekliliği zaman çerçevelerinin beklentileri, kılavuzlara ve düzenleyici/yasal gerekliliklere uyum ihtiyacı hususlarına bu bölümde yer verilebilir.

İş sürekliliği yönetimi planlama parametreleri: İş sürekliliği yönetim programının varsayımları, sınırlamaları ve limitlerinin belirtildiği bölümdür. Örneğin, kesinti süresi ve planlanan kaybın boyutu, insanların ve kaynakların mevcudiyeti, yedek veri ve tesislerin mevcudiyeti ve erişilebilirliği vb. hususlar bu başlık altında detaylandırılabilir.

İş sürekliliği yönetimi gereksinimleri: İşletmenin iş sürekliliği yönetim programının gerekliliklerini yerine getirmek için yapması gerekenlerin belirtildiği bölümdür. Örneğin, iş etki analizi yapmak, kritiklik analizi yapmak, risk değerlendirmesi yapmak, iş sürekliliği yönetim planının test, bakım ve eğitimini gerçekleştirmek gibi gereklilikler bu bölümde yer alabilir.

İş sürekliliği yönetimi roller ve sorumluluklar: İşletme yönetiminin, üst düzey yöneticilerin, birim yöneticilerinin ve çalışanların iş sürekliliği yönetimine ilişkin sorumluluklarının belirlendiği bölümdür.

Politika yönetişimi: İş sürekliliği yönetim politikasının gözetiminden sorumlu kişilerin ve politikaya uygunluğun nasıl izlenip raporlanacağının belirlendiği bölümdür.

Yürürlük tarihi: Politikanın yürürlük tarihi ve ne sıklıkla gözden geçirileceğine ilişkin bilgilerin yer aldığı bölümdür.

3.2.3. İş Etki Analizi ve Risk Değerlendirme Süreci

İş Etki Analizi Süreci

Kapsamlı bir iş etki analizi, iş sürekliliği planlamasının temel adımlarından biridir. İşletmenin vermiş olduğu ürün ve hizmetler açısından, kritik iş süreçlerinin analiz edilmesi ve bir iş kesintisinin ürün veya hizmetin sürdürülmesi üzerindeki etkilerinin anlaşılması sürecidir. Ayrıca bir iş etki analizi, işletmenin temel hizmetlerinin devam ettirilme sırasını, bunların devamlılığını veya yeniden başlatılmasını kolaylaştırmak için gereken kaynakları onaylar. Kritik iş süreçlerinin kesinti sonuçlarını tahmin eder ve kurtarma stratejileri geliştirmek için gereken bilgileri (RTO, RPO, WRT, MTPoD vs.) sunar. Kritik iş süreçlerini ve bu süreçlerin devamlılığına yönelik potansiyel tehditleri tanımlar. İş süreçlerinin önceliklendirilmesine yardımcı olur.

Etkili ve uygulanabilir bir iş etki analizi tamamlamak için; işletmenin üst yönetiminin, iş etki analizi sürecini desteklemesi ve işletmenin tüm iş birimlerine, iş sürekliliği sorumlusuna yardımcı olmaları için talimat vermesi gerekir. İş etki analizinin amacının, hedeflerinin ve kapsamının açıkça tanımlanması ve iş etki analizinden ve iş süreçlerinden sorumlu kişilerin belirlendiği bir organizasyon şemasının oluşturulması gerekir. Ayrıca, işletmenin ürün veya hizmetlerini destekleyen kritik süreçler ve politikalar arasındaki bağımlılıklar, bilgi sistemleri bağımlılıkları ve süreçler arasındaki karşılıklı bağımlılıklar belirlenmelidir.

Öte yandan, iş etki analizi işletmeye aşağıdaki konularda yardımcı olabilir:

- İşletme iş etki analizi ile her kritik sürecin veya hizmetin tahammül edebileceği kesinti süresi konusunda net bir anlayışa sahip olur.

- Kritik iş süreçlerinin ve bu süreçlerin kesintiye uğraması durumunda geri yüklenmesi veya faaliyete geçirilmesi gereken hedef zaman dilimleri belirlenir.

- Kritik iş süreçlerinin kesintiye uğramasıyla ilişkili maliyetleri ve uzun vadeli etkileri belirler. Bunlar arasında finansal etkilerin yanı sıra, çevresel etkiler, müşteri kaybı etkisi, itibar kaybı etkisi de sayılabilir.

Bir iş etki analizi, önemli bir iş sürekliliği kesintisinin ardından kısa bir zaman dilimi içinde kritik ve/veya hayati önem taşıyan süreçleri diğer süreçlerden ayırarak somutlaştırır. Böylece, işletmenin tüm iş birimleri, kesinti boyunca minimum hizmet standartlarının korunmasını sağlar ve derhal geri yüklenmesi gereken süreçlere uygun şekilde öncelik verir.

Bir işletmenin karmaşıklığı ve büyüklüğünden bağımsız olarak, işletmenin bir kısmı veya tamamına yönelik kapsamlı bir iş etki analizini tamamlamak için temel adımlar aşağıda sıralanmıştır:

1) Kapsamın Tanımlanması

Bir iş etki analizinin kapsamı tanımlanırken aşağıdaki hususlar dikkate alınmalıdır:

- Amaçlanan iş etki analizinin işletmenin tamamına mı yoksa bir kısmına mı yönelik olduğuna karar verilmelidir. İşletmenin büyüklüğü ve karmaşıklığı veya iş etki analizini tamamlamak için mevcut kaynaklar gibi bazı faktörler bu kararı etkileyecektir.

- Bir iş kesintisi durumunda iş birimlerine neyin kritik olduğunu sormadan önce, iş etki analizi tanımları ve işletme politikasına ilişkin net bir anlayışa sahip olunmalıdır.

- Kritiklik analizi için kıyaslama kriterleri tanımlanmalı ve iş birimleri tarafından konu hakkında bilgi sahibi olunmalıdır. Böylece tüm işletme genelinde tutarlı bir yaklaşım sağlanır.

- İş etki analizinin amacı ve önerilen kapsamı, işletmenin üst yönetimi ve iş birimi yöneticilerine sunulmalıdır.

2) İş Etki Analizinin Hazırlanması

Bir iş etki analizi; veri toplama yöntemi, işletmenin büyüklüğü, karmaşıklığı ve kültürü göz önünde bulundurularak hazırlanmalıdır. İşletme yöneticileri iş süreçlerini önceliklendirmemelidir. Bunun yerine, işletmenin tüm iş birimlerinin her personel düzeyinde (çalışanlar, yönetim kurulu, yöneticiler) katılım sağlanabilecek anketler aracılığıyla iş sürekliliği yönetim sorumlusu tarafından bir bütün olarak iş süreçleri önceliklendirilmelidir.

Ayrıca iş etki analizleri işletmenin kilit alanlarına odaklanmalıdır. İşletmenin kritik iş süreçlerini yerine getirmek için gerekli becerilerin sağlanması açısından tüm personelin sağlığı ve güvenliği, işletmenin sahip olduğu maddi ve maddi olmayan varlıklar açısından kritik iş süreçlerinin yürütüldüğü tesisleri, kritik iş süreçlerini destekleyen bilgi sistemleri, işletme içinde veya dışındaki paydaşlar ve işletmenin itibarının, sözleşmelere, mevzuata ve yükümlülüklere uyumu açısından işletme profili kilit alanlardan sayılabilir.

3) Veri Toplama: Kapsam ve Yöntemler

İşletmenin her iş birimi için veri toplama kapsamının tanımlanması önemlidir. Buna göre iş etki analizinde veri toplama sürecinde veri için iletişime geçilecek kişi, istenen verinin bulunduğu lokasyon ve verinin güvenilirliği ile güncelliği belirlenmelidir.

Verilerin toplanıp doğrulanabileceği çeşitli yöntemler vardır ve seçilen yöntemlerin istenen sonuçları üretmesi ve işletme ihtiyaçlarını karşılamak için esneklik sunması gerekir. Seçilecek yöntemler, her bir iş biriminin bilgi gereksinimlerine ve organizasyonel kapasitesine uygun olmalıdır. İş etki analizi veri toplama yöntemleri genellikle şunlardır:

Anketler: Bu yöntem, soruların elektronik veya manuel olarak dağıtılabileceği basit, uygun maliyetli yazılı bir formattır. Görüşülen kişiler, anketleri bağımsız olarak ve anket geliştiricisinden yani iş sürekliliği yönetim sorumlusundan minimum destek alarak tamamlar.

Çalıştaylar: Bu yöntem, farklı görüşleri paylaşma ve görüşülen kişilerle ortak bir zemin veya fikir birliği arama fırsatı sunar. Daha küçük gruplar daha ayrıntılı ve bilgilendirilmiş geri bildirim sağlama eğilimindedir, ancak hem zaman hem de kaynaklar açısından maliyeti önemli ölçüde artırabilir.

Kişisel görüşmeler: Bu yöntem, görüşmeci ve katılımcı arasında uzun süreli etkileşimi sağlayan bire bir, ayrıntılı görüşmelerdir. Görüşmeci ek sorular sorabilir veya görüşülen kişi tarafından gündeme getirilebilecek diğer ipuçlarını keşfedebilir.

Fiziksel inceleme: Bu yöntem, incelemeyi yapan kişinin, işletmenin iş birimlerinin çalışma ortamını fiziksel olarak inceleyerek, personel ile operasyonel süreçler hakkında doğrudan konuşma ve çevresel risklerin profesyonel bir değerlendirmesini tamamlama fırsatına sahip olduğu bir yöntemdir. Bu veri toplama yönteminin riski, incelemeyi yapan kişinin iş biriminin iş süreçleri hakkında yakından bilgi sahibi olmaması olasılığıdır.

4) Veri Toplama Sonrası Faaliyetler

İş etki analizi görüşmesinden elde edilen veriler tutarlı bir şekilde kaydedilmelidir. Elde edilen verilerin sonuçları iş birimleri yöneticileri ile teyit edilmelidir. Anket ve mülakat benzeri görüşmelerden elde edilen geri bildirimler sonucunda iş sürekliliği yönetim sorumlusu; kritik iş süreçlerini tanımlar, iş kurtarma gereksinimlerini, hedeflere ulaşmak için iç ve dış kaynak bağımlılıklarını ve bir kesintinin iş süreci üzerindeki etkisini belirler, iş süreçleri arasındaki öncelikleri ve sınıflandırmaları geliştirir, kurtarma süresi ve noktası hedeflerini geliştirir ve finansal, operasyonel, itibari ve yasal etkileri belirleyerek her süreç için maksimum tahammül edilebilir kesinti süresi hakkında bir görüş oluşturur.

5) Veri İşleme

Tüm iş birimlerinden toplanan veriler ile iş süreçlerinin kritikliğe göre düzenlenmiş bir listesi oluşturulmalıdır. Bu adım, bir kesintinin ardından hızla geri yüklenmesi gereken ve ertelenebilecek süreçleri belirlemek için gereklidir. Kritikliği belirlemek rekabet eden birimler arasında zorlayıcı olabilir. Bu nedenle kritikliği değerlendirmek için her birimin iş süreçlerinin temel misyonu ve işletmenin iş hedefleri için önemi ölçüt olarak kullanılmalıdır.

İşletmenin ürün veya hizmetlerini destekleyen iş süreçlerinin durmasına yol açabilecek bilgi sistemlerindeki bir kesinti durumunda, kesintinin işletmeye yönelik etkilerinin değerlendirilmesi de o sürecin işletme için kritikliğini belirlemede önemli bir rol oynar. Kapsamlı bir iş etki analizi, iş süreçlerinin birbirleriyle olan bağımlılıklarını, bu süreçleri destekleyen bilgi sistemleri ve dış kaynaklar arasındaki bağımlılıkları belirlemelidir. Tüm bağımlılıklar iş sürekliliği planı dâhilinde tanımlanmalıdır. Böylece bir iş kesintisinin etkileri mantıksal sonuçlara göre değerlendirilebilir.

6) Veri Kontrolü

Bir iş etki analizi çalışmasının sonuçları raporlanmadan önce, toplanan verilerin sağlıklı kararlara yol açmasını sağlamak için veri kontrolünün yapılması önemlidir. Bu şu şekilde yapılabilir:

- Mevcut veri çıktısının önceki iş etki analizi incelemelerinin sonuçlarıyla (varsa) karşılaştırılması.
- Benzer süreçleri gerçekleştiren iş birimleri arasında kapsamlı bir karşılaştırma yapılması.
- Tüm iş birimlerinin yöneticilerinden, iş etki analizi çalışmalarının sonuçları hakkında geri bildirim veya düzeltme talep edilmesi.

7) Nihai İş Etki Analizi Raporu

Bir iş etki analizi raporu, işletmenin taraf olduğu sözleşmeleri veya yasal yükümlülükleri dikkate alarak operasyonel gereksinimleri sunması gereken bir rapor veya beyandır. Bu rapor, toplanan, analiz edilen ve yönetilen verilere dayanmaktadır. Rapor, bir işletmenin mevcut operasyonel ve kurtarma gereksinimlerini sunar. İş etki analizi raporunda, işletmenin politika ve prosedürlerine, yasal yükümlülüklerine ve en iyi uygulamalara yer verilerek iş etki analizinin amacı hakkında açıklamalar yer alır. Bunun yanı sıra iş etki analizini uygulamak için kullanılan yöntemler tanımlanır. İş etki analizi verilerini doğrulamak ve kontrol etmek için atılan adımlar açıklanır. Kritik iş süreçlerinin ve bunlarda meydana gelebilecek kesintinin etkileri, kritiklik sırasına göre yani maksimum tahammül edilebilir kesinti süresine (MTPoD) göre gruplandırılarak sunulur. Her bir kritik iş sürecinin kurtarılması için gerekli minimum kaynaklar belirlenir.

Risk Değerlendirme Süreci

Bir işletmenin ürün veya hizmetleri sunma becerisinde aksamalara yol açan bir durum, iş sürekliliği planı kapsamında bir risktir. Risk değerlendirmeleri daha önce de bahsedildiği üzere meydana gelme olasılığı ve meydana gelme etkisi olmak üzere iki faktör göz önünde bulundurularak tamamlanır. Kesintileri önlemeye ve iş sürekliliğini sağlamaya ilişkin tamamlanmış bir risk değerlendirme süreci, işletmenin kritik iş süreçlerinin sağlanmasına yönelik risklerin anlaşılmasını, farklı türlerdeki riskler arasında karşılaştırmalar yaparak, risk yanıt stratejilerinin önceliklendirilmesini ve işletmenin kritik iş süreçlerinin riske açıklığının değerlendirilmesini sağlar.

Başarılı bir risk değerlendirmesi için işletmenin kritik iş süreçleri herhangi bir risk değerlendirme sürecinin başlatılmadan yani iş etki analizi sürecinde tanımlanmalıdır. Risk değerlendirme sürecine katılacak iş birimleri tarafından, seçilen risk değerlendirme yöntemi tam olarak anlaşılmalıdır. Risk değerlendirme sürecinde öngörülemeyen riskler nihai değerlendirmede dikkate alınmalıdır. İşletme yönetimi tarafından risk değerlendirmesi sonuçları onaylanmalıdır. Risk değerlendirmeleri en azından yıllık olarak gözden geçirilmeli ve işletmede önemli bir değişiklik olduğunda eksiksiz olarak tekrar gerçekleştirilmelidir.

Aşağıda TS ISO 31000 Risk Yönetim Standardı'na göre bir risk değerlendirmesinin örnek bir incelemesi yer almaktadır.

1) Risk tanımlaması

Spesifik riskler, tanımlama süreci altında isimlendirilir ve tanımlanır. Risk tanımlama yöntemleri arasında anketler, görüşmeler, odak grupları, çalıştaylar, önceden onaylanmış politika belgeleri, mevzuat ve geçmiş veriler yer alır.

2) Risk analizi

Risk analizinin amacı, tanımlanan risklerin meydana gelme olasılığı ve kritik süreçler üzerindeki etkisi açısından riski anlamaktır. Bir riskin meydana gelme olasılığının ve etkisinin belirlenmesinin birçok yolu vardır, ancak en yaygın olarak kullanılan iki analiz yöntemi nicel analiz ve nitel analiz yöntemleridir.

Nicel analiz, riskler için belirli istatistiksel değerlerin karşılaştırılmasından oluşur. Genel olarak bu yöntem en çok, bir kesintinin etkisine sayısal bir değer atamak mümkünken, bir riskin olasılığına sayısal bir değer atamak mümkün olmadığında, olasılıktan ziyade bir kesintinin etkisini karşılaştırmak için kullanılır. Örneğin, işletmenin tesislerinin bulunduğu bölgede ne sıklıkla sel meydana geleceği tahmin edilemezken, işletmenin tesislerinde meydana gelebilecek bir selden dolayı oluşacak maddi kayıplar bellidir.

Nitel analiz, sayısal olarak ölçülemeyen özelliklere ilişkin araştırmaları kapsar ve gözleme dayalıdır. Nitel bir değerlendirmede, olasılık ve etki sayısal olarak tahmin edilmez, ancak yüksek olabilirlik, düşük olabilirlik vb. niteleyiciler kullanılarak sözlü olarak değerlendirilir. Niteliksel risk analizinin amacı, diğerlerine göre öncelik verilmesi gereken kısa bir risk listesi oluşturmaktır.

Hem nitel hem de nicel teknikler, bir riskin olasılığını ve etkisini belirlemede faydalıdır, ancak her iki yöntem de üstün değildir. Nicel analiz daha spesifiktir, ancak bir karşılaştırmanın faydalı olması için riskle ilgili tüm bilgilerin ayrıntılı, doğru ve tutarlı olması gerekir. Nitel analiz, önceki yönteme göre daha az spesifik olmakla birlikte, potansiyelleri daha iyi tanımlayabilir.

Risk analizinde önemli hususlar şunlardır:

- Riskin sıklığı.
- Riskin öngörülebilirliği.
- Riskin etki hızı (örneğin bir yangın riskinin etki hızı yüksek, pandemilerin hızı düşüktür).
- Risk uyarısı ile risk oluşumunun etkisi arasındaki süre.
- Belirli bir riskin neden olabileceği muhtemel kesinti süresi.
- Belirli bir riskin neden olabileceği kesintinin kalıcılık derecesi (örneğin bir yangın riski nedeniyle tahrip edilen bir tesis yüksek derecede kalıcılığa sahipken, bir pandeminin neden olduğu personel kesintileri riski düşük derecede kalıcılığa sahiptir).

3) Risk irdelemesi

Risk irdelemesi, bir riskin kabul edilebilir veya tolere edilebilir olup olmadığını belirlemek için risk seviyelerini belirlenmiş kriterlerle karşılaştırma sürecidir ve bir işletmenin risklere karşı savunmasızlığının belirlenmesine yardımcı olur. Aşağıdaki risk irdelemesi için örnek bir sınıflandırma yöntemi yer almaktadır:

	Olasılık			
Etki	**Düşük**	**Orta**	**Yüksek**	**Çok Yüksek**
Büyük				
Orta				
Küçük				
İhmal Edilebilir				

	Bu riskler çok yüksektir. Bu riskleri azaltmak için önerilen karşı önlemler mümkün olan en kısa sürede uygulanmalıdır.
	Bu riskler orta düzeydedir. Karşı önlem uygulaması yakın gelecekte planlanmalıdır.
	Bu riskler düşüktür. Karşı önlem uygulaması, kuruluşun hazırlık durumunu artıracaktır. Yukarıdaki risklerden daha az aciliyet taşırlar.

Şekil 10: Risk irdeleme sınıflandırma yöntemi

4) Risk yanıtı

Risk yanıt stratejileri arasında kritik sistemlerin yedekliliğinin artırılması, personel artırımı veya değiştirilecek personelin belirlenmesi, alternatif tesislerin belirlenmesi vb. yer alır. Risk yanıt stratejisinin kilit yönlerinden biri ilgili maliyetlerdir ve kaynakların kısıtlı olduğu bir ortamda her olası riske karşı yanıt stratejisi oluşturmak mümkün olmayabilir. Riskleri kabul etme konusundaki nihai karar işletme yönetiminin olmalıdır. Risk kabulü, riskten kaçınma, risk transferi, riski azaltma olmak üzere dört temel risk yanıt stratejisi vardır.

İşletmenin kritik iş süreçlerinde meydana gelen kesintiye sebep olan riskin işletme üzerindeki potansiyel etkisi minimumsa, bu riskin meydana gelme olasılığı çok düşükse ve işletmenin bu riskten kaynaklanan potansiyel kaybı, riskten kaçınmanın getireceği maliyetten büyük değilse, işletme riski kabul edebilir.

İşletmenin kritik iş süreçlerinde meydana gelen kesintiye sebep olan riskin işletme üzerindeki etkisi düşük ancak bu riskin meydana gelme olasılığı yüksekse, işletme riski azaltabilir.

İşletmenin kritik iş süreçlerinde meydana gelen kesintiye sebep olan risklerin işletmeye olan etkisinin üçüncü bir tarafla paylaşılmak istenmesi durumunda, işletme riski transfer edebilir.

İşletmenin kritik iş süreçlerinde meydana gelen kesintiye sebep olan riskin olasılığı ve etkisi yüksekse işletme riskten kaçınabilir.

3.2.4. İş Sürekliliği Yönetim Stratejisi

İş etki analizine ve risk değerlendirmesine dayalı uygun bir stratejinin seçimi, iş sürekliliği yönetim planını geliştirmek için bir sonraki adımdır. İş sürekliliği stratejisi, olağanüstü durum da dâhil olmak üzere kesinti durumunda bir sistemi kurtarmanın en iyi yolunu tanımlar ve hangi ayrıntılı kurtarma prosedürlerinin geliştirilebileceğine dayalı olarak rehberlik sağlar. İş sürekliliği stratejisi, işletmenin, bir felaket ya da bir iş kesintisi ile karşılaşıldığında sürekliliği ve kurtarmayı sağlayan yaklaşım olarak tanımlanır. İş sürekliliği yönetim sürecinin bu aşaması, bir afetin meydana gelmesi ile

normal operasyonların geri kazanıldığı zaman arasında işletmenin ürün ve hizmetlerinin sunumunu destekleyen kritik iş süreçlerini sürdürmek için yapılacak eylemleri belirlemekle ilgilidir. Her bir kritik iş süreci için önceden kurtarma hedefi zamanı (RTO) ve kurtarma hedefi noktası (RPO) belirlendikten sonra, işletmenin onu karşılamak için bir strateji belirlemesi gerekmektedir. Bu aşama, işletmenin iş hedeflerini sağlamaya yönelik süreçlerdeki kesintinin ve kaynaklardaki kaybın azaltılması için uygun adımların atılmasını içerir.

İş sürekliliği stratejileri, büyük bir aksama karşısında işletmenin gereksinimlerini destekleyecek kapsamlı yaklaşımı ve metodolojiyi belirleyen profesyonel uygulamalardır. Tamamlanmış risk değerlendirmeleri ve iş etki analizleri bu stratejilerin girdilerini oluşturur. İş sürekliliği stratejileri aşağıdaki şekillerde olabilir:

- **Önleme stratejileri:** Olayı önlemeye odaklanmıştır.
- **Azaltma stratejileri:** Azaltma, sınırlama veya sonuçların kontrolüne odaklanmıştır.
- **Hazırlık stratejileri:** Etkili bir müdahalenin hazırlanmasına, süreklilik ve kurtarma yönetimi planlamasına odaklanmıştır.
- **Müdahale stratejileri:** İnsanları, mülkü, çevreyi ve operasyonların sürekliliğini tehdit eden olaylara müdahaleye odaklanmıştır.
- **Süreklilik stratejileri:** Kritik hizmetlerin devamlılığına odaklanmıştır.
- **Kurtarma stratejileri:** Hizmetleri kabul edilebilir bir düzeye getirmeye odaklanmıştır.
- **İletişim stratejileri:** Etkili iletişime odaklanmıştır.
- **Eğitim ve öğretim stratejileri:** Yeterliliğe dayalı eğitim ve öğretime odaklanmıştır.

Stratejiler, işletmenin ilgili tüm yöneticilerinin katkılarını ve görüşlerini dikkate almalıdır. İş etki analizi ve risk değerlendirme süreçlerine benzer şekilde, işletmenin yönetim ekibi iş sürekliliği stratejileri için nihai otoritedir. Bu nedenle stratejiler, yönetici düzeyinde kabul edilmeli ve finanse edilmelidir. Bunun yanında, operasyonel düzeyde uygulanması ve test edilmesi gerekir.

3.2.5. İş Sürekliliği ve Felaket Kurtarma Planının Uygulanması

İş sürekliliği ve felaket kurtarma planı iş sürekliliği yönetiminin önemli bir bileşenidir. İşletmenin kritik iş süreçlerine odaklanır ve işletmenin büyüklüğüne ve karmaşıklığına göre değişir. Bir iş sürekliliği planı, strateji belirlendikten sonra olay müdahalesi, felaket kurtarma ve kriz yönetimi gibi belirli unsurları içerir. Daha küçük işletmelerin bu unsurları içeren tek bir iş sürekliliği planı olabilirken, büyük ve karmaşık işletmelerin birden fazla planı olabilir. Bir iş sürekliliği planını gerçekleştirmek için bazı aşamaların yerine getirilmesi gerekir.

İş sürekliliği planının etkinleştirme aşaması, bir iş kesintisi sırasında ve hemen sonrasındaki zamanı ele alır. Bu aşamada işletmenin iş sürekliliği planını ne zaman ve ne şekilde etkinleştirileceğinin tanımlanması gerekir. İşletme iş süreçlerini kesintiye uğratan her küçük aksaklık için iş sürekliliği planını etkinleştirmek istemez. Bu nedenle iş sürekliliği planının etkinleştirilip etkinleştirilmeyeceğinin veya ne zaman etkinleştirileceğinin belirlenmesi için prosedürler belirlenmelidir. Ek olarak, planı etkinleştirme yetkisinin kimde olduğu ve o yetkilinin iş sürekliliği faaliyetlerini başlatmak için hangi adımları atacağı da dâhil olmak üzere planın nasıl etkinleştirildiği prosedürlerde belirtilmelidir.

Etkinleştirme aşamasında, iş sürekliliği planının ne zaman ve nasıl uygulanacağının bilinmesi için felaket türlerinin ve kesinti seviyelerinin tanımlanması gerekir. Örneğin bir siber saldırı yaşanması ile sunucu odasında yangın çıkması durumlarında planın farklı aşamaları etkinleştirilmelidir. Bu nedenle, iş sürekliliği ve felaket kurtarma planı uygulamasını neyin tetiklemesi gerektiğini anlamak için çeşitli felaket türleri ve düzeyleri tanımlamak önemlidir. Felaketler büyük, orta ve küçük olarak sınıflandırılabilir. Örneğin büyük bir felaket veya kesintinin meydana gelme olasılığı düşük olmasına rağmen, işletme üzerindeki etkisi son derece yüksektir. Böyle bir felaket durumunda işletmenin normal iş operasyonlarının tamamı veya kritik iş süreçlerinin çoğu kesintiye uğrar. Bu durumda iş sürekliliği

planının neyi gerektirdiği tanımlandıktan sonra, planın hangi bölümlerinin etkinleştirileceği ve hangi ekip üyelerinin çağrılacağı hususlarını tanımlamak gerekir.

İş sürekliliği planı kendi kendine etkinleştirilemediğinden, birinin veya bir ekibin felaket durumuyla ilgili uygun değerlendirmeler yapması ve planı veya planın bölümlerini etkinleştirip etkinleştirmeme konusunda bir karar vermesi gerekir. Bu nedenle, iş sürekliliği ve felaket kurtarma ekipleri oluşturmak ve sürdürmek de önemlidir.

Her bir kesinti seviyesi, açıkça tanımlanmış tetikleyicilere sahip olmalıdır. Tetikleyiciler; işletmenin ticari faaliyetlerinde kesinti meydana geldiğinde veya bir veya daha fazla sunucunun hizmet dışı kalması, fiziksel bir tesisin yangın nedeniyle kesintiden etkilenmesi, iletişim ağının bir kısmının hizmet dışı kalması gibi durumlar meydana geldiğinde devreye sokulabilir.

İş sürekliliği planında bir diğer önemli çalışma ise kesinti öncesinde, sırasında ve sonrasında çeşitli ihtiyaçları karşılayacak ekipler oluşturmak ve karar verici personellerin kim olacağını tanımlamaktır. Bu çalışmada, iş sürekliliği ve felaket kurtarma ekiplerinin türlerini, rollerini ve sorumluluklarını net bir şekilde tanımlamak gerekir. Ekipler için tanımlanan rol ve sorumluluklara uygun belirli kişiler veya pozisyon tanımları atanmalıdır. Bu çalışmadaki bir diğer önemli görev, önemli iletişim bilgilerinin bir listesini oluşturmaktır. Bilgisayar sistemleri genellikle ağ güvenliği ihlallerinden sel ve yangınlara kadar çeşitli iş kesintilerinden etkilendiğinden, iletişim bilgilerinin elektronik ve basılı olarak saklanması ve erişilebilir olması gerekir. Hatta tesis dışında bir konumdan da bu iletişim bilgilerine ulaşılması sağlanmalıdır. Ancak bu veriler kişisel veri olduğundan, aynı zamanda gizli ve hassas veriler olarak ele alınmalı ve bu şekilde güvence altında tutulmalıdır. Bir irtibat listesi geliştirmenin ve sürdürmenin yanı sıra, bir irtibat ağacı da tanımlamak gerekir. Bu, işletme içinde diğer ekiplerle, üst düzey yöneticilerle, işletme yönetimiyle ve işletmenin paydaşlarıyla iletişim kurmaktan kimin sorumlu olduğunu tanımlar. Bu şekilde her ekip üyesine belirli kişilere veya paydaşlara özel çağrılar yapma görevi verilir ve bildirim süreci kolaylaştırılır.

İş sürekliliği planında oluşturulan ekiplere görevleri ve kaynakları atanmalıdır ve işletmenin iş sürekliliği stratejileriyle uyumlu olmalıdır. Bu, önemli sunucular için yeni kesintisiz güç kaynakları satın almayı ve kurmayı, yangın söndürme sistemlerini güncellemeyi veya alternatif bir site düzenlemeyi içerebilir. Diğer yandan, bir kesintiden önce planın tetikleyicilerinin tanımlanması veya iş etki analizi çalışmalarındaki veri toplama gibi görevler de belirlenmelidir. Bu görevler geliştirilirken aşağıdaki adımlar uygulanabilir:

- Üst düzey görevlerin belirlenmesi.
- İş birimi yönetilebilir hale gelene kadar büyük görevlerin daha küçük görevlere bölünmesi.
- Görevlerle ilgili sürenin veya son teslim tarihlerinin tanımlanması.
- Görev sahiplerinin atanması.
- Görev kaynaklarının ve diğer görev gereksinimlerinin tanımlanması.
- Görev için teknik ve işlevsel gereksinimlerin belirlenmesi.
- İç ve dış bağımlılıkların tanımlanması.

İş sürekliliği planı etkinleştirme uygulama aşamasında işletmenin geliştirmesi gereken çeşitli iletişim planları vardır ve açıkça tanımlanması gereken kritik bir hususdur. Büyük bir felaket yaşayan bir işletmenin böyle bir krize karşı etkili bir iletişim stratejisinin olması işletmenin itibarının zarar görmesini önlemede çok önemli bir rol oynar. Bir iş kesintisi meydana gelirse, işletmenin tüm çalışanlarının nasıl bilgilendirileceği tanımlanmış olmalıdır. Ayrıca, kesintinin neden kaynaklandığı, sorunu çözmek için neler yapıldığı ve daha fazla bilgi için sorumlunun kim olduğu gibi temel soruların yanıtlarının bildirilmesi gerekir. Örneğin, işletme tesislerinden birinde gece saatlerinde çıkan bir yangından haberdar edilmeyen çalışanlar planlandığı gibi sabah işe gelebilir. İş sürekliliği ekibi hâlihazırda faaliyette olabilir ancak işletmenin diğer çalışanlarının bilgiye ihtiyacı vardır. Müşteriler ve satıcılar genellikle farklı iletişim türleri gerektirir, ancak bilgiler genellikle benzerdir. İş kesintisi, sorunu düzeltmek için atılan temel adımlar, tahmini kurtarma süresi ve bu arada ihtiyaç duyulan herhangi bir geçici çözüm hakkında bilgilendirilmeleri gerekebilir. İşletmenin yatırımcılarının da bir kesinti

durumunda bilgilendirilmeye ihtiyacı vardır. Çoğu durumda, kesintinin işletme üzerindeki kısa vadeli mali etkisi ile ilgilenirler. Bu nedenle, yatırımcı grubuyla iletişim, çalışanlarınkinden çok farklı olarak belirli konuların ele alınmasını gerektirir. Bu nedenle bu iletişimden yatırımcı ilişkileri konusunda bilgili bir çalışanın veya yöneticinin sorumlu olması beklenir. Diğer tüm paydaşlarla iletişim kurmanın yanı sıra, toplumla da iletişim kurulması gerekebilir. Yerel gazetelerin, televizyon ve radyo istasyonlarının doğal bir felaketin etkileriyle ilgilenmesi beklenir. Daha da önemlisi olay bir şekilde benzersizse veya yaygın bir felaketin parçasıysa, ulusal ve uluslararası medyanın da ilgisini çekebilir. Böyle bir durumda medya ile iletişim kurulması istenebilir. Bu duruma önceden hazırlıklı olmak gerekir. Çünkü bir kriz sırasında kamuoyuna (veya medyaya) uygun şekilde tepki vermek kolay değildir.

Çeşitli olayları ve kilometre taşlarını izlemek için bir iş sürekliliği ve felaket kurtarma olay günlüğü oluşturmak gerekebilir. İşletmenin iş süreçlerinde meydana gelen bir kesintinin sebebi birkaç felaket veya olay sebebiyle gerçekleşmiş olabilir. Kronolojik bir olay günlüğüne sahip olmak koşulları netleştirmeye yardımcı olabilir, böylece uygun kararlar zamanında alınabilir.

İşletmede iş sürekliliği ve felaket kurtarma planını etkileyen bazı değişiklik kontrolleri gerekebilir. İlk olarak, mevcut planda bir değişiklik meydana geldiğinde planı güncellemek için bir yöntem tasarlamak gerekir. İkinci olarak ise, mevcut plana yeni risklerin veya belirsizliklerin eklenmediğinden emin olmak için plandaki değişiklikleri izleme yöntemine ihtiyaç duyulur.

Son olarak, nihai iş sürekliliği ve felaket kurtarma planını ilgili ekiplere dağıtmak ve saklamak için bir strateji geliştirilmelidir. Plana dair en son revizyonu dağıtmak veya ekibe yeni bir sürümün var olduğunu bildirmek için bir yönteme ihtiyaç duyulabilir. Böyle bir durumda plan, sürüm kontrolü ve revizyon bildirimi yapan bir yazılım programında saklanabilir.

3.2.6. Bilgi Sistemleri Felaket Kurtarma Planı

Bilgi sistemleri felaket kurtarma planlaması, kritik iş süreçlerini destekleyen bilgi sistemlerinin kesinti durumunda kullanılabilirliğini yönetmek veya bu bilgi sistemlerini geri yüklemek için oluşturulan bir kontrol sürecidir. Bu planın amacı, olması muhtemel bilgi sistemleri kesintilerini önlemek ve bir kesinti durumunda işletmenin kritik iş süreçlerini devam ettirebilecek bilgi sistemleri kapasitesini geri yüklemek için maliyet açısından uygun kontrollerin mevcut olduğundan emin olmaktır. Burada önemli olan nokta, işletmenin hangi bilgi sistemlerinin kullanılabilirliğinin önemli olduğuna karar vermektir. Bilgi sistemlerinin kullanılabilirliğinin önemi, bu sistemlerin destekledikleri iş süreçlerine bağlıdır. İşletmelerin birçok kilit iş süreçleri bilgi teknolojileri altyapısına ve bu altyapıda işlenen bilgilere bağlı olduğundan, bir işletmenin bilgi sistemlerinin işler vaziyette bulunması kritik öneme sahiptir. Bu nedenle bilgi sistemleri felaket kurtarma planlaması, iş sürekliliği planlaması sürecinin önemli bir parçasıdır.

Bilgi sistemleri felaket kurtarma planlaması süreci, iş süreçlerinin ve bunları destekleyen bilgi sistemlerinin kritikliği tanımlandıktan sonra periyodik olarak gözden geçirildiği bir süreçtir. Bilgi sistemleri felaket kurtarma planlamasının amacı, personeli ve işletmenin ürün ve hizmetlerini sunmasını etkileyebilecek olaylara yanıt vermek ve yasal gerekliliklere uymaktır. Felaket kurtarma planlamasının en önemli unsuru insan güvenliğini sağlamaktır. İşletmenin kritik iş süreçlerini devam ettirmek ikincil faaliyettir. Örneğin, işletme tesislerinde bir yangın olduğunda, ilk olarak güvenli bir tahliyenin yapılması hedeflenir. Hizmetleri geri yüklemek kurtarma stratejisinde ikinci öneme sahiptir.

İşletmenin üst yönetiminin uygun bir bilgi sistemleri felaket kurtarma stratejisini seçebilmesi, bilgi sistemlerinin destekledikleri iş süreçlerinin kritikliğini belirleyen iş etki analizi ile tanımlanan kurtarma hedefi zamanı (RTO) ve kurtarma hedefi noktasına (RPO) bağlıdır.

RPO, daha önce de ifade edildiği gibi, işletmenin iş süreçlerinde meydana gelen bir kesinti durumunda, kabul edilebilir veri kaybı olarak tanımlanır. Verilerin kurtarılmasının kabul edilebilir olduğu en erken zaman noktasını gösterir. Örneğin bir işletme meydana gelecek herhangi bir felaketten 2 saat öncesine kadar olan verileri kaybetmeyi göze alıyorsa, işletmenin verilerinin son yedeklemesi 2 saat kadar olmalıdır. RPO, kesinti durumunda izin verilen veri kaybı miktarını etkin bir şekilde ölçer. RPO, verileri yedeklemek ve kurtarmak için kullanılan teknolojiyi doğrudan etkiler.

RTO ise, işletmenin iş süreçlerinde meydana gelen bir kesinti durumunda, kabul edilebilir kesinti süresidir. Kesintiden sonra iş süreçlerinin ve bunları destekleyen bilgi sistemlerinin yeniden başlaması gereken en erken zamanı gösterir.

RTO ve RPO için zaman süreleri felaket anına ne kadar yakın olursa, işletmenin kurtarma stratejilerinin maliyeti o kadar yüksek olur. Örneğin bankalar ve benzeri finansal kuruluşlarda finansal, yasal ve itibari etkilerden dolayı veri kaybına tahammül olmadığından (yani RPO sıfıra yakın olduğundan), veri yansıtma (İng. data mirroring) veya gerçek zamanlı çoğaltma (İng. real time replication) teknolojilerinin kullanılması ve kesinti süresine tahammül olmadığından (yani RTO sıfıra yakın olduğundan), ikincil sistem olarak sıcak site, ya da kümeleme teknolojilerinin oluşturulması bu tür işletmelerin kurtarma stratejilerinin maliyetini artırmaktadır. RTO bilgi sistemlerinde kullanılacak teknolojiyi etkilerken, RPO bu bilgi sistemlerinde işlenen verileri koruma çözümlerini etkiler. ISACA'nın RTO ve RPO'ya ek olarak, kurtarma stratejilerinin tanımlanmasında önemli gördüğü bazı ek parametreler aşağıda yer almaktadır:

Kesinti penceresi (İng. Interruption window): Kesinti anından işletmenin kritik iş süreçlerinin ve bunları destekleyen bilgi sistemlerinin geri yüklenmesine kadar beklenebilecek maksimum süredir. Bu süreden sonra kesintinin sebep olduğu kayıplar karşılanamaz.

Hizmet sağlama hedefi (İng. Service Delivery Objective-SDO): Normal süreçler geri yüklenene kadar alternatif işlem modu sırasında ulaşılacak minimum hizmet düzeyini tanımlar.

Maksimum kabul edilebilir/tolere edilebilir kesinti (İng. Maximum Acceptable/Tolerable Outages-MAO): İşletmenin alternatif modda işlemeyi destekleyebileceği maksimum süredir. MTPoD ile birbirilerinin yerlerine kullanılır.

İşletmenin kritik iş süreçlerini destekleyen her bilgi sistemi bir kurtarma stratejisine ihtiyaç duyar. Kurtarma stratejisi, herhangi bir kesinti durumunda işletmenin iş süreçlerini destekleyen bilgi sistemlerini kurtarmanın en iyi yolunu belirler ve hangi detaylı kurtarma prosedürlerinin geliştirilebileceğine dayalı bir rehberlik sağlar. Geri kazanılacak maliyet ve etki maliyeti açısından en uygun alternatif, iş etki analizinde belirlenen risk düzeyine göre işletmenin üst yönetimi tarafından seçilmelidir. Kurtarma için belirlenen risk düzeyine dayalı kurtarma stratejileri şunları geliştirmeyi içerir:

- **Sıcak siteler:** Bir felaket durumunda kullanılmak üzere, hem donanım hem de sistem yazılımının bulunduğu, kullanıma tamamen hazır bir dış saha bilgi işleme tesisi.
- **Ilık siteler:** Sıcak bir siteye benzer, ancak kurtarma için gerekli olan tüm donanımlarla tam olarak donatılmamış site.
- **Soğuk siteler:** Bir bilgisayar tesisinin gerekli elektriksel ve fiziksel bileşenlerine sahip olan, ancak bilgisayar donanımına sahip olmayan bir bilgi sistemleri yedekleme tesisi.
- **İkiz siteler:** Esas aslı ile aynı bilgileri içeren alternatif bir site. İkiz siteler yedekleme ve felaketten kurtarma için kurulmuş ve yoğun yükleme taleplerini yerine getirmek için trafik yükünü dengeleyecek şekilde tasarlanmıştır.
- **Mobil siteler:** Bir işi yeniden başlatma lokasyonu olarak hizmet vermek için bir mobil tesis kullanımı. Tesis genellikle herhangi bir siteye taşınabilir ve bilgi teknolojileri ve personelini barındırabilir.
- **Diğer işletmelerle karşılıklı anlaşmalar:** Benzer ekipman veya uygulamalara sahip iki veya daha fazla işletme arasındaki acil işlem anlaşması. Genellikle karşılıklı bir anlaşmanın katılımcıları, bir acil durum ortaya çıktığında birbirlerine işlem sürelerini sağlamak için söz verir.

Alternatif site yani ikincil sistemler, planda dikkate alınan herhangi bir felaketten etkilenen coğrafi alanın ötesinde yer alacağı dikkate alınarak seçilmelidir. Hangi tür ikincil sistemin kullanıldığına bakılmaksızın, planın ikincil sisteme ağ bağlantısı kurması gerekir. Beklenmedik herhangi bir nedenle normal sürecin kesilmesinin ardından, ikincil sistemlere iletişimin kurulabilmesini sağlamak için çözümler sağlamalıdır.

İkincil sistemler, üçüncü taraf satıcılar tarafından veya işletmenin kendisi tarafından kurulabilir. İkincil sistemler işletmeye ait olduğunda, bir kesintinin ardından işletme yönetimi tarafından hızlıca önlem alınabilir. Ancak bu hizmet üçüncü taraf satıcılar tarafından yerine getirildiğinde, işletmenin bir kesintinin ardından ihtiyaç duyduğu kaynaklara gecikmeden erişebilmesini açıkça temin eden sözleşmelere sahip olması gerekir. İkincil bir sistem oluşturmayı planlayan işletmeler, bu alternatif siteler için gerekli donanım ve yazılımları tedarik edebilir ya da gerektiğinde temin edilmesi için bir satın alma planlayabilir.

İşletmelerin bilgi sistemi ortamları birbirinden farklılaşabilir. Bu nedenle her bir bilgi sistemi ortamı için oluşturulacak esneklik ve kurtarma yöntemi farklıdır. Bunlardan bazılarına aşağıda yer verilmiştir.

Uygulama Esnekliği ve Kurtarma Metodu: İşletmenin kritik iş süreçlerini destekleyen bir uygulamayı bir felakete karşı korumak onu en kısa sürede eski haline getirmeyi sağlamakla ilgilidir. Örneğin, kümeleme (İng. clustering) ile uygulamaların felakete karşı korunması sağlanabilir. Kümeleme yönteminde işletmenin kullandığı bir uygulama farklı bir sunucuda tekrar başlatılabilir. Böylece tek arıza noktasına karşı koruma sağlar. İki ana uygulama kümeleme yöntemi vardır. Bunlardan ilki aktif-pasif kümeleme, ikincisi aktif-aktif kümelemedir. Aktif-pasif kümelemede, uygulama yalnızca bir aktif düğümde çalışır. Diğer pasif düğümlerdeki uygulamalar, aktif düğümdeki uygulama başarısız olduğunda kullanılır. Aktif-aktif kümelemede ise, uygulama kümenin her düğümünde çalışır. Böyle bir kümeleme yönteminde uygulamada hiçbir kesinti yaşanmaz.

Veri Depolama Esnekliği ve Felaket Kurtarma Metodu: Bağımsız Diskler Yedek Dizisi (İng. Redundant Array of Independent Disks-RAID), bir disk arızasına karşı korumanın en yaygın ve temel yoludur. RAID, bir sürücü arızası durumunda verileri korumak için aynı verileri birden çok sabit diskte farklı yerlerde depolamanın bir yoludur. RAID disk ikizleme ve disk şeritleme tekniklerini kullanır. Disk ikizleme, verilerin depolama işlemini daha fazla hataya toleranslı hale getirmek için iki sabit diske ayrı bölümlerde kopyalanmasıdır ve bir disk arızası durumunda veri koruması sağlar. Çünkü veriler sürekli olarak her iki diske de güncellenir. Disk şeritleme, birden çok küçük diskin tek bir büyük disk gibi davrandığı bir tekniktir. İşlem, büyük verileri veri bloklarına böler ve bunları birden çok depolama aygıtına yayar.

İşletme, kurtarma stratejilerinde yalnızca üretim ortamına odaklanmakla kalmayıp, veri yedekleme ve çoğaltma dâhil tüm veri yinelemeleri için veri gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamalıdır. Veri yedekleme ve yeniden oluşturma, kesinti durumunda kritik iş süreçlerinin kurtarılması için önemlidir. Yedekleme dosyaları genellikle elektronik olarak oluşturulur ve dış lokasyona yansıtılabilir, çıkarılabilir medyaya yedeklenebilir, dış lokasyona döndürülene kadar ağ sunucularında geçici olarak saklanabilir veya bir bulut ortamına yedeklenebilir. Yedekler, kolayca erişilebilir olmalı ve işletmenin bilgi güvenliği politikasına uygun olmalıdır.

İletişim Ağları Esnekliği ve Felaket Kurtarma Metodu: İşletmenin iş süreçlerinin sürekliliğinde kilit öneme sahip olan iletişim altyapısının esnekliğini sağlamaya yönelik prosedürlere yüksek öncelik verilmelidir. İletişim ağları, veri depolama merkezleriyle aynı doğal afetlere karşı hassastır, ancak aynı zamanda telekomünikasyona özgü tehditlere de açıktır. Bunlara örnek olarak kablo kesikleri, iletişim yazılım hataları, telefon korsanları ve insan hataları sayılabilir. Merkezi iletişim sağlayıcıları, iletişim ağlarının esnekliğine ilişkin bir hizmet vermek zorunda olmadıklarından, işletme kendi iletişim ağlarını korumak için politika ve prosedürler oluşturmalıdır.

3.2.7. Test ve Bakım

İş sürekliliği planını test etmenin birçok nedeni vardır. En önemlilerinden biri, gerçek bir aksama veya felaket durumunda planın çalışacağından emin olmaktır. Ancak, test etmenin planın daha etkili çalışmasına yardımcı olmasının altında yatan nedenler aşağıda yer almaktadır:

1) Süreçlerin Anlaşılması: Plan etkinleştirildikten sonra çeşitli ekip üyeleri tarafından uygulanan süreçler, prosedürler ve adımlar, test aşamasının ilk adımı olmalıdır. Bu aşamada, eksik iş süreçleri ortaya çıkarılmalı ve bu süreçlerin bilgi sistemleri ve dış bağımlılıkları ile bunların karşılıklı bağımlılıkları tanımlanmalı ve doğrulanmalıdır. Öncelikli olarak işletmenin kritik iş süreçleri tekrar gözden geçirilmeli ve planın bu süreçlere ilişkin kritikliği etkin bir şekilde ele aldığından emin

olunmalıdır. Böylece test çalışmalarına katılanlar bu süreçlerden geçerek kritik iş süreçlerini öğrenmiş olur.

2) Görev Dağılımının Doğrulanması: İşletmelerin büyük ve karmaşık olduğu bir yapıda, iş sürekliliği planında tanımlanan görevler düzgün bir şekilde dağıtılıp sıralanmazsa planların çoğu uygulamada başarısız olur. Böyle bir durumda sorunun kaynağının ortaya çıkarılması saatler, haftalar veya günler alabilir. Bu görevlerin doğru bir şekilde dağıtıldığının doğrulanması acil bir durum esnasında değil, planın test aşamasında yapılmalıdır.

3) Adımların Onaylanması: Görevleri ve bunların dağılımını test etmenin yanı sıra, iş sürekliliği planında belirtilen adımların her biri doğrulanmalıdır. Plandaki adımların tek tek gözden geçirilerek doğrulanması sonucunda hatalar ve eksiklikler ortaya çıkarılır. Eğer adımlarda herhangi bir hatayla karşılaşılmazsa, planda uygulanması gereken tüm adımların doğru listelendiği ve doğru sırada olduğu onaylanmış olur.

4) Kaynakların Onaylanması: Test aşamasında tekrardan gözden geçirilen her adımda, bu adımı gerçekleştirmek için hangi kaynaklara ihtiyaç duyulduğu sorusu sorulmalı ve cevaplanmalıdır. Böylece adımlar üzerinde senaryolar oluşturulur ve adımın gerçekleştirilmesi için gerekli kaynakların neler olduğu konusunda fikir sahibi olunur. Örneğin işletme tesislerinde meydana gelen bir yangın esnasında, yangına müdahale edecek ekibe yangın söndürücü olmadan yangının nasıl söndürüleceğine ilişkin eğitim vermek doğru bir yaklaşım olmaz. Bu nedenle işletmenin yangın söndürmeye ilişkin bir müdahale planı varsa yangın söndürücü ekipmanları da olması gerekir. Buna benzer kaynak ihtiyaçları kriz esnasında ortaya çıkarsa, işletmenin iş sürekliliği planı başarısız olabilir. Dolayısıyla gerekli kaynakların test aşamasında sürekli olarak gözden geçirilerek doğrulanması gerekir. Test aşamasında işletme bu kaynaklara sahip değilse bu adımlar eksik veya kaynak ihtiyacı olarak işaretlenmeli ve bu kaynakların en kısa sürede temin edilmesi için bir eylem planı oluşturulmalıdır.

5) İletişimin Test Edilmesi: Daha önce de bahsedildiği gibi bir iş kesintisi veya felaket sırasında iletişim son derece önemlidir ve acil durumlarda veya kesinti sırasında sürdürülmesi çok zor olabilir. Testin bu aşamasında, kimin, neyi ne zaman bilmesi gerektiği test edilir. Personel, iş sürekliliği planı aracılığıyla bilgi akışını test ettikçe, gerçek bir olay sırasında bu akış hakkında daha yüksek bir farkındalığa sahip olur. Bir afet sırasında bazı iletişimler doğal olarak kopacaktır, ancak planın bilgi akışını test ederek verilecek bir eğitim, ciddi bir iletişim ve bilgi akışı kesintisi olasılığını azaltmaya yardımcı olur.

6) Boşlukların veya Zayıf Yönlerin Belirlenmesi: İş sürekliliği planı test edilirken, planın boşlukları ve varsa zayıf yönleri ortaya çıkarılmalıdır. Örneğin, işletme tesisinde çıkan bir yangının ihbar edileceği numaranın planda yer almadığı ortaya çıkarılabilir. Planın boşlukları veya zayıflıkları test aşamasında belirlenirse, bunlar iş sürekliliği planındaki değişikliklerle giderilebilir.

7) Maliyet ve Fizibilitenin Belirlenmesi: İş sürekliliği planı aşamasında, planı uygulamanın olası maliyetlerini tam olarak anlamak zordur. Ancak planı test ederken, planı uygulamak ve sürdürmek için potansiyel maliyetleri anlamak daha olasıdır. Böylece plan tamamlanmadan planın bazı adımları işletmenin bütçe kısıtlamaları nedeniyle tekrar revize edilebilir. Planın adımları gerçekten bir teste tabi tutulduğunda, bu adımların beklendiği gibi uygulanmasının veya sürdürülmesinin imkânsız olduğu ortaya çıkabilir. Bu nedenle plandaki adımların, süreçlerin ve geçici çözümlerin fizibilitesi test edilmeli ve gerçeği yansıtacak şekilde revize edilmelidir.

Riskler ve teknoloji sıklıkla değiştiği için, işletme iş sürekliliği planını mevcut ortamı yansıtacak şekilde düzenli olarak gözden geçirmeli ve güncellemelidir. Periyodik gözden geçirmeler, işletmenin iş sürekliliği planını iş hedefleriyle uyumlu hale getirmesine olanak tanır. İşletme, sistem ve süreç düzeltmeleri ve geliştirmelerine öncelik vermek ve bunlara odaklanmak için bu bilgileri kullanmalıdır. İş sürekliliği planının bakımını ve iyileştirilmesini gerektiren tetikleyiciler aşağıdakileri içerebilir:

- Kurumsal stratejilerdeki değişiklikler.
- Yeni veya yeniden yapılandırılmış ürünler, hizmetler veya altyapı.
- Üçüncü taraf hizmet sağlayıcılar tarafından sunulan ürün ve hizmetlerdeki değişiklikler.

- Üçüncü taraf hizmet sağlayıcının iş sürekliliği süreçlerinde tespit edilen eksiklikler.
- Yeni mevzuat, düzenleyici gereklilikler veya dayanıklılık uygulamaları.
- Bütçelenen ve gerçekleşen iş sürekliliği giderleri arasındaki farklılıklar.
- Alıştırmalardan, testlerden ve öğrenilen derslerden çıkan sonuçlar.
- Tehdit ortamındaki değişiklikler (örneğin yeni yetenekler, tehdit aktörlerinin amacı).
- Öneriler (örn. denetimlerden, güvenlik açığı değerlendirmelerinden ve sızma testlerinden).

Kurumsal birleşmeler, satın almalar, bölünmeler ve yeniden yapılandırma faaliyetleri de iş sürekliliği planları üzerinde önemli bir etkiye sahip olabilir. Bilgi sistemleri altyapısındaki ve süreçlerindeki değişiklik en yaygın değişikliktir ve potansiyel olarak iş sürekliliği planı üzerinde en büyük etkiye sahip olandır. Yasal, düzenleyici veya uyumluluk alanlarındaki değişiklikler de işletmede veya iş sürekliliği ve felaket kurtarma planında zorunlu değişikliklere neden olabilir. Her durumda işlemlerde yapılan değişiklikler, değişiklik bildirimlerini veya değişiklik isteklerini tetiklemelidir.

İş sürekliliği planındaki değişikliklerin kapsamını belirlemek için iş sürekliliği yöneticisi, iş, yapı, sistem, yazılım, donanım, personel veya tesislerdeki herhangi bir değişikliğin niteliğini değerlendirmek için iş birimi yöneticileriyle düzenli olarak iletişime geçmelidir.

Değişiklik talepleri oluşturulduğunda iş sürekliliği ekibi, değişikliği değerlendirmek ve plana dâhil etmek için açık ve tutarlı bir metodolojiye sahip olmalıdır. Tüm değişiklik talepleri çeşitli nedenlerle uygulanmamalıdır. Değişiklikler kabul edilmeden önce maliyet, fizibilite, arzu edilirlik, mevcut süreçlerle etkileşim ve risk etkisi gibi faktörler değerlendirilmelidir. Bir değişiklik kabul edilirse plana dahil edilmeli, plan revize edilmeli ve plan paydaşlarına bildirilmelidir.

3.2.8. Eğitim

İş sürekliliği planı eğitiminin iki ayrı bölümü vardır. Birincisi, kesintiye veya acil duruma verilen fiziksel tepkidir. Bu, bir yangın varsa bir binayı tahliye etmeyi, sunucu odasındaki yangını söndürmek için bir yangın söndürücü kullanmayı veya tesis içinde sel varsa ana su kaynağını bulmayı içerebilir. Bu eylemlerin tümü bazı temel eğitimler gerektirir, böylece müdahale ekipleri neyi, nasıl güvenli bir şekilde yapacaklarını bilirler. Bu, eğitimin bir yönüdür. Eğitimin ikinci yönü, çeşitli müdahale ekiplerinin iş sürekliliği planını nasıl uygulayacaklarını bilmelerini ve bunu yapmak için gereken becerilere sahip olmalarını sağlamakla ilgilidir. Örneğin, en son tehditler ve güvenlik önlemleri hakkında güncel kalabilmeleri için bilgi teknolojileri personeline sistem geri yükleme ve doğrulama rutini gerçekleştirme konusunda periyodik eğitim sağlanabilir.

3.2.9. İş Sürekliliği Yönetim Planı Denetimi

Bilgi sistemleri denetimi daha çok işletmenin veri gizliliğinin, bütünlüğünün ve kullanılabilirliğinin saldırılara karşı korunmasını sağlamakla ilgilenir. Bazı durumlarda bu saldırılar, bir işletmenin kritik iş süreçlerini devre dışı bırakarak işletme için önemli bir yasal veya mali sorumluluk yaratır. Bu nedenle bir bilgi sistemleri denetimi, işletmenin sistem ve süreçlerinin denetiminin yanı sıra, iş sürekliliği planlarının denetimini de içermelidir.

BS Denetçisi iş sürekliliği yönetimi planı denetiminde aşağıdaki hususları kontrol etmelidir;

- İş sürekliliği planının sürdürülebilirliğinin sağlanması,
- Plan ile ilgili dokümanların yazılı ve anlaşılır olması,
- Bulut tabanlı uygulamaların incelenmesi,
- İş etki analizi bulgularının, iş önceliklerine göre aksiyon alınmış olduğunun incelenmesi,
- İşletmenin güvenlik ve çevre kontrollerinin gözden geçirilerek yeterliliğinin değerlendirilmesi,
- Son kullanıcı tarafından gerçekleştirilen testlere ait sonuçların değerlendirilmesi,

- İş sürekliliği planının iş hedefleri ve stratejisi ile uyumlu olmasının değerlendirilmesi,
- Çalışan farkındalığını arttırmak için, acil durum prosedürlerinin, çalışan eğitimlerinin, test ve tatbikat sonuçlarının gözden geçirilmesi,
- Güvenlik gereksinimleri kapsamında yedekleme sürecinin gözden geçirilmesi,
- İş sürekliliği planının uluslararası standartlara ve yasal düzenlemelere uyumluluğu, yeterliliği ve güncelliğinin denetlenmesi.

İş sürekliliği yönetim planı denetiminin amacı, işletmenin kritik iş süreçlerinde herhangi bir kesinti meydana geldiğinde bu kritik süreçleri destekleyen bilgi sistemlerinin hizmet verme durumu, sistemin tekrar çalışabilmesini kısıtlayan sorunlar ve işletmenin iş sürekliliği planının, bilgi güvenliği politikalarına, işletme tarafından uyulması gereken diğer standartlar ve yasal düzenlemelere uyumu hususundaki değerlendirmelerin işletme yönetimi, düzenleyici kuruluşlar veya ilgili diğer üçüncü kişilere sağlanmasıdır. İş sürekliliği yönetim planı denetimi, iş sürekliliği yönetim planının işletme politikalarına, uyulması gereken standartlara, yönergelere, prosedürlere, yasalara ve bilgi sistemleri hizmetlerinin sürdürülmesine yönelik düzenlemelere uyumuna odaklanmalıdır.

Bilgi sistemleri denetçisi, iş sürekliliği planını gözden geçirirken, planın temel unsurlarının açık olduğunu doğrulamalıdır. Büyük bir olay veya felaket durumunda işletmenin kritik iş süreçlerinin ve bunları destekleyen bilgi sistemleri tesislerinin kurtarılmasını sağlamak için işletme tarafından yeterli ve etkili acil durum planlarının oluşturulduğundan emin olmalıdır. İşletme için en uygun iş sürekliliği planlarının seçilip seçilmediğini ve maliyet etkin bir biçimde planların uygulanıp uygulanmadığını kontrol etmelidir. İşletmenin kritik iş süreçlerinin başarılı bir şekilde kurtarılması için ihtiyaç duyulan kilit personelle görüşmelidir. İş sürekliliği planlarının uygunluğu ve etkililiği açısından işletme tarafından periyodik olarak test edilip edilmediğini kontrol etmelidir. Tesis dışında bulunan ikincil sistemlerin güvenliği, uygun fiziksel ve çevresel erişim kontrollerine sahip olması açısından değerlendirilmelidir.

BS Denetçisi iş sürekliliği denetimi kapsamında yerine getirmesi gerektiği görevlerden bazıları aşağıdaki gibidir:

- İş sürekliği planı ve iş hedefleri arasındaki bağlantıları anlamak,
- İş sürekliliği planını değerlendirmek ve onun hatasızlığını ve güncel olduğunu tespit etmek,
- Plan testini inceleyerek iş sürekliliği planının etkinliğini doğrulamak,
- Bulut temelli mekanizmaları ve kuruluş dışı depolamayı değerlendirmek,
- Bir olay sırasında personelin müdahale yetkinliğini değerlendirmek.

BS Denetçisi, kuruluştan kuruluşa değişiklik gösterebilecek takım sorumlulukları bilgisine sahip olmalıdır.

BS denetçisi, tüm planların düzenli olarak test edildiğini, test zamanlamasının ve testlerin tüm kritik işlevler için yapıldığını denetlemelidir.Test dokümantasyonu ön test, test ve test sonrası raporları ile testin tam olarak belgelendiğini doğrulamak için BS denetçisi tarafından incelenmelidir. Test sırasında tehlikeye girmediğinden emin olmak için bilgi güvenliğinin doğrulanması da önemlidir.

Değerlendirme Soruları

Soru 1: Aşağıdaki risk yanıt stratejilerinden hangisinde riskin paylaşılması önemli bir etmendir?

A) Risk transferi

B) Riskin kabulü

C) Riskin reddedilmesi

D) Risk azaltma

E) Riskten kaçınma

Cevap: A

A) Risk transferi: Risk transferi, bir işletmenin karşılaştığı olumsuz bir sonuçtan kaynaklanan potansiyel zararın üçüncü bir tarafa kaydırıldığı veya üçüncü bir tarafla paylaşıldığı yaygın bir risk yönetimi tekniğidir.

B) Riskin kabulü: Bu strateji, işletmenin bir riskten kaynaklanan potansiyel kaybının, bu riskten kaçınmanın getireceği maliyet kadar büyük olmadığını kabul ettiği zaman veya işletmenin risk toleransı içinde ise uygulanır.

C) Riskin reddedilmesi: İştah puanı altında kalması ya da herhangi bir etkisinin olmadığı risklerin değerlendirmeye alınmamasıdır.

D) Riski azaltma: Bir işletmenin kritik iş süreçlerinde veya sistemlerinde potansiyel bir kayba neden olabilecek bir riskin oluşturabileceği zararı hafifletmek için önleyici eylem planlarının uygulandığı bir stratejidir.

E) Riskten kaçınma: Bu strateji, işletme için potansiyel bir kayba neden olabilecek bir riskin meydana geleceği kritik değeri yüksek olan sistemin veya sürecin tamamen ortadan kaldırılmasını içerir.

Soru 2: Aşağıdakilerden hangisi bir felaket durumunda kullanılmak üzere, hem donanım hem de sistem yazılımının bulunduğu, kullanıma tamamen hazır bir dış saha bilgi işleme tesisidir?

A) Mobil siteler

B) Ilık siteler

C) Sıcak siteler

D) Soğuk siteler

E) Hepsi

Cevap: C

A) Mobil siteler: Bir işi yeniden başlatma lokasyonu olarak hizmet vermek için bir mobil tesis kullanımı. Tesis genellikle herhangi bir siteye taşınabilir ve bilgi teknolojileri ve personelini barındırabilir.

B) Ilık siteler: Sıcak bir siteye benzer, ancak kurtarma için gerekli olan tüm donanımlarla tam olarak donatılmamış site.

C) Sıcak siteler: Bir felaket durumunda kullanılmak üzere, hem donanım hem de sistem yazılımının bulunduğu, kullanıma tamamen hazır bir dış saha bilgi işleme tesisi.

D) Soğuk siteler: Bir bilgisayar tesisinin gerekli elektriksel ve fiziksel bileşenlerine sahip olan, ancak bilgisayar donanımına sahip olmayan bir bilgi sistemleri yedekleme tesisi.

E) Sadece sıcak site bu tanıma doğrudan uymaktadır.

Soru 3: İşletmenin iş hedefleri için hangi süreçlerin kritik olduğunu ve bu süreçlerdeki bir kesintinin işletmeye potansiyel etkisini belirleme süreci aşağıdakilerden hangisidir?

A) Risk değerlendirme

B) İş etki analizi

C) Kritiklik analizi

D) Boşluk analizi

E) Fırsat değerlendirme

Cevap: B

A) Risk değerlendirme: İşletmenin iş sürekliliğinin amaçlarına ulaşmasına olumsuz etki eden ve kayba yol açan risklerin belirlenmesi ve bu risklerin yönetilmesi çalışmalarını içermektedir.

B) İş etki analizi: İşletmenin iş hedefleri için hangi süreçlerin kritik olduğunu ve bu süreçlerdeki bir kesintinin işletmeye potansiyel etkisini belirleme sürecidir.

C) Kritiklik analizi: İşletmenin iş süreçlerinin potansiyel risklerine göre bir kritiklik derecesi atama sürecidir.

D) Boşluk analizi: Bir kesinti durumunda işletmenin normal iş süreçlerini sürdürmek veya kurtarmak için ne tür planlara ihtiyacı olduğunun ve mevcut iş sürekliliği planlamasının sağladığının bir karşılaştırmasıdır.

E) Fırsat Değerlendirme: Riskin olumlu yanlarının sağladığı ya da direk kazançlardır.

Soru 4: Veri yansıtma (İng. data mirroring), verilerin bir konumdan yerel veya uzak bir depolama ortamına tam bir kopya olarak kopyalanmasının gerçek zamanlı işlemini ifade eder. Buna göre veri yansıtma aşağıdaki durumlardan hangisinde bir kurtarma stratejisi olarak uygulanmalıdır?

A) Kurtarma hedef noktası (RPO) düşük.

B) Kurtarma hedef noktası (RPO) yüksek.

C) Kurtarma hedef zamanı (RTO) yüksek.

D) Maksimum tahammül edilebilir kesinti süresi (MAO) yüksek.

E) Hiçbiri

Cevap: A

A) Kurtarma hedef noktası (RPO), verilerin kurtarılmasının kabul edilebilir olduğu en erken noktadır. Başka bir deyişle, RPO, kurtarılan verilerin "yaşı" (yani, verilerin ne kadar süre önce yedeklendiği) RPO çok düşükse, örneğin dakikalar, işletmenin birkaç dakikalık veriyi bile kaybetmeyi göze alamayacağı anlamına gelir. Bu gibi durumlarda, veri yansıtma (eşzamanlı veri çoğaltma) bir kurtarma stratejisi olarak kullanılmalıdır.

B) Kurtarma hedef noktası (RPO) yüksekse, örneğin saatler, disk yedekleme ve kurtarma gibi diğer yedeklemeler kullanılabilir.

C) Yüksek bir kurtarma hedef zamanı (RTO), kesintiden hemen sonra bilgi sistemlerine ihtiyaç duyulmayabileceği anlamına gelir.

D) Maksimum tahammül edilebilir kesinti süresi (MAO) işletmenin alternatif modda çalışmayı destekleyebileceği maksimum süredir. MAO, RTO'dan büyük olması gerektiğinden, kesintiden hemen sonra bilgi sistemlerine ihtiyaç duyulmayabileceği anlamına gelir.

E) RPO ve/veya RTO düşük olduğu durumlar için veri yansıtma uygulanabilir bir stratejidir.

Soru 5: Aşağıdakilerden hangisi bir iş etki analizi yürütmenin adımlarından biridir?

A) SLA takibinin yapılması.

B) Risk analizi yapmak.

C) İş sürekliliği planını gözden geçirmek.

D) Müdahale ekiplerine periyodik eğitim sağlamak.

E) Yöneticilerle görüşmek.

Cevap: E

A) SLA takibi iş etki analizi adımlarından biri değildir. Daha çok hizmet sağlayıcı (tedarikçi) ile son kullanıcı (müşteri) arasında, beklenen hizmet düzeyini belirleyen bir sözleşmedir.

B) İş sürekliliğinin bir parçası olan risk değerlendirmesi (İng. risk assessment); risk tanımlama (İng. risk identification), risk analizi (İng. risk analysis) ve risk irdelemesi (İng. risk evaluation) aşamalarının genel sürecidir.

C) Test ve bakım aşamasında işletme iş sürekliliği planını mevcut ortamı yansıtacak şekilde düzenli olarak gözden geçirmeli ve güncellemelidir.

D) Müdahale ekiplerinin iş sürekliliği planını nasıl uygulayacaklarını bilmelerini ve bunu yapmak için gereken becerilere sahip olmalarını sağlamaları konusunda periyodik eğitim sağlanabilir.

E) Bir iş etki analizi, veri toplama yöntemi, işletmenin büyüklüğü, karmaşıklığı ve kültürü göz önünde bulundurularak hazırlanmalıdır. İşletme yöneticileri iş süreçlerini önceliklendirmemelidir. Bunun yerine, işletmenin tüm iş birimlerinin her personel düzeyinde (çalışanlar, yönetim kurulu, yöneticiler) katılım sağlanabilecek anketler aracılığıyla iş sürekliliği yönetim sorumlusu tarafından bir bütün olarak iş süreçleri önceliklendirilmelidir.

KAYNAKÇA

Kurumsal Çerçeve, Kütüphane, Standart, Yönetmelik ve Tebliğler:

COBIT 2019, Governance Management Objectives, ISACA, 2018.

ITIL kütüphanesi v3F

ISO Standartları

SPK Bilgi Sistemleri Yönetimi Tebliğ Madde 4 Tanımlar

SPK Bilgi Sistemleri Yönetimi Tebliği Madde 10

Kitap:

ISACA, "CISA Gözden Geçirme Kılavuzu 27. Baskı", ISBN 978-1-60420-855-9

Information Reference Model: Quality Criteria for Information, COBIT 2019, Introduction and Methodology, 2018.

APO14.06 Ensure a data quality assessment approach, COBIT 2019, Governance and Management Objectives, 2018.

EBA Guidelines on ICT and security risk Management, 28 Kasım 2019, European Banking Authority.

The NIST Definition of Cloud Computing (NIST Special Publication 800-145).

Cloud Security Alliance, "Best Practices for Mitigating Risks in Virtualized Environments.", 2015.

Web:

ISACA, www.isaca.org

https://kolaydokuman.com/2020/balik-kilcigi-diyagrami-nedir.html , Balık kılçığı diyagramı

https://www.yeniisfikirleri.net/gercek-problemi-anlama-teknigi-5-neden-analizi/ , 5 neden analizi

CSA, https://cloudsecurityalliance.org/blog/2021/04/06/what-an-auditor-should-know-about-cloud-computing-part-1/

CSA, https://cloudsecurityalliance.org/blog/2021/04/27/what-an-auditor-should-know-about-cloud-computing-part-3/

CSA, https://cloudsecurityalliance.org/research/working-groups/internet-of-things/

CSA, https://cloudsecurityalliance.org/research/working-groups/blockchain/