T.C.
Radyo ve Televizyon Üst Kurulu

BİLGİ İŞLEM MERKEZLERİNDE KURUMLARIN İŞ SÜREKLİLİĞİ AÇISINDAN ÖNEM ARZ EDEN FELAKET KURTARMANIN İNCELENMESİ VE ÇÖZÜM ÖNERİLERİ

UZMANLIK TEZİ

Ahmet Can ÖZDEMİR

ANKARA

HAZİRAN/2021

T.C.
Radyo ve Televizyon Üst Kurulu

BİLGİ İŞLEM MERKEZLERİNDE KURUMLARIN İŞ SÜREKLİLİĞİ AÇISINDAN ÖNEM ARZ EDEN FELAKET KURTARMANIN İNCELENMESİ VE ÇÖZÜM ÖNERİLERİ

UZMANLIK TEZİ

Ahmet Can ÖZDEMİR

DANIŞMAN
DAİRE BAŞKAN YARDIMCISI İbrahim ESER

ANKARA

HAZİRAN/2021

RADYO VE TELEVİZYON ÜST KURULU BAŞKANLIĞINA

Bu çalışma, Tez Değerlendirme Komisyonu tarafından oy birliği/oy çokluğu ile Uzmanlık Tezi olarak kabul edilmiştir.

	Adı Soyadı	İmza
Başkan	:	
Üye	:	
Üye	:	
Üye	:	
Üye	:	

ONAY

... / ... / 2021

Ebubekir ŞAHİN

Üst Kurul Başkanı

TEZ TESLİM TUTANAĞI VE DOĞRULUK BEYANI

Radyo ve Televizyon Üst Kurulunda görev yapan Üst Kurul Uzman Yardımcısı olarak, Radyo ve Televizyon Üst Kurulu Tez Hazırlama Yönergesi'ne uygun şekilde hazırlamış olduğum uzmanlık tezi ilişikte sunulmuştur.

Bu uzmanlık tezindeki bütün bilgileri akademik kurallara ve etik davranış ilkelerine uygun olarak toplayıp sunduğumu; ayrıca, bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi beyan ederim.

Bilgilerinizi ve gereğini arz ederim.

… / 08 / 2021
Ahmet Can ÖZDEMİR
Üst Kurul Uzman Yardımcısı

Uzmanlık Tezinin Adı:
Bilgi İşlem Merkezlerinde Kurumların İş Sürekliliği Açısından Önem Arz Eden Felaket Kurtarmanın İncelenmesi ve Çözüm Önerileri
EK:
-Tez (6 adet)
-CD (1 adet)

Tezi Teslim Alan
Daire Başkanı
... / … / 2021

TEŞEKKÜR

"Bilgi İşlem Merkezlerinde Kurumların İş Sürekliliği Açısından Önem Arz Eden Felaket Kurtarmanın İncelenmesi ve Çözüm Önerileri" isimli bu tezin hazırlanması sürecinde araştırma konusunun belirlenmesinde emeği geçen Üst Kurul Başkanı Sayın Ebubekir ŞAHİN'e, değerli Üst Kurul Üyelerine, yoğun çalışma temposuna rağmen desteğini esirgemeyen tez danışmanım Bilgi Teknolojileri Dairesi Başkan Yardımcısı Sayın İbrahim ESER'e, tezin yazılma sürecindeki değerli katkılarından dolayı Üst Kurul Uzman Yardımcısı Sayın Sefa Yılmaz'a, değerli mesai arkadaşlarıma, anlayış ve destekleri ile her zaman yanımda olan aileme ve sevgili eşime teşekkürlerimi sunarım.

İÇİNDEKİLER

İÇİNDEKİLER ..... **I**
KISALTMALAR ..... **IV**
ŞEKİLLER LİSTESİ ..... **VI**
TABLOLAR LİSTESİ ..... **VII**
GİRİŞ **1**
Tezin Amacı **3**
Tezin Önemi **4**
Tezin Yöntemi **5**
Veri Toplama ve Analiz Teknikleri **6**
Tezin Kapsam ve Sınırlılıkları **7**
BİRİNCİ BÖLÜM **8**
FELAKET KURTARMA YÖNETİMİ **8**
1.1. FELAKET NEDİR? **9**
1.2. FELAKET TÜRLERİ **9**
1.2.1. Doğal Felaketler 11
1.2.2. İnsan Kaynaklı Felaketler 13
1.2.3. Kazalar ve Teknolojik Felaketler 15
1.3. FELAKET KURTARMA NEDİR? **17**
1.4. İŞ SÜREKLİLİĞİ NEDİR? **18**
1.4.1. İş Sürekliliği Planlamasının Kamuda Şekillenmesi 20
1.5. FELAKET KURTARMA YÖNETİMİ VE İŞ SÜREKLİLİĞİ ARASINDAKİ FARKLAR VE ORTAK NOKTALAR **20**
1.6. FELAKET KURTARMA YAKLAŞIMLARI **22**
1.6.1. Sıcak Mekân Yaklaşımı 24
1.6.2. Soğuk Mekân Yaklaşımı 25
1.6.3. Ilık Mekân Yaklaşımı 26
1.7. FELAKET KURTARMA STANDARTLARI **28**
1.8. FELAKET KURTARMANIN ÖLÇÜLMESİNDE KULLANILAN PERFORMANS METRİKLERİ **30**
1.8.1. Kabul Edilebilir En Fazla Çalışılamaz Durumda Bulunma Süresi (Maximum Tolerable Downtime-MTD) 30

1.8.2. Felaket Kurtarma Süresi (Recovery Time Objective-RTO) 31
1.8.3. Felaket Kurtarma Noktası (Recovery Point Objective-RPO) 33
İKİNCİ BÖLÜM 35
FELAKET KURTARMA YÖNETİMİNDE İZLENECEK TEDBİRLER VE UYGULAMALAR 35
2.1. FELAKET KURTARMA YÖNETİM VE OPERASYON EKİBİ 35
2.2. RİSK DEĞERLENDİRMESİ 38
2.3. İŞ ETKİ ANALİZİ (BUSINESS IMPACT ANALYSIS-BIA) 38
2.4. SİSTEM KURTARMA ÖNCELİK LİSTESİ 41
2.5. SANALLAŞTIRMA 43
2.5.1. Sunucu Sanallaştırma 44
2.5.1.1. Sanal Makine Nedir? 44
2.5.1.2. Sanal Makinelerin Kullanım Amacı, Avantaj ve Dezavantajları 44
2.5.1.3. Sunucu Sanallaştırma Türleri 47
2.5.2. Veri Depolama Sistemi Sanallaştırma 48
2.5.3. Veri İletişim Ağı (Network) Sanallaştırma 49
2.5.3.1. Veri İletişim Ağı Kullanım Amacı 50
2.5.3.2. Veri İletişim Ağı Sanallaştırma Teknolojisi Nasıl Çalışmaktadır? 50
2.5.3.3. Veri İletişim Ağı Sanallaştırmanın Faydaları 51
2.6. SUNUCU KÜMELEME (SERVER CLUSTERING) 52
2.7. VERİ YEDEKLEME VE GERİ YÜKLEME 55
2.7.1. Kurumsal Veri Yedekleme Yaklaşımları 57
2.7.1.1. Teyp Tabanlı Yedekleme 57
2.7.1.2. Disk Tabanlı Yedekleme 58
2.7.1.3. Bulut Tabanlı Yedekleme 59
2.7.2. Veri Yedekleri Depolama Ortamları\Donanımları 60
2.7.2.1. Katı Hâl Depolama Cihazları (Solid State Storage) 60
2.7.2.2. Sabit Disk Sürücüsü (Hard Disc Drive-HDD) 60
2.7.2.3. Mıknatıslı Kaset (Magnetic Tape) 61
2.7.2.4. Optik Diskler 61
2.7.3. Alınan Yedeğin Boyutuna Göre Yedekleme Türleri 62
2.7.3.1. Tam Yedekleme (Full Backup) 62
2.7.3.2. Artırımlı Yedekleme (Incremental Backup) 63
2.7.3.3. Kademeli Yedekleme (Diffirential Backup) 64
2.7.3.4. Tam Yedek ve Kademeli Yedek Kombinasyonu 65
2.7.3.5. Tam Yedek ve Artırımlı Yedek Kombinasyonu 66

2.7.3.6. Artırımlı Sonsuza Kadar Yedekleme 67
2.7.3.7. Sentetik Yedekleme 68
2.7.3.8. Ayna Tipi Yedekleme 69
2.7.4. İşlevselliğine Göre Yedekleme Türleri 69
2.7.5. Veri Depolama Sisteminin Konumuna Göre Yedekleme Türleri 70
2.7.6. Mimariye Göre Yedekleme Türleri 70
2.7.7. Dağıtım Modeline Göre Yedekleme Türleri 73
2.7.8. Veri Geri Yükleme Yaklaşımları 75
2.7.8.1. Sanal Makine Düzeyinde Geri Yükleme 75
2.7.8.2. Dosya Seviyesinde Geri Yükleme 76
ÜÇÜNCÜ BÖLÜM 78
DÜNYADA GERÇEKLEŞTİRİLMİŞ FELAKET KURTARMA UYGULAMALARI 78
3.1. COMMERZBANK 78
3.2. TULANE ÜNİVERSİTESİ 85
3.3. VIRGINIA DEVLETLER TOPLULUĞU 91
DÖRDÜNCÜ BÖLÜM 96
TÜRKİYE'DE GERÇEKLEŞTİRİLMİŞ FELAKET KURTARMA UYGULAMALARI 96
4.1. ORTA DOĞU TEKNİK ÜNİVERSİTESİ (ODTÜ) 96
4.2. İNÖNÜ ÜNİVERSİTESİ 97
4.3. DUMLUPINAR ÜNİVERİTESİ 98
4.4. DAİKİN 100
4.5. SİMİT SARAYI 101
4.6. TÜRKSAT 102
4.7. FORD OTOSAN 103
SONUÇ VE ÇÖZÜM ÖNERİLERİ 105
Çözüm Önerileri 105
Radyo ve Televizyon Üst Kurulu Bağlamında Felaket Kurtarmanın Değerlendirilmesi ve Öneriler 108
KAYNAKÇA 110
ÖZET 115
ABSTRACT 117
ÖZGEÇMİŞ 118

KISALTMALAR

a.g.e	Adı Geçen Eser
a.g.k	Adı Geçen Kaynak
a.g.m	Adı Geçen Makale
AD	Active Directory (Aktif Dizin)
ASR	Azure Site Recovery
BC	Business Contiunity (İş Sürekliliği)
BCI	Business Contiunity Institute (İş Sürekliliği Enstitüsü)
BCP	Business Contiunity Planning (İş Sürekliliği Planlaması)
BIA	İş Etki Analizi (Business Impact Analysis)
BİDB	Bilgi İşlem Daire Başkanlığı
BSTA	Binary Search Tree Algorithm (İkili Arama Ağacı Algoritması)
BT	Bilişim Teknolojileri
BTYK	Bilim ve Teknoloji Yüksek Kurulu
CD	Compact Disc (Kompakt Disk)
CPU	Central Processing Unit (Merkezi İşlem Birimi)
CSP	Cloud Service Provider (Bulut Servis Sağlayıcı)
DC	Domain Controller (Etki Alanı Sunucusu)
DMV	Department of Motor Vehicles (Motorlu Taşıtlar Kurumu)
DNS	Domain Name System (Alan Adı Sistemi)
DPT	Devlet Planlama Teşkilatı
DR	Disaster Recovery (Felaket Kurtarma)
DRJ	Disaster Recovery Journal (Felaket Kurtarma Dergisi)
DRP	Disaster Recovery Planning (Felaket Kurtarma Planlama)
DVD	Digital Versatile Disc (Çok Amaçlı Sayısal Disk)
EXC	Exchange (E-Posta Sunucusu)
FEMA	Federal Emergency Management Agency (Federal Acil Durum Yönetim Kurumu)
FSRV	File Server (Dosya Yönetim Sunucusu)
FKM	Felaket Kurtarma Merkezi
HVAC	Heating Ventilating Air Conditioning (Isıtma Havalandırma Klima)

IP	Internet Protocol (İnternet Protokolü)
IRT	Incident Response Team (Olay Müdahale Ekibi)
ISO	International Standard Organization (Uluslararası Standart Kurumu)
IT	Bilgi Teknolojileri (Information Technology)
IBM	Uluslararası İş Makinesi (International Business Machine)
LAN	Local Area Network (Yerel Alan Ağı)
MTD	Maximum Tolerable Downtime (Kabul Edilebilir En Fazla Çalışılamaz Durumda Bulunma Süresi)
NV	Network Virtualization (Veri İletişim Ağı Sanallaştırma)
ODTÜ	Orta Doğu Teknik Üniversitesi
PC	Kişisel Bilgisayar (Personal Computer)
RAID	Redundant Array of Inexpensive Disks
RPO	Felaket Kurtarma Noktası (Recovery Point Objective)
RTO	Felaket Kurtarma Zamanı (Recovery Time Objective)
RRT	Rapid Response Team (Acil Müdahale Ekibi)
SAN	Storage Area Network (Depolama Alan Ağı)
SAP	System, Application and Products (Sistem, Uygulama ve Ürünler)
SD	Secure Digital
SDDC	Software Defined Data Center (Yazılım Tanımlı Veri Merkezi)
SLA	Service Level Agreement (Hizmet Düzeyi Anlaşması)
SSD	Solid State Storage (Katı Hâl Diski)
STSC	Share Technical Steering Comittee (Share Teknik Yönetim Komitesi)
TB	Terabayt
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Merkezi
USB	Universal Serial Bus (Evrensel Seri Veri Yolu)
UPS	Kesintisiz Güç Kaynağı (Uninterruptible Power Supply)
WAN	Wide Area Network (Geniş Alan Ağı)
WTC	World Trade Center (Dünya Ticaret Merkezi)
VITA	Virginia Information Technologies Agency (Virginia Bilgi Teknolojileri Ajansı)
VM	Sanal Makine (Virtual Machine)

ŞEKİLLER LİSTESİ

Şekil 1.1 Bilgisayar Verisinin Elektronik Olarak Taşınması 29
Şekil 1.2 Zaman Düzleminde Felaket Kurtarma Süresi 32
Şekil 1.3 Zaman Düzleminde Felaket Kurtarma Noktası 33
Şekil 2.1 Sunucu Kümeleme Mimarisi 53
Şekil 2.2 Tam Yedekleme Süreci 63
Şekil 2.3 Tam ve Kademeli Yedekleme Kombinasyonu 65
Şekil 2.4 Tam ve Artırımlı Yedekleme Kombinasyonu 66
Şekil 2.5 Sonsuza Kadar Artırımlı Yedekleme 67
Şekil 2.6 Sentetik Yedekleme Süreci 68
Şekil 2.7 Sanal Makine Düzeyinde Geri Yükleme Süreleri 76
Şekil 2.8 Dosya Düzeyinde Geri Yükleme Süreleri 77
Şekil 2.9 Veri Merkezi Isıtma Soğutma ve Havalandırma Sistemi 80
Şekil 3.1 Katrina Kasırgası 85
Şekil 3.2 Veri Yedekleme Bandı 88
Şekil 3.3 Depolama Alan Ağı(SAN) Çalışma Mantığı 91
Şekil 4.1 Sistem Odası ile FKM Çalışma Mantığı 96
Şekil 4.2 Rektörlük Binası Ana Veri Merkezi 99
Şekil 4.3 Kütüphane Binası İkincil Veri Merkezi 99

TABLOLAR LİSTESİ

Tablo 1.1 Felaket Kurtarma ve İş Sürekliliği Arasındaki Farklar 22
Tablo 1.2 Felaket Kurtarma Yaklaşımlarının Kıyaslaması 28
Tablo 1.3 Felaket Kurtarma Hizmet Seviyeleri Kıyaslaması 30
Tablo 1.4 Kurum ve Kuruluşların Veri Merkezi Sunucu Sistemleri ve IT Servisleri İçin Hazırlanmış Örnek Felaket Kurtarma Süresi Çalışması 32
Tablo 1.5 Kurum ve Kuruluşların Veri Merkezi Sunucu Sistemleri ve IT Servisleri İçin Hazırlanmış Örnek Felaket Kurtarma Noktası Çalışması 34
Tablo 2.1 Felaket Kurtarma Yönetim Ekibi Örnek Çalışması 36
Tablo 2.2 Felaket Kurtarma Operasyon Ekibi 37
Tablo 2.3 İş-Etki Analiz Tablosu 40
Tablo 2.4 Kurum Kuruluşların Veri Merkezi Sunucu Sistemleri ve IT Servisleri İçin Hazırlanmış Sistem Kurtarma Öncelik Listesi Çalışması 42
Tablo 2.5 Sanal Makinelerin Avantaj ve Dezavantajları 46
Tablo 2.6 Veri İletişim Ağı Sanallaştırmanın Faydaları 51
Tablo 2.7 İşlevselliğine Göre Yedekleme Türlerinin Mukayesesi 69
Tablo 2.8 Mimariye Dayalı Yedekleme Türlerinin Kıyaslaması 72
Tablo 2.9 Dağıtım Modeline Göre Yedekleme Tiplerinin Kıyaslaması 74

GİRİŞ

Bilgi teknolojileri endüstrisi yıllardır hızlı bir gelişme göstermektedir. Bu yüzden bilgi teknolojileri disiplini, kurum ve kuruluşların hayati bir unsurunu teşkil etmektedir. Kurumların iş süreçlerinde bilgi teknolojilerinin yadsınamaz bir rolü bulunmaktadır. Bu rol, içinde bulunulan ileri teknolojik çevrede her kurumun temel iş süreçlerinin ayrılmaz bir parçası olmuştur.

Birey, kurum ve kuruluşların daha fazla bilgi teknolojilerine bağımlı hâle geldiği bu günlerde, teknolojinin dokunmadığı bir kurum ve kuruluş köşesini bulmak zorlaşmakta ve kurumların çoğu bilişim sistemleri olmadan iş süreçlerine devam edememektedir. Teknoloji; organizasyonların her seviyesinde kurumsal operasyonlara daha fazla entegre olmaya devam ettikçe bilgi teknolojileri neredeyse her şeyi kapsayacak şekilde genişlemektedir.

Kurum ve kuruluşlar verilere, bilgiye ve teknolojiye giderek daha fazla güvenirken bilişim sistemlerine yönelik herhangi bir felaket meydana geldiğinde kurumlar felaketi bizatihi yaşayıp tanıklık etmektedir ve kurumları etkileyen yeni tehditler ortaya çıkmaktadır.

Veri merkezi altyapısı üzerinde koşan bilişim sistemleri geliştikçe kurum ve kuruluşların; işledikleri, aktardıkları ve depoladıkları bilgilere yönelik günümüzün hatırı sayılır miktardaki tehditlerine karşı da korunmaları gerekmektedir. Dolayısıyla bilişim sistemlerinde herhangi bir felaketin sebep olduğu arıza veya yıkım kurum ve kuruluşlar için ciddi sonuçlar doğurabilmektedir.

Kurumların çoğunun bilişim sistemlerine bağımlı olmasının bir sonucu olarak hiçbir kurum ve kuruluş, bilişim sistemlerine yönelik etkin bir veri merkezi felaket kurtarma yönetimi ve uygulaması ihtiyacını göz ardı etmemelidir. Kurum büyüklüğü, geliri veya personel sayısı ne olursa olsun iş sürekliliğinin sağlanması, kurum hizmetlerinde olası kesintiler yaşanmaması için felaket kurtarma yönetimi planlaması ihtiyacı katlanarak artmış ve zorunlu hâle gelmiştir. Yıkıcı felaketlerin yol açtığı tehditler karşısında bilişim teknolojileri çalışanları için veri merkezi bilişim sistemlerini korumak, bir yükümlülük ve uzmanlık alanı hâline gelmiştir.

Bu bağlamda, bu çalışmanın birinci bölümünde kurumların iş sürekliliğinin sağlanmasının önemli bir unsuru olan felaket kurtarma yönetimi başlığı altında felaket türleri, iş sürekliliği felaket kurtarma yönetimi ilişkisi, felaket kurtarma yaklaşımları, felaket kurtarma standartları, felaket kurtarma yaklaşımının performans ölçütleri olan felaket kurtarma noktası ve felaket kurtarma zamanı detaylı olarak incelenecektir.

Çalışmanın ikinci bölümünde etkin ve doğru bir felaket kurtarma yönetiminin önemli unsurlarından olan, felaket kurtarma yönetiminin hazırlık aşamasında herhangi bir veri merkezi felaketi meydana gelmeden önce alınabilecek tedbirler arasında yer alan ve olası felaketlere müdahale açısından önemlilik arz eden, bilişim sistemleri için sistemin sağlığı, devamı ve iş sürekliliğinin korunmasına katkıda bulunacak felaket kurtarma ve operasyon ekibi, iş etki analizi, risk değerlendirmesi, sistem kurtarma öncelik listesi, sunucu kümeleme, sanallaştırma, veri yedekleme ve veri geri yükleme konuları incelenecektir.

Çalışmanın üçüncü bölümünde Commerzbank, Tulane Üniversitesi ve Virginia Devletler Topluluğu gibi kurum ve kuruluşlar tarafından tatbik edilmiş dünyadaki felaket kurtarma yönetimi örnekleri detaylı olarak incelenecektir.

Çalışmanın dördüncü bölümünde Orta Doğu Teknik Üniversitesi, İnönü Üniversitesi, Dumlupınar Üniversitesi, Daikin, Simit Sarayı, TÜRKSAT ve Ford Otosan gibi kurum ve kuruluşlar özelinde Türkiye'de gerçekleştirilmiş felaket kurtarma yönetimi uygulama ve örneklerine yer verilecektir.

Sonuç ve çözüm önerileri bölümünde tez boyunca yapılan incelemeler doğrultusunda kurum ve kuruluşların olası bir felaket senaryosu ile karşı karşıya kaldıklarında, kurumsal iş sürekliliklerinin aksamaması için etkin ve doğru bir felaket yönetimini gerçekleştirmek adına izlemeleri gereken tedbir ve uygulamalar ile Radyo ve Televizyon Üst Kurulu bağlamında değerlendirme ve önerilere yer verilecektir. Kurum ve kuruluşların krizden başarılı bir şekilde çıkmaları, kurumsal bilişim sistemlerinin istikrarlı çalışmasını sürdürmesi, kurum ve kuruluşların bilişim sistemleri noktasında yeterli gücü ve kaynağı korumaları için izleyebilecekleri bir tavsiye listesi ortaya konacaktır.

Tezin Amacı

Bu tezin temel amacı, kurumsal bilgi işlem merkezlerinde olası bir felaket senaryosu ile karşılaşıldığında erişilebilirliğini yitiren verilerin tekrar kullanıma hazır hâle gelmesini sağlayan, iş süreçlerinin kesintiye uğramasına engel olan ve kurumlar için hayati öneme sahip verilerin zarar görmesinin önüne geçen felaket kurtarma yönetimi adlı disiplini incelemek, kurum ve kuruluşların felaketler konusunda bilgi birikimlerini ve farkındalıklarını artırmaları için etkili ve doğru bir felaket kurtarma yönetimi noktasında yapılması gerekenlerin yer aldığı bir tavsiye listesi ortaya koymaktır. Bu temel amaçlara ulaşmak için belirlenen ikincil amaçlar şunlardır:

- Kurumsal veri merkezi felaket kurtarma yönetiminde önemlilik arz eden birtakım kavramların açıklamasını yapmak
- İş sürekliliği kavramını ortaya koymak ve iş sürekliliği ile felaket kurtarma kavramlarının ilişkisine değinmek

- Etkin ve doğru bir felaket kurtarma yönetiminin gerçekleştirilmesi adına alınacak tedbirleri, uygulamaları ortaya koymak ve incelemek
- Dünyadaki veri merkezi felaket kurtarma yönetimi örnekleri hakkında incelemelerde bulunmak
- Türkiye'de gerçekleştirilmiş felaket kurtarma yönetimi örnek ve uygulamaları hakkında incelemelerde bulunmak
- Kurumsal veri merkezi felaket kurtarma yönetimi kavramının iş sürekliğinin önemli bir parçası olduğu ve bu kavramın iş sürekliliği açısından önemi konusunda farkındalık oluşturmak
- İş sürekliliğini kalıcı hâle getirmenin, kurumsal bilişim sistemlerinin sağlıklı çalışmasını her şartta, istikrarlı bir biçimde sürdürmesine bağlı olduğunu ve bunun etkin, doğru bir felaket kurtarma yönetimi ile mümkün olduğunu vurgulamak

Tezin Önemi

Günümüzde bilgi teknolojilerinde gerçekleştirilen atılım ve kaydedilen gelişmelerle hem insan yaşamında hem de kurum ve kuruluşları kapsayan kurumsal ölçekte, bilgi teknolojileri tabanlı uygulamaların yaygın bir şekilde kullanımı baş göstermiştir. Son kullanıcıların istenilen herhangi bir zamanda bilgisayar verilerine ve uygulamalarına erişimi önem kazandıkça kurumsal bilgisayar verisini güvenle muhafaza edebilme kabiliyetinin ve bilgisayar veri iletişim ağı (network) üzerinden haberleşmeyi devam ettirebilme yeteneğinin önemi gittikçe artmaya başlamıştır.

Bilgi teknolojilerindeki devamlılık ve sürdürülebilirlik, iş sürekliliğinin ayrılmaz bir parçasını teşkil etmektedir. Bilgi teknolojileri tabanlı yazılım ve uygulamalarda yaşanabilecek hizmet kesintileri kurumların iş sürekliliğini sekteye uğratacaktır.

Kurumsal bilgisayar yazılımlarının sağlıklı kullanımının temini de kurumsal veri merkezlerindeki sunucu sistemlerinin sağlıklı işletimi, sunucularda tolere edilebilir kesinti süresi ve tolere edilebilir kesinti noktalarına başarılı geri dönüş yapılabilmesini bünyesinde ihtiva eden felaket kurtarma disiplininin bilimsel, çağdaş, etkili icrasına bağlıdır.

Bu gereksinimler dikkate alınarak hazırlanan tez çalışması, felaket kurtarma disiplinini detaylı olarak incelemesinin yanında, kurum ve kuruluşların iş sürekliliğini temin etmeleri için etkin, doğru bir felaket kurtarma yönetimi hususunda yapılması gereken hazırlıkları, felaket kurtarmaya önemli katkılar sağlayan bilişim teknolojisi uygulamalarını açıklayarak yol gösterici mahiyette olacaktır.

Tezin Yöntemi

Bu tez çalışmasında verilerin derinlemesine incelendiği, veriler arasındaki ilişkileri ortaya koymayı amaçlayan nitel araştırma yöntemi kullanılmıştır. Nitel araştırmalar; gözlem, görüşme, doküman analizi gibi veri toplama yöntemlerinin kullanılarak araştırılan durumun doğal ortamında gerçekçi bir şekilde ortaya konulmasının amaçlandığı yöntemdir.[1] Uluslararası kuruluşlara ait raporlar, uluslararası dergilere ait makaleler, kitaplar, bilimsel tezler taranarak veriler toplanmış ve toplanan veriler incelenerek bütünlük arz edecek şekilde sistematik olarak derlenmiştir. Önemsenen, gerek duyulan konuların detaylarına inilerek derinlemesine incelemede bulunulmuştur. Tez çalışmasının sonunda bütün bir tez boyunca yapılan incelemeler sonucu elde edilen bilgiler doğrultusunda veri merkezlerinde etkin ve doğru bir felaket kurtarma yönetimi gerçekleştirme noktasında tavsiye mahiyetinde çözüm önerileri sıralanmıştır.

[1] Ali Yıldırım, Hasan Şimşek, *Sosyal Bilimlerde Nitel Araştırma Yöntemleri*, Seçkin Yayınları, Ankara 2013, s. 17-18.

Veri Toplama ve Analiz Teknikleri

Bu tez çalışmasında, nitel araştırma yöntemlerinden doküman/metin analizi tekniği kullanılmıştır. Araştırmada incelenen olgu veya olaylarla ilintili bilgiler içeren yazılı belgelerin ayrıntılı olarak taranması ve bu bilgilerden yeni bir bütünlük oluşturulması, doküman/metin analizi olarak adlandırılmaktadır.[2]

Veri toplama tekniği olarak kaynak tarama (review) yöntemi kullanılmıştır. Kaynak tarama yöntemi, tüm klasik ve güncel kaynakların taranması ile ortaya konulan araştırmanın tarihsel ve bilimsel gelişimini birlikte ele alan yöntemdir.[3] Araştırmacının araştırma konusuyla ilgili mevcut kaynakları incelemesi yoluyla veri elde ettiği kaynak tarama yöntemi, ön tarama ve detaylı tarama olmak üzere iki aşamaya ayrılmaktadır. Ön tarama, konu başlıklarının belirlenebilmesi; detaylı tarama ise tüm ana ve yardımcı kaynakların elde edilebilmesi amacıyla gerçekleştirilmektedir.[4]

Ön tarama aşamasında tez konusu ile ilgili verilere kaynaklık etmesi amacıyla tez konusu ile ilgili başka çalışmalar incelenerek konu başlıkları belirlenmiş ve tezin genel çerçevesi çizilmiştir.

Detaylı tarama aşamasında ise Felaket Kurtarma Dergisi (Disaster Recovery Journal-DRJ) ve İş Sürekliliği Enstitüsü (Business Contiunity Institute-BCI) gibi uluslararası kuruluşlara ve dergilere ait raporların yanında yayımlanmış tezler, kitaplar, makaleler, kurumsal internet siteleri olmak üzere belli başlı veri toplama araçları taranarak güncel bilgi ve veriler elde edilmiştir. Söz konusu bilgi ve verilere, tezin amacı doğrultusunda bilimsel etik ve kurallara uygun olarak yer verilmiştir.

---

[2] John W. Cresswell, *Educational research: Planning, Conducting, and Evaluating Quantitative Research*, Prentice Hall Upper Saddle River, New Jersey, 2005.
[3] Kazım Özdamar, *Modern Bilimsel Araştırma Yöntemleri*, Kaan Kitabevi, Eskişehir, 2003, s. 71.
[4] Mehtap Yıldız, *Araştırmalarda Kaynak Tarama Yöntemleri*, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara, 2005, s. 3.

Toplanan verilerin analizi için kullanılan veri analiz yöntemi, betimsel analizdir. Nitel veri analizlerinde en çok karşılaşılan kavramlardan biri betimleme denilebilir.[5] Betimsel analiz, elde edilen verilerin önceden belirlenen temalara\konulara göre kategorize edilmesidir. Dört basamaktan oluşur: betimsel analiz için çerçeve oluşturma, tematik çerçeveye göre verilerin işlenmesi, bulguların tanımlanması ve yorumlanmasıdır.[6] Betimsel analizde asıl amaç, olayı olduğu gibi özetlemek olduğu için alıntılara da yer verilmektedir.[7]

Tezin Kapsam ve Sınırlılıkları

Bu tezin konusunu; felaket kurtarma ve iş sürekliliği kavramlarının incelenmesi, iki kavram arasındaki ilişkinin ortaya konulması, bilgi işlem merkezlerinde kurum ve kuruluşların iş sürekliliğini sürdürebilmeleri, etkin ve doğru bir felaket kurtarma yönetimini icra edebilmeleri adına uygulanması gereken tedbir ve teknolojilerin incelenmesi, dünya ve Türkiye'deki felaket kurtarma yönetimi örnek ve uygulamalarına yer verilmesi ve tez boyunca yapılan incelemeler sonucu elde edilen bilgiler doğrultusunda etkin, doğru bir felaket kurtarma yönetimi noktasında izlenmesi gereken uygulamaların yer aldığı bir tavsiye listesi aracılığı ile çözüm önerilerinin kurum ve kuruluşlar için ortaya konulması ve felaket kurtarma disiplininin Radyo ve Televizyon Üst Kurulu özelinde değerlendirilmesi oluşturmaktadır. İş sürekliliği, felaket kurtarmayı da içine alan geniş kapsamlı bir kavramdır. Tez çalışmasında, iş sürekliliği alt kavramı olan felaket kurtarma incelenmiş ve bir bütün olarak iş sürekliliği incelemesine yer verilmemiştir.

[5] Özlem Üzümcü, "Nitel Araştırma Yöntemine Sahip Tezlerin Bazı Değişkenler Açısından İncelenmesi*", Akademik Sosyal Araştırmalar Dergisi*, Cilt 4, Sayı 32, 2016, s. 327-340.
[6] a.g.m, s. 327-340.
[7] a.g.m, s. 327-340.

BİRİNCİ BÖLÜM

FELAKET KURTARMA YÖNETİMİ

Pasifik Okyanusundaki güçlü depremin tetiklemiş olduğu tsunami, Denver'da otoyolların çökmesine neden olan çığ, Katrina Kasırgası, Georgia'daki tornado gibi vakalar sadece dünyanın dört bir tarafındaki insanın dikkatini çekmemiş, aynı zamanda bilişim profesyonelleri (IT professionals) üzerinde de güçlü bir etki oluşturmuştur.[8] Teknoloji, kurumların her düzeyindeki iş süreçlerine daha fazla entegre oldukça bilişim uzmanlarının iş kapsamı da genişlemektedir. Bu günlerde teknolojinin temas etmediği bir kurum köşesine rastlamak pek mümkün görünmemektedir. Sonuç olarak teknoloji hizmetlerine yönelik olası kesintileri planlama ihtiyacı katlanarak artmıştır.[9]

İş sürekliliği için her zaman verilerin korunması ve bilişim sistemlerinin kesintisiz olarak çalışmasının sağlanması gerekmektedir.[10] Ayrıca altyapılarda yaşanan sorunlar, kurum ve kuruluşları geri dönüşü olmayan felaketlere sürükleyebilmekte ve onarılması zor sorunlara yol açabilmektedir. Kurumsal verilerin birden fazla merkezde saklanması gerekmektedir.[11] Felaket kurtarma, kurumsal iş uygulamalarının kesintisiz çalışması ve kurumsal verilerin kaybolmaması için tüm

[8] Susan Snedaker, *Business Contiunity and Disaster Recovery Planning For IT Professionals*, Syngress Publishing Inc, ABD 2007, s. 2.
[9] a.g.e, s. 2.
[10] https://www.teknotel.com/felaket-kurtarma-cozumu-disaster-recovery (30.09.2020)
[11] a.g.k.

sistem ve bilgilerin farklı lokasyonda bir veri merkezinde tutulduğu bir disiplindir. Bu yönüyle iş sürekliliğinin ayrılmaz bir parçası ve temel gereklerinden biridir.[12]

1.1. FELAKET NEDİR?

Felaket, kuruluşların normal işleyişlerini engelleyen veya kritik süreçlerini kesintiye uğratan ani ve planlanmamış olay olarak tanımlanmaktadır.[13] Bir felaketin olası sonuçları arasında tesislerin hasara uğraması, önemli veri kaybı, çalışanların maddi ve manevi olarak etkilenmesi, gelir elde etme yeteneğinden mahrum kalma, sermaye kaybı, itibar ve güven zedelenmesi ya da kurumun tamamen kontrolü kaybetmesi gibi geniş çapta meydana gelebilecek zararlar yer almaktadır.[14] Bir bilişim sisteminin zarara uğramasına neden olan muhtemel durum ya da olaylar, felaket olarak adlandırılmaktadır.[15]

1.2. FELAKET TÜRLERİ

Genel tehditler (felaket kaynakları) doğa kaynaklı, insan kaynaklı ya da çevresel kaynaklı olabilmektedir.[16] Tehditler, felaketler ya da tehlikeler üç kategoriye ayrılmaktadır.[17]

- Doğal Felaketler
- İnsan Kaynaklı Felaketler
- Kazalar ve Teknolojik Felaketler

Enformasyon teknolojilerinde (bilgi teknolojilerinde) felaketin dış kaynaklı deprem, yangın veya sabotaj olması gerekmez. Belki de en önemli felaket kaynağı,

[12] https://www.teknotel.com/felaket-kurtarma-cozumu-disaster-recovery (30.09.2020)
[13] Martin Hinca, *Business Contiunity and Disaster Recovery for IS*, Masarykova Univerzita Fakulta Informatiky, Çek Cumhuriyeti 2006, s. 6.
[14] Chad Bahan, *The Disaster Recovery Plan*, SANS Institute Press, ABD 2003, s. 4-5.
[15] John W. Rittinghouse, James F. Ransome, *Business Contiunity and Disaster Recovery for InfoSec Managers*, Elsevier Digital Press, Birleşik Krallık, 2005, s. 23.
[16] a.g.e, s. 23.
[17] S. Snedaker, 2007, s. 17-18.

sistemin kendi oluşturduğu felaketler olacaktır.[18] Örneğin; yeterince denenmemiş bir yazılımın uygulama sırasında veri kaybına yol açması veya insan hatalarından kaynaklanan felaketler, dış kaynaklı felaketlerden çok daha tahrip edici olabilir. London Business School tarafından yapılan bir araştırmada felaketler arasında % 57 ile enformasyon teknolojileri ile doğrudan ilişkili felaketlerin başı çektiği belirlenmiştir.[19] Benzer şekilde PricewaterhouseCoopers tarafından yapılan bir başka araştırmada, işletmelerin % 35'inin bilgisayar felaketleri neticesinde 250.000 Sterlin'den daha fazla para kaybettikleri, başka araştırmalarda ise felaketlerin % 30'unun yazılım veya donanım hatalarından kaynaklandığı belirtilmektedir. Bu durumda ister istemez felaketlerin başrol oyuncusunun bilgisayar sistemleri olduğu görülmektedir.[20]

Açıkça ifade etmek gerekirse doğal felaketler ya da doğa kaynaklı felaketler (natural hazards) bazen tahmin edilebilen ve etkisi azaltılabilen felaketlerdir.[21] Doğal felaketler ile bazen de uyarı olmaksızın önceden tahmin edilmeyen bir şekilde karşı karşıya kalınmaktadır ve müdahale gerektirmektedir. Aynı zamanda insan kaynaklı felaketler de bazen tahmin edilmektedir ama bu durum söz konusu olmadığında da bir sürpriz olarak vuku bulmaktadır.[22] Son olarak kazalar ve teknolojik felaketler de meydana gelmektedir ve bu tür felaketler küçükten büyüğe geniş yelpazede bir felaket senaryosunu kapsamaktadır.

Bu kategori sıklıkla teknolojik tehditler olarak adlandırılmaktadır çünkü bu kategori felaket tipleri açısından bina ve teknoloji altyapısındaki arızaları da içermektedir. Felaket kategorileri, aşağıda detaylı olarak incelenecektir.[23]

[18] Haldun Akpınar, *Enformasyon Teknolojilerinde İş Sürekliliği Yönetimi ve Felaket Planlaması*, İstanbul Teknik Üniversitesi Yayını, İstanbul, 2009, s. 175-185.
[19] a.g.e, s. 175-185.
[20] a.g.e, s. 175-185.
[21] S. Snedaker, 2007, s. 17-18.
[22] a.g.e, s. 17-18.
[23] a.g.e, s. 17-18.

1.2.1. Doğal Felaketler

Doğal felaketler, felaket kurtarma ve iş sürekliliğinden bahsedildiğinde akla derhâl gelen felaket olaylarındandır. Geçtiğimiz birkaç yılda, birçok doğal felaket olayı meydana gelmiştir.[24] Örneğin; 26 Aralık 2005'te Endonezya'yı vuran tsunami bir doğal felaket olayı sayılmaktadır. Aynı zamanda körfez sahili ve ABD'yi vuran kasırgalar, en önemlisi Katrina Kasırgası olmak üzere, büyük çapta zararlar meydana getirmiştir.[25] Doğal felaketler küçük, büyük ve devasa ölçekte meydana gelebilmektedir bu yüzden felaket kurtarma yönetimi üç olası tehdit seviyesini dikkate almalıdır. Ek olarak doğal afetler tahmin edilmekte veya edilememektedir.[26]

Endonezya'yı vuran tsunami, dünyanın dört yanındaki bilim adamlarınca denizaltı depreminin gücünün ölçüldüğü şiddetle doğru orantılı bir olasılıkla beklenmektedir.[27] Büyük bir su duvarının birkaç saat içinde Tayland'dan Kenya'ya kadar kıyı şeritlerine çarpacağını çok az kişi bilmektedir ve bu durumu tahmin etmek son derece zordur. Katrina Kasırgası bilim adamları tarafından olası sonuçları göz önünde tutularak öngörülmüştür ama kamu sektörü ve özel sektör tarafından büyük ölçüde hafife alınmıştır.[28] Ne olursa olsun her iki durumda da etki, tam bir yıkıma sebebiyet vermiştir. Felaket kurtarma yönetimi sınırlı etkiye sahip çok sayıda kurum ve kuruluş vakası bulunmaktadır çünkü bu olaylardan önce kimse yıkımın düzeyini hayal edememiştir.[29]

Amerika'da, Federal Acil Durum Yönetim Kurumu (Federal Emergency Management Agency-FEMA) Katrina Kasırgası sonrası New Orleans'ta bir afet planını etkili bir şekilde uygulayamadığı ve yönetemediği için yaygın olarak

[24] S. Snedaker, 2007, s. 18-19.
[25] a.g.e, s. 18-19.
[26] a.g.e, s. 18-19.
[27] a.g.e, s. 19.
[28] a.g.e, s. 19.
[29] a.g.e, s. 19.

eleştirilmiştir.[30] Büyük kafa karışıklığı ve düzensizlik nedeniyle insanların acı çekmesi ve ölümler meydana gelmiş ve kurumsal iş süreçleri aksamıştır.[31] Bu durumda felaket kurtarma yönetimi hazırlığı bulunmayan kurum ve kuruluşlar oldukça savunmasız durumdadır ancak tahliye, uzaktan veri yedekleme (remote data backup), veri depolama (data storage) ve benzeri planları olan kurum ve kuruluşlar, bu tür planları olmayanlara göre daha hızlı ve daha etkili bir şekilde ayağa kalkmıştır.[32] Doğa kaynaklı felaketler seller, depremler, heyelanlar, tornadolar, elektrik fırtınaları ve diğer bazı olaylardan teşekkül etmektedir.[33] Aşağıda kategorize edilmiş doğa kaynaklı felaket tipleri gösterilmiştir.[34]

Soğuk Hava İlişkili Felaketler

- Çığ
- Şiddetli Kar Yağışı
- Buz Fırtınası, Dolu Fırtınası
- Şiddetli veya Uzun Süreli Rüzgâr

Sıcak Hava İle İlişkili Felaketler

- Şiddetli veya Uzun Süreli Yağmur
- Yoğun Yağış ve\veya Su Baskını
- Sel
- Kuraklık
- Yangın
    - Orman Yangını
    - Şiddetli Yangın- Kentsel, Kırsal ve Tarımsal Yangın
    - Şehir Yangını
- Tropik Fırtına
- Kasırga, Siklon, Tayfun (ad, olayın konumuna bağlıdır)
- Tornado
- Rüzgâr Fırtınası

[30] S. Snedaker, 2007, s. 19.
[31] a.g.e, s. 19-20.
[32] a.g.e, s. 19-20.
[33] J. W. Rittinghouse, J. F. Ransome, 2005, s. 23.
[34] a.g.e, s. 19-20.

Jeolojik Felaketler

- Deprem
- Tsunami
- Volkanik Patlama
    - Volkanik Kül
    - Lav Akışı
    - Çamur Akışı (yıkıcı çamur akışı, lahar)
- Toprak Kayması (çökme ve yükselme; su tabakasındaki değişiklikler, insan kaynaklı unsurlar (tüneller, yeraltı yapıları), jeolojik faylanma, doğal gazların yeraltından çıkarımı sebebiyet vermektedir)

Bu liste bütün varyasyonları içermemesine rağmen coğrafik konuma göre hangi felaketlerin meydana geleceğini belirlemede başlangıç noktasını teşkil etmektedir.[35] Örneğin; eğer Londra, Mumbai, ya da New York'taki iş ofisleri düşünüldüğünde, sözü geçen şehirlerin coğrafyasına dayalı olarak potansiyel tehlikeler etkili bir şekilde gözden geçirilmeli ve sayılan iş merkezi ofis konumları kendi özelinde değerlendirilmelidir.[36]

1.2.2. İnsan Kaynaklı Felaketler

İnsan kaynaklı felaketler, aynı zamanda antropojenik (insan kökenli eylemler için kullanılan terim) olarak da adlandırılmaktadır ve doğaları gereği biraz fazla çeşitlilik arz etmektedir. İnsan kaynaklı felaketler arasında, bilgi sistemine yanlışlıkla veri girişi gibi kasıtsız eylemler, veri iletişim ağı tabanlı saldırılar, kötü niyetli yazılım yüklemeleri, güvenli bilgiye yetkisiz erişim gibi kasıtlı eylemler de yer almaktadır.[37] Listedeki bazı ögeler sürpriz olarak değerlendirilebilir ama çoğu kasıtlı\niyetli olduğu için kategorize edilmeden listelenecektir.[38]

[35] S. Snedaker, 2007, s. 20.
[36] a.g.e, s. 20.
[37] J. W. Rittinghouse, J. F. Ransome, 2005, s. 23.
[38] a.g.e, s. 20.

- Terörizm
    - Bombalar
    - Silahlı Saldırı
    - Tehlikeli Madde Salınımı (biyolojik, radyoaktif tehlike)
    - Siber Saldırı
    - Biyolojik Saldırı (hava, su, yiyecek)
    - Taşımacılık Saldırısı (havaalanları, limanlar, tren yolları)
    - Altyapı Saldırıları (havaalanları, hükümet binaları, askeri üsler, kamu hizmetleri, su kaynakları)
    - Adam Kaçırma
- Patlama
- Yangın
    - Kundakçılık
    - Kazara Çıkmış Yangın
- Siber Saldırı
    - Tehdit veya Sahte Siber Saldırı
    - Küçük Çaplı İzinsiz Giriş
    - Büyük Çaplı İzinsiz Giriş
    - Toptan Kesinti
    - Yaygın Veri İletişim Ağı Altyapısı Bozulması (İnternet, Omurga vs.)
- Sivil İtaatsizlik, İsyan, Huzursuzluk
- Protesto
    - Yaygın Siyasi Protesto
    - Hedefli Protesto (örneğin; bir kurumu spesifik olarak hedef alan protesto)
    - Ürün Sabotajı (product tampering)
    - Radyoaktif Kirlilik
- Zimmete Para Geçirme
- Adam Kaçırma
- Gasp

- Çökme (insan kaynaklı\doğa kaynaklı etkilerin bina ya da altyapıda meydana getirdiği değişiklik nedeniyle toprak kayması)

1.2.3. Kazalar ve Teknolojik Felaketler

Kazalar ve teknolojik felaketler çoğunlukla insan kaynaklı felaketler ile ilgilidir fakat ondan sıklıkla plansız\istemsiz olması nedeniyle ayrılmaktadır.[39] Durum kasıtlı olduğunda, burada sayılacak felaketler, insan kaynaklı felaketler kategorisinde sıralanacaktır.[40] Kaza sonucu, istemeden meydana gelmiş felaketler, hangi kategoriye koyulursa koyulsun felaket kurtarma yönetimi sürecinde gözden kaçırılabilme niteliği arz etmektedir.[41] Çevresel tehditler, uzun dönemli güç kesintileri, kirlilik, kimyasal sıvı sızıntıları gibi olaylardan meydana gelmektedir.[42] Aşağıda kazara veya teknolojik bir yolla oluşmuş felaketler listelenecektir.[43]

- Taşımacılık Kazaları ve Hataları
    - Otoyol Çökmesi veya Büyük Kazalar
    - Havaalanı Çökmesi, Havada Çarpışma veya Kaza
    - Tren Yolu Çökmesi veya Kazası
    - Su Kazası veya Liman Kazası
    - Boru Hattı Çökmesi veya Kazası
- Altyapı Kazaları veya Arızaları
    - Elektrik-güç kesintisi, voltaj kesintisi, geçici kesinti, altyapı arızası
    - Gaz-kesintisi, patlama, tahliye, sistemin çökmesi
    - Su-kesintisi, kirlilik, kıtlık, sistemin çökmesi
    - Kanalizasyon-tıkanma, geri akış, kirlilik, sistemin çökmesi
- Bilgi Teknolojileri Altyapısı
    - İnternet Altyapısı Kesintisi

[39] S. Snedaker, 2007, s. 22-23.
[40] a.g.e, s. 22-23.
[41] a.g.e, s. 22-23.
[42] J. W. Rittinghouse, J. F. Ransome, 2005, s. 23.
[43] a.g.e, s. 22-23.

    - Haberleşme Altyapısı Kesintisi (denizaltı, kablolama, uydu vs.)
    - Büyük Hizmet Sağlayıcı Kesintisi (internet, haberleşme vs.)
    - Sistem Arızaları
- Güç Şebekesi veya Trafo Merkezi Arızası
- Nükleer Enerji Tesisi Olayı
- Baraj Arızası
- Tehlikeli Madde Olayı
    - Yerel, Sabit Kaynak
    - Yerel Olmayan Ya da Geçiş Kaynağı (radyoaktif ya da kimyasal atıklar kamyonla taşınırken yaşanan çarpışmalar)
- Bina Çökmeleri (çeşitli olaylar)

Yukarıdaki afet listesi olaylarından bir tanesi ile karşı karşıya kalındığında yapılması gereken başı yastığın altına gizlemek ve felaketlerin geçmesini beklemek değildir. Maalesef ki bu olaylar ihtimal dâhilindedir ve meydana gelmektedir ve bu tür hayal dahi edilemeyecek belirsizliklerle başa çıkmanın en iyi yolu, onları hayal etmek ve onlarla başa çıkmak için metodolojik bir felaket kurtarma yöntemi geliştirmektir.[44] Bu olayların bir tanesi meydana geldiğinde ve bu sorunla baş edilmek zorunda kalındığında felaket kurtarma yönetiminin harfiyen yerine getirilmesi olasılığı düşüktür.[45] Tecrübe edilecek her şeyi düşünmek imkânsızdır fakat test edilmiş ve uygulanmış sağlam bir felaket kurtarma metodolojisine sahip olmak, olayın stresini azaltacak ve karşılaşılan olayları önceden tahmin etme olasılığını artıracaktır.[46]

Zor durumlarda, iyi bir felaket kurtarma yönetimi icra edebilme yeteneği, hayatta kalma\kalamama veya geri kazanım yapma\yapamama noktasında fark ortaya koymak anlamına gelmektedir.[47]

[44] S. Snedaker, 2007, s. 20.
[45] a.g.e, s. 20.
[46] a.g.e, s. 20.
[47] a.g.e, s. 20.

1.3. FELAKET KURTARMA NEDİR?

Felaket Kurtarma Dergisi (Disaster Recovery Journal-DRJ) ve İş Sürekliliği Enstitüsünün (Business Contiunity Institute-BCI) ortak tanımına göre, bir afet veya kesinti sonrasında bir kuruluş için hayati önem taşıyan teknoloji altyapısının, sistemlerin ve uygulamaların kurtarılmasına veya devam ettirilmesine yönelik hazırlıklarla ilgili süreç, politikalar ve prosedürlere felaket kurtarma denmektedir.[48]

Felaket Kurtarma (Disaster Recovery-DR) bir kurumun doğal veya insan kaynaklı ortaya çıkan bir felaket karşısında bilgi teknolojileri (information technology-IT) altyapısının etkili bir şekilde yeniden kazanımı ve ayağa kaldırılması için hazırlanmış prosedürler, işlemler ve politikaları kapsayan bir disiplindir.[49] Siber saldırılardan donanım arızalarına ve doğal afetlere kadar felaket kurtarma (disaster recovery-DR) disiplini, bilgi teknolojileri altyapısını (information technology infrastructure) tehdit eden herhangi bir senaryo olasılığını bertaraf etmek için gerekli önlemleri alma yeteneğine ve çözüm önerilerine sahiptir.[50]

Felaket kurtarma, bir kurumun doğal afet, siber saldırı, KOVİD-19 salgını gibi felaket tipleri karşısında iş kesintilerinin önüne geçmek adına tekrardan bilişim sistemleri altyapısına erişim ve işlevsellik kazandırma yöntemidir.[51] Felaket kurtarma, felaketten etkilenmeyen kurum dışı bir yerde verilerin ve bilgisayar işlemlerinin kopyalanmasına dayanmaktadır.[52]

Sunucular; doğal afet ya da ekipman arızası nedeniyle devre dışı kaldığında, bir işletmenin kaybolan verilerinin, verilerin yedeklendiği ikinci bir yerden yeniden

[48] https://www.rockdovesolutions.com/blog/the-differences-between-business-continuity-and-disaster-recovery (10.08.2020)
[49] https://www.imperva.com/learn/availability/disaster-recovery/ (05.10.2020)
[50] a.g.k.
[51] a.g.k.
[52] https://www.vmware.com/topics/glossary/content/disaster-recovery (13.08.2020)

kazanılması gerekmektedir.[53] İdeal olarak; kurum ve kuruluşların iş süreçlerine devam edebilmeleri için kendilerine ait bilgisayar ortamı verilerini (computer media data) uzak bir yere transfer edebilmeleri gerekmektedir.[54]

Enformasyon teknolojileri açısından bir işletmenin en önemli ögesi, ürettiği veriler olsa da, bu verilerin tek başına bir anlam ifade etmesi söz konusu değildir. Veriler ancak diğer üç ögenin, yani yazılım, donanım ve bu sistemden fayda üretebilecek insan gücünün varlığı ile önem kazanacaktır.[55] Bu nedenle enformasyon teknolojileri açısından felaket planlaması, herhangi bir felaket sonrası sistemin işlerlik kazanmasını sağlayacak şekilde, sistemin bu dört öğesinin nasıl bir araya getirileceğinin planlanması olacaktır. Ancak karşılaşılacak felaketin yapısına, boyutuna ve işletmenin felaket planlaması için ayırmayı istediği veya ayırabileceği bütçe miktarına göre çok farklı senaryolar üretilebilecektir.[56]

1.4. İŞ SÜREKLİLİĞİ NEDİR?

Felaket Kurtarma Dergisi ve İş sürekliliği Enstitüsünün ortak tanımına göre, iş operasyonlarını önceden tanımlanmış kabul edilebilir bir seviyede devam ettirmek için organizasyonların olayları planlama ve bunlara müdahale etme stratejik ve taktik yeteneğine iş sürekliliği denmektedir.[57] İş sürekliliği planlaması (Business Contiunity Planning-BCP), afetler ve yıkıcı olaylar öncesinde sürekli iş operasyonlarını sürdürmek için bir plan oluşturmak ve bu planı doğrulamak için kullanılan bir metodolojidir.[58] İş sürekliliği planlaması; kurum ve kuruluşların çeşitli risklere maruz kalmaları karşısında bu riskler için etkili bir değerlendirme ve hazırlık sağlamak için

[53] https://www.vmware.com/topics/glossary/content/disaster-recovery (13.08.2020)
[54] a.g.k.
[55] H. Akpınar, 2009, s. 175-185.
[56] a.g.e, s. 175-185.
[57] https://www.rockdovesolutions.com/blog/the-differences-between-business-continuity-and-disaster-recovery (10.08.2020)
[58] S. Snedaker, 2007, s. 3.

kaynakları bir araya getirmenin yanında riskler konusunda müdahale ve iyileştirme planları sunmaktadır.[59]

İş sürekliliği (Business Contiunity-BC), kurum ve kuruluşların operasyonlarının ve temel iş fonksiyonlarının, kritik sistemleri çevrim dışı duruma getiren bir felaket veya planlanmamış olaydan ciddi şekilde etkilenmemesini sağlama becerisidir.[60] İş sürekliliği planlaması; genellikle bilişim teknolojilerinin önderlik ettiği bir bölümler arası süreçtir ve belirli bir süre içinde normal iş akışlarını geri yüklemek için kullanılan taktikleri uygulamak, iş için kabul edilen veri kaybı miktarını tanımlamak ve kritik bilgileri kurumsal paydaşlara iletmek için kullanılan bir bölümler arası süreçtir.[61]

İş sürekliliği, kurum ve kuruluşların acil durumlar sırasında kritik iş fonksiyonlarını icra edebilme kapasitesine sahip olması anlamına gelmektedir ve bu yeteneği haiz olmak için etkili bir felaket kurtarma yönetiminin planlama ve hazırlığını haiz olmak gerekmektedir.[62] Acil durumlar; doğal felaketler, iş krizi, salgın (pandemic), iş yerinde şiddet ya da iş operasyonlarının kesintiye uğraması ile sonuçlanabilecek herhangi bir olayı içerebilmektedir.

İş süreçlerini tamamen veya kısmen durduracak olaylara hazırlanmayı ve önlemler almayı ihmal etmemek önemlilik arz etmektedir.[63] Kurum ve kuruluşlar; olası risk, tehdit veya kesinti durumları fark etmeksizin iş sürekliliklerini devam ettirmek zorundadır.[64]

[59] Bob Hayes, Kathleen Kotwica, *Business Contiunity:Playbook*, Elsevier Inc, ABD, 2013, s. 1.
[60] https://www.inap.com/blog/business-continuity/ (12.09.2020)
[61] a.g.k.
[62] https://www.mha-it.com/2017/08/01/what-is-business-continuity/ (04.09.2020)
[63] a.g.k.
[64] S. Snedaker, 2007, s. 3.

1.4.1. İş Sürekliliği Planlamasının Kamuda Şekillenmesi

27 Şubat 2003 tarihinde yayımlanan E-Dönüşüm Türkiye Projesi Genelgesi ve Devlet Planlama Teşkilatı-DPT tarafından 2005 yılında yayımlanan Eylem Planı kapsamında yer alan 33. eylem ile "Kamu Bilgi Sistemleri Acil Durum Yönetimi Çözüm Önerileri" çalışması, Türkiye Bilimsel ve Teknik Araştırma Kurumu Ulusal Elektronik ve Kriptoloji Araştırma Merkezi-TÜBİTAK UEKAE'ye verilmiştir.[65] 2006 yılında yayımlanarak yürürlüğe giren "Bilgi Toplumu Stratejisi Eylem Planı" 76 numaralı eylemi ile "Bilgi Sistemleri Olağanüstü Durum Yönetim Merkezleri" görevi sorumlu kuruluş olarak Türksat'a, ilgili kuruluş olarak da Başbakanlık, Devlet Planlama Teşkilatı-DPT ve TÜBİTAK UEKAE'ye verilmiştir.[66] 2013 yılında yapılan Bilim ve Teknoloji Yüksek Kurulu-BTYK 25. toplantısında alınan "Kamu kurumlarının veri merkezlerinin birleştirilmesine yönelik hukuki, teknik ve idari yapılanma modelinin oluşturulmasına ve Türkiye Kamu Entegre Veri Merkezi'nin kurulması çalışmalarının yapılması." kararı için ilgili kuruluş olarak TÜRKSAT belirlenmiştir.[67]

1.5. FELAKET KURTARMA YÖNETİMİ VE İŞ SÜREKLİLİĞİ ARASINDAKİ FARKLAR VE ORTAK NOKTALAR

İki kavram birbiri yerine kullanılabilmektedir fakat iş sürekliliği ve felaket kurtarma kavramları aynı şeyler değildir.[68] Felaket kurtarma, yıkıcı olayların ortasında bir işletmenin tüm iş akışlarını sürdürmeyi amaçlayan iş sürekliliği kavramının aksine iş süreçlerinin devamının bir parçasını teşkil eden bilgi ve teknoloji sistemlerine odaklanmaktadır.[69] Pratik anlamda iş sürekliliği ise kurum ve kuruluşların iş süreçlerini devam ettirmek için sahip oldukları plan manasına gelmektedir.[70] Bu,

[65] https://bilisim.turksat.com.tr/bilisim-sistemleri-barindirma-ve-fkm-hizmetleri (12.01.2021)
[66] a.g.k.
[67] a.g.k.
[68] https://www.rockdovesolutions.com/blog/the-differences-between-business-continuity-and-disaster-recovery (10.08.2020)
[69] a.g.k.
[70] a.g.k.

herhangi bir felakette iş süreçlerini devam ettirebilecek hizmet binası, personel, kurumsal sözleşmeler ve fiziki altyapıyı kapsamaktadır yani iş sürekliliği yönetimi denildiği zaman kurum ve kuruluşlar açısından hizmet binası, sahip olunan teknoloji veya üçüncü taraflarla yapılan sözleşmeler dâhil işin tüm yönleri düşünülmelidir.[71]

Felaket kurtarma, iş sürekliliğinin bir alt unsurudur.[72] Felaket kurtarma, iş sürekliliğinin bir parçasıdır ve olayların ani etkileri ile ilgilenmektedir. Bir sunucu kesintisi, bilgi güvenliği (information security) ihlali veya bir kasırganın yıkıcı etkisinden kurtulmanın tümü bu kategoriye girmektedir.[73]

Felaket kurtarma yönetimi; veri, teknoloji, altyapı ve sistemlerin nasıl geri kazanılacağına odaklanmaktadır. Felaket kurtarma disiplini, iş sürekliliğini meydana getirmek için gereklilik arz etmektedir. Felaket kurtarma; verinin nasıl depolandığı, servis edildiği ve paylaşıldığı ile ilgilenmektedir.[74] Kurum ve kuruluşlar, çalışanlarının nereden çalıştıklarına bakmaksızın (evden, uzak ofisten ya da kahve dükkânından) tüm çalışanlarının dosyalar, klasörler, sunucular, e-posta, sunumlar vs. gibi önemli kurumsal verilere erişebilmelerini garanti etmelidir. Felaket kurtarma yönetimi olmadan iş sürekliliğinin sağlanması mümkün olmamaktadır. [75]

Felaket kurtarma, yüzde yüz iş sürekliliğini garanti etmemektedir.[76] Her iki disiplinin de yerinde, doğru olması ve birlikte çalışması gerekmektedir. Bir tehdit ya da felaket karşısında sadece tek disiplinin yönetimini sağlamak iş başarısını garanti etmeyecektir.[77]

[71] https://www.rockdovesolutions.com/blog/the-differences-between-business-continuity-and-disaster-recovery (10.08.2020)
[72] S. Snedaker, 2007, s. 4.
[73] a.g.e, s. 4.
[74] a.g.k.
[75] a.g.k.
[76] a.g.k.
[77] a.g.k.

İşletmelerin en az kesintiyle veya hiç kesinti olmadan iş süreçlerine devam etmesini sağlayan bir iş sürekliliği planı, tüm verilerin ve bilişim sistemlerinin erişilebilir ve kurtarılabilir olmasını sağlayan bir felaket kurtarma yönetimi gerektirmektedir.[78]

Çoğu zaman felaket kurtarma ve iş sürekliliği aynı kavram olarak telakki edilerek hataya düşülmektedir fakat iki kavram arasında açık farklar mevcuttur. Tablo 1.1'de felaket kurtarma ile iş sürekliliği kavramları arasındaki farklar gösterilmektedir.

Tablo 1.1 Felaket Kurtarma ve İş Sürekliliği Arasındaki Farklar[79]

Felaket Kurtarma ve İş Sürekliliği Arasındaki Farklar	
Felaket Kurtarma	**İş Sürekliliği**
Felakete müdahale için aktiviteler önceden planlanır.	Felaket meydana geldiğinde kurumun varlıkları ve iş süreçleri üzerinde ters etki yapacak, riskleri azaltıcı planlar yapılmaktadır.
Felaket kurtarma, veri merkezi yönelimlidir (data centric).	İş sürekliliği, iş yönelimlidir.
Ana fikir, bilişim sistemlerinin çalışmasını felaket durumundan normale döndürmek.	Ana fikir, kritik iş süreçlerini devam ettirmek.

1.6. FELAKET KURTARMA YAKLAŞIMLARI

En iyi felaket planı, ilgili kurum veya kuruluşun verilerinin tıpkı kopyasına tanımlanan felaketlerin erişemeyeceği bir coğrafi konumda sahip olmaktır.[80] İlk başta en iyi yaklaşımın bu olduğu düşünülse de, farklı nedenlerden dolayı bu yaklaşımı gerçekleştirmek mümkün olmayacaktır.[81] İşletmelerin aynı anda iki veri merkezinin

[78] https://www.rockdovesolutions.com/blog/the-differences-between-business-continuity-and-disaster-recovery (10.08.2020)
[79] Vyshnavi Jorrigala, *Business Contiunity and Disaster Recovery Plan for Information Security Rebublic*, St. Cloud State University, Minnesota 2017, s. 20.
[80] H. Akpınar, 2009, s. 175-185.
[81] a.g.e, s. 175-185.

maliyetini karşılayabilmesinin imkânsızlığı yanında, iki kopyanın aynı anda aynı felaketlere maruz kalmasını engellemenin de garantisi yoktur.[82]

En kötü felaket planı ise, herhangi bir plana ve tedbire sahip olmamak olacaktır.[83] Her ne kadar günümüzde birçok kurum ve kuruluş için bu şekildeki bir plansızlığı engellemek amacı ile bu alanda çeşitli kanuni zorunluluklar getirilmiş olsa da bu durumun hâlâ geçerli senaryolardan birisi olduğunu kabul etmek gerekmektedir.[84] Ancak bu noktada güvenilir bir felaket planı olmayan ve bir felaket sonrası önemli veri kaybına uğrayan işletmelerde yapılan bir araştırmada, işletmelerin % 43'ünün yeniden açılamadığını, % 51'inin iki yıl içinde kapandığını ve sadece % 6'sının varlıklarını sürdürebildiğini, bu klasikleşmiş iş sürekliliği yönetimi örneğini vererek vurgulamakta yarar bulunmaktadır.[85]

Tüm işletmelerin finansal kısıtlar söz konusu olmasa, sıfır çalışılamazlık süresini gerçekleştirecek sistemleri isteyecekleri açıktır.[86] Ancak küçük bir perakendecinin, hatta elektronik ticaret yapan bir perakendecinin iş kesintileri sonucunda uğrayacağı zarar, yapacağı yatırımın yanında çok küçük kalacaksa bu yatırıma girmeyeceği açıktır.[87]

Bir felaketi engelleyebilmek veya felaketin etkilerini asgari düzeyde tutabilmek amacı ile alınan tüm önlemlere rağmen, herhangi bir doğal felaket veya terörizm gibi insandan kaynaklanan bir felaket sonrasında karşılaşılabilecek durumlara ilişkin senaryolardan bir tanesi, mevcut veri merkezinin kaybı ve geçici veya uzun süreli olarak veri işlem uygulamalarının başka bir yerde sürdürülmesidir. Sistemin donanım ögesinin geçici veya sürekli olarak devre dışında kalması hâlinde,

[82] H. Akpınar, 2009, s. 175-185.
[83] a.g.e, s. 175-185.
[84] a.g.e, s. 175-185.
[85] a.g.e, s. 175-185.
[86] a.g.e, s. 175-185.
[87] a.g.e, s. 175-185.

günümüzde iş sürekliliği yönetiminin bir parçası olarak değerlendirilmesi gereken farklı mekân seçeneklerini sınıflandırabilmek mümkündür.[88]

1.6.1. Sıcak Mekân Yaklaşımı

Sıcak mekân yaklaşımı (hot site approach), birincil veri merkezinin anbean yansıtılmış bir kopyasından oluşmaktadır.[89] Sıcak mekân veri merkezi, kritik verinin neredeyse gerçek zamanlı bir yedeği ve birincil veri merkezinin (primary data center) yansıtılmış bir kopyasının işletilmesini olanaklı kılan donanım (hardware), yazılım (software) ve gerekli ağ bağlantısı (network connectivity) ile donatılmıştır.[90] Dakikalar içerisinde birincil veri merkezinin herhangi bir felakete uğraması durumunda sıcak mekân yaklaşımı, minimum kesinti ve sıfır veri kaybını garanti etmektedir.[91]

Sıcak mekân yaklaşımından beklenen, veri merkezleri arasındaki hattın her zaman çevrim içi vaziyette olması, kesinti olmaksızın çalışması ve ana veri merkezi ile ikincil veri merkezi (secondary data center) arasında veri senkronizasyonunu (data synchronization) anlık olarak gerçekleştirmesidir. Felaket kurtarma yaklaşımları (disaster recovery approaches) içerisinde en maliyetli olan sıcak mekân yaklaşımıdır.[92] Sıcak mekân yaklaşımında dikkat edilmesi gereken nokta, ikincil veri merkezinin birincil veri merkezinin yer aldığı konumdan yeterince uzağa kurulması gerektiğidir ve böylelikle herhangi bir felaket durumunda veri merkezlerinin aynı felaketten etkilenme olasılığı düşürülmektedir.[93]

Sıcak mekân yaklaşımı, esasında veri merkezi (data center) altyapısının birebir yansımalarından (mirror) oluşmaktadır. İkincil veri merkezi; sunucular, soğutma

[88] H. Akpınar, 2009, s. 175-185.
[89] https://www.nakivo.com/blog/overview-disaster-recovery-sites/ (08.10.2020)
[90] a.g.k.
[91] a.g.k.
[92] a.g.k.
[93] a.g.k.

sistemleri, güç sistemleri ve eğer uygunsa ofis alanı ile donatılmalıdır.[94] Sıcak mekân yaklaşımının en önemli özelliği, veri merkezlerinin aynı anda senkronize bir şekilde çalışmasıdır. Bu senkronizasyon, iş operasyonlarının (business operations) minimum düzeyde etkilenmesine imkân tanımaktadır.[95] Birincil veri merkezi önemli bir kesintiye maruz kaldığında, ikincil veri merkezi ivedilikle kesintiden olumsuz etkilenmiş veri merkezinin yerini almaktadır. Fakat bu yaklaşımın maliyeti ucuz değildir ve bu durumda kurum ve kuruluşların fayda maliyet- analizini (benefit cost analysis-BCA) gözetmeleri gerekmektedir.[96]

Sistemin hemen kurtarılması gerekiyorsa sıfır kesinti çözümünü garanti eden sıcak mekân yaklaşımını kullanmak daha faydalı ve maliyetli olacaktır fakat sistemin yeniden ayağa kalkması için yeterli süre varsa daha fazla seçenek mevcuttur ve bu seçenekler genellikle daha ucuzdur.[97]

1.6.2. Soğuk Mekân Yaklaşımı

Soğuk mekân yaklaşımı (cold site approach) çok az veya hiç donanım ekipmanı olmaması üzerine kurulu bir kurumsal veri yedekleme (corporate data backup) çözümüdür.[98] Soğuk mekân yaklaşımı; temelde güç sistemi, havalandırma sistemi, klima ve haberleşme ekipmanı gibi donanımlarla hazır bulunan bir ofis alanına dayanmaktadır.[99] Tüm veri merkezi cihazlarının taşınması için güç kaynakları, kesintisiz güç kaynakları (uninterruptible power supply-UPS) gibi donanımlar sunan hazır bir tesis yer almaktadır.[100] Felaket kurtarma yaklaşımları içinde maliyet açısından en uygun olanı soğuk mekân yaklaşımı olmasına rağmen önceden kurulmuş hiç ekipman olmamasından dolayı iş operasyonlarını tamamen sürdürmek için gereken

[94] https://www.seguetech.com/three-stages-disaster-recovery-sites/ (10.10.2020)
[95] a.g.k.
[96] a.g.k.
[97] S. Snedaker, 2007, s. 222.
[98] J. W. Rittinghouse, J. F. Ransome, 2005, s. 91.
[99] a.g.e, s. 91.
[100] a.g.e, s. 91.

altyapının kurulması uzun zaman almaktadır.[101] Bir felaket durumunda kurum ve kuruluşlar (corporations) birincil veri merkezindeki iş yükünü transfer etmek için gerekli sunucuları göç ettirmek (migrate) ve fonksiyonel hâle getirmek noktasında bilgi teknolojileri (information technology-IT) personelinin desteğine ihtiyaç duymaktadır.[102]

Soğuk mekân yaklaşımı esasında herhangi bir sunucu ilintili ekipman kurulu olmaksızın bir veri merkezi veya ofis alanı oluşturulması düşüncesine dayanmaktadır.[103] Ana veri merkezinin herhangi bir kayda değer kesintiye maruz kalması durumunda ikincil veri merkezi; güç sistemi, soğutma ve ofis alanı desteği sunmaktadır.[104] Soğuk mekân yaklaşımı, tüm gerekli sunucuları ve ekipmanları göç ettirmek ve işlevsel konuma getirmek için kapsamlı mühendisliğin yanında donanımlı personel desteği ihtiyacı doğurmaktadır. Soğuk yer yaklaşımı kurumlar için en düşük maliyetli geri kazanım (recovery) seçeneğini sunmaktadır.[105]

1.6.3. Ilık Mekân Yaklaşımı

Ilık mekân yaklaşımı (warm site approach), soğuk mekân ve sıcak mekân yaklaşımlarının ortasında yer alıyormuş gibi düşünülmektedir ve bu yaklaşımda ağ bağlantısı ve gerekli donanım ekipmanı zaten önceden kurulu durumda bulunmasına rağmen ılık mekân veri merkezi, sıcak mekân yaklaşımı ile aynı performansı gerçekleştirememektedir çünkü her iki senaryodaki veri merkezi aynı ölçüde ekipmanla donatılmamıştır.[106] Bu yüzden ılık mekân yaklaşımı, sıcak mekân yaklaşımına kıyasla daha az işlevseldir. Dahası, birincil ve ikincil veri merkezleri

[101] J. W. Rittinghouse, J. F. Ransome, 2005, s. 91.
[102] https://www.nakivo.com/blog/overview-disaster-recovery-sites/ (08.10.2020)
[103] https://www.seguetech.com/three-stages-disaster-recovery-sites/ (10.10.2020)
[104] a.g.k.
[105] a.g.k.
[106] a.g.k.

arasındaki veri senkronizasyonu günlük ya da haftalık olarak icra edilmektedir bu yüzden küçük de olsa veri kayıplarına yol açılabilmektedir.[107]

Ilık mekân yaklaşımı, daha az kritik verinin işlendiği ve kısa bir kesinti süresinin tolere edilebildiği durumlarda etkin bir çözüm olmaktadır.[108] Maliyet açısından sıcak mekân yaklaşımının ardından ikinci en maliyetli çözümdür.[109] Ilık mekân alternatif veri merkezi, transfer edilen birincil veri merkezi iş operasyonlarını üstlenmek için hazır durumdadır.[110]

Çoğu durumda alternatif veri merkezi, birincil veri merkezi veya sistem için normal operasyonel çözüm olarak hizmet verebilmektedir.[111] Felaket kurtarma planı devreye alındığında kesintiye uğrayan veri merkezi aktiviteleri, alternatif veri merkezine taşınmaktadır.[112]

Ilık mekân veri merkezi, önceden kurulmuş (pre-installed) sunucu donanımları yanında ofis alanı ve veri merkezi alanı da sunmaktadır.[113] Sıcak mekân yaklaşımı birincil veri merkezinin birebir kopyası anlamına gelirken; ılık mekân yaklaşımı sadece birincil veri merkezindeki verileri yüklemek için hazır durumda bulunan sunucuları içermektedir.[114] Ilık mekân yaklaşımı, kurum için kritik olmayan fakat bir seviye yedeklilik gerektiren veriler için uygun bir çözüm özelliği göstermektedir.[115]

Tablo 1.2'de Felaket Kurtarma Yaklaşımlarının Kıyaslaması gösterilmiştir.

[107] https://www.seguetech.com/three-stages-disaster-recovery-sites/ (10.10.2020)
[108] https://www.nakivo.com/blog/overview-disaster-recovery-sites/ (08.10.2020)
[109] a.g.k.
[110] a.g.k.
[111] a.g.k.
[112] J. W. Rittinghouse, J. F. Ransome, 2005, s. 91.
[113] a.g.k.
[114] a.g.k.
[115] a.g.k.

Tablo 1.2 Felaket Kurtarma Yaklaşımlarının Kıyaslaması[116]

FELAKET KURTARMA YAKLAŞIMLARININ KIYASLAMASI		
Soğuk Mekân Yaklaşımı	**Ilık Mekân Yaklaşımı**	**Sıcak MekânYaklaşımı**
Az ya da Hiç Ekipman Gereksinimi	Kısmen Fazla Ekipman	Tamamen Fazla Ekipman
İnternet Bağlantısı Yok	İnternet Bağlantısı Var	İnternet Bağlantısı Var
Otomatik Yük Devretme İçin Hazır Değil	Yük Devretme Saatler ya da Günler İçinde Devreye Girer	Yük Devretme Saniyeler ve Dakikalar İçinde Devreye Girer
Veri Senkronizasyonu Yok	Günlük ya da Haftalık Veri Senkronizasyonu	Neredeyse Gerçek Zamanlı Veri Transferi
Veri Kaybı Açısından Yüksek Risk Mevcut	Minimum Veri Kaybı	Sıfıra Yakın Veri Kaybı
Maliyet Açısından Ucuz	Maliyet Açısından Ucuz-Pahalı Arası	Maliyet Açısından Pahalı

1.7. FELAKET KURTARMA STANDARTLARI

1980'lerde IBM (International Business Machine) ile çalışan Share Teknik Yönetim Komitesi (Share Technical Steering Comittee-STSC) felaket kurtarma hizmet seviyelerini katman sıfırdan katman altıya kadar tanımlamıştır. Katman sıfır, uzak veri merkezinden en az miktarda geri kazanımı (recoverability) ifade ederken katman altı en çok miktarda geri kazanımı tanımlamaktadır.[117]

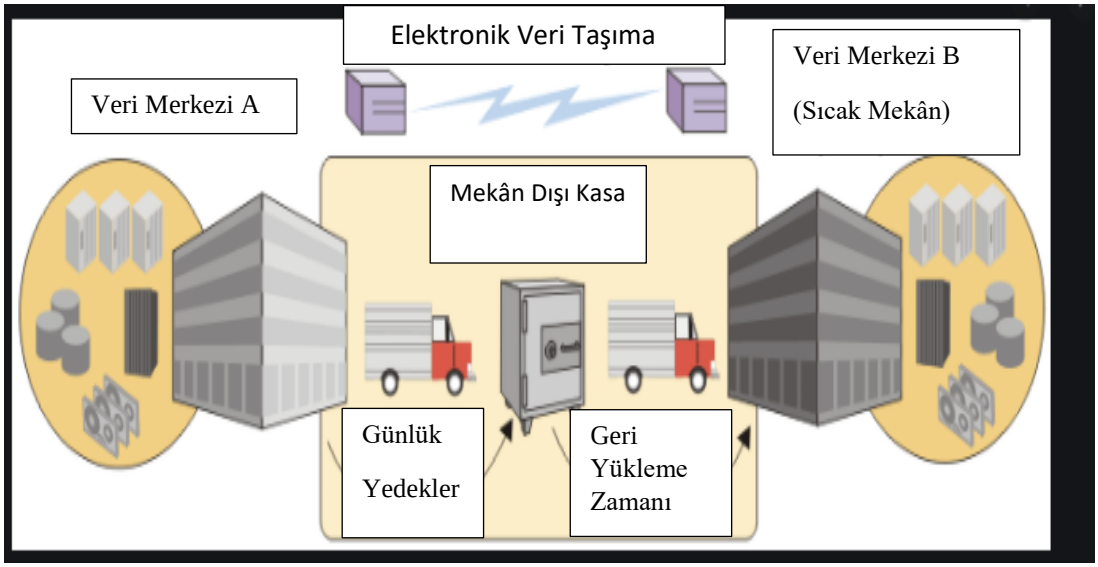
Katman 0 (Tier 0): Dış ortamda veri yoktur, Sadece yerinde geri kazanım vardır.[118]

Katman 1 (Tier 1): Soğuk mekân yaklaşımı ile yönetilen ikincil veri merkezinde fiziksel yedek tutulmaktadır, veri manyetik kasette olduğu gibi önceden herhangi bir donanım kurulu olmayan uzak lokasyona transfer edilmektedir.[119]

[116] https://www.nakivo.com/blog/overview-disaster-recovery-sites/ (08.10.2020)
[117] https://www.barracuda.com/glossary/disaster-recovery (07.11.2020)
[118] a.g.k.
[119] a.g.k.

Katman 2 (Tier 2): Sıcak mekân yaklaşımı ile yönetilen ikincil veri merkezinde fiziksel yedek tutulmaktadır, veri manyetik kasette olduğu gibi birincil veri merkezi anahtar sistemlerine destek vermek için önceden kurulmuş gerekli donanıma sahip uzak lokasyona gönderilmektedir.[120]

Katman 3 (Tier 3): Veri elektronik olarak (electronic vaulting) sıcak mekân veri merkezine taşınmaktadır.[121] Şekil 1.1'de bilgisayar verisinin elektronik olarak taşınması gösterilmektedir.



Şekil 1.1 Bilgisayar Verisinin Elektronik Olarak Taşınması[122]

Katman 4 (Tier 4): Anlık veri transferi ve aktif bir ikincil veri merkezi mevcuttur. Hayati öneme haiz veri, veri merkezleri arasında kopyalanmaktadır.[123]

Katman 5 (Tier 5): İki veri merkezi işlem bütünlüğü içerisindedir. Veri sürekli olarak iki merkez arasında gönderilmektedir.[124]

Katman 6 (Tier 6): Neredeyse sıfır veri kaybı yaşanmaktadır, veri kazanımı anlıktır ve sıklıkla disk kopya yansıları içermektedir.[125]. Tablo 1.3'te felaket kurtarma hizmet seviyeleri kıyaslaması gösterilmektedir.

[120] https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery (13.10.2020)
[121] a.g.k.
[122] https://www.ibm.com/support/knowledgecenter/SSGSG7_7.1.0/com.ibm.itsm.srv.doc/c_tier3.html (12.06.2020)
[123] a.g.k.
[124] a.g.k.
[125] a.g.k.

Tablo 1.3 Felaket Kurtarma Hizmet Seviyeleri Kıyaslaması[126]

Felaket Kurtarma Hizmet Seviyeleri Kıyaslaması	
Katman 0	Dışarıya veri gönderimi yok
Katman 1	Dışarıya veri gönderimi var
Katman 2	Dışarıya veri gönderimi var (sıcak mekân ile)
Katman 3	Elektronik veri taşıması var
Katman 4	Elektronik veri taşıması var (sıcak mekân ile)
Katman 5	İki veri merkezi var, her ikisinde de veri işleniyor
Katman 6	Sıfır veri kaybı

1.8. FELAKET KURTARMANIN ÖLÇÜLMESİNDE KULLANILAN PERFORMANS METRİKLERİ

1.8.1. Kabul Edilebilir En Fazla Çalışılamaz Durumda Bulunma Süresi (Maximum Tolerable Downtime-MTD)

İlgili sürece tekrar işlerlik kazandırılması için, işletmede yaşamsal sorunlara neden olmayacak kabul edilebilir azami süredir.[127] İlgili sürecin özelliklerine bağlı olarak bu süre saat, gün veya daha uzun olabilmekle birlikte elektronik ticaret yapan bir perakendeci için bu süre satış hacmine bağlı olarak bir kaç gün olabilecekken, bir havayolu işletmesi için saatlerle ölçülebilecektir.[128]

[126] https://www.ibm.com/support/knowledgecenter/SSGSG7_7.1.0/com.ibm.itsm.srv.doc/c_tier3.html (12.06.2020)
[127] H. Akpınar, 2009, s. 175-185.
[128] a.g.e, s. 175-185.

1.8.2. Felaket Kurtarma Süresi (Recovery Time Objective-RTO)

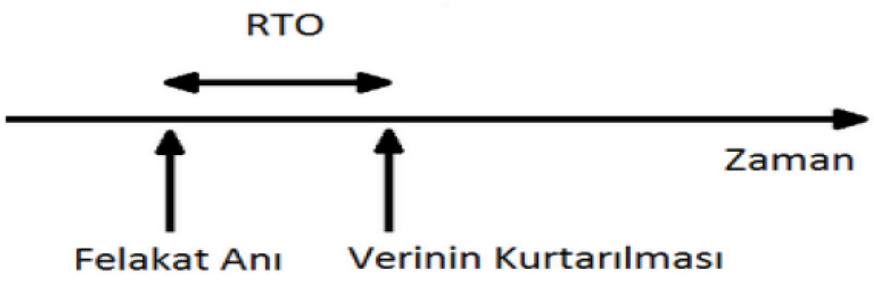
İşletmenin çalışamaz durumda bulunan bir süreci tekrar çalışır duruma getirmek için öngördüğü süredir.[129] Amaçlanan bu sürenin "Kabul Edilebilir En Fazla Çalışılamaz Durumda Bulunma Süresi"nden daha kısa olması gerektiği açıktır ancak amaçlanan süre kısaldıkça katlanılacak maliyet de muhtemelen artacaktır.[130] Örneğin; tamir edilemeyecek bir sunucu (server) arızasında amaçlanan sürenin 1 ay olması durumunda yeni bir sunucunun satın alınıp kurulması mümkün olabilecekken, bu sürenin 1 saat olarak amaçlanması durumunda muhakkak sıcak mekân (warm site) stratejisinin benimsenmiş olması gerekecektir.[131] Bu örneklerde görüldüğü üzere her iki senaryoda maliyetler önemli ölçüde farklılık gösterecektir.[132]

Felaket Kurtarma Süresi, felaketten sonra sistemin ne kadar sürede ayağa kaldırılmasının amaçlandığını belirtmektedir.[133] Açıkça belirtmek gerekirse sistemin hemen ayağa kalkması ideal olandır fakat mümkün olan tolere edilebilir sürenin belirlenmesi gerekmektedir.[134]

Felaket Kurtarma Süresi (Recovery Time Objective-RTO) veri merkezi ve IT servislerinin felaket durumunda ne kadar süre içerisinde kurtarılacağı, ne kadar sürede veri merkezi sunucu ve servislerinin tekrar çalışabilir hâle getirileceğini ifade etmektedir yani bir sistem için kabul edilebilir en fazla kesinti süresi ve tahammül sınırı olarak da ifade edilebilmektedir.[135] Şekil 1.2'de zaman düzleminde felaket kurtarma süresinin ne anlama geldiği gösterilmektedir.

---

[129] H. Akpınar, 2009, s. 175-185.
[130] a.g.e, s. 175-185.
[131] a.g.e, s. 175-185.
[132] a.g.e, s. 175-185.
[133] http://www.clarecomputer.com/pdf/CCS_e-book_BusinessContinuity_DR.pdf (12.09.2020)
[134] a.g.k.
[135] Yasin Akıllı, *Sanal Sunucu Sistemlerinde Felaket Kurtarma Yönetimi ve Felaket Kurtarma Plan Önerisi*, İstanbul Aydın Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi, İstanbul, 2016, s. 67.



Şekil 1.2 Zaman Düzleminde Felaket Kurtarma Süresi[136]

Tablo 1.4'te kurum ve kuruluşların veri merkezinde hizmet veren sunucu sistemleri ve IT servisleri için hazırlanmış olan örnek bir felaket kurtarma süresi çalışması (RTO) gösterilmektedir.

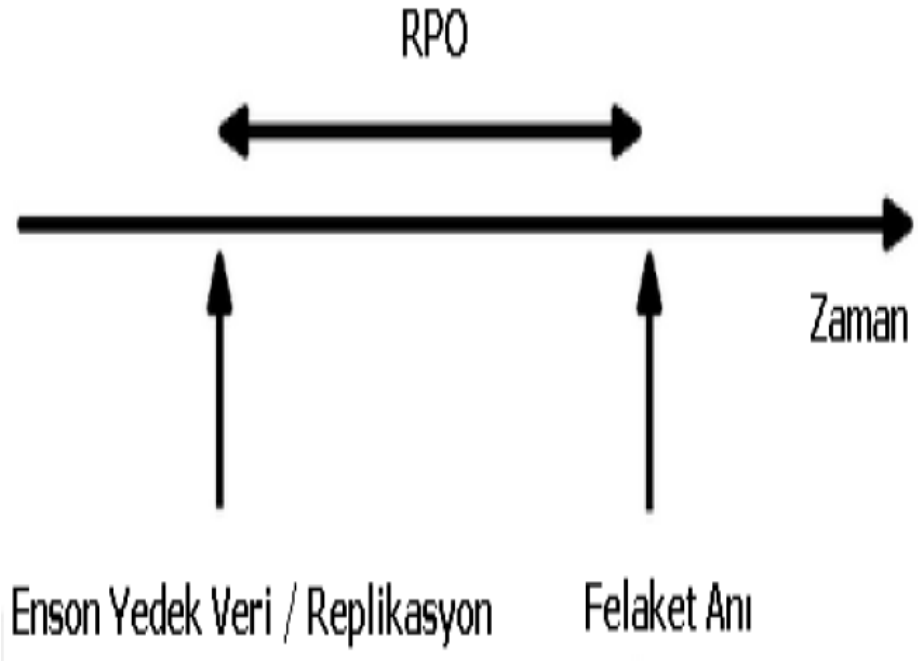
Tablo 1.4 Kurum ve Kuruluşların Veri Merkezi Sunucu Sistemleri ve IT Servisleri İçin Hazırlanmış Örnek Felaket Kurtarma Süresi Çalışması

Felaket Kurtarma Süresi (RTO)			
Sunucu Sistemleri	**Kabul Edilebilir Minimum Kurtarma Süresi (Saat)**	**Kesintiden Etkilenecekler (Kişi Sayısı)**	**Risk Seviyesi (Müdahale Önceliği)**
Tüm Kullanıcılar(DC, EXC, FSRV[137])	2 saat	2000	1.Öncelikli
Muhasebe Yazılımı	4 saat	60	2.Öncelikli
İnsan Kaynakları Yazılımı	4 saat	60	2.Öncelikli
Yazılım Geliştirme Sunucusu	6 saat	40	5.Öncelikli
Turnike Sistemi	5 saat	2000	4.Öncelikli
Yazıcı Sistemi	6 saat	2000	3.Öncelikli

[136] Y. Akıllı, 2016, s. 64.
[137] Etki Alanı Sunucusu (Domain Controller-DC), E-Posta Sunucusu (Exchange-EXC), Dosya Yönetim Sunucusu (File Server-FSRV)

1.8.3. Felaket Kurtarma Noktası (Recovery Point Objective-RPO)

Bir sürecin kesintiye uğradığı zaman noktası ile sürece tekrar işlerlik kazandırıldığı zaman noktası arasında geçen süredeki azami kayıp veri miktarıdır.[138] Felaket Kurtarma Noktası (Recovery Point Objective-RPO) veri merkezi ve IT servislerinin hizmet veremez duruma gelmesine sebep verecek beklenmedik bir felaket durumunda zarar gören sistem veya servislerin en son hangi tarihli yedek veya replikasyona geri dönüleceği olarak ifade edilmektedir.[139] Şekil 1.3'te zaman düzleminde felaket kurtarma noktasının ne ifade ettiği gösterilmektedir.



Şekil 1.3 Zaman Düzleminde Felaket Kurtarma Noktası[140]

Tablo 1.5'te kurum ve kuruluşların veri merkezlerinde hizmet veren sunucu sistemleri ve IT servisleri için hazırlanmış olan bir felaket kurtarma noktası çalışması (RTO) gösterilmektedir.

[138] H. Akpınar, 2009, s. 175-185.
[139] Y. Akıllı, 2016, s. 67.
[140] a.g.e, s. 67.

Tablo 1.5 Kurum ve Kuruluşların Veri Merkezi Sunucu Sistemleri ve IT Servisleri İçin Hazırlanmış Örnek Felaket Kurtarma Noktası Çalışması

FELAKET KURTARMA NOKTASI (RPO)			
Sunucu Sistemleri	**Kabul Edilebilir Minimum Geri Yükleme Noktası Süresi (Saat\gün)**	**Kesintiden Etkilenecekler (Kişi Sayısı)**	**Risk Seviyesi (Müdahale Önceliği)**
Tüm Kullanıcılar(DC, EXC, FSRV)	2 saat	2000	1.Öncelikli
Muhasebe Yazılımı	3 saat	60	2.Öncelikli
İnsan Kaynakları Yazılımı	3 saat	60	2.Öncelikli
Yazılım Geliştirme Sunucusu	4 saat	40	5.Öncelikli
Turnike Sistemi	8 saat	2000	4.Öncelikli
Yazıcı Sistemi	12 saat	2000	3.Öncelikli

Yedekleme sıklığını belirten bir kurtarma noktası hedefi (RPO) ve bir felaketten sonra izin verilen maksimum kesinti süresini hesaplayan bir kurtarma zamanı hedefi (RTO) belirlenmelidir.[141]

Bu metrikler, bir kuruluşun felaket kurtarma planını oluşturan bilişim teknolojileri stratejisi özelinde iş süreçleri ile ilgili işlemlerin ve prosedürlerin seçimine rehberlik etmek için limitler oluşturmaktadır. Bir kuruluşun başa çıkabileceği kesinti süresi ve kuruluşun verilerini ne sıklıkla yedeklediği felaket kurtarma stratejisi için ipuçları sağlayacaktır.[142]

[141] https://www.vmware.com/topics/glossary/content/disaster-recovery (13.08.2020)
[142] a.g.k.

İKİNCİ BÖLÜM

FELAKET KURTARMA YÖNETİMİNDE İZLENECEK TEDBİRLER VE UYGULAMALAR

Bu bölümde anlatılacak bilişim teknolojileri ve uygulamaları, olası kurumsal bilişim sistem felaketleri meydana gelmeden önce alınacak aksiyon ve tedbirler mahiyetindedir. Bu teknoloji ve uygulamaların zamanında icra edilmesi, kurumsal bilişim sistemleri olası bir felaket senaryosu ile karşı karşıya kaldığında etkilenecek zararın azaltılmasında, asgari düzeye indirilmesinde, bilimsel ve çağdaş bir felaket kurtarma yönetiminin gerçekleştirilerek iş sürekliliğinin sürdürülmesinde etkin rol oynamaktadır.

2.1. FELAKET KURTARMA YÖNETİM VE OPERASYON EKİBİ

Felaket kurtarma yönetim ve operasyon ekibi; felaket kurtarma planının oluşturulması, uygulanması ve yönetiminden sorumlu olacaktır ve bu ekipler meydana getirilirken her bir ekip üyesinin rol ve sorumluluğu tanımlanmalıdır.[143] Bir felaket durumunda, felaket kurtarma ekibi birbirleriyle, çalışanlarla, satıcılarla ve kurumun hitap ettiği üçüncü kişilerle nasıl iletişim kuracağını bilmelidir.[144] Acil durumla başa çıkmak için bir felaket kurtarma ekibi kurmak gereklidir.[145] Felaket kurtarma ekibi, daha önce acil durumlarla başa çıkma tecrübesine sahip olmak üzere görevlendirilmiş

[143] https://www.vmware.com/topics/glossary/content/disaster-recovery (13.08.2020)
[144] a.g.k.
[145] a.g.k.

uzman gurubundan oluşmalıdır.[146] Bu uzman grubunun iş operasyonları kurtarma ekibinin üyeleri ile aynı kişiler olmaması gerekmektedir.[147] Olay müdahale ekibi (Incident Response Team-IRT) anlık gerçekleşecek olaylara müdahale etmek konusunda her an tetikte olmalıdır.[148] Olaylar donanım arızaları, güç kesintileri ya da kurumdan hoşnut olmayan bir çalışanın kurum politikalarını ihlali gibi geniş bir ölçekte çeşitlilik arz etmektedir.[149] Olay müdahale ekibinin çalışması kurumun bilişim sistemlerinde ortaya çıkabilecek aksaklıkların düzeltilmesi noktasında faydalı olacaktır.[150] Tablo 2.1'de kurum ve kuruluşlar için hazırlanmış Felaket Kurtarma Yönetim Ekibi örnek çalışması gösterilmektedir.

Tablo 2.1 Felaket Kurtarma Yönetim Ekibi Örnek Çalışması

Felaket Kurtarma Yönetim Ekibi			
İsim	**Acil Durum Telefonu**	**Cep Telefonu**	**Sorumlu Olduğu Sistem ve Yazılımlar**
Levent B.	0312 xxx	0541 xxx	Felaket Kurtarma Yönetimi Ekip Lideri
Hakan A.	0312 xxx	0530 xxx	Felaket Kurtarma Ekip Lider Yardımcısı
Ahmet D.	0312 xxx	0544 xxx	Sunucu Sistemleri, Ekip Sorumlusu
Emre M.	0312 xxx	0544 xxx	Veri Depolama ve Yedekleme Sistemleri Ekip Sorumlusu
Ercan C.	0312 xxx	0541 xxx	Network Sistemi, Ekip Sorumlusu
Filiz H.	0312 xxx	0545 xxx	Yazılım Sistemleri, Ekip Sorumlusu
Murat S.	0312 xxx	0530 xxx	Kullanıcı Destek Sistemleri, Ekip Sorumlusu

[146] J. W. Rittinghouse, J. F. Ransome, 2005, s. 91.
[147] a.g.e, s. 91.
[148] V. Jorrigala, 2017, s. 18.
[149] a.g.e, s. 18.
[150] a.g.e, s. 18.

Felaket Kurtarma ekibi, sürekli gelişen tehditleri ve iş ihtiyaçlarını karşılamak için stratejisini sürekli olarak test etmeli ve güncellemelidir.[151] Kurum ve kuruluşların afet durumlarında en kötü senaryolarla yüzleşmeye sürekli hazır olmasını sağlamalıdır.[152] Örneğin; kuruluşların felaket kurtarma ekiplerinin bir siber saldırıya nasıl yanıt verileceğini planlarken, güvenlik ve koruma stratejilerini sürekli olarak test ve optimize etmeleri ve olası güvenlik ihlallerini tespit etmek için koruyucu önlemler almaları gerekmektedir.[153] Tablo 2.2'de kurum ve kuruluşlar için hazırlanmış Felaket Kurtarma Operasyon Ekibi örnek çalışması gösterilmektedir.

Tablo 2.2 Felaket Kurtarma Operasyon Ekibi

Felaket Kurtarma Operasyon Ekibi				
Kurtarılacak Sistem	**Operasyon Personeli**	**Cep Numarası**	**Kurtarma Seviyesi**	**Operasyon Durumu**
Aktif Dizin	Adem B.	0544 xxx	1.Öncelikli	Tamamlandı
Dosya Sunucusu	Ece N.	0530 xxx	1.Öncelikli	Devam Ediyor
Yazıcı Sistemi	Ali E.	0542 xxx	3.Öncelikli	Devam Ediyor
Exchange Sunucusu	Hasan U.	0545 xxx	1.Öncelikli	Başarısız
İnsan Kaynakları Yazılımı	Ahmet T.	0545 xxx	2.Öncelikli	Tamamlandı

[151] https://www.vmware.com/topics/glossary/content/disaster-recovery (13.08.2020)
[152] a.g.k.
[153] a.g.k.

2.2. RİSK DEĞERLENDİRMESİ

Kurum ve kuruluşlar kendilerini riske sokacak olası tehlikeleri değerlendirmelidir.[154] Olayın türüne bağlı olarak iş sürekliliği için hangi önlemlerin alınacağı ve kaynakların gerekli olacağı konusunda strateji belirlenmelidir. Örneğin; siber saldırı karşısında, felaket kurtarma ekibi saldırıya karşılık vermek için hangi veri koruma önlemlerini almalıdır.[155] İş sürekliliğinin önemli bir parçası, işletmeler için afetlerden ya da acil durumlardan kaynaklanabilecek potansiyel risklerin değerlendirilmesidir. Olası tüm olayların kurum ve kuruluşların normal iş hizmetlerini sunmaya devam etme yeteneği üzerindeki etkisini dikkate almak gerekmektedir.[156] İş sürekliliği planlamasının (BCP-Business Contiunity Planning) risk değerlendirme bölümü, iş operasyonlarını aksatan ciddi durumların olasılığını ve bu tür olayların potansiyel etkisini incelemelidir.[157] Risk değerlendirmesi, özelde iş sürekliğinin bir parçası sayılmasına rağmen iş etki analizi ile yakından ilişki içinde olup iş etki analizinin belirlenmesinde göz önüne alınmalıdır.

2.3. İŞ ETKİ ANALİZİ (BUSINESS IMPACT ANALYSIS-BIA)

İş etki analizi, bir iş kesintisi sırasında ve sonrasında operasyonel esnekliği ve operasyonların sürekliliğini sağlamak için iş faaliyetlerinin ve ilgili kaynak gereksinimlerinin kritikliğini belirleme sürecidir.[158] İş etki analizi, iş unsurları ile ilgili risklerin belirlenmesinde önemli rol oynamaktadır ve aynı zamanda bir kurtarma noktası hedefi ve kurtarma noktası süresi biçiminde ölçülebilir bir şekilde iş gereksinimlerinin tanımlanmasına yardımcı olmaktadır.[159]

---

[154] https://www.vmware.com/topics/glossary/content/disaster-recovery (13.08.2020)
[155] a.g.k.
[156] J. W. Rittinghouse, J. F. Ransome, 2005, s. 23.
[157] a.g.e, s. 23.
[158] https://www.gartner.com/en/information-technology/glossary/bia-business-impact-analysis (23.10.2020)
[159] Premathas Somesekaram, *A Component-Based Business Contiunity and Disaster Recovery Framework*, Uppsala Universitet, Department Of Information Technology, İsveç, 2017, s. 41.

Bir işletmenin felaketler karşısındaki mukavemetini artırabilmek için, bu işletmenin yaşamsal önemdeki süreç ve sistemlerinin belirlenmesi, bu süreç ve sistemler için felaket planlarının hazırlanması gerekmektedir.[160] İş Etki Analizi (Business Impact Analysis-BIA) olarak isimlendirilen bu süreçte,

- Kritik süreçlerin ve bu süreçler arasındaki ilişkilerin belirlenerek bir envanter çıkartılması,
- Her bir kritik süreç için potansiyel tehditlerin analiz edildiği bir tehdit modelinin (threat model) kurulması,
- Bu süreçlere ilişkin risk analizlerinin yapılması,
- Bu süreçlere ilişkin belirlenen riskin azaltılması (mitigation) için alınabilecek tedbirlerin belirlenmesi gerekmektedir.[161]

İş etki analizi (Business Impact Analysis-BIA), bir şirketin veya kurumun kritik iş süreçlerini ve bilgi teknolojileri-BT sistemlerini tanımlama, bir felaket durumunda neyin başarısız olabileceğini belirleme ve bu tür başarısızlıkların şirketin işi üzerindeki potansiyel etkisini değerlendirme aşamalarından oluşmaktadır.[162] İyi bir iş etki analizinin ilk aşaması, bir kurumun tüm ağının ve bilişim teknolojileri-BT sistemi yapılandırmalarının belgelendirilmesidir.[163]

Kurum ve kuruluşlar; tüm sunucularının, uygulamalarının, veri iletişim ağlarının, yönlendiricilerinin, platformlarının, anahtarlarının ve bağımsız masaüstü istasyonlarının doğru bir kaydını veya taslağını üretmek için derinlemesine araştırma yapmalı ve ayrıntılı bir envanter oluşturmalıdır.[164] Tablo 2.3'te kurum ve kuruluşlar için hazırlanmış, örnek iş-etki analiz durumu gösterilmektedir.

[160] H. Akpınar, 2009, s. 175-185.
[161] a.g.e, s. 175-185.
[162] https://www.mayerbrown.com/public_docs/events/bank_12Jun03_DisasterRecovery.pdf (04.09.2020)
[163] a.g.e, s. 175-185.
[164] a.g.k.

Tablo 2.3 İş-Etki Analiz Tablosu

İŞ ETKİ ANALİZİ		
Sistem	**Etki Alanı**	**Kurtarma Seviyesi**
Aktif Dizin[165]	Tüm kullanıcı hesaplarının oluşturulduğu, DNS[166] ve DHCP[167] hizmetlerinin sunulduğu ana sunucudur	1.Öncelikli
File Server	Tüm kullanıcılara dosya paylaşım hizmeti veren sunucudur	1.Öncelikli
Ebys	Tüm kullanıcıların resmî belge işlemlerinin yürütüldüğü sunucudur	1.Öncelikli
Exchange	Tüm kullanıcıların e-posta işlemlerinin yürütüldüğü sunucudur.	1.Öncelikli
Turnike Sistemi	Tüm kullanıcıların giriş ve çıkış işlemlerinin yürütüldüğü sunucudur.	4.Öncelikli
İnsan Kaynakları Yazılımı	Tüm kullanıcıların personel, maaş ve özlük işlemlerinin yürütüldüğü sunucudur**.**	2.Öncelikli
Yazıcı	Tüm kullanıcıların güvenli baskı işlemlerinin yürütüldüğü sunucudur.	3.Öncelikli
Yemekhane	Tüm kullanıcıların yemekhane giriş ve çıkışlarının yürütüldüğü sunucudur.	5.Öncelikli
Kütüphane	Tüm kullanıcıların kütüphane işlemlerinin yürütüldüğü sunucudur.	6.Öncelikli

[165] Aktif Dizin (Active Directory-AD)
[166] Dinamik Uç Birim Kontrol Protokolü (Dynamic Host Control Protocol-DHCP)
[167] Alan Adı Sistemi (Domain Name System-DNS)

2.4. SİSTEM KURTARMA ÖNCELİK LİSTESİ

Veri merkezi ve IT servisleri için felaket kurtarma yönetiminde en önemli noktalardan biri de tüm sunucu sistemleri ve kritik iş servislerinin zarar görebileceği beklenmedik bir felaket durumunda kurtarma operasyonu sırasında hangi sistemlerin hangi öncelik sırası ile kurtarılmaya başlanması gerektiğinin önceden bilinmesi gerektiğidir.[168]

Kriz anında böyle bir problemin oluşmaması ve kurtarma operasyonlarının daha etkin ve hızlı sonuçlandırılması için "Sistem Kurtarma Öncelik Listesi'nin" belirlenmesi gerekmektedir.[169]

İş açısından kritik varlık tanımlama olarak da adlandırılabilecek sistem kurtarma öncelik listesi; iş sürekliliği için hangi sistemlerin, uygulamaların, verilerin ve diğer kaynakların en kritik olduğunu belirtmektedir ve verilerin kurtarılması için gerekli adımları içermektedir.[170]

Sistem kurtarma öncelik listesi oluşturulurken, veri merkezi ve IT servisleri için felaket kurtarma planı oluşturma süreçlerinin en önemli kriterlerinden biri olan felaket iş etki analiz sonuçlarına göre belirlenmiş felaket kurtarma süresi (RTO) ve felaket kurtarma noktası (RPO) değerlerinin göz önünde tutulması gerekmektedir.[171]

Tablo 2.4'te kurum kuruluşlar için hazırlanmış örnek sistem kurtarma öncelik listesi gösterilmektedir.

[168] Y. Akıllı, 2016, s. 71.
[169] a.g.e, s. 71.
[170] https://www.vmware.com/topics/glossary/content/disaster-recovery (13.08.2020)
[171] a.g.e, s. 71.

Tablo 2.4 Kurum Kuruluşların Veri Merkezi Sunucu Sistemleri ve IT Servisleri İçin Hazırlanmış Sistem Kurtarma Öncelik Listesi Çalışması

Sistem Kurtarma Öncelik Listesi					
Sunucu Sistemi ve IT Servisi	**Sistemin Görevi ve Etki Alanı**	**Kurtarma Seviyesi**	**Felaket Kurtarma Noktası**	**Felaket Kurtarma Süresi**	**Sistem Operasyon Sorumlusu**
Aktif Dizin Sunucusu	Tüm bilgisayar kullanıcılarının hesaplarının oluşturulduğu ve yönetildiği sunucudur.	1.Öncelikli	Felaket anından 2 saat öncesi	2 saat	Adem B.
İnsan Kaynakları Yazılımı	Tüm kullanıcıların personel, maaş ve özlük işlemlerinin yürütüldüğü sunucudur**.**	2.Öncelikli	Felaket anından 3 saat öncesi	4 saat	Ahmet T.
Yazıcı	Tüm kullanıcıların güvenli baskı işlemlerinin yürütüldüğü sunucudur.	3.Öncelikli	Felaket anından 12 saat öncesi	6 saat	Ali E.

2.5. SANALLAŞTIRMA

Kurum ve kuruluşların iş operasyonlarını yürütürken, kurumsal verilere erişimi ve kurumsal veri güvenliğini sağlaması hayati role sahiptir.[172] İnsan ya da doğa kaynaklı meydana gelen felaketler karşısında izlenenecek felaket kurtarma yönetimi, kurum ve kuruluşların IT ve iş operasyonları açısından son derece önemlidir.[173] Sanallaştırma; sahip olduğu kaynak tüketimi, yüksek erişilebilirlik, güç yönetiminin kolaylığı, geri kazanım yönetimi ve dinamik altyapı gibi özellikler sayesinde felaket kurtarma yönetimi bakımından bilişim sistemlerinde uygulanması elzem teknolojilerden biridir.[174]

Sanallaştırma olmadan yönetilen bilgi sistemlerinde, felaket meydana geldiğinde yeni bir sunucu temin edilmeli ya da iş için kullanılan işletim sistemleri ve uygulamalar elle (manuel) tekrar yüklenmelidir.[175] Sanallaştırma olmaksızın yapılacak bütün sistem geri yükleme işlemleri manuel olarak gerçekleştirilebilecektir. Sanallaştırma, felaket kurtarma yönetimini basitleştirmektedir çünkü fiziksel sunucu çevresinin yeniden inşa edilmesine gerek kalmamaktadır.[176] Tam esneklik sağlanmakta ve kurum içi donanıma (in-house hardware) bağımlılık elimine edilmektedir. Bunun yerine sistemi yönetmek ve olası felaketler durumunda tekrar ayağa kaldırmak için sadece internet erişimi ve uzak masaüstü uygulaması gerekmektedir.[177]

Bilgi sistemlerini donanım bağımlılığından kurtarması, anılan sistemlerin fiziki olarak zarar görmesinin önüne geçecek ve bütün bir sistemin yönetimi tek elden yapıldığı için anılan sistemlerin ayağa kaldırılması hızlı bir şekilde

[172] https://scialert.net/fulltext/?doi=jai.2013.60.67 (06.08.2020)
[173] a.g.k.
[174] a.g.k.
[175] https://www.gowhiteowl.com/blog/virtualization-benefits-disaster-recovery/ (13.07.2020)
[176] a.g.k.
[177] a.g.k.

gerçekleştirilecektir. Sanallaştırmanın, felaket kurtarma süresine ve dolayısı ile felaket kurtarma yönetimine olumlu anlamda ciddi bir katkısı bulunmaktadır.

2.5.1. Sunucu Sanallaştırma

2.5.1.1. Sanal Makine Nedir?

Sanal makine, uygulamaları dağıtmak ve programları çalıştırmak için fiziksel bilgisayar yerine yazılım kullanan bir hesaplama kaynağıdır.[178] Bir ya da daha fazla misafir makine (guest) fiziksel bir ev sahibi (host) makine üzerinde çalışmaktadır. Her bir sanal makine, her biri aynı fiziksel host üzerinde çalışsa dahi, kendi işletim sistemini kullanmaktadır ve her bir makinenin işlevleri diğer sanal makinelerden ayrıdır. Bu şu anlama gelmektedir: Macintosh-macOS işletim sistemine sahip bir sanal makine, kişisel bir bilgisayar (Personal Computer-PC) üzerinde çalışabilmektedir.[179] Sanal makineler, gerçek bir işletim sistemi gibi çalışmaktadır ve son kullanıcıya (end user) yüksek seviyeli fonksiyon sunmaktadır.[180]

Sanal makine teknolojisi, kurum içi (on-premises) ortamlarda ve bulut ortamlarında birçok durumda kullanılmaktadır. Son zamanlarda, genel bulut hizmeti sağlayıcıları maliyet verimliliği ve esnek çalışma koşullarından dolayı sanal makineleri kullanmaktadır. [181]

2.5.1.2. Sanal Makinelerin Kullanım Amacı, Avantaj ve Dezavantajları

Sanal makineler, bilgisayardaki bir uygulama penceresinde tamamen farklı bir bilgisayar gibi davranan işletim sistemini çalıştırmak için kurumlara imkân

[178] https://www.vmware.com/topics/glossary/content/virtual-machine (12.12.2020)
[179] a.g.k.
[180] Arunkumar Jayaraman ve Parankumar Rayapudi, *Comparative Study of Virtual Machine Software Packages with Real Operating System*, Blekinge Tekniska Högskolva, İsveç 2012, s. 5.
[181] a.g.k.

sunmaktadır.[182] Sanal makineler, farklı seviyelerdeki işlem gücünü karşılamak, farklı bir işletim sisteminin gereksinimlerini karşılayan yazılımları çalıştırmak ya da güvenli, korumalı (sandboxed) bir ortamdaki uygulamaları test etmek için kulanılmaktadır.[183]

Sanal makineler geçmişten günümüze kadar IT ekiplerine işlem kaynaklarını ve verimliliğini geliştirme imkânı sunan sunucu sanallaştırması (server virtualization) şeklinde kullanılmıştır.[184] Ek olarak sanal makineler, fiziksel ortamlarda icra edilmesi çok riskli görülen virüsten etkilenmiş verilere (virus-infected data) erişmek ve işletim sistemlerini test etmek gibi spesifik görevleri gerçekleştirmek için de kullanılmaktadır.[185]

Sanallaştırma teknikleri, gerçek makine hizmetleri gibi hizmetler sunmaktadır. Bunun yanı sıra tek fiziksel makine üzerinde farklı tipte işletim sistemleri çalışabilmektedir.[186]

Sanal makineler ev sahibi (host) cihazları üzerinde koşmaktadır ve ev sahibi cihazın kaynaklarını paylaşmaktadır. Sanal makineler aynı ev sahibi cihaz üzerinde birbirlerinin işletim sistemlerine zarar vermeden çalışabilmektedir.[187]

Sanal makineler; sistemin geri kalanından izole tutulduğu için sahip oldukları işletim sistemi, ev sahibi bilgisayara müdahale edememektedir. Birçok kurum sanal makinelerle ilgili avantaj ve dezavantajları dengelemek için fiziksel ve sanal makinelerden oluşan bir kombinasyon kullanmaktadır.[188]

[182] https://www.vmware.com/topics/glossary/content/virtual-machine (12.12.2020)
[183] a.g.k.
[184] a.g.k.
[185] a.g.k.
[186] a.g.k.
[187] A. Jayaraman, P. Rayapudi, 2012, s. 7.
[188] a.g.k.

Tablo 2.5'te sanal makinelerin avantajları ve dezavantajları gösterilmektedir.

Tablo 2.5 Sanal Makinelerin Avantaj ve Dezavantajları[189]

Sanal Makinelerin Avantajları ve Dezavantajları	
Avantajlar	**Dezavantajlar**
Farklı İşletim Sistemlerinde Çalışabilme	Performans Sorunları
Fiziksel Alan Verimliliği	İstikrarsız Çalışabilme
Yönetim\Maliyet Açısından Tasarruf	Fiziksel Bilgisayara Göre Daha Az Verimlilik
Felaket Kurtarma Açısından Bütünlük	Fiziksel Bilgisayarlara Göre Daha Yavaş Çalışma

Sunucu sanallaştırma, fiziksel bir sunucuyu bir yazılım uygulaması aracılığı ile eşsiz ve yalıtılmış sanal sunuculara ayırma işlemine denmektedir.[190] Her bir sanal sunucu kendi işletim sisteminde bağımsız olarak çalışabilmektedir.[191] Sunucu sanallaştırma, web barındırma hizmetleri sağlamak ve IT altyapısındaki var olan kaynakların verimli kullanımını temin etmek için maliyet açısından etkin (cost-effective) bir yöntemdir.[192]

Sunucu sanallaştırma olmaksızın sunucular, işlem güçlerinin yalnızca küçük bir bölümünü kullanmaktadır ve bu durum sunucuların kaynaklarının boşta kalmasına sebebiyet vermektedir çünkü iş yükü, iletişim ağı sunucularının yalnızca bir bölümüne dağıtılmaktadır.[193] Veri merkezleri aşırı kullanılan sunucularla aşırı kalabalık hâle gelmektedir ve bu durum da kaynak ve güç israfına neden olmaktadır.[194]

[189] https://www.vmware.com/topics/glossary/content/virtual-machine (12.12.2020)
[190] https://www.vmware.com/topics/glossary/content/servervirtualization?SRC=WWW_US_GP_virtual-machine_SiteLink (03.12.2020)
[191] a.g.k.
[192] a.g.k.
[193] a.g.k.
[194] a.g.k.

Her bir fiziksel sunucunun birden fazla sanal sunucuya bölünmesiyle gerçekleştirilen sunucu sanallaştırma, her bir sanal sunucuya bağımsız fiziksel bir cihaz olarak hareket etme imkânı tanımaktadır.[195] Her sanal sunucu kendi uygulamaları ve işletim sisteminde çalışabilmektedir.[196] Bu işlem her bir sanal sunucuya bağımsız bir fiziksel sunucu olma niteliği kazandırması yönüyle kaynakların etkin kullanımını ve her bir fiziksel makinenin kapasitesini de artırmaktadır.[197]

2.5.1.3. Sunucu Sanallaştırma Türleri

2.5.1.3.1. Tam Sanallaştırma

Tam sanallaştırma, fiziksel bir sunucunun disk alanına ve işlemcisine (Central Processing Unit-CPU) direk erişim sağlayan bir yazılım tipi olan hipervizör (hypervisor) kullanmaktadır.[198] Hipervizör, fiziksel sunucunun kaynaklarını gözlemlemektedir ve her bir sunucunun bilgisini diğer sunuculardan bağımsız olarak tutmaktadır ve bunun yanında uygulamaların çalışması için kaynakları fiziksel sunucudan sanal sunuculara aktarmaktadır.[199] Tam sanallaştırmanın en büyük açmazı, hipervizörün çalışırken kendisinin kaynak ihtiyacı duymasıdır. Bu durum uygulamaları yavaşlatmaktadır ve sunucu performansını etkilemektedir.[200]

2.5.1.3.2. Sanallaştırma Benzeri (Paravirtualization)

Tam sanallaştırmanın aksine, sanallaştırma benzeri bütün iletişim ağının uyumlu bir birim olarak birlikte çalışmasını gerektirmektedir.[201] Sanallaştırma

[195] https://www.vmware.com/topics/glossary/content/servervirtualization?SRC=WWW_US_GP_virtual-machine_SiteLink (03.12.2020)
[196] a.g.k.
[197] a.g.k.
[198] a.g.k.
[199] a.g.k.
[200] a.g.k.
[201] a.g.k.

benzerinde, sanal sunuculardaki her bir işletim sistemi diğerinden bağımsız olduğu için hipervizör işletim sistemini yönetmek adına çok fazla işlemci gücü sarf etmemektedir.[202] Misafir işletim sistemi, sanal makinenin üzerinde direkt çalışmamaktadır. Tam sanallaştırma kadar fonksiyonel değildir fakat misafir işletim sisteminin fonksiyonelliğini artırmaktadır.[203]

2.5.1.3.3. İşletim Seviyesi Düzeyinde Sanallaştırma

Tam ve hayali sanallaştırmanın aksine, işletim sistemi düzeyinde sanallaştırma bir hipervizör kullanmamaktadır.[204] Bunun yerine, fiziksel sunucu işletim sisteminin bir parçası olan sanallaştırma kapasitesi hipervizörün tüm görevlerini üstlenmektedir ve fakat bu sanallaştırma yönteminde tüm sunucular aynı işletim sistemi üzerinde koşmaktadır. [205]

2.5.2. Veri Depolama Sistemi Sanallaştırma

Veri depolama sistemi sanallaştırma, asıl yapılandırılmalarına veya fiziksel konumlandırılmalarına bakılmaksızın veri depolama sistemi cihazlarına tek mantıksal görüş sağlamaktadır. Temel sistemler arasındaki farklılıkları minimize etmektedir ve veri depolama sistemi yönetimini basitleştirmektedir. Geleneksel senaryoda, uygulama tipi ile veri depolama sistemi (storage) ihtiyacını eşleştirmek her zaman mümkün bulunmamaktadır.[206] Örneğin; dosya sunucuları (file servers), e-posta sunucularından daha fazla depolama alanı tüketmektedir. Aynı zamanda, depolama kullanımındaki herhangi bir büyük artış tüm donanım sisteminde bir güncelleme yapılmasını gerektirmektedir.[207] Depolama sistemi sanalaştırma, depolama birimlerinin koleksiyonudur ve tek bir depolama birimini temsil etmektedir.

[202] https://www.vmware.com/topics/glossary/content/servervirtualization?SRC=WWW_US_GP_virtual-machine_SiteLink (03.12.2020)
[203] A. Jayaraman, P. Rayapudi, 2012, s. 9.
[204] a.g.k.
[205] a.g.k.
[206] J. W. Rittinghouse, J. F. Ransome, 2005, s. 145.
[207] a.g.e, s. 145.

Sanallaştırılmış depolama birimi, merkezi görüş noktasından tek depolama cihazı olarak görülmektedir. Yönetimi kolaydır ve kurumsal iletişim ağı yapılandırmasını değiştirmeksizin depolama alanı miktarı artırılabilmektedir.[208]

Veri depolama sistemi sanallaştırmada, depolama sisteminin mantıksal ve fiziksel görünümü ayrıldığı için sunucu kullanılabilirliğini etkilemeden kolayca depolama sistemi eklemek, değiştirmek ve sürüm yükseltmesi yapmak mümkün olabilmektedir.[209] Bu durum verinin gerçek paylaşımını olanaklı kılmaktadır çünkü böylelikle heterojen sunucuların veri depolama sistemine bağlanmasına izin verilmektedir. Bu çözüm aynı zamanda sunucusuz veri yedekleme ve geri yüklemenin faydalarını sunmaktadır.[210] Sanallaştırma, iletişim ağı ilişkili veri depolama sistemi (Network-Attached Storage-NAS) ve depolama alan ağının (Storage Area Network-SAN) tamamlayıcısıdır.[211]

2.5.3. Veri İletişim Ağı (Network) Sanallaştırma

Veri iletişim ağı sanallaştırması (Network Virtualization-NV), geleneksel olarak donanımdan yazılıma teslim edilen iletişim ağı kaynaklarının soyutlanması anlamına gelmektedir.[212] İletişim ağı sanallaştırması, çok sayıdaki fiziksel iletişim ağını yazılım tabanlı tek bir sanal iletişim ağına indirgeyebileceği gibi bir fiziksel iletişim ağını birbirinden ayrı, bağımsız sanal iletişim ağlarına da bölebilmektedir.[213]

İletişim ağı sanallaştırma yazılımı, veri iletişim ağı yöneticilerine (network administrators) veri iletişim ağlarını yeniden yapılandırmaksızın farklı etki alanları

[208] A. Jayaraman, P. Rayapudi, 2012, s. 11.
[209] J. W. Rittinghouse, J. F. Ransome, 2005, s. 145.
[210] a.g.e, s. 145.
[211] a.g.e, s. 145.
[212] https://www.vmware.com/topics/glossary/content/networkvirtualization?SRC=WWW_US_GP_virtual-machine_SiteLink (03.12.2020)
[213] a.g.k.

arasında sanal makineleri göç ettirme (migration) seçeneği sunmaktadır.[214] Yazılım, aynı fiziksel veri iletişim ağ yapısı üzerinde ayrı sanal ağ katmanları çalıştırabilen bir veri iletişim ağı oluşturmaktadır.[215]

2.5.3.1. Veri İletişim Ağı Kullanım Amacı

Veri iletişim ağı sanallaştırma, hizmetlerin yazılım tanımlı veri merkezinden (Software Defined Data Center-SDDC) buluta ve uca kadar teslim edilme şekli için kuralları yeniden yazmaktadır.[216] Bu yaklaşım; veri iletişim yaklaşımlarını durağan, esnek olmayan ve verimsiz bir durumdan dinamik, esnek ve iyileştirilmiş hâle getirmektedir.[217] Modern ağlar, uygulamaları daha hızlı pazarlamak için ihtiyaç duyulan hızı ve çevikliği sunarken bulutta barındırılan dağıtık uygulama taleplerine ve artan siber suç tehditlerine aksiyon alarak ayak uydurabilmelidir.[218] Veri iletişim ağı sanallaştırma ile yeni bir uygulamanın geliştirilebilmesi için harcanan gün ya da haftalardan tasarruf edilmektedir ve böylece kısa sürede değer elde etmek için uygulamalar dakikalar içinde dağıtılmaktadır ve güncellenmektedir.[219]

2.5.3.2. Veri İletişim Ağı Sanallaştırma Teknolojisi Nasıl Çalışmaktadır?

Tüm veri iletişim ağı tek bir modda birleştirilmektedir ve bant genişliği, kanallar ve diğer kaynaklar iş yüküne göre tahsis edilmektedir.[220]Veri iletişim ağı sanallaştırma, ağ hizmetlerini temel donanımdan ayırmaktadır ve tüm iletişim ağının sanal olarak sağlanmasını mümkün kılmaktadır.[221] Ağları tamamen yazılım içinde programlı olarak oluşturmayı, sağlamayı ve yönetmeyi imkân dahiline getirmektedir. Fiziksel ağ kaynakları; anahtar (switch), yönlendirici (router), güvenlik duvarı

[214]https://www.vmware.com/topics/glossary/content/networkvirtualization?SRC=WWW_US_GP_virtual-machine_SiteLink (03.12.2020)
[215] a.g.k.
[216] a.g.k.
[217] a.g.k.
[218] a.g.k.
[219] a.g.k.
[220] A. Jayaraman, P. Rayapudi, 2012, s. 11.
[221] a.g.e, s. 11.

(firewall), yük dengeleyici (load balancer) ve daha fazlası havuzlanmaktadır ve yazılım ile gönderilmektedir.[222] Temel fiziksel ağdan yalnızca internet protokolü paketlerinin gönderiminin yapılması gerekmektedir.[223]

Yazılımdaki ağ ve güvenlik servisleri; sanal bir katmana dağıtılmaktadır ve her bağlı uygulama için tanımlanan ağ ve güvenlik politikalarına göre sanal makineler (virtual machine-VM) ve kapsayıcılar (conteyner) gibi bireysel iş yüklerine eklenmektedir.[224] Bir iş yükü başka bir ev sahibi fiziksel cihaza taşındığında ağ hizmetleri ve güvenlik politikaları da oraya taşınmaktadır. Bir uygulamayı ölçeklendirmek için yeni iş yükleri oluşturulduğunda, gerekli politikalar dinamik olarak bu yeni iş yüklerine uygulanmaktadır ki bu da ağ politikası tutarlılığını ve ağ çevikliğini sağlamaktadır.[225] Tablo 2.6'da veri iletişim ağı sanallaştırmanın faydaları gösterilmektedir.

2.5.3.3. Veri İletişim Ağı Sanallaştırmanın Faydaları

Tablo 2.6 Veri İletişim Ağı Sanallaştırmanın Faydaları[226]

Veri İletişim Ağı Sanallaştırmanın Faydaları
İş yüklerini fiziksel topolojiden bağımsız olarak saklama ve transfer etme
Veri merkezindeki donanım ihtiyacını ortadan kaldırarak ağ güvenliğini sağlama
Ağın ayağa kaldırılma süresini haftalardan dakikalara düşürme
Ağın hızlı bir şekilde ayağa kaldırılması ile hedeflenen felaket kurtarma süresinin (RTO) yakalanması ve dolayısı ile etkin bir felaket kurtarma yönetimine zemin hazırlama

[222] A. Jayaraman, P. Rayapudi, 2012, s. 11.
[223] https://www.vmware.com/topics/glossary/content/networkvirtualization?SRC=WWW_US_GP_virtual-machine_SiteLink (03.12.2020)
[224] a.g.k.
[225] a.g.k.
[226] a.g.k.

2.6. SUNUCU KÜMELEME (SERVER CLUSTERING)

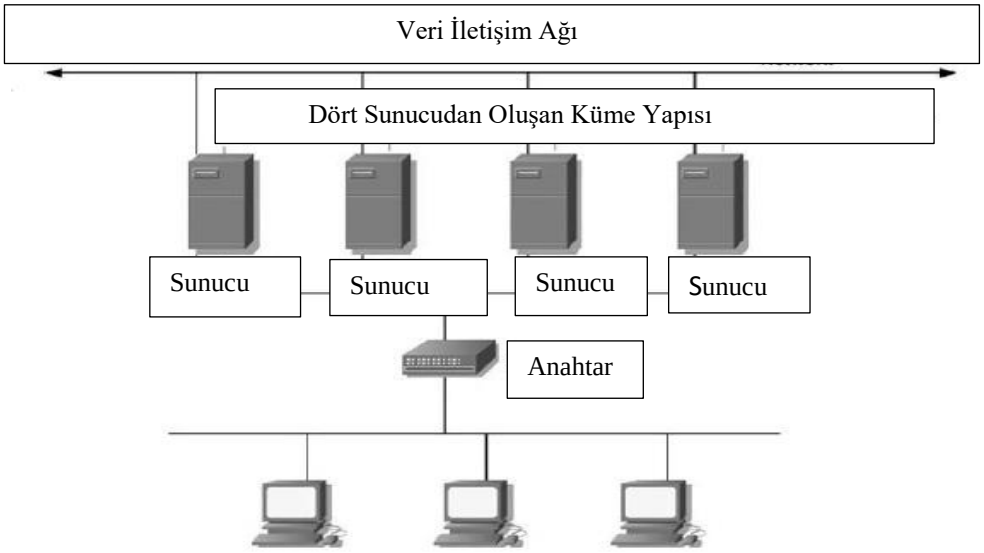
Sunucu kümeleme, yüksek kullanılabilirlik (high availability) için tercih edilen bir çözüm olarak değerlendirilmektedir.[227] Sistemin amacı, birincil sunucu (primary server) felaket durumunda arızalandığında veri ve uygulamalara erişmek için ikincil bir sunucu (secondary server) kullanmaktır.[228] Eğer kullanılan yerel bir kümeleme ise iki sunucu durumlarını belirtmek için periyodik olarak kalp atışı (heartbeat) değişimi yapmaktadır.[229]

Donanım ögesinin sürekliliği konusunda, bir felaket karşısında mevcut bilgisayar ağının düşük kapasite ile de olsa varlığını sürdürebilmesi için en uygun yöntemlerden biri sunucu küme (server cluster) yapısının uygulanması olacaktır.[230] Sunucu küme yapısı, kullanıcı açısından tek ve birleşik bir hesaplama kaynağı olarak görülen ve faydalanılan, paralel veya dağıtılmış olarak birbirine bağlı bilgisayarlardan meydana gelen sistemdir.[231] Sunucuların farklı coğrafi mekânlarda konumlandırılmasının belirtildiği coğrafi olarak dağıtılmış küme yapısı, işletmenin veri merkezinin felaketten etkilenmesi durumunda dahi fonksiyonlarını sürdürmeye devam edebilecektir.[232]

Kümeleme simetrik ya da asimetrik olabilmektedir.[233] Asimetrik kümelemede, ikincil sunucu normal koşullarda aktif durumda bulunmamaktadır. Hem birincil hem de ikincil sunucu paylaşılmış ya da yansıtılmış depolamayı kullanarak veri ve uygulamalara erişmektedir. Sunucu kümeleme, birkaç yinelenen sistemi birbirine bağlayan ve böylece iş birliği içinde hareket etmeyi mümkün kılan bir teknolojidir.[234] Bir sunucu kümesi çöktüğünde, diğer sistemler çöken sistemin yerini almaktadır. Bir

[227] J. W. Rittinghouse, J. F. Ransome, 2005, s. 143.
[228] a.g.e, s. 143.
[229] a.g.e, s. 143.
[230] H. Akpınar, 2009, s. 175-185.
[231] a.g.e, s. 175-185.
[232] a.g.e, s. 175-185.
[233] a.g.e, s. 143.
[234] a.g.e, s. 143.

kullanıcının perspektifinden bir küme sistemi tek kaynak erişim adına sahip tek bir varlıktır.[235] Şekil 2.1'de sunucu kümeleme mimarisi gösterilmektedir.



Şekil 2.1 Sunucu Kümeleme Mimarisi [236]

Sunucu kümeleme, bugünün iş ortamında yedi gün yirmi dört saat desteğe ihtiyaç duyan hizmetlerin ölçeklenebilirliği ve yüksek kullanılabilirliğini sağlamak için gereklidir.[237] Bu gereksinim; veri iletişim ağı işletim sistemlerini, uygulama hizmetlerini ve yerel alan ağı (Local Area Network-LAN) ile geniş alan ağı (Wide Area Network-WAN) esnekliğini de kapsamaktadır.[238]

Kümeleme, internet tabanlı sistemlerin güvenilirliğini iyileştirmektedir çünkü bu teknoloji ile birlikte tek bir sunucu sisteminde meydana gelmesi muhtemel birçok tek hata noktası ortadan kaldırılmaktadır.[239] Örneğin; kümeleme ile kurumsal bir internet sitesine destek veren iki ya da daha fazla sunucuya sahip olunmaktadır. Sunuculardan bir tanesi devre dışı kaldığında, sistemin verim oranı (throughput) bir dereceye kadar etkilenebilmektedir fakat internet sitesine ikincil veya kümelemeye

[235] J. W. Rittinghouse, J. F. Ransome, 2005, s. 143.
[236] a.g.e, s. 143.
[237] a.g.e, s. 144.
[238] a.g.e, s. 144.
[239] a.g.e, s. 143.

dahil bir başka sunucu aracılığı ile erişim sağlanabilmektedir.[240] Bu örnekte, ikincil sunucu aktif duruma geçer, ikincil sunucunun depolama sistemine erişimi vardır ve veri iletişim ağı bağlantısı da aktif durumdadır. Bu sunucu, birincil sunucunun yapageldiği işlevi yerine getirebilmektedir.[241]

Simetrik kümelemede, iki sunucu her zaman aktif konumda bulunmaktadır ve her biri kendi uygulamalarını çalıştırmaktadır.[242] Bir sunucunun devre dışı kalması durumunda diğer sunucu devre dışı kalanın icra ettiği fonksiyonu da devralmaktadır. Her iki sunucu da aynı uygulamaları çalıştırıyor olabilmektedir.[243] Normal zamanlarda, kümeleme sistemi içerisindeki sunucular yük dengeleme (load balancing) için hizmet vermektedir ve bir felaket durumunda her biri bütün yükü devralmaktadır.[244]

Birincil ve ikincil sunucuların depolama sistemini paylaşmamaları mümkündür.[245] Bu çözüm, iki sunucu birbirinden bağımsız uygulamalar çalıştırdığında uygulanmaktadır; yedekleme sunucusu aracılığı ile sunuculardan birisi devre dışı kaldığında kümeleme yapısı içerisindeki diğer sunucunun depolama sistemine ulaşma yetkisi tanımlanmaktadır.[246] Diğer bir seçenek de her bir sunucunun depolama sistemini diğer sunucunun depolama sistemine yansıtmaktır (mirroring). Felaket durumlarında yedekleme sunucusu yansıtılmış depolamaya erişebilmektedir.[247]

Sunucu kümleme bir diğer adıyla simetrik kümeleme, yüksek kullanılabilirlik (high availability) konusunda çözüm olmanın yanı sıra yük dengelemeye de yardımcı

[240] J. W. Rittinghouse, J. F. Ransome, 2005, s. 143.
[241] a.g.e, s. 143.
[242] a.g.e, s. 144.
[243] a.g.e, s. 144.
[244] a.g.e, s. 144.
[245] a.g.e, s. 144.
[246] a.g.e, s. 144.
[247] a.g.e, s. 144.

olmaktadır, bu pahalı bir alternatiftir ve uygulanmadan önce maliyet-fayda analizi (cost-benefit analysis) yapılması yerinde olacaktır.[248]

2.7. VERİ YEDEKLEME VE GERİ YÜKLEME

Gittikçe artan bir şekilde daha çok insan ve kurum bilgi teknolojileri altyapısına (IT infrastructure) güvenmektedir.[249] Bu bağımlılık, sıklıkla bilgi teknolojileri altyapısı düzgün çalışmadığında bariz şekilde ortaya çıkmaktadır.[250] Bilgi teknolojileri altyapısının başına gelebilecek insan ya da doğa kaynaklı afetler, bilgi teknolojileri hizmetlerinin kesintiye uğramasına neden olmaktadır.[251]

İnsanların kişisel verilerinin kaybolduğunu öğrenmeleri hâlinde (felaket meydana geldiğinde) kurumlara olan güvenleri sarsılacaktır.[252] Örnek vermek gerekirse, tüccarlar sipariş kayıtlarını kaybettiğinde ya da satış sektöründeki insanlar birçok emek vermelerine rağmen aldıkları siparişleri karşılayamadıklarında gelir, moral ve itibar kaybı ile karşılaşacaklardır.[253]

Felakete maruz kalınması durumunda, bilgi teknolojileri altyapısını ve iş süreçlerini yeniden ayağa kaldırmak için elde mevcut düzgün alınmış yedekler olmalıdır çünkü arızaya uğramış donanım yeniden satın alınabilse de kritik öneme haiz bir verinin geri dönüşü mümkün değildir.[254] Bu nedenle, güncel veri yedeklerine sahip olmak bilgisayar sistemlerini kullanan herkes için oldukça önemlidir.[255]

[248] J. W. Rittinghouse, J. F. Ransome, 2005, s. 144.
[249] Florian Pritz, *Concept of a Server Based Open Source Backup Process with an Emphasis on IT Security*, TU Viyana, Viyana 2016, s. 2.
[250] a.g.e, s. 2.
[251] a.g.e, s. 2.
[252] a.g.e, s. 2.
[253] a.g.e, s. 2.
[254] a.g.e, s. 2.
[255] a.g.e, s. 2.

Bugünlerde bu problemlerin önüne geçmek adına, bir başka deyişle bilgi teknolojileri altyapısı hizmetlerinin düzenli çalışmasını sürdürmesi için birçok çözüm önerilmektedir.[256] Bu çözümlerden birisi verilerin düzenli yedeklerinin alınmasıdır. Fakat çoğu sistemin yedeği düzgün biçimde alınamamaktadır.[257]

Sistem verilerinin ve özellikle işletme içi hazırlanan yazılım ögelerinin yedeklenmesi, felaket planlamasında en önemli yapı taşlarıdır.[258] Enformasyon ve iletişim teknolojilerinde herhangi bir nedenden dolayı ortaya çıkan veri kaybı durumunda, kaybedilen verinin tekrar geri yüklenebilmesi (restore) için orijinal verinin periyodik olarak kopyasının alınması işlemine veri yedekleme (backup), verilerin kopyasının alınması işlemine yedekleme süreci ve bu işlemin gerçekleştirilmesi için harcanan süreye de backup window adı verilmektedir.[259] Backup window ve herhangi bir felaket durumunda işletmenin kabul edebildiği en fazla çalışılamaz durumda bulunma süresini etkileyecek olan yedeklerin sisteme geri yüklenme süresi, yedekleme sürecinde yedekleme ortamının, modelinin ve sıklığının belirlenmesinde ana etkenlerdir.[260]

Bu bölümde bilgi teknolojileri altyapısı zarar görüp veriler etkilendiğinde sistemi tekrar ayağa kaldırmak için gerekli, felaket kurtarma karşısında alınabilecek en etkili önlem/hazırlık aksiyonlarından kurumsal veri yedekleme ve yedeklenen veriler üzerinden sistemin eski hâline dönmesini sağlayan ve kurumsal verilerin tekrar kazanımı için önem arz eden kurumsal veri geri yükleme konuları incelenecektir.

[256] F. Pritz, 2016, s. 2.
[257] a.g.e, s. 2.
[258] H. Akpınar, 2009, s. 175-185.
[259] a.g.e, s. 175-185.
[260] a.g.e, s. 175-185.

2.7.1. Kurumsal Veri Yedekleme Yaklaşımları

2.7.1.1. Teyp Tabanlı Yedekleme

Teypler 1960 ve 1970'lerden başlayarak ana veri yedekleme metodu olmuştur. Çünkü uzun zamandır teypler veri yedeklemenin bir parçasını oluşturmaktadır.[261] Teyp teknolojisini kullanan kurumların altyapılarını sık güncellemesine gerek yoktur. Altyapı geliştirmeye ihtiyacın ortadan kaldırılması sadece maliyet açısından fayda sağlamamaktadır, bunun yanında zamandan da tasarruf edilmektedir ve ek olarak teyplerin diğer veri depolama yöntemleri ile mukayese edildiklerinde daha ucuz olduğu görülmektedir.[262] Fakat teyplerin maliyeti, düzgün aralıklarla yedeklenecek verinin tipi ve miktarı tarafından doğrudan etkilenmektedir.[263]

Teyp tabanlı yedeklemenin bir diğer olumlu yanı da birden fazla merkezli veri depolama sistemlerine olanak tanımasıdır.[264] Çoklu mekân veri yedekliliğini uygulamak, veri merkezlerinden birindeki bir felaket durumunda kritik verilerin kaybolmasının önüne geçmeyi temin etmektedir.[265] Teyp teknolojisi ile çoklu mekân veri depolama uygulaması mümkün olmasına rağmen maliyet açısından pahalılık arz edebilmekte ve veri merkezleri arasında güvenli veri transferi ve depolamasını mümkün kılmamaktadır.[266]

Ek olarak teyp tabanlı yedekleme yaklaşımı, diğer yedekleme yaklaşımlarına oranla daha uzun süreler almaktadır.[267] Teypleri kullanırken verinin doğru bir şekilde

[261] https://solutionsreview.com/backup-disaster-recovery/tape-based-disk-based-and-cloud-based-backup-how-do-you-choose/ (12.06.2020)
[262] a.g.k.
[263] a.g.k.
[264] a.g.k.
[265] a.g.k.
[266] a.g.k.
[267] a.g.k.

okunmasına engel olacak veri bozulmaları meydana gelebilmektedir.[268] Bu durum, herhangi bir verinin geri yüklemesinin doğru sıra ile gerçekleştirilmesinin önünde bir handikap olarak yer almaktadır.[269]

2.7.1.2. Disk Tabanlı Yedekleme

Disk tabanlı yedekleme, veri geri yükleme durumlarında genelde teyp tabanlı yedeklemeye kıyasla daha güvenilir ve hızlıdır.[270] Teyp tabanlı yedeklemede olduğu gibi verileri sırayla geri yüklemeye ve disklere olduğu gibi teker teker yansıtmaya (replication) gerek yoktur ve fakat diskler, çoklu mekân yedekliliği ve veri depolaması için uygun değildir.[271] Disk tabanlı yedekleme, kurumlarda yerinde veri depolaması anlamına gelmektedir. Bu durum, kurumların yerinde yedeklilik veya üçüncü mekân yedekliliği gerçekleştirmek için bir üçüncü taraf sağlayıcıya ihtiyaç duyacağı anlamına gelmektedir. [272]

Kurumlar harici bir sağlayıcıyı kullanmaktan vazgeçtiklerinde disk alanı satın almanın maliyeti hızla artabilmektedir.[273] Bu noktada bir hibrit metot daha bulunmaktadır ve diskten teybe yedekleme olarak adlandırılmaktadır.[274]

Bu yaklaşımda kurumlar, disk kopyalarını teyplere yedeklemektedir ve bu çözüm disk alanı maliyetinden kaçınmanın bir yoludur fakat bunun yanı sıra altyapı maliyeti ve teypler ile disklerin bakım ve korunması için sarf edilecek ek çabalar göz önüne alınmalıdır.[275]

---

[268] https://solutionsreview.com/backup-disaster-recovery/tape-based-disk-based-and-cloud-based-backup-how-do-you-choose/ (12.06.2020)
[269] a.g.k.
[270] a.g.k.
[271] a.g.k.
[272] a.g.k.
[273] a.g.k.
[274] a.g.k.
[275] a.g.k.

2.7.1.3. Bulut Tabanlı Yedekleme

Veri depolama için bulut tabanlı yedekleme, maliyet verimliliği en fazla olan yöntemdir.[276] Disk ve teyp satın almaya devam etme gereği bulunmamaktadır. Buna ek olarak, verilerin kopyalarını yansıtma (replication) ile ilgili az iş yükü mevcuttur çünkü süreç tipik olarak yedekleme sağlayıcısı tarafından idame ettirilmektedir.[277] Kurumlar aynı zamanda; yedekleri fiziksel olarak yönetmek için zaman yönünden de tasarrufta bulunmaktadır.[278]

Yerel bir veri kopyası (local data copy) yerel veri merkezinde gerçekleştirilebilirken aynı zamanda üçüncü taraf sağlayıcıya veya veri merkezine de çoğaltılabildiğinden çoklu mekân veri yedekliliği bulut tabanlı yedekleme ile daha basit olmaktadır.[279] Bu yöntemde bant genişliği (bandwith) sorun olabilmektedir. Bant genişliği kapasitesine bağlı olmak kaydıyla kurumlar, potansiyel olarak kurumsal veri iletişim ağında (network) daha az veya daha fazla miktarda veri yansıtmak durumunda kalmaktadır. Fakat bu çözüm buluta verilerinizin sadece bir kısmını transfer etmek istediğinizde mümkün olmaktadır. [280]

Kurumların ihtiyacına binaen, yukarıda anlatılan veri yedekleme yaklaşımlarından herhangi biri daha kullanışlı olabilmektedir. İhtiyaç duyulan çözüme karar verilirken; kurumların bant genişliği kapasitesi, ne kadar kurumsal verinin düzenli yedekleneceği, bilgi teknolojileri bütçesi, kurumsal verilerin kopyalarının gönderileceği lokasyon sayısı dikkate alınmalıdır. Bu bilgilere sahip olunduktan sonra yedekleme metodu seçimi ile ilgili verilecek karar daha kolay olacaktır. Ayrıca kurumsal verilerin kritiklik seviyesine göre bir kurumsal veri yedekleme politikası oluşturulmalıdır.

[276] https://solutionsreview.com/backup-disaster-recovery/tape-based-disk-based-and-cloud-based-backup-how-do-you-choose/ (12.06.2020)
[277] a.g.k.
[278] a.g.k.
[279] a.g.k.
[280] a.g.k.

2.7.2. Veri Yedekleri Depolama Ortamları\Donanımları

Günümüz koşullarında yedekleme süreci manyetik teyp, hard disk veya blu-ray gibi veri depolama ortamlarında gerçekleştirilmektedir.[281] Onlarca yıldır en favori yedekleme ortamı olan manyetik teyplerin, giderek hard disklere karşı olan fiyat avantajını yitirmesi ile yakın bir zamanda yeni kurulan sistemlerde ürün yaşam eğrilerinin son noktasına gelmeleri kaçınılmazdır.[282] Bununla birlikte sistemlerini manyetik teyp üzerine kurmuş olan işletmelerin tüketim talepleri bir süre daha devam edecektir.[283]

2.7.2.1. Katı Hâl Depolama Cihazları (Solid State Storage)

SSD, uçucu olmayan (non-volatile) bellek kullanılan tipik bir depolama birimidir. Güç kesildiğinde veriyi muhafaza etmektedir. Hareketli bütünleşik parçalar olmadan tümleşik devreler kullanılarak veri depolanmakta ve geri alınmaktadır. Katı hâl depolama birimleri arasında aşağıdaki cihazlar bulunmaktadır[284]:

- Katı Hâl Sürücüsü (Solid State Drive-SSD)
- Sayısal Güvenlik Kartı (Secure Digital Card-SD Card)
- USB (Universal Serial Bus) Bellek

2.7.2.2. Sabit Disk Sürücüsü (Hard Disc Drive-HDD)

Depolama için mıknatıslı (magnetic) depolama kullanılmaktadır ve veriyi tekrar kullanmak için hızlı sert dönüş plâkalarından (rapidly rigid rotation platters) yararlanılmaktadır.[285]

[281] H. Akpınar, 2009, s. 175-185.
[282] a.g.e, s. 175-185.
[283] a.g.e, s. 175-185.
[284] Jaroslav Vasak, *Analysis of Backup for Small and Medium-sized Enterprises (SME) in the Czech Rebublic*, Czech Technical University, Prag 2017, s. 16.
[285] a.g.e, s. 16.

2.7.2.3. Mıknatıslı Kaset (Magnetic Tape)

Verilere sıralı erişim yöntemini kullanan bir depolama ortamıdır. Kaset teknolojileri giriş seviyesi, orta seviye ve kurumsal seviye olarak kategorize edilmektedir.[286] Mıknatıslı kaset veri depolama cihazı, şu anda daha çok sistem veri yedekleme, veri arşivleme ve veri değişimi işlevlerini yerine getirmede kullanılmaktadır.[287] Maliyetlerinin ucuz olması, veri depolama ve arşivleme konularında mıknatıslı kaset donanımının uzun vadede çözüm olmasını mümkün kılmaktadır.[288]

Bazı kasetler yazmayı devre dışı bırakmak için anahtarlara sahiptir çünkü bir defa yedek oluşturulduğunda ve anahtar çevrildiğinde verilerin kazara silinmesinin önüne geçilmektedir.[289] Veri depolama ortamında kasetler kullanıldığında çok dikkatli seçim yapmak gerekmektedir çünkü kasetler manyetiklik özelliğine sahiptir ve ısıya karşı duyarlıdır. Eğer kasetler üzerindeki manyetik alanlarda uzun zaman periyotlarında veri depolanacaksa kaset bundan etkilenebilmekte ve verilerin bozulması olasılığı doğabilmektedir.[290]

2.7.2.4. Optik Diskler

Kompakt Disk (Compact Disc-CD), Çok Amaçlı Sayısal Disk (Digital Versatile Disc-DVD), Blu-ray, Optik Disk Arşivi gibi optik olarak okunabilen ortamlardır.[291] Optik Disk Arşivi, veri merkezleri için dayanıklılık, ölçeklenebilirlik

[286] J. Vasak, 2017, s. 16.
[287] M. K. Roy, Debabrata Ghosh Dastidar, *Cobol Programming*, McGraw-Hill Education, ABD 1983, s. 18.
[288] Tom Coughlin, The Costs Of Storage, *Forbes*, 24 Haziran 2016. https://www.forbes.com/sites/tomcoughlin/2016/07/24/the-costs-of-storage/?sh=4ba555cc3239 (13.12.2021)
[289] Simson Garfinkel, Gene Spafford, and Alan Schwartz, *Practical UNIX and Internet security*, O'Reilly Media, Inc., ABD 2003.
[290] a.g.k.
[291] Sony, Optical Disc Archive Generation 2, 2016. http://www.everspan.com/wpcontent/uploads/2016/04/ODA_Gen2_WhitePaper_20160408_English.pdf (14.07.2020)

ve uzun vadede arşivleme amaçlarına ulaşmak için geliştirilmiş başlıca çözümdür. Depolama ortamı teorik olarak bin yıllık uzun yaşama süresine haizdir. [292]

2.7.3. Alınan Yedeğin Boyutuna Göre Yedekleme Türleri

2.7.3.1. Tam Yedekleme (Full Backup)

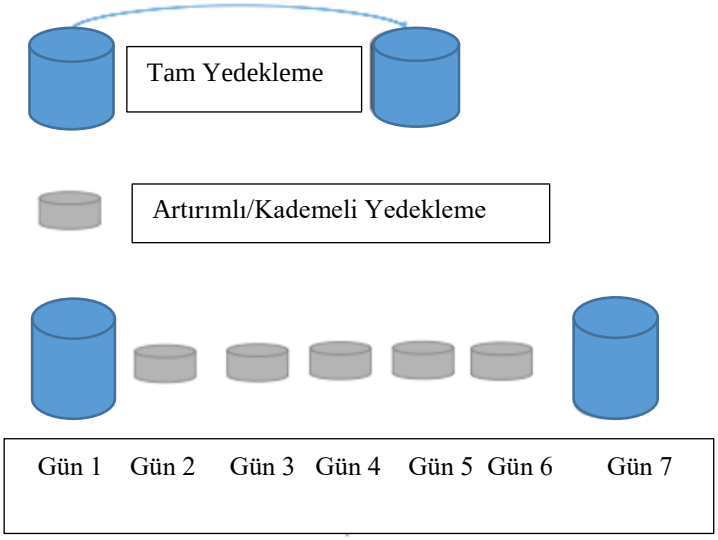
Tam yedek alma sürecinde bütün dosyalar ve klasörler yedekleme sürecine dâhil edilmektedir ve bu yedekleme türü genellikle kurumlarda başlangıç yedeklemesi olarak kullanılmaktadır.[293] Bu yedekleme tipi genelde başlatıcı\tetikleyici yedekleme (iniator backup) tipi olarak kullanılmaktadır ve bu evreden sonra kademeli (diffirential) ve artırımlı (inceremental) yedekleme tipleri sırasıyla her biri ayrı ayrı (respectively) olarak gerçekleştirilmektedir. Tam yedekleme, önceki orijinal tam yedeğin güncellenmesi için artırımlı ve kademeli yedekleme tipleri gerçekleştirildikten sonra tekrar edilmektedir.[294] Az sayıda kurum, yedekleme verisi yalnızca asgari depolama alanı (minimum storage space) gerektirdiğinde tam yedekleme işlemini icra ettirmektedir.[295]

Tam yedek tipi, temelde en son ne zaman değiştirildiğine bakılmaksızın seçilen sistemdeki bütün verinin yedeklenmesi mantığına dayanmaktadır ve bu teknik yedeklemenin diğer türleri için ön koşul niteliğine sahiptir.[296]

---

[292] Sony, Optical Disc Archive Generation 2, 2016. http://www.everspan.com/wpcontent/uploads/2016/04/ODA_Gen2_WhitePaper_20160408_English.pdf (14.07.2020)
[293] Sindhura Yarrapothu, *Effectiveness of Backup and Disaster Recovery in Cloud,* Blekinge Institute of Technology, İsveç 2015, s. 11-12.
[294] a.g.e, s. 11-12.
[295] a.g.e, s. 11-12.
[296] J. Vasak, 2017, s. 6.

Tüm klasör ve veri listesini tek bir yedekleme setinde yönetme ve veri korumanın kolay olması bu yöntemin olumlu özellikleridir.[297] Tam yedeklemenin çalıştığı her dakika her dosya tekraren yedeklendiği için tam yedekleme süreci uzun süreler almaktadır ve aynı zamanda büyük miktarda depolama alanı kullanımı (massive storage space) gerekmektedir.[298] Nerdeyse aynı dosyaların tekrar tekrar depolanması söz konusu olduğu için verimsiz bir depolama kullanımına (inefficient use of storage) sebebiyet verilmiş olmaktadır.[299] Şekil 2.2'de Tam Yedekleme Süreci gösterilmektedir.



Şekil 2.2 Tam Yedekleme Süreci [300]

2.7.3.2. Artırımlı Yedekleme (Incremental Backup)

Artırımlı yedeklemede, son tam yedek veya son artırımlı yedeklemenin üzerine yapılmış tüm değişiklikler veya yeni eklemeler yedeklenmektedir.[301] Bu yol genellikle her gün tam yedeklemenin üzerine yapılmış değişiklikleri yedekleyerek zaman kazanmak için tam yedeklemeden sonra kullanılmaktadır. [302] Artırımlı yedek, tam ya

[297] S. Yarrapothu, 2015, s. 11-12.
[298] a.g.e, s. 11-12.
[299] a.g.e, s. 12.
[300] http://support.unitrends.com/ikm/questions.php?questionid=980 (12.09.2020)
[301] Alexander Lenk and Stefan Tai, *Cloud standby: Disaster Recovery of Distributed Systems in the Cloud*, Springer Berlin Heidelberg, Berlin 2014, s. 32-46.
[302] a.g.e, s. 32-46.

da artırımlı yedek olup olmadığına bakılmaksızın sadece son yedeklemeden beri değişen dosyaları içermektedir. Veri geri yükleme (restore) işlemi sonucunda elde edilen veri, son tam yedeklemenin yanı sıra takip eden tüm artırımlı yedeklemeleri içermektedir.[303]

Artırımlı yedekleme tekniğinde, hızlı yedek alma süreleri test edilmektedir ve dosyaların kopyaları yeniden üretilmediği için verimli depolama alanı kullanımı sağlanmaktadır. Veri geri kazanım (restore) süresi uzundur ve karmaşıktır.[304] Geri kazanım işlemini gerçekleştirmek için tam yedekler ve bunları takip eden tüm ardışık artırımlı yedeklere ihtiyaç duyulmaktadır. [305]

2.7.3.3. Kademeli Yedekleme (Diffirential Backup)

Kademeli yedeklemede, son tam ya da kademeli yedekten itibaren yapılmış tüm değişiklikler yedeklenmektedir ve her kademeli yedek, geri kazanım işlemi daha hızlı yürütülerek bir sonraki günün artırımlı yedeği ile birleştirilmektedir.[306] Kademeli yedek, sadece son tam yedekten itibaren değişen dosyaları içermektedir. Geri kazanım süreci, tam yedeğin üzerine yapılmış son kademeli yedeği içermektedir.[307]

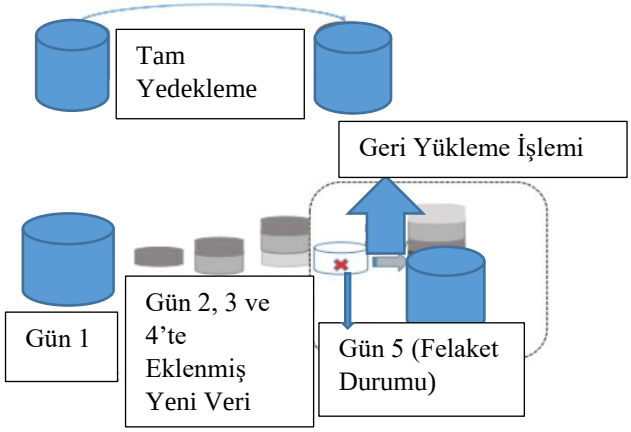
Bu yedekleme tipinde, hızlı yedekleme ve hızlı geri kazanım sürelerine ulaşılmaktadır.[308] Verimli bir depolama kullanım alanı vaat edilmemektedir. Kademeli yedeklemeden sonra eklenen ve değiştirilen tüm dosyalar takip eden tüm kademeli yedeklerde yeniden üretilecektir.[309] Geri kazanım süreci (restore) hafif sayılabilecek

[303] http://www.encyclopedia.com/computing/dictionariesthesauruses-pictures-and-press-releases/full-backup (18.06.2020)
[304] S. Yarrapothu, 2015, s. 11-12.
[305] a.g.e, s. 11-12.
[306] a.g.e, s. 13.
[307] a.g.k.
[308] a.g.e, s. 14.
[309] a.g.e, s. 14.

düzeyde karmaşıktır. Tam yedek ve son kademeli yedek, geri kazanım sürecinin gerçekleştirilmesi adına bu süreçte azami düzeyde elzem role sahiptir. [310]

2.7.3.4. Tam Yedek ve Kademeli Yedek Kombinasyonu

Tümleşik yedek alma sürecinde, başlangıçta tüm klasör ve dosyalar ilk tam yedekle güvenceye alınmaktadır ve sistemdeki güncellemeleri müteakip (subsequent) kademeli yedeklerle birlikte korunmaktadır.[311] Kademeli yedekleme süreci yürütülürken sadece değişiklikler yedeklenmektedir. Bir dizi kademeli yedek alındıktan sonra tam yedek süreci tekrar edilmektedir. Herhangi bir veriyi geri kazanmak için son yedekleme zamanından beri son tam yedek ve bütün kademeli yedeklere ihtiyaç duyulmaktadır.[312] Şekil 2.3'te tam ve kademeli yedekleme kombinasyonu gösterilmektedir.



Şekil 2.3 Tam ve Kademeli Yedekleme Kombinasyonu[313]

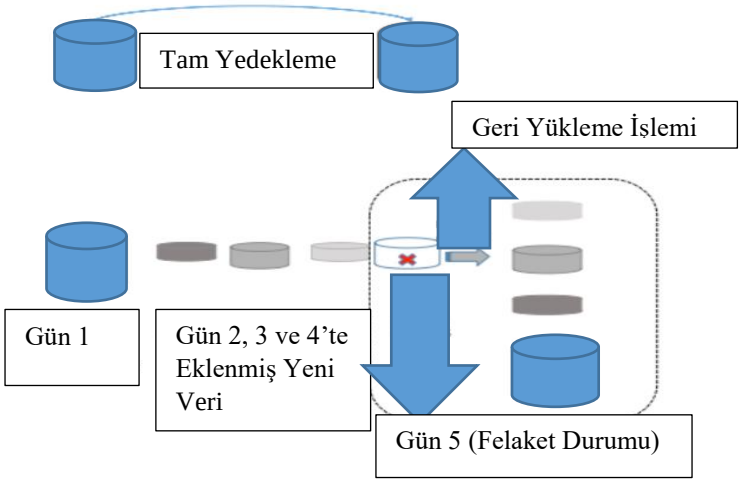
Şekil 2.3'te görüldüğü üzere ilk gündeki yedekleme süreci tipik şekilde devam etmektedir ve ikinci günde kademeli yedekleme aracılığı ile alınmış taze ve ek veriler elde mevcuttur.[314] Beşinci gündeki felaket meydana gelene kadar kademeli yedekleme

[310] S. Yarrapothu, 2015, s. 14.
[311] A. Zrnec, D. Lavbič, "Comparison of Cloud vs. Tape Backup Performance and Costs with Oracle Database", *Journal of Infirmation and Organizational Sciences*, Sayı: 26/1, s. 135–142.
[312] a.g.m, s. 135-142.
[313] a.g.e, s. 14.
[314] a.g.e, s. 14.

süreci devam etmiştir. Beşinci gündeki veri kaybını geri kazanmak için birinci gündeki tam yedek ve dördüncü gündeki kademeli yedek verisine ihtiyaç duyulmaktadır.[315]

2.7.3.5. Tam Yedek ve Artırımlı Yedek Kombinasyonu

Bu kombinasyonel yedekleme sürecinde, ilk tam yedek ve devamındaki artırımlı yedeklemeler aracılığı ile alınmış tüm dosyalar ve klasörler yedeklenmektedir.[316] Sadece artırımlı yedekleme aracılığı ile alınmış yedekler mevcuttur. Tam yedek bir dizi artırımlı yedekten sonra icra edilmektedir. Herhangi bir verinin geri kazanımı için son tam yedekten itibaren eldeki son tam yedek ve artırımlı yedeklere ihtiyaç duyulmaktadır.[317] Şekil 2.4'te tam ve artırımlı yedekleme kombinasyonu gösterilmektedir.



Şekil 2.4 Tam ve Artırımlı Yedekleme Kombinasyonu[318]

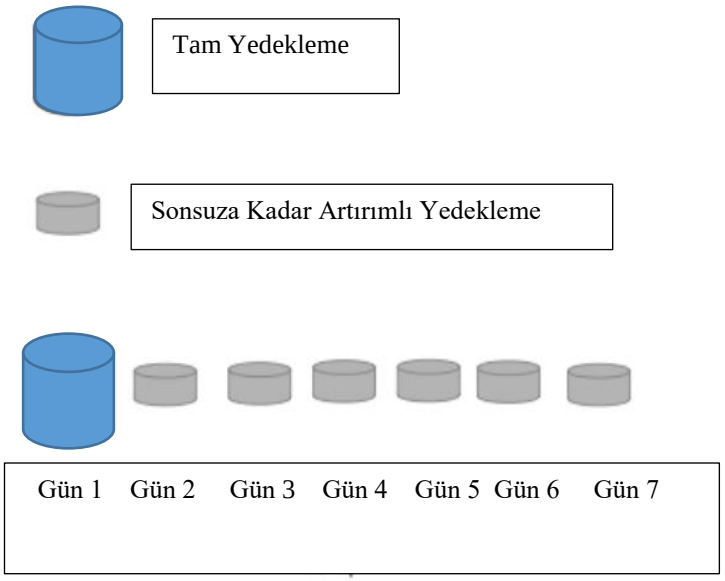
Şekil 2.4'te görüldüğü üzere birinci günde olağan şekilde tam yedek alınmıştır ve ikinci günde artırımlı yedekleme aracılığı ile alınmış taze ek veriler elde mevcut bulunmaktadır.[319] Bu işlemler beşinci günde felaket olana kadar sürmektedir. Beşinci

[315] S. Yarrapothu, 2015, s. 14.
[316] A. Zrnec, D. Lavbič, 2011, s. 135–142.
[317] a.g.m, s. 135-142.
[318] a.g.e, s. 13.
[319] a.g.e, s. 13.

gündeki veri kaybının geri kazanımı için birinci gündeki tam yedek, ikinci-üçüncü-dördüncü günlerdeki artırımlı yedek dizilerine ihtiyaç duyulmaktadır.[320]

2.7.3.6. Artırımlı Sonsuza Kadar Yedekleme

Artırımlı sonsuza kadar yedekleme sürecinde, ilk tam yedekten itibaren ortaya çıkan tüm değişiklikler yedeklenmektedir. Genellikle ilk tam yedeklemeden sonra gerçekleştirilmektedir ve sonsuza kadar ardışık artırımlı yedekler alınmaktadır.[321] Veri yedekleme zaman aralığı (backup window) kısalmaktadır. Tam yedekleme planlaması zarureti ortadan kalkmıştır. Bilgisayar ağ sistemlerine (computer network systems) düşen veri trafiği (band traffic) azalmıştır. Geri kazanım sürecinde şeffaflık ve otomatiklik sağlanmıştır.[322] Geri kazanımda, tam yedek ve tüm artırımlı yedek kopyalarına ihtiyaç duyulması bu çözümü karmaşık hâle getirmiştir.[323] Şekil 2.5'te Artırımlı Sonsuza Kadar Yedekleme süreci gösterilmektedir.



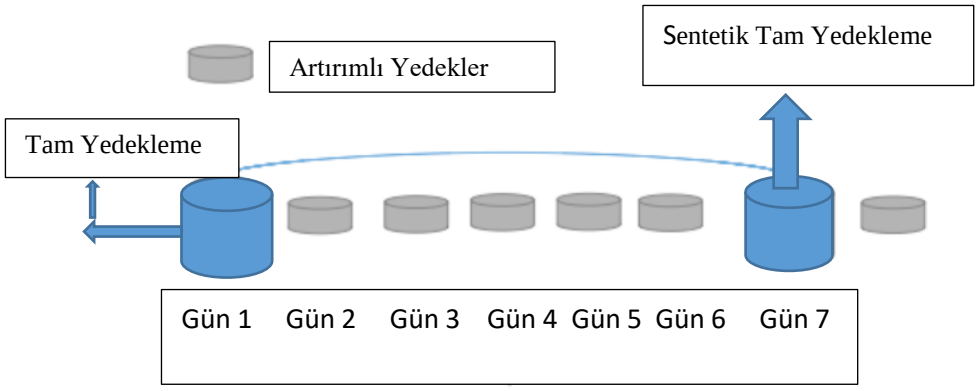
Şekil 2.5 Sonsuza Kadar Artırımlı Yedekleme[324]

[320] S. Yarrapothu, 2015, s. 13.
[321] a.g.e, s. 14.
[322] a.g.e, s. 14.
[323] a.g.e, s. 14.
[324] a.g.e, s. 15.

2.7.3.7. Sentetik Yedekleme

Sentetik Yedekleme sürecinde, ilk tam yedek alınmaktadır ve akabinde artırımlı yedekler ardışık olarak gerçekleştirilmektedir. İsminden de anlaşılacağı üzere sentetik yedekler, orijinal veriden (original data) elde edilmemektedir.[325] Tam yedekler, sentetik tam yedeği biçimlendirmek için takip eden artırımlı yedekler ile birleşmektedir. Artırımlı yedek sadece güncellemelerden oluşmaktadır.[326]

Sentetik yedekleme, önceki tam yedek ve devamındaki artırımlı yedeklerden tam yedek oluşturma sürecidir. Sınırlı bant genişliği (bandwidth) söz konusu olduğunda başvurulan bir yöntemdir. Bu prosedür, orijinal veriden yedek oluşturulmadığı için sentetik olarak adlandırılmıştır.[327] Yedekleme sürecini gerçekleştirmek için az miktarda zaman harcanmaktadır. Maliyetler düşüktür ve geri kazanım süresi azalmıştır. Sentetik yedeklemede, bir sistemdeki ilk yedek ve aynı zamanda sentetik yedek, tam yedeğin müteakip yedeği (following backup) niteliğine haiz değildir.[328] Aşağıdaki şekil 2.6'da sentetik yedekleme süreci gösterilmektedir.



Şekil 2.6 Sentetik Yedekleme Süreci[329]

[325] "What are synthetic backups?, Techworld, 2015. http://www.techworld.com/storage/what-are-synthetic-backups-1149/ (03.10.2020)
[326] a.g.k.
[327] V. Beal, Synthetic Backup. http://www.webopedia.com/TERM/S/synthetic_backup.html (01.10.2020)
[328] a.g.k.
[329] S. Yarrapothu, 2015, s. 15.

2.7.3.8. Ayna Tipi Yedekleme

Ayna tipi yedekleme, yedeklenen kaynağın bir yansımasıdır, gerçek zamanlı yeniden üretimidir (duplication)[330]. Bazı çevrelere göre ayna tipi yedekleme, bir yedekleme çeşidi olarak görülmemektedir çünkü ayna tipi yedeklemede, ana kaynaktaki bir dosya silindiğinde bu dosya nihayetinde ayna yedekten de silinecektir. Bu nedenle ayna tipi yedekleme, kazara dosya silme, sabotaj, bilgisayar virüsü istilası gibi durumların farkındalığı ile uygulanmalıdır.[331] Ayna tipi yedeklemede, dosyalar üzerinde veri sıkıştırma (data compression) ve şifre koruma (password protection) uygulanamamaktadır.[332]

2.7.4. İşlevselliğine Göre Yedekleme Türleri

Tablo 2.7'de işlevselliğine göre yedekleme türlerinin mukayesesi gösterilmektedir.

Tablo 2.7 İşlevselliğine Göre Yedekleme Türlerinin Mukayesesi[333]

İŞLEVSELLİĞİNE GÖRE YEDEKLEME TÜRLERİNİN MUKAYESESİ				
Yedekleme Türü	**Yedeklenen Veri**	**Yedekleme Süresi**	**Geri Kazanım Süresi**	**Veri Depolama Alanı**
Tam Yedekleme	Bütün veri	En yavaş	Hızlı	Yüksek
Artırımlı Yedekleme	Yeni veya değiştirilmiş	Hızlı	Orta	En düşük
Kademeli Yedekleme	Tam yedekten beri yeni/değiştirilmiş	Orta	Hızlı	Orta
Ayna Tipi Yedekleme	Yeni veya değiştirilmiş	En hızlı	En hızlı	En yüksek

[330] J. Vasak, 2017, s. 6.
[331] a.g.e, s. 6.
[332] a.g.e, s. 6.
[333] a.g.e, s. 7.

2.7.5. Veri Depolama Sisteminin Konumuna Göre Yedekleme Türleri

- Yerinde Yedekleme (On-Site Backup), yerel olarak konumlandırılan depolama ortamı (storage media) üzerinde alınan herhangi bir yedeği ifade etmektedir. Depolama ortamı direkt olarak ya da yerel alan ağı (local area network) aracılığı ile yedeği alınacak ana veri kaynağına bağlanabilmelidir.[334] Yedekler sadece yerinde depolama sunucu sistemlerinde tutulmamalıdır. Çünkü, yerinde yedeklemenin yazılım (software) ve donanım (hardware) ile ilişkili handikaplarının yanı sıra ana binadaki birincil veri merkezinde yangın vs. meydana gelebilecek yerel felaketlere karşı ikincil veri merkezinde yedekleme yapılmalıdır.[335] Maliyet nedenlerinden ötürü ikincil yedekleme sistemi genelde sabit disklerden (hard disc) oluşmaktadır. Bunun nedeni yedekleme kasetlerinin (tapes) oldukça pahalı sürücüler gerektirmesi ve optik ortamının bütün bir sistemin çok sayıda yedeğini depolamak için yeterli kapasite sunamamasıdır.[336]

- Dış Ortamda Yedekleme (Off-Site Backup), Veri Kopyalarının (Data Copies) coğrafik olarak örneğin; farklı bir şehir gibi, farklı bir konuma ya da bulut depolama sistemine gönderilmesidir. [337]

2.7.6. Mimariye Göre Yedekleme Türleri

- Dosya Düzeyinde Yedekleme (File Level Backup), örneğin; dosya izinleri adı altında yüksek düzeyli dosya sistemi (high-level file system) verisi gibi özel dosyaları içermektedir. İki farklı türü mevcuttur[338]:

[334] S. Gregory, Local Backup, 2012. http://typesofbackup.com/local-backup/ (13.01.2021)
[335] a.g.k.
[336] Florian Pritz, *Concept of a Server Based Open Source Backup Process with an Emphasis on IT Security*, TU Viyana, Viyana 2016, s. 46.
[337] J. Vasak, 2017, s. 7.
[338] https://social.technet.microsoft.com/wiki/contents/articles/206.backup-and-restore-classification-ofscenarios.Aspx (17.11.2020)

- Uygulama Duyarlı Yedeklemede, (Application Aware Backup) uygulama düzeyinde işlem yapılmaktadır. Örneğin; bir veri tabanı duyarlı yedekleme sistemi (database-aware backup system), veri tabanı dosyaları ve işlem günlüklerini tek bir birim olarak içermektedir.
- Sistem Durum Yedeklemesi, Windows İşletim Sistemi (Windows Operating System-Windows OS) için hayati öneme sahip işletim sistemine özgü varsayılan dosya grubunu içermesiyle bir seçenek sunmaktadır.

- Sistem Görüntüsü Düzeyinde Yedekleme (Image-Level Backup), daha çok sistem görüntüsü düzeyinde ya da Kitle Düzeyinde Yedekleme (Block Level Backup) olarak adlandırılmaktadır.[339] Aynı zamanda çıplak metal yedekleme/geri kazanım (Bare Metal Backup/Recovery-BMR), Hacim Düzeyi Yedekleme (Volume Level Backup), Felaket Kurtarma Yedeklemesi (Disaster Recovery Backup), Hayalet Yedekleme (Ghost Backup) ya da makinenin klonlanması olarak adlandırılmaktadır.[340] Sistem görüntüsü düzeyinde yedekleme ile belirli bir zamanda uygulama yapılandırma durumu ya da sistem durumunu da içeren tüm bağlantılı veri ile işletim sisteminin bir kopyası da tek dosyada/görüntüde saklanmaktadır. Bu tekniğin bir bilgisayar ya da sanal makine (virtual machine) için kullanılması ihtimal dâhilinde bulunmaktadır.[341]

Tablo 2.8'de mimariye dayalı yedekleme türlerinin kıyaslaması gösterilmektedir.

[339] M. Rouse, What is image-based backup?,2011. http://searchdatabackup.techtarget.com/definition/image-based-backup (11.12.2020)
[340] a.g.k.
[341] a.g.k.

Tablo 2.8 Mimariye Dayalı Yedekleme Türlerinin Kıyaslaması[342]

MİMARİYE DAYALI YEDEKLEME TÜRLERİNİN KIYASLAMASI		
Yedekleme Türü	**Avantajlar**	**Dezavantajlar**
Dosya Düzeyinde Yedekleme	• Az sayıda dosyayı geri kazanmada verimlilik • Sistemdeki bireysel dosyaları ve klasörleri yedekleme ve geri yüklemede esneklik • Aynı veri birimindeki veri tipleri için esnek yedekleme politikaları oluşturabilme	• Büyük dosya ya da çok sayıdaki küçük dosya yedeklenirken zaman kaybı • Küçük bir dosyadaki küçük bir değişikliğin bütün dosyanın tekrardan yedeklenmesi zaruriyetine sebebiyet vermesi
Sistem Görüntüsü Düzeyinde Yedekleme	• Bütün sistemi geri kazanmada verimlilik • Hızlı geri kazanım süresi • Az sayıda performansa dayalı sorun teşkil etme	• Az sayıda dosyayı geri kazanırken yavaşlık • Fazla miktarda veri depolama alanı gerektirme

[342] J. Vasak, 2017, s. 8.

2.7.7. Dağıtım Modeline Göre Yedekleme Türleri

- Yerel Yedeklemede, veri yerel olarak konumlandırılmış veri depolama sistemine yedeklenmektedir.[343]

- Bulut Yedekleme\Çevrim İçi Yedeklemede (Cloud\Online Backup), veri direkt olarak tescilli ya da izin verilmiş/kamuya açık ağ (public network) aracılığı ile bulut depolama sistemine gönderilmektedir.[344] Veri, bir bulut sağlayıcının depolama sisteminde ya da kamuya açık Amazon Web Services-AWS, Azure ya da Google vs. gibi bir Bulut Hizmet Sağlayıcı (Cloud Service Provider-CSP) aracılığı ile depolanmaktadır.[345]

- Hibrit Bulut Yedekleme (Hybrid Cloud Backup), yerel ve bulut yedeklemenin bir karışımıdır. Bu yöntem, en az bir tam yedek ve onu takip eden artırımlı yedeklerin depolanması gereken yerinde bir araç (on-premises appliance) içermelidir. Veri ilk olarak yerelde depolanmaktadır ve sonrasında bulut hizmet sağlayıcıya kopya gönderme işlemi (replication) yapılmaktadır.[346]

Tablo 2.9'da dağıtım modeline göre yedekleme tiplerinin karşılaştırması yapılmaktadır.

[343] J. Vasak, 2017, s. 9.
[344] M. Rouse, E. Sullivan, Cloud Backup (Online Backup), 2016. http://searchdatabackup.techtarget.com/definition/cloud-backup (03.11.2020)
[345] a.g.k.
[346] a.g.k.

Tablo 2.9 Dağıtım Modeline Göre Yedekleme Tiplerinin Kıyaslaması[347]

DAĞITIM MODELİNE GÖRE YEDEKLEME TİPLERİNİN KIYASLAMASI		
Yedekleme Tipi	**Avantajlar**	**Dezavantajlar**
Yerel Yedekleme	• Hızlı yedekleme ve geri kazanım	• Karmaşıklık • Olası tek veri merkezi ile karşılaşma (felaket durumunda)
Bulut Yedekleme	• Dayanıklılık • Ölçeklenebilirlik • Yüksek kullanılabilirlik • Erişilebilirlik • Tek veri merkezi problemi yoktur (birden çok bölge çözümü vardır)	• İnternet bağlantısına bağımlılık • Bant genişliği ile sınırlandırılmış yedekleme ve geri yükleme • Yasal problemler (hassas verinin farklı merkezlerde bulunması)
Hibrit Yedekleme	• Uygun yedekleme politikası ile hızlı yedekleme ve geri yükleme gerçekleştirimi • Geliştirilmiş dayanıklılık • Geliştirilmiş kullanılabilirlik • Artırılmış yük paylaşımı	• Karmaşıklık

[347] J. Vasak, 2017, s. 9.

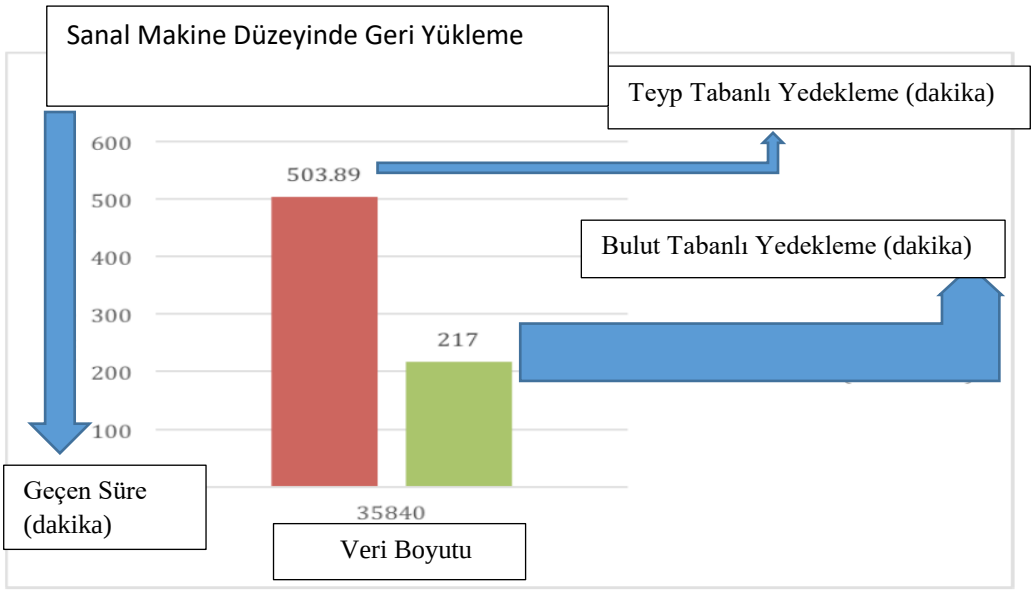
2.7.8. Veri Geri Yükleme Yaklaşımları

Kurumsal veri yedekleri üzerinden başarılı alınmış veri yedekleri sağlıklı bir şekilde temin edildikten sonra istenilen veri ve uygulamaların tekrar işlevsel hâle getirilmesi için veri geri yükleme disiplininden faydalanılmaktadır. Bu kısımda sanal makine ve dosya düzeyinde gerçekleştirilmiş testler doğrultusunda elde edilen verilere yer verilecektir.

2.7.8.1. Sanal Makine Düzeyinde Geri Yükleme

Symantec Backup Exec 2010 yazılımı ile teyp tabanlı yedekleme ve felaket kurtarma yaklaşımlı veri geri yükleme işlemini gerçekleştirmek için harcanan zaman, aynı miktarda veride Asigra yazılımı ile bulut tabanlı yedekleme ve felaket kurtarma yaklaşımlı veri geri yükleme işlemine oranla tartışmalı şekilde daha fazladır.[348] Şekil 2.7'de geri yükleme işlemi aracılığı ile alınmış verilerin gözlenmiş değerlerinin görsel bir sunumu yer almaktadır ve veri doğruluğunu yerine getirmek için üç adet tekrarlama gerçekleştirilmiştir. Şekil 2.7'de gösterildiği gibi ortalama değer not edilmiştir ve değerleri ayırt etmek için kullanılmıştır. Sanal makine seviyesinde teyp tabanlı yedekleme, bulut tabanlı yedeklemeye kıyasla yaklaşık üç yüz dakika daha fazla zaman almıştır.[349]

[348] S. Yarrapothu, 2015, s. 26.
[349] a.g.e, s. 26.

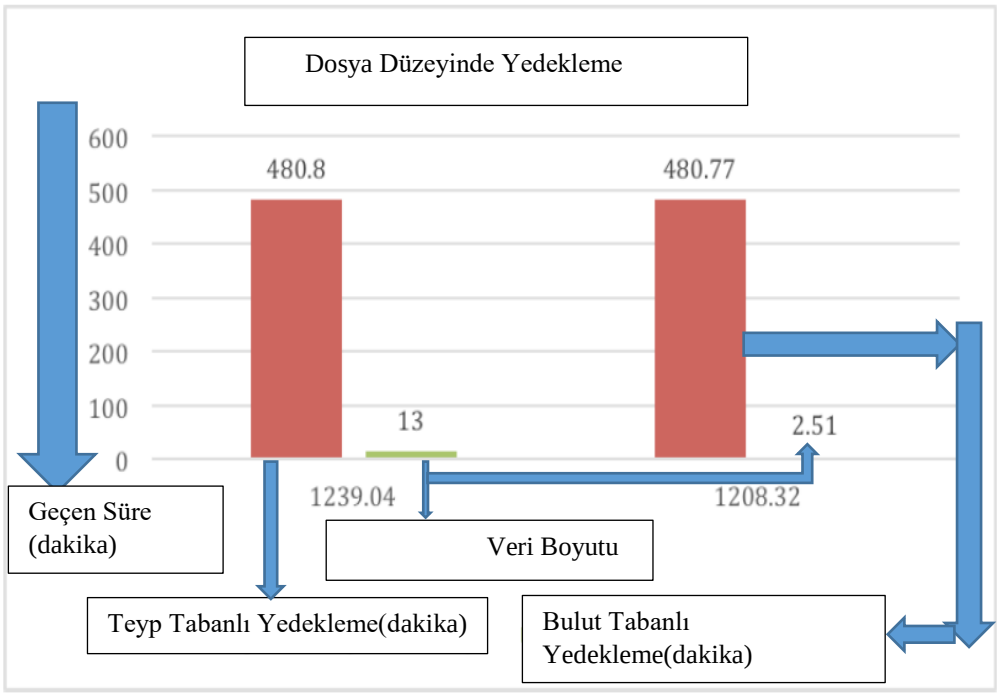


Şekil 2.7 Sanal Makine Düzeyinde Geri Yükleme Süreleri[350]

2.7.8.2. Dosya Seviyesinde Geri Yükleme

Bulut tabanlı yedekleme ve felaket kurtarmadaki (cloud-based backup and DR) geri yükleme prosedürü, verilere erişmek ve gerektiğinde geri yükleme prosedürlerini başlatmak adına verinin merkezini işaretlemek için bir konsol (console) gerektirmektedir.[351] Ancak teyp tabanlı yedekleme ve felaket kurtarma hâlinde teypler tanımlanmakta ve barkod sistemini kullanarak gerekli teyplerin araması aracılığı ile kurum dışı veri depolama ortamından alınmaktadır. Kurumsal veriler bir defa ana veri merkezine alındıklarında, donanım şifrelemeli (hardware encrypted) oldukları için şifreleme anahtarı aracılığı ile teyp kütüphanesine (tape library) eklenmektedir.[352] Şekil 2.8'de iki farklı boyutta, her biri üç yineleme içeren dosyanın, dosya seviyesi yaklaşımına göre zamana dayalı geri yükleme süreleri gösterilmektedir.[353]

[350] S. Yarrapothu, 2015, s. 26.
[351] a.g.e, s. 26.
[352] a.g.e, s. 26.
[353] a.g.e, s. 26.



Şekil 2.8 Dosya Düzeyinde Geri Yükleme Süreleri[354]

[354] S. Yarrapothu, 2015, s. 26.

ÜÇÜNCÜ BÖLÜM

DÜNYADA GERÇEKLEŞTİRİLMİŞ FELAKET KURTARMA UYGULAMALARI

3.1. COMMERZBANK

1870'te kurulan Commerzbank firması, Almanya'nın ikinci büyük bankasıdır. 2001 yılında Commerzbank dünyanın en büyük on altıncı bankası durumundadır. Banka, kuruluşundan bu yana Birinci Dünya Savaşı ve sosyalizm gibi birçok olumsuzluğun üstesinden gelmeyi başarmıştır.[355] Banka bunun yanı sıra Amerika'daki 1992 Chicago Seli ve 1993 Dünya Ticaret Merkezi bombalaması da dâhil felaketlerde hayatta kalmayı başarmıştır. Commerzbank'ın New York ofisi Dünya Finans Merkezi'nin 31 ile 34'üncü katları arasında yer almaktadır. Bu konum, Dünya Ticaret Merkezi kulelerine yalnızca yaklaşık doksan iki metre uzaklıktadır.[356]

11 Eylül 2011'de, Dünya Ticaret Merkezi (World Trade Center-WTC) Amerika tarihinin en büyük terörizm saldırısına uğramıştır. Saldırı sonucunda yaklaşık üç bin insan yaşamını yitirmiştir.[357] Yalnızca New York ekonomisine etkisi seksen üç milyar dolardır. Saha temizliği, sekiz aydan fazla sürmüştür. İşletmelerin çoğu saldırıların neden olduğu yıkımdan kurtulamamıştır. Genel ekonomik etkiler, bugün

[355] Availability Digest, The State of Virginia – Down for Days, 2010. http://www.availabilitydigest.com/public_articles/0510/virginia.pdf (03.09.2020)
[356] a.g.k.
[357] http://www.cdc.gov/mmwr/preview/mmwrhtml/mm51spa6.htm (12.09.2020)

devam etmektedir ve her bir Amerika vatandaşının günlük yaşamı dolaylı da olsa etkilenmiştir.[358]

Commerzbank, Dünya Ticaret Merkezine o kadar yakındır ki enkaz, camların parçalanmasına neden olmuştur.[359] Commerzbank'ın bulunduğu binanın içi enkaz, cam parçaları ve boğucu inşaat malzemeleri ile kaplanmıştır. Veri merkezi klimaları zarar görmüş ve patlama, veri merkezi bilgisayarlarında kademeli etkisi olan yüksek sıcaklıklara neden olmuştur.[360]

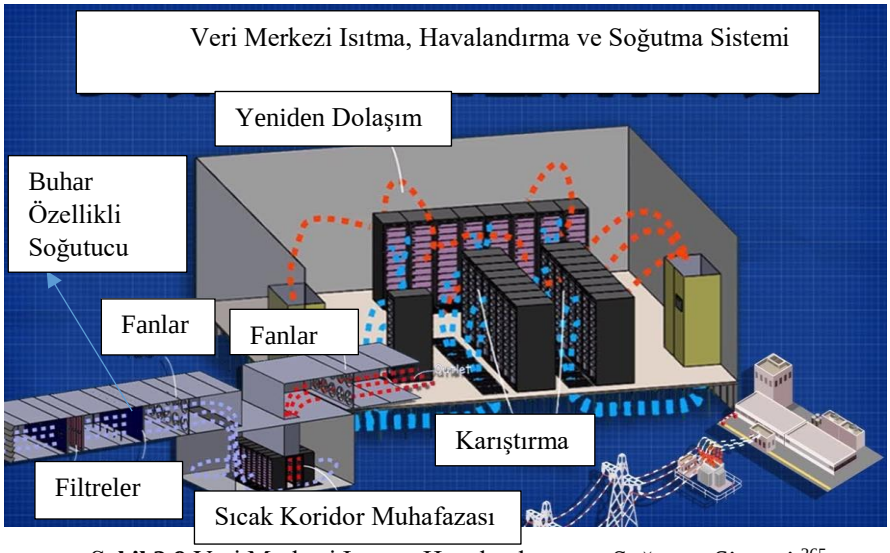
Çoğu yerel veri merkezi diskinin başarısız olması, uzak konumdaki veri merkezine yük binmesine neden olmuştur.[361] Olay boyunca uzak lokasyona yük devretme toleransına sahip sistem, olay boyunca kurumun çalışabilmesine imkân tanımıştır. Kurumun veri merkezindeki ekipmanları zarar görse de iş yapabilme yeteneği sekteye uğramamış ve iş devamlılığı sağlanmıştır.[362]

Öncelikle ilk çarpışmadan sonra kaybolan Federal Rezerv ve New York Borsası ile haberleşmeleri tekrar kazanmak için bağlantılar uzaktaki veri merkezine yönlendirilmiştir.[363] İkinci jetin saldırısı başladığında Dünya Ticaret Merkezi saldırı altındayken Commerzbank derhâl tahliyeye başlamıştır. Binanın elektriği kesildiğinde Commerzbank'ın yedekleme güç jeneratörü devreye girmiştir ama ısıtma, havalandırma ve klima (Heating Ventilating and Air Conditioning-HVAC) sistemi veri merkezinin çökmesine neden olan enkaz nedeniyle gereği gibi çalışamamıştır.[364]

---

[358] http://www.cdc.gov/mmwr/preview/mmwrhtml/mm51spa6.htm (12.09.2020)
[359] Editorial Staff of SearchStorage.com, Banks avoids data disaster, 2002. http://searchstorage.techtarget.com/tip/0,289483,sid5_gci808783,00.html (13.01.2021)
[360] a.g.k.
[361] Hewlett-Packard, Hp AlphaServer Technology Helps Commerzbank Tolerate Disaster on September 11, 2002. http://h71000.www7.hp.com/openvms/brochures/commerzbank/commerzbank.pdf?jumpid=reg_R1002USEN (26.01.2021)
[362] a.g.k.
[363] Heather M. Brotherton, *Data Center Recovery Best Practises:Before, During and After Disaster Recovery Execution*, Purdue University, Indiana 2011, s. 23.
[364] a.g.e, s. 23.

Şekilde 2.9'da veri merkezi ısıtma, havalandırma ve klima sistemi gösterilmektedir.



Şekil 2.9 Veri Merkezi Isıtma, Havalandırma ve Soğutma Sistemi [365]

Otomatik yük devretme süreçleri, çalışanlar felaket kurtarma merkezine getirilene kadar devam etmiştir. Burası takip eden günlerde birincil veri merkezi (primary data center) olarak hizmet vermiştir.[366]

Commerzbank'ın depolama sistemi uzaktaki veri merkezine veri kopyalamak yerine kartuşa yazılan verileri geri kazanmak için sürekli çalışmıştır.[367] EMC firması takip eden 36 saat boyunca yedekleme sistemi kapasitesini artırmak için birden fazla terabayt depolama alanı ekleyerek yeni yedeklerin oluşturulmasının yanı sıra 'görev açısından kritik' verilerin geri yüklenmesini sağlamıştır.[368]

Commerzbank'ın ana veri merkezi firmanın kendi jeneratörü, yakıt deposu, soğutma kulesi, kesintisiz güç kaynağı (UPS), yangın söndürme sistemi sayesinde çok

[365] https://theengineeringmindset.com/data-center-hvac-cooling-systems/ (18.12.2020)
[366] K. Parris, Who Surives Disasters and Why, Part 2:Organizations, 2010. http://www2.openvms.org/kparris/Bootcamp2010_Disasters_Part2_Organizations.pdf (12.02.2021)
[367] http://searchstorage.techtarget.com/tip/0,289483,sid5_gci808783,00.html (13.01.2021)
[368] a.g.k.

iyi korunmaktadır.[369] Commerzbank, depolama sistemini sanallaştırma işinin yarısını gerçekleştirmiştir ve saldırıdan önce dönüşümün çoğu tamamlanmıştır. Commerzbank bilgi teknolojileri personeli, düzenli test ve ikili arama ağacı algoritması (Binary Search Tree Algorithm-BSTA) içeren bir iş sürekliliği planı tasarlamıştır.[370] Bu sayede iş sürekliliğinin temel şartlarından sıfır kesinti gereksinimini karşılama yeteneği sağlanmıştır. Bu amaca ulaşabilmek için Commerzbank, uzak konumda bulunan veri merkezinde "her şeyi" kopyalamıştır.[371]

Dünya Ticaret Merkezi'nden otuz mil uzaklıkta, Rye kentinde bulunan ikincil veri merkezi bu iş sürekliliği planının temel taşıdır. Dünya Ticaret Merkezindeki ana veri merkezi, yedekli sürücüler ve ekstra işlemciler ile güçlendirilmiştir.[372]

Commerzbank'ın destek aldığı EMC firmasının; müşteri işlemleri, finansal veri tabanları, e-posta ve diğer önem arz eden uygulamaları korumak için yedekleme yazılımı mevcuttur.[373] Bu yedekleme yazılımı, ana verinin kopyalarını oluşturarak bu kopyaları bir ya da daha fazla uzak veri merkezine iletmektedir. Bu sistem kritik veriler için derhâl standart, işlevsel bir ortam sağlamıştır.[374] İkincil veri merkezi, Dünya Ticaret Merkezindeki kümenin üyesi olan sunucuların kopyalarını sağlamıştır. Bu sunucular ana veri merkezindeki depolama sistemi zarar gördükten sonra uzak veri merkezindeki kopyalanmış veriyi kullanarak hizmet vermeye devam etmiştir.[375]

Commerzbank'ın 'güneşi takip et' tabanlı personel sistemi (Follow the Sun Personel Staffing[376]) gün boyunca desteğin devam etmesi anlamına gelmektedir.[377] HP

[369] http://searchstorage.techtarget.com/tip/0,289483,sid5_gci808783,00.html (23.12.2020)
[370] a.g.k.
[371] a.g.k.
[372] H. M. Brotherton, 2011, s. 23.
[373] a.g.e, s. 23.
[374] a.g.e, s. 23.
[375] a.g.e, s. 23.
[376] 'Güneşi takip et' tabanlı personel sistemi kurumların Dünya'nın anlık olarak güneşin batmadığı dört bir tarafında ilgili iş süreçlerine destek verecek personel bulundurmaları modelini ifade etmektedir.
[377] a.g.e, s. 23.

(Hewlett Packard) firmasının sonradan bir parçası hâline geldiği EMC firması, Compaq gibi üreticilerle kurulan ilişkiler sayesinde herhangi bir hizmet veya donanım ihtiyacında, bu üreticilerin desteğine haiz durumda bulunmaktadır.[378]

Commerzbank'ın kurumsal başkan yardımcısı Richard Arenaro, iş sürekliliği planının bir parçası olan felaket kurtarma kısmının başarıyla uygulandığını açıklamıştır.[379] Bütün kritik veri elde mevcuttur fakat normal iş süreçlerine yeniden dönmek, yaklaşık dört saat sürecektir. Firma, sıfır kesinti gerektiren iş gereksinimlerini karşılama noktasında başarısız olmuştur. Sunucular yeteri kadar esnek değildir ve çok sayıda insanın müdahalesini gerektirmiştir.[380]

Uzak lokasyondaki yedekleme sunucuları özdeş değildir ki bu da işletim sistemleri ile uygulama uyumluluğu sorunlarına neden olmuştur.[381] Commerzbank kurum başkan yardımcısı Arenaro, ekibiyle birlikte ana ve ikincil veri merkezlerine bir sunucu almak anlamına gelen teknolojinin birebir kopyalanması gibi yanlış bir strateji izlediklerini söylemiştir. Böyle bir durumla karşılaşıldığında gerçekten donanıma sahip olmanın en az kaygı güdülecek konu olduğunu, önemli olanın veri ve sistemlerin mevcut ve kullanıma hazır olması gerektiğini eklemiştir.[382]

Commerzbank, uyumluluk problemlerini sunucuları sanallaştırarak ve tescilli işletim sistemlerini kullanmayı bırakarak düzeltmiştir.[383] Bir başka problem sunucunun kendi üzerinde yer alan; aynı zamanda o sunucuya sabit kimlik veren disk, ağ arayüz kartı, depolama arayüzü gibi donanımlar nedeniyle sunucuların elle yapılandırılması yüzünden gecikmelerin yaşanmasıdır.[384]

---

[378] H. M. Brotherton, 2011, s. 25.
[379] a.g.e, s. 25.
[380] a.g.e, s. 25.
[381] a.g.e, s. 25.
[382] a.g.e, s. 25.
[383] Case Study: Commerzbank North America, 2011. www.egenera.com/1157984790/Link.htm (12.11.2020)
[384] a.g.k.

Sanallaştırılmış ortam, bir talep hâlinde herhangi bir uygulamayı çalıştırmak için ağ donanımı ve depolama sistemi ile paylaşılmış bir sunucu havuzu sağlamaktadır.[385] Yeni sistem, herhangi bir zamanda herhangi bir kimliği üstlenebilecek şekilde depolama alan ağı (Storage Area Network-SAN) bağlantısı için tasarlanmıştır ki bu da hangi verilerin kaybedildiği ve hangi verilerin yakalandığını açıklamaktadır. Veri merkezi için soğutma gereksinimleri, sanallaştırılmış sunucular sayesinde azaltılmıştır. Bunun yanı sıra toplam fiziksel karmaşıklık da azaltılmıştır.[386]

Sanallaştırılmış konfigürasyon problem çözme süresini kısaltmıştır.[387] Yeni sunucuları yapılandırma işlemi, olayın vuku bulduğu vakitlerde bir saatten az süre almaktadır ve bu süre önceden on altı saate kadar çıkabilmektedir. Ana ve ikincil veri merkezleri, etkin sunucu kümesinin üyeleri olan sunucular içermektedir.[388] Uygulamalar ve veriler, her türlü hizmetin iki yönlü eş zamanlı çoğaltma kullanılarak konumlar arasında sorunsuz bir şekilde değiştirilmesine imkân tanıyan SAN'de depolanmaktadır. İkincil veri merkezi, günlük veri işlemenin aktif bir parçası hâline gelmiştir ve yüzde kırklık bir işlem kapasitesi ile başa çıkmaktadır.[389]

Bu çalışma, doğru gerçekleştirilmiş bir felaket kurtarmanın örnek bir çalışmasını sunmaktadır.[390] Bilişim teknolojileri dairesi, olasılık planlamasına katılmış ve düzenli testler gerçekleştirmiştir ve her ekip üyesi ne yaptığının farkındadır. Ana veri merkezi ve ikincil veri merkezinin New York'ta bulunması, bir zayıflık olarak görülmektedir.[391] Zira New York'un büyük ölçekte zarar görmesi durumunda şehir dışında üçüncü bir veri merkezinin olmaması, sıfır-kesinti ile iş sürekliğinin sağlanmasının önünde engel olarak görünmektedir. Sunucu sanallaştırma, yüzde

[385] Case Study: Commerzbank North America , 2011. www.egenera.com/1157984790/Link.htm (12.11.2020)
[386] a.g.k.
[387] a.g.k.
[388] a.g.k.
[389] a.g.k.
[390] a.g.k.
[391] a.g.k.

altmış alan tasarrufu sağlamıştır. Bu ekstra alan, yedekli çalışan donanımın barındırılması açısından bakım destek çalışmalarını yürüten firmaya ve kuruma avantaj sağlamıştır.[392]

Bu örnekte, Katrina Kasırgasında olduğu gibi veri merkezindeki donanım zarar görmüştür. Katrina Kasırgasındaki birçok başarısız örneğin aksine sistemi tekrar ayağa kaldırma planı çalışmıştır.[393] Commerzbank, bu olayda birçok avantaja sahiptir. New York altyapısı zarar görmemiştir.[394] Commerzbank, bir şehrin ayağa sıfırdan kaldırılması gibi bir yükle karşı karşıya kalmamıştır zira sadece ana veri merkezi ayağa kaldırılmıştır. Afetler zaman zaman çeşitli ölçeklerde gerçekleşmektedir.[395]

Commerzbank; 11 Eylül'den görece rahat kurtulurken pek çok firma, telafi edilemeyen kayıplara uğramıştır.[396] Birçok firma, büyük donanım ve personel kayıplarına uğramanın önüne geçmek maksadı ile iyi bir planlama ve hazırlığa sahip olmadığı için sistemi tekrar ayağa kaldırmak noktasında başarısızlığa uğramıştır.[397]

Commerzbank, bankanın öncelikleri ve hassasiyetlerini belirlemiş ve yatırımlarını bu minvalde yapmıştır.

Geçmiş felaketler firmaya; hayatta kalmayı, yüksek seviyeli yönetimi, olayları yönetmek için personelin eğitilmesinin önemini öğretmiştir.[398]Alınan tedbirlerle kesinti süresi kısaltılmıştır ve felaketin finansal boyutu minimize edilmiştir.[399]

[392] Case Study: Commerzbank North America, 2011. www.egenera.com/1157984790/Link.htm (12.11.2020)
[393] H. M. Brotherton, 2011, s. 25.
[394] a.g.e, s. 25.
[395] a.g.e, s. 25.
[396] a.g.e, s. 26.
[397] a.g.e, s. 26.
[398] a.g.e, s. 26.
[399] a.g.e, s. 28.

3.2. TULANE ÜNİVERSİTESİ

Tulane Üniversitesi, New Orleans'ta kurulmuştur. Üniversite, 1834'te Tropik Hastalıklar Araştırma Merkezi olarak kurulmuştur.[400] Tulane'nin sonbahar ara tatilinden iki gün önce meydana gelen Katrina Kasırgası, New Orleans'ı yıkıma uğratmıştır. Bu kasırga, Amerika tarihindeki en kötü doğal afet olarak görülmektedir. New Orleans'ın almış olduğu gerçek hasar, kasırgadan saatler sonra ortaya çıkmıştır.[401] Şekil 3.1'de Katrina Kasırgasına ait bir görüntü yer almaktadır.



Şekil 3.1 Katrina Kasırgası[402]

Felaketin boyutları, Tulane Üniversitesi kampüsünün çok ötesine uzanmaktadır fakat bu durum örnek olayın incelemesinin odak noktasıdır ve bunun Tulane Üniversitesi üzerine doğrudan ya da kademeli etkileri ele alınacaktır.[403]

---

[400] Thomas Gerace, Raymond Jean, Adam Krob, "Decentralized and centralized it support at Tulane University: a case study from a hybrid model", *SIGUCCS 07*, Ekim 2007, Proceedings of the 35th Annual ACM SIGUCCS Fall Conference, Florida ABD, s. 125-128.

[401] http://www.blackboard.com/CMSPages/GetFile.aspx?guid=39a0b112-221d-4d04-be80-f2024d16943a (23.12.2020)

[402] https://www.vox.com/2015/8/23/9191907/hurricane-katrina (19.11.2020)

[403] http://issue.com/thebooksmithgroup/docs/tulane (22.02.2021)

Katrina'nın üzerinden bir haftadan fazla bir zaman geçmesiyle beraber Tulane Üniversitesi kampüsünün yüzde sekseni su altında bulunmaktadır. Üniversitenin ödeme sistemi ve e-posta sistemi çökmüştür, öğrenci ve fakülte kayıt sistemleri çalışmamaktadır.[404]

Öğrenciler diğer okullara ziyaretçi öğrenci olarak gönderilmiştir.[405] Bazı öğrencilerden gittikleri okullarda ücret istenmiştir. Bunun üzerine, üniversite yönetimi veri tabanı (database) kayıtlarına erişir erişmez öğrenim ücretleri ile ilgili mağduriyetin giderileceği noktasında söz vermiştir.[406] Tulane Üniversitesi, haberleşme ve bilgi sistemlerinin tekrar işlevsel hâle getirilmesini acil mesele olarak ele almıştır. Üniversite yönetimi, Tulane'nin felaketten kurtarılması planlarını yaparken hiçbir bilgisayar kaydına erişim bulunmamaktadır. Hesap bilgilerinin yer aldığı sunucular kurtarılamaz durumdadır çünkü bu sunucular ana veri merkezinden bağımsız çalışmaktadır.[407]

Felakete müdahale etmek adına Tulane bilgi teknolojileri ekibi, veri merkezi felaket kurtarma planı (data center disaster recovery plan) dikkate alınarak yedekleme politikasını (backup policy) devreye sokmuştur. Bilgi sistemleri pasif konuma getirilmiştir.[408] Yedekleme jeneratörleri ve güç kaynakları, kampüs binalarına yerleştirilmiştir. Tulane kampüsü su altında kaldığı için yedekleme jeneratörlerinin çalışması sekteye uğramıştır ve sonuç olarak haberleşme sistemleri; e-posta, sabit telefonlar ve cep telefonu haberleşmelerinin kaybıyla kesintiye uğramış ve metin mesajlaşması, haberleşmenin yegâne kaynağı hâline gelmiştir.[409]

---

[404] N. Kevin Krane, Kahn, Marc J., Markert, Ronald J., Whelton, Paul K., Traber, Peter G., Taylor, Ian L.,"Surviving Hurricane Katrina: Reconstructing the Educational Enterprise of Tulane University School of Medicine", *Tulane University School of Medicine*, Cilt 82, Sayı:8, 2007, s. 757-762 .
[405] John Lawson, "A Look Back at a Disaster Plan: What Went Wrong and Right", *Information Technology Supplement*, Cilt 52, Sayı:16, 2005.
[406] a.g.k.
[407] a.g.k.
[408] a.g.k.
[409] a.g.m, s. 757-762.

Tulane bilgi teknolojileri ekibi, bir felakete nasıl hazırlanılacağı konusunda gerekli planlara sahiptir. Personel eğitimli ve afet planını uygulama konusunda tecrübelidir. Yedeklemelerin otuz altı saatte tamamlanabileceği bilinmektedir.[410] Uzak lokasyondaki yedekler, New Orleans'ta bir binanın on dördüncü katında muhafaza edilmektedir. Tulane, aynı zamanda acil bilgiler ve telefon iletişim bilgileri için yedek bir web sitesini saklamaktadır.[411]

Kategori dört ya da daha yüksek bir felaket durumunda veri merkezi kapatılacak ya da tahliye edilecektir. Kapatma için uzakta barındırılan acil durum web sitesinin aktif duruma getirilmesi gereklidir.[412]

Tulane Üniversitesinin birinci önceliği, personel maaşlarını ödemektir. Bu başarılması zor bir görevdir çünkü felaket kurtarma planında belirlendiği gibi maaş bordrolarını, dosya sunucusundan alma konusunda başarısızlığa uğranmıştır.[413]

Tulane bilgi teknolojileri ekibine on dördüncü katta bulunan yedekleme veri merkezindeki yedeklerden dönüş sağlama işlemini gerçekleştirme görevini yerine getirirken polis eşlik etmiştir. Geri kazanılan yedekleme bantlarındaki veriler, Philadelphia'da işlenmiştir.[414]

Şekil 3.2'de yedekleme sistemlerinde kullanılan veri yedekleme bandı gösterilmektedir.

[410] H. M. Brotherton, 2011, s. 36.
[411] a.g.e, s. 36.
[412] J. Lawson, 2005.
[413] a.g.k.
[414] a.g.k.



Şekil 3.2 Veri Yedekleme Bandı[415]

Houston'daki Baylor Üniversitesi, Tulane Üniversitesinin yeniden yönlendirilmiş web sitesini barındırmıştır ve operasyonlarını yeniden başlatabilmesi için Tulane Üniversitesini davet etmiştir fakat bu işlem ip (internet protocol-IP) adresi ataması statik olmadığı için planlandığı gibi yürümemiştir.[416] Bu derhâl düzeltilmiş ve Tulane Üniversitesi, devamlı ve kırılmayan zincir güncellemeler alan web sitesi sunucusu aracılığı ile paydaşları ile haberleşmek için acil yönlendirilmiş web sitesini kullanmıştır. E-posta, tekrar çevrim içi duruma getirilen ilk sistem olmuştur.[417]

Tulane şu anda web siteleri, e-posta ve diğer kritik sistemlerin yedeklerini de bünyesinde barındıran, yıllık olarak güncellenen yedekleme sunucularına sahiptir.[418] Felaket kurtarma planı, fırtınadan fazlasını kapsayacak şekilde yenilenmiştir ve bilgi teknolojileri personeli de artık planlama çalışmalarına katılmaktadır.[419]

[415] https://www.cloudpro.co.uk/it-infrastructure/backup/7836/does-tape-still-have-a-place-in-my-backup-strategy (23.08.2020)
[416] J. Lawson, 2005.
[417] a.g.k.
[418] http://www.computerworld.com/s/article/print/314109/Tulane_University (07.01.2021)
[419] a.g.k.

Tulane, Sungard taşınabilir veri merkezi ile acil durumlar için kontrat imzalamıştır.[420] Katrina Kasırgasının olumsuz etkilediği New Orleans'taki yedek veri merkezi, veri yedeklerinin daha uzak bir lokasyonda haftada üç defa alınarak saklanılması gerektiğini ortaya koymuştur.[421] Çalışanlara acil durumlarda kritik dosyalarını güvence altına almak konusunda hazırlık için taşınabilir bellekler (Universal Serial Bus-USB) temin edilmiştir.[422]

Alternatif bir geri kurtarım merkezi Philadelphia'da kurulmuştur ve artık Tulane Üniversitesinde yerinde güçlendirilmiş bir kontrol merkezi vardır.[423] Kampüs merkezine acil durum jeneratörlerini kullanarak daha uzun süre çalışabilen, enerji verimliliğine haiz sistemler kurulmuştur.[424]

Tulane Üniversitesi, basit e-posta (e-mail) gönderebilmek için sayısal amatör radyo ağını (digital ham-radio network) ve üniversite insan kaynakları bölümünün direkt olarak üniversite web sayfasında tasarımlar yapabilmesi için acil güncellemeleri devreye almıştır.[425] Şiddetli fırtına vb. felaket durumlarında sadece medyaya bağımlı olmamak adına Tulane üniversitesi, özel bir hava durumu tahmincisi görevlendirmiştir.[426]

Öğrencilerin bir felaket esnasında eğitim süreçlerini aksatmamak adına dizüstü bilgisayarlar tahsis edilmiş olup felaket sonrası üniversite çevrim içi derslere devam etmiştir.[427] Tulane Üniversitesinin durumu kendine münhasır ama uç bir örnek olmuştur. Felaket kurtarma disiplini adına birçok uygulama doğru yapılmış ve felaket

[420] H. M. Brotherton, 2011, s. 46.
[421] a.g.k.
[422] a.g.k.
[423] a.g.e, s. 46.
[424] a.g.e, s. 46.
[425] a.g.e, s. 46.
[426] a.g.e, s. 46.
[427] T. Gerace, R. Jean, A. Krob, 2007, s. 125-128.

sonrasında üniversite bilgi sistemleri tekrar işlevsel hâle getirilebilmiştir.[428] Kurum dışı bir lokasyonda verileri yedeklemenin bunca yatırıma değeceği tartışma konusudur ama ikincil bir veri merkezinin olmaması, iradi olarak seçilmiş bir mali karar olacaktır.[429]

Tulane'de fırtınanın verdiği zarar, bilgi teknolojileri altyapısını koruma yeteneğinin ötesindedir.[430] Yine de bu olay göstermiştir ki bir felakette en değerli, en elzem görev veri merkezi altyapısının çalışma yeteneğinin tamamen kaybının önüne geçebilme yeteneğidir. New Orleans'ta ayakta kalabilme yeteneğine sahip hiçbir kurum yokken Tulane hayatta kalmayı başarabilmiştir. [431]

Tulane Üniversitesi, Katrina Kasırgasından alınan tecrübe ve dersle üniversitenin can damarı olan verilerin nasıl korunması gerektiğini öğrenmiştir.[432] Katrina Kasırgası, Tulane Üniversitesinin öğrencileri dikkate almadan yani başka bir deyişle öğrencilere dönük hizmet ve verilere çare bulmadan hayatta kalamayacağını göstermiştir.[433]

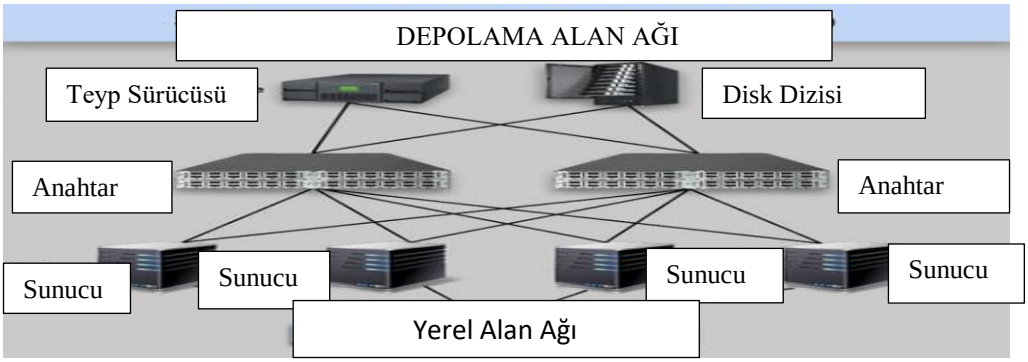
New Orleans şehri, Tulane Üniversitesine bağımlıdır. En büyük işveren kurum, sağlık ve eğitim kurumu olarak Tulane Üniversitesi etkili bir felaket kurtarma yönetimi ile kısa zamanda yaralarını sarmış ve daha özerk ve güçlü bir kurum hâline gelmiştir.[434]

[428] T. Gerace, R. Jean, A. Krob, 2007, s. 125-128.
[429] a.g.e, s. 125-128.
[430] H. M. Brotherton, 2011, s. 48.
[431] J. Lawson, 2005.
[432] a.g.e, s. 48.
[433] a.g.e, s. 48.
[434] a.g.e, s. 48.

3.3. VIRGINIA DEVLETLER TOPLULUĞU

Virginia eyalet polisinin üç gün boyunca internetsiz kalmasına neden olan hizmet kesintisi 2009 yılında yaşanmıştır.[435] Virginia eyaleti, geniş kapsamlı bir kesinti ile karşı karşıya kalmıştır. Kesinti, yenilenmesi planlanan bir sunucuda 'neredeyse eşzamanlı bir dizi donanım arızasından' kaynaklanmıştır.[436] Arıza yıllık gerçekleştirilen felaket kurtarma testinden sonra meydana gelmiştir. Yirmi yedi tane devlet kurumu bu kesintiden etkilenmiştir.[437]

Kesinti süresince eyaletin dosya sunucularının yüzde otuzu kullanılamayacak durumdadır ve Richmond yakınlarındaki veri merkezinde iki yüz yirmi sekiz adet depolama (storage) sunucusu, devre dışı konuma gelmiştir.[438] Arızalanan donanımdan bir tanesi SAN'in iki hafıza kartından bir tanesidir. SAN arızası Virginia eyaletinin dört yüz seksen üç sunucusunu olumsuz etkilemiştir. Motorlu taşıtlar kurumu (Department of Motor Vehicles-DMV) en çok etkilenen kurum olmuştur.[439] Sürücülerin lisansı kesinti süresince yenilenememiş ve yaşanan aksama pazar günü tatil günü olmasına rağmen kurumun mesai yapmasına neden olmuştur.[440] Şekil 3.3'te SAN sisteminin yapısını anlatan şema gösterilmektedir.



Şekil 3.3 Depolama Alan Ağı(SAN) Çalışma Mantığı[441]

[435] H. M. Brotherton, 2011, s. 51.
[436] a.g.e, s. 51.
[437] a.g.e, s. 51.
[438] a.g.e, s. 52.
[439] a.g.e, s. 52.
[440] a.g.e, s. 56.
[441] http://espanol.siemon.com/sis/storage-area-networks/ (20.07.2020)

SAN kesintisinden etkilenen tek kurum, Motor Taşıtları Kurumu olmamıştır. Sosyal Hizmetler Kurumuna göre dört yüz sosyal yardım alıcısı, ödenek çeklerini iki gün gecikmeli olarak almak zorunda kalmıştır.[442] Bu kurumdaki çalışanlar arızaları minimuma indirmek için mesai yapmıştır. Bunun yanı sıra, nafaka ve vergi ödemeleri yapmak için gereken internet erişimi, devre dışı kalmıştır. Eyalet Vergi Dairesinde (Department of Taxation), vergi mükellefleri web sitesi üzerinden yeni bir işletme kaydı veya ödeme yapmak için başvuruda bulunamamıştır.[443]

Olayın üzerinden birkaç saat geçtikten sonra veri depolama ünitesi, bir hata mesajı yollamıştır.[444] Hata mesajının nedeni, makine üzerindeki iki hafıza kartından birinin değişmesi olarak belirlenmiştir.[445] Birkaç saat sonra bir teknisyen hafıza kartını değiştirmiştir. Kartın değiştirilmesinden kısa süre sonra Depolama Alan Ağı (Storage Area Network-SAN) sağlıklı çalışmasını sürdürememiştir. Sonrasında, yanlış kartın değiştirilmiş olabileceği kanısına varılmıştır.[446]

Virginia Bilgi Teknolojileri Ajansı (Virginia Information Technologies Agency-VITA) ve Northrop Grunman firması acil müdahale ekibini (rapid response team) aktive etmiştir ve hizmeti tekrardan ayağa kaldırmak için çalışmalar başlatılmıştır. Gece boyunca çalışmalar sürmüştür ve fakat arızalanmış sunucular yüzünden veri erişimi ilk etapta geri kazanılamamıştır.[447]

Yirmi dört devlet kurumu uygun önlemleri almaları için SAN arızasına göre öncelendirilerek belirlenmiştir. SAN sistemi arızası gece saatlerinde giderilmiştir.[448] Arıza ile ilişkili sunucuların yarısından fazlası sabah saatlerinde yeniden işlevsel hâle

[442] H. M. Brotherton, 2011, s. 53.
[443] a.g.e, s. 53.
[444] a.g.e, s. 54.
[445] a.g.e, s. 54.
[446] a.g.e, s. 53.
[447] a.g.e, s. 54.
[448] http://www.wvec.com/news/local/Northrop-Grumman-to-pay-for-computeroutageinvestigation-102796459.html (30.11.2020)

gelmiştir.[449] Motorlu Taşıtlar Kurumu, Eyalet Vergi Dairesi (Department of Taxation) ve Eyalet Seçim Kurulu (State Board of Elections) SAN arızasından en çok etkilenen kurumlar olmuştur.[450] VITA, hizmetin sağlık durumunu ve sistemin tekrardan kazanımını müşterilerle doğrulamak amacıyla müşterilerden geri bildirimler alarak çalışmalar gerçekleştirmiştir.[451]

Bu senaryodaki SAN arızası, yerinde alınmış tedbirlerle çözülmüştür.[452] Yalnızca hata toleransı olan SAN sistemine sahip olmamakla birlikte manyetik bant (tape) yedeklemeleri daha önce gerçekleştirilmiştir ve personel daha önce felaket kurtarma testleri ile felaket kurtarma konusunda donanımlı bir hâle gelmiştir.[453] Donanım sağlayıcısı (vendor) firma EMC ile kurulmuş iyi ilişkiler kesintiyi çözmede ek tecrübe sağlamıştır.[454]

VITA, olayın ardından yapılan çalışmalar sonucu, ana ve ikincil olmak üzere iki veri merkezine sahip olmuştur. Kullanılan SAN donanımı en iyilerinden biridir ve mükemmel güvenilirliğe sahiptir.[455] VITA aynı zamanda acil olay çözme konusunda görevli acil müdahale ekibine (Rapid Response Team-RRT) sahiptir.[456] Göz ardı edilen felaketlerin her an başa gelmesi olasıdır. Virginia Eyaleti, bir felaketin olası zararlı etkilerini minimum zararla atlatabilmek için Northrop Grumman ile uzun vadeli bakım destek anlaşmasına dayalı bir ortaklık yapmıştır.[457]

Virginia Eyaleti, tecrübeli bir bilgi teknolojileri personel kadrosu tarafından yönetilen daha istikrarlı, modern bir altyapıya sahip olmak için gerekli mali yatırımları

[449] http://www.vita.virginia.gov/communications/publications/networknews/default.aspx?id=12906 (23.10.2020)
[450] http://www.vita.virginia.gov/library/default.aspx?id=545 (26.10.2020)
[451] a.g.k.
[452] H. M. Brotherton, 2011, s. 55.
[453] a.g.e, s. 55.
[454] a.g.e, s. 55.
[455] a.g.e, s. 55.
[456] a.g.e, s. 55.
[457] a.g.e, s. 55.

yapmıştır.[458] VITA'nın katıldığı felaket kurtarma tatbikatlarından sonra iki konunun önemi ortaya çıkmıştır. Bunlardan bir tanesi yedeklenen verinin geri kazanımıdır diğeri ise veri doğrulamadır (data verification). Günlük işlemler için günlük yedekler almak, veri kayıplarından kaçınmak için yedekleme politikası açısından tavsiye edilen çözüm önerisidir.[459]

Bu kesintide izleme araçları (monitoring tools) önemli bir role sahip olmuştur.[460] Bilgi teknolojileri personeli hem uyarıları göz ardı etmiştir hem de uyarıları anlamamıştır; aynı zamanda izleme araçları doğru şekilde yapılandırılmamıştır.[461] İzleme araçları hangi SAN'in arızalı olduğunu veya herhangi bir arıza durumunu doğru şekilde bildirmelidir. Bilgi teknolojileri ekibine verilecek doğru eğitimler izleme araçlarının etkin kullanımını ve personelin arıza bildirimlerini doğru algılamasını sağlayacaktır.[462]

Dış kaynaktan bilişim hizmeti alımı; toplu indirimlere, gelişmiş hizmetlere ve yüksek kalitedeki bilgi işlem uzmanlarına erişmeye olanak sağlayacak şekilde olmalıdır.[463] Dış kaynaktan hizmet alımının maliyetleri, düşen donanım maliyetlerinden ötürü aşağı inmelidir. Ancak, Virginia donanım yenilemesi için iki yüz otuz altı milyon dolar daha ödemek zorunda kalmıştır.[464] Mali faydalar, Virginia-Northrop Grumman sözleşmesinde gözetilmemiştir. Northrop Grumman ile var olan on yıllık kontrat, Virginia'ya kontratı sonlandırmak ve yeni teklifler almak için şans vermemiştir çünkü böyle bir şeye kalkışmak oldukça maliyetlidir.[465] Ayrıca sözleşme yapmak için hem bilişim hem de hukuktan anlayan personel sayısı çok azdır.[466]

[458] H. M. Brotherton, 2011, s. 56.
[459] a.g.e, s. 56.
[460] a.g.e, s. 60.
[461] a.g.e, s. 60.
[462] a.g.e, s. 60.
[463] a.g.e, s. 62.
[464] a.g.e, s. 62.
[465] a.g.e, s. 62.
[466] a.g.e, s. 63.

Bu ortaklıktan çıkarılması gereken ders, bu tip dış kaynak hizmet alımı sözleşmelerinin çok uzun vadeli yapılmaması gerektiği ve bilişim personeli kadrosunun bilişim yanında hukuki kavramlara da vakıf olması gerçeğini kuvvetlendirir mahiyettedir.

DÖRDÜNCÜ BÖLÜM

TÜRKİYE'DE GERÇEKLEŞTİRİLMİŞ FELAKET KURTARMA UYGULAMALARI

4.1. ORTA DOĞU TEKNİK ÜNİVERSİTESİ (ODTÜ)

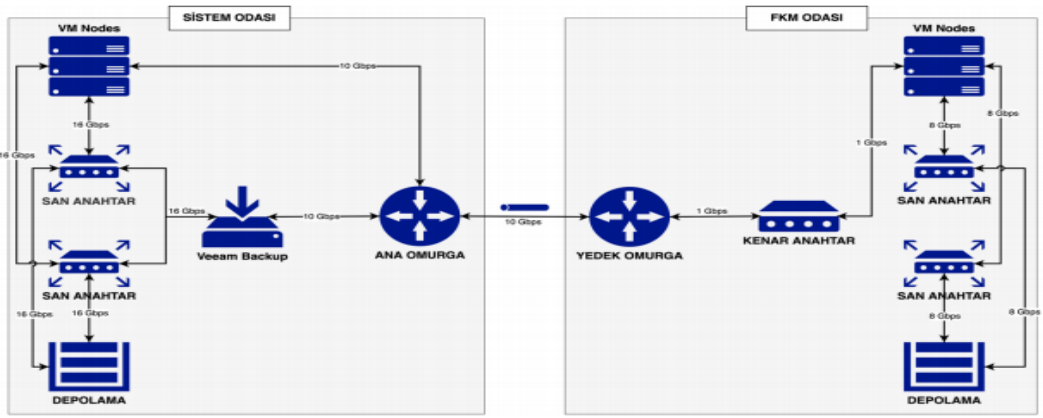
Felaket Kurtarma Merkezi, Orta Doğu Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı-ODTÜ BİDB sistem odasını etkileyebilecek, yangın, sel, deprem gibi doğal afetler sonucunda oluşabilecek kurumsal veri ve altyapı kaybının yaşanması durumunda yedek sunucu, yedek veri depolama ve yedek ağ altyapısını kullanarak güncel veri ile ODTÜ bilişim servislerinin uzak noktadan hizmet verebilmesini sağlamaktadır.[467]

Turkcell Superonline'ın Ankara Söğütözü veri merkezinde üniversiteye tahsis edilen güvenli, paylaşımsız ve erişimi sadece üniversitenin görevlendirdiği yetkili personele açık olan alanda Mayıs 2017 tarihinde kurulumu tamamlanan Felaket Kurtarma Merkezi, BİDB sistem odasından ODTÜ'ye hizmet veren bilişim servislerinin tamamına yakınının anlık yedeklerini tutmakta ve servisler felaket durumunda hizmet vermeye hazır hâlde bekletilmektedir.[468] ODTÜ Bilgi İşlem Daire Başkanlığı Sistem Odası ve Felaket Kurtarma Merkezi arasındaki veri eşitlemesi; paylaşımsız, güvenli ve yedekli fiber optik hatlardan anlık olarak sağlanmaktadır.[469]

[467] https://faq.cc.metu.edu.tr/tr/sss/felaket-kurtarma-merkezi-ve-surekliligi-nasil-saglanmaktadir (03.01.2021)
[468] a.g.k.
[469] a.g.k.

4.2. İNÖNÜ ÜNİVERSİTESİ

Şekil 4.1'de İnönü Üniversitesi ana kampüs alanı içerisinde gerçekleştirilen proje kapsamında, ana sistem odası ile felaket kurtarma merkezinin çalışma mantığı gösterilmiştir.[470] Felaket Kurtarma Merkezi-FKM kurulum aşamalarında TÜBİTAK'ın 2017 yılında hazırlamış olduğu Felaket Kurtarma Merkezi Kurulumu Rehberi dikkate alınmıştır.[471] Felaket kurtarma merkezlerinin temel prensibi, ana sistem odasında herhangi bir felaket (deprem, yangın, sel vb.) meydana geldiğinde çalışan sistemler kesintiye uğramadan (aktif-aktif) veya çok kısa bir süre kesintiden sonra (aktif-pasif) otomatik veya manuel olarak devreye alınmasıdır. Bunu gerçekleştirebilmek için, Şekil 4.1'de gösterildiği gibi, Veeam yedekleme yazılımı sayesinde, aktif olarak çalışmakta olan ana sistem odasında gerçekleşen bütün değişimler FKM sistemine aktarılmaktadır. Bu sayede herhangi bir felaket durumunda veri kaybı olmaksızın FKM devreye alınabilmektedir.[472] FKM, ana sistem odasının tekrar aktif edilmesinden sonra ise, devreye alınmasından ana sistem odasının tekrar kurulumuna kadar süre içerisinde gerçekleşmiş olan değişimleri tekrar sistem odasına çiftlemektedir (replikasyon). Bu sayede veri kaybı olmadan sistemlerin sürekliliği sağlanmış olmaktadır.[473]



Şekil 4.1 Sistem Odası ile FKM Çalışma Mantığı[474]

[470] Kenan İnce, Cemile İnce, Ahmet Topal, M. Tahir Çiçekli, Kerem Adanur, Bünyamin Kuzu "Bilişim Altyapı Sistemi Yenileme Çalışması: İnönü Üniversitesi Örneği", *Anatolian Journal of Computer Sciences*, Cilt 5, Sayı 1, 2020, s. 54-61.
[471] a.g.m, s. 54-61.
[472] a.g.m, s. 54-61.
[473] a.g.m, s. 54-61.
[474] a.g.m, s. 54-61.

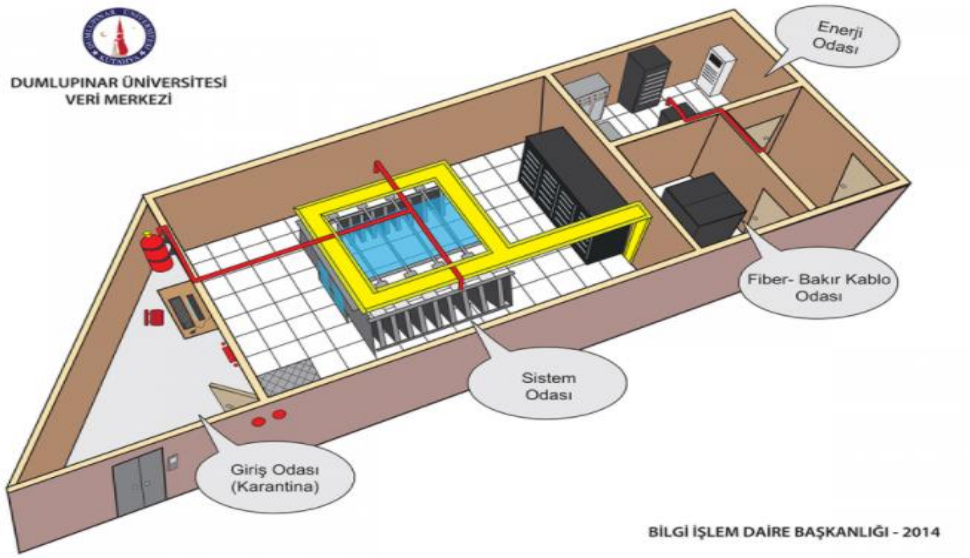
4.3. DUMLUPINAR ÜNİVERİTESİ

Kurumlar için, vermekte oldukları hizmetleri herhangi bir nedenden dolayı veremez duruma gelmek önemli sorunlara yol açabilmektedir. Bu nedenle, oluşabilecek sorunlar için önceden tedbirler almak ve risk yönetimi oluşturmak gerekmektedir.[475] Bu planlamada öncelikle olası riskler ve bu riskleri ortadan kaldırmak için alınması gereken tedbirler ile her türlü tedbire rağmen bu risklerin gerçekleşmesi durumunda yaratacağı etkilere rağmen hizmet sürecinin aksamadan nasıl devam ettirileceği çözümlenmelidir.[476] Bu amaçla olası bir felaket durumunda dahi üniversite bilişim hizmetlerini kesintisiz yürütebilmek amacı ile bilgi işlem birimi tarafından Felaket Kurtarma Merkezi ve İş Sürekliliği Projesi hayata geçirilmiştir.[477] Bu proje kapsamında, hem mevcut depolama alanı genişletilmiş hem de verilerin tek bir depolama alanında meydana gelebilecek arızalardan kaynaklanacak kayıplarını ortadan kaldırmak amacıyla sistem odaları birbirinin yedeği olarak çalışacak şekilde yeniden yapılandırılmıştır. Bu sayede hem daha fazla veri alanı hem de veri yedekliliği sağlanmıştır. Bu bağlamda toplam kapasite, iki yüz yirmi TB'ye yükseltilmiştir. Proje kapsamında yapılan çalışmalar şu şekildedir:

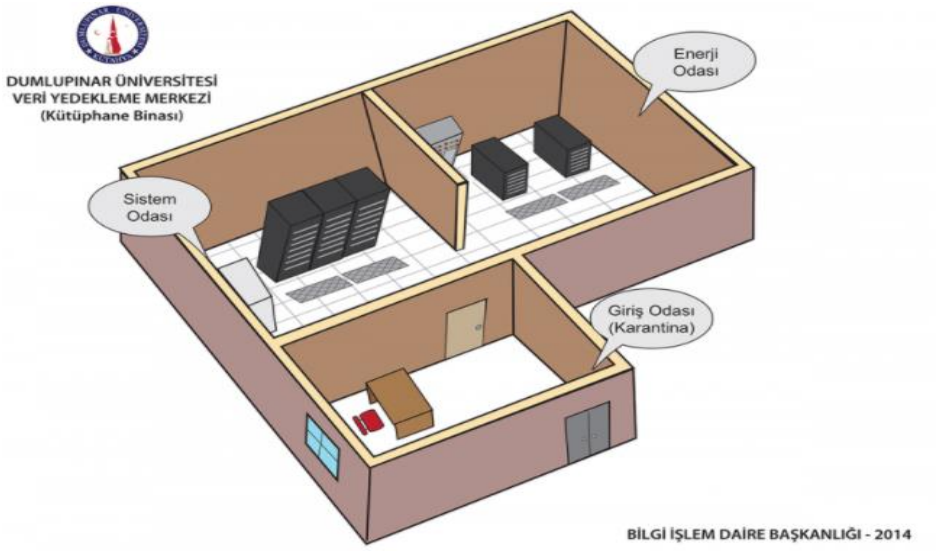
- Rektörlük binasındaki mevcut sistem ve enerji odalarının yeniden düzenlenmesi
- Mevcut sistem odasındaki kabinet yapısının değiştirilerek fanus yapıya geçilmesi
- İklimlendirme ve enerji alt yapıları ve kablolama sisteminde gerekli değişiklikler yapılarak alttan soğutma sistemine geçilmesi
- Server (sunucu) ve veri depolama birimlerinin yedeklilikleri sağlanacak şekilde konumlandırılması.
- İki sistem odası arasındaki gerekli fiber altyapı çalışmalarının yapılması
- Her iki sistem noktasının aktif-aktif çalışır konuma getirilmesi.

[475] https://bidb.dpu.edu.tr/tr/index/slide/1130/sistem-odasi-felaket-kurtarma-merkezi-fkm-is-surekliligi-projesi (04.03.2021)
[476] a.g.k.
[477] a.g.k.

- Bu süreçte eski depolama alanındaki tüm veriler yeni depolama alanına taşınmıştır ve eski depolama alanı, yeni depolama alanındaki verilerin yedeklerinin muhafaza edildiği bir sistem hâline dönüştürülmüştür. Şekil 4.2 ve 4.3'te sırasıyla ana ve ikincil veri merkezleri gösterilmektedir.



Şekil 4.2 Rektörlük Binası Ana Veri Merkezi[478]



Şekil 4.3 Kütüphane Binası İkincil Veri Merkezi[479]

[478] https://bidb.dpu.edu.tr/tr/index/slide/1130/sistem-odasi-felaket-kurtarma-merkezi-fkm-is-surekliligi-projesi (04.03.2021)
[479] a.g.k.

4.4. DAİKİN

Daikin veri merkezleri ve IT servisleri için başarılı bir felaket kurtarma projesi yapmış işletmelerden biridir.[480] Daikin felaket kurtarma merkezi ihtiyacını İstanbul merkez ofisi dışında bulunan bir veri merkezinde sunucu kiralayarak çözümlemiştir. Ancak, yerel bir sağlayıcıdan aldığı bu hizmette diğer birçok kullanıcının yaşadığı sorunları yaşamıştır.[481]

Kiralama maliyeti, bant genişliklerinde yaşanan sıkıntılar, esnek altyapı imkânının olmaması, taleplerin hızlı bir şekilde karşılanamaması, tedarikçinin ek maliyet ve taahhüt talepleri sorunlardan sadece birkaçıdır.[482]

Azure[483] yazılımı ile tüm temel iş ihtiyaçları çok uygun bir maliyetle karşılanmaktadır.[484] Azure'un ASR (Azure Site Recovery) servisi ile Daikin, 10-12 saniye seviyelerinde RPO (Recovery Point Objective) değerlerine ve 3 dakika seviyesinde RTO (Recovery Time Objective) değerlerine sahip bir felaket kurtarma çözümüne sahip olmuştur.[485]

Azure'un yedekleme servisi ile Daikin, depolama alanı endişesi olmadan mevcut tüm verilerin yedeklenmesi çözümüne sahip olurken, geriye dönük yedek saklama sürelerindeki sınırlamalardan da kurtulmuştur.[486] Gelecekteki kapasite artırımları için sipariş, on-prem (sistem odasında yerinde) storage temini, kurulum vs. tüm iş yüklerinden kurtulmuştur.[487]

---

[480] Y. Akıllı, 2016, s. 48.
[481] a.g.e, s. 48.
[482] a.g.e, s. 48.
[483] Azure, Microsoft firmasına ait bulut yedekleme yazılım çözümüdür.
[484] a.g.e, s. 48.
[485] Microsoft Azure, Simit Sarayı Microsoft Azure ile Felaket Kurtarma Yönetimi Projesi, Microsoft Başarı Hikayeleri, 2015.
https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=1252 (24.01.2021)
[486] a.g.e, s. 48.
[487] a.g.k.

4.5. SİMİT SARAYI

Simit Sarayı, veri merkezi ve IT servisleri için başarılı bir felaket kurtarma projesi yapmış işletmelerden biridir.[488] Simit Sarayı, tüm üretim ve satış süreçlerinin kesintisiz çalışması için İstanbul merkez ofisi dışında farklı bir şehirde bulunan bir veri merkezinde sunucu kiralayarak felaket kurtarma ihtiyacını çözmüştür.[489]

Felaket kurtarma senaryosu ve geliştirme platformu için esnek ve çevik bir altyapıya ihtiyaç duyulmuştur. Seçilecek çözümün maliyet avantajı getirmesi de beklenmiştir.[490]

Azure (Microsoft Firması Bulut Yedekleme Yazılım Çözümü), kullanımının en büyük faydası Simit Sarayı'na sağladığı esneklik olmuştur. Sistem, Uygulama, Ürün (System, Application and Products-SAP) teknolojisi geliştirme ortamlarında ihtiyaç duyulan iş yükleri için gerekli altyapıyı dakikalar içinde sunulabilir duruma getirmiştir.[491]

Aynı şekilde Azure'un ölçeklenebilirliği de büyük fayda sağlamıştır. Projenin hayata geçmesinden önce dosya sunucularında departmanlar için kota uygulanmıştır fakat bulut entegre mimarisi sayesinde neredeyse sınırsız boyutta dosya sunucularına erişim mümkün olmuştur.[492]

Düşük ve ön görülebilen maliyetlendirme ile Felaket Önleme Merkezi kurulmuştur. Bu felaket önleme ortamı aynı zamanda tüm yapının yüksek

---

[488] Y. Akıllı, 2016, s. 47.
[489] a.g.e, s. 47.
[490] a.g.e, s. 47.
[491] a.g.e, s. 47.
[492] a.g.e, s. 47.

erişilebilirliğine (high availability) de büyük katkı sağlamıştır.[493] Birden fazla lokasyon üzerinde dosyaların ve hizmetlerin barındırılmasından dolayı kesinti riski neredeyse sıfıra inmiştir.[494]

Burada Microsoft'un Azure için sunduğu SLA'ler (Service Level Agreement) de çok önemlidir.[495] Güvenlik ve erişilebilirlik kriterleri, IT departmanının ISO (Uluslararası Standart Kuruluşu-International Standard Organization) 27001 Bilgi Güvenliği Yönetim Sistemi gibi süreçlere hazırlığında da fayda sağlamıştır. Yıllık Felaket Kurtarma Merkezi maliyetlerinin %30-40 arasında azalması beklenilmektedir.[496]

4.6. TÜRKSAT

İhtiyaç duyulması hâlinde TÜRKSAT tarafından sadece verilerin yedeklenebileceği ve veri yedeklemeyi esas alan bir yedekleme çözümü sunulmaktadır. Bu çözüm, düşük veri trafiğine sahip ve/veya bilişim alanındaki veri kaybı riskleri yüksek olan kurumlar için önerilmektedir.[497] Kurumlarının ihtiyaçları kapsamında, mevcut bilişim altyapıları, veri yedekleme, geri dönüş süresi ve hedef veri kayıpları ile risk analizleri yapılarak aktif / pasif olarak çalışacak, ölçeklendirilmiş kapasiteli felaket kurtarma merkezi projeleri sunulmaktadır.[498]

Bir kuruluşta olağanüstü durum; deprem, yangın, su basması, sabotaj, terörist saldırıları ve savaş hâli gibi nedenlerle bilişim sistemleri altyapısının kullanılamayacak

[493] Y. Akıllı, 2016, s. 47.
[494] a.g.e, s. 47.
[495] Microsoft Azure, Simit Sarayı Microsoft Azure ile Felaket Kurtarma Yönetimi Projesi, Microsoft Başarı Hikayeleri, 2015.
https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=1252 (24.01.2021)
[496] a.g.k.
[497] TÜRKSAT (2015), *Faaliyet Raporu*, Ankara.
[498] a.g.k.

derecede zarar görmesi sonucunda ilan edilebilir.[499] Olağanüstü durum ilanının ardından kurumun veya kuruluşun daha önceden hazırlanmış olan bir yerleşkeye olağanüstü durum öncesinde belirlenmiş bir plan doğrultusunda gidilmek suretiyle kritik iş süreçlerini yönetmesi, Olağanüstü Durum Yönetimi olarak ifade edilmektedir. e-Devlet Kapısı sistemleri, yedekli bir yapıda, sistem odalarında bulunmaktadır.[500] Sistemler, herhangi bir sorunla karşılaşılması durumunda, yedek üzerinden çalışacak şekilde tasarlanmıştır. Hâlihazırda Veri Merkezi ve Felaket Kurtarma Merkezi-FKM projeleri kapsamında, kurumlara veri yedekleme, fiziksel ve sanal sunucu barındırma, web sitesi barındırma ile aktif / pasif FKM çözümleri sunulmaktadır.[501]

Kurum içi kritik sistemler için Felaket Kurtarma Merkezi devreye alınmış ve ISO 22301[502] İş Sürekliliği Yönetim Sistemi kurularak işletilmeye başlanmıştır. Açık kaynak kodlu yazılımlar yaygınlaştırılmıştır.[503] Tüm sistemlerin 7/24 izlenilmesine e-Devlet Kapısı iletişim personeli ile devam edilmektedir. Fiziksel ve sanal sunucular, veri tabanları, veri depolama üniteleri ve işletim sistemlerinin güncelleme ve iyileştirme çalışmaları gerçekleştirilmiştir.[504]

4.7. FORD OTOSAN

Ülkemizde felaket kurtarma planlarını düzenli bir şekilde uygulayan ve bu konuda olumlu sonuçlar elde eden firmalar bulunmaktadır.[505] Ford Otosan "Felaket Kurtarma" ve "İş Sürekliliği Projesini" gerçekleştirmek için önceden bir plana sahip olan ve bu konuda büyük başarı gösteren kurumlardan bir tanesidir.[506] Uygulanan

[499] TURKSAT (2015), *Faaliyet Raporu,* Ankara.
[500] a.g.k.
[501] a.g.k.
[502] Türk Standartları Enstitüsü-TSE tarafından belgelendirilmesi yapılan, iş sürekliliğinin oluşturulması, uygulanması, gözden geçirilmesi, devamlılığının sağlanması ve iyileştirilmesi için risk yaklaşımını esas alan bir yönetim sistemi standardıdır.
[503] a.g.k.
[504] a.g.k.
[505] Yrd. Doç. Dr. Atik Kulaklı, Serpil Aslan, "İşletmelerde Bilgi Teknolojilerindeki Gelişmelerin İşletme ve Yönetim Fonksiyonları Üzerine Etkileri*", Sosyal Bilimler Dergisi*, Cilt 4, Sayı 1, 2010, s. 1-16.
[506] a.g.m, s. 1-16.

projede öncelikle kurumun sahip olduğu yetkili satıcı ağı, yan sanayi ağı ve Türkiye‟nin dört farklı yerleşiminde (Acıbadem, Kartal, Eskişehir, Kocaeli) yer alan fabrika ve operasyon merkezi ile büyük bir veri ağına sahip olan Ford Otosan'ın, dağınık yapıda yer alan verilerinin konsolide edilmesi, tek merkezden yönetilmesi, güvenliğinin ve sürekliliğinin sağlanması amacı ile "Felaket Kurtarma" ve "İş Sürekliliği" projesini başlatılmıştır.[507] Proje kapsamında yapılan çalışmalar şunlardır[508]:

- Geniş alan ağları, yerel alan ağları ve sistem odaları yedeklenmiştir. Bu yedekleme, merkezi bir yedekleme çözümü olan depolama alan ağı üzerinden yapılmıştır. Böylece yerel alan ve geniş alan ağındaki tüm sunucular var olan depolama alan ağına bağlanmış ve oradanda bu ağa bağlı olan yedekleme kütüphanesine aktarılmıştır.
- Hata düzeltme ve süreklilik yeteneğinin artırılması sağlanmıştır. Bunun için kurum, Redundant Array of Inexpensive Disks-RAID teknolojisinden faydalanarak sahip olduğu disklerde meydana gelebilecek arızalara karşı önceden önlem almıştır.
- Konsolide edilmiş verinin ayrıca yedeklenmesiyle hedeflenen mimari tamamlanmıştır.

Projenin firmaya sağladığı faydalar şunlardır[509]:

- Veri tabanları konsolide edilmiş ve performans artırılmıştır.
- Dağınık veri konsolide edilmiştir.
- Verinin senkron ve asenkron yedeklenmesi sağlanmıştır. Burada replikasyon yöntemi ile veri senkron ve asenkron olarak farklı bir lokasyona aktarılarak üretim verisinin bir başka lokasyonda bulundurulması hedeflenmiştir. Böylece firma üretim lokasyonunda oluşabilecek herhangi bir felakete karşı önlem almıştır

[507] Yrd. Doç. Dr. Atik Kulaklı, Serpil Aslan, "İşletmelerde Bilgi Teknolojilerindeki Gelişmelerin İşletme ve Yönetim Fonksiyonları Üzerine Etkileri*", Sosyal Bilimler Dergisi*, Cilt 4, Sayı 1, 2010, s. 1-16.
[508] a.g.m, s. 1-16.
[509] a.g.m, s. 1-16.

SONUÇ VE ÇÖZÜM ÖNERİLERİ

Günümüzde bilişim sistemleri kurum ve kuruluşların iş süreçlerinin ayrılmaz parçası hâline gelmiştir. Kurum ve kuruluşlar iş süreçlerine devam edebilmek için bilişim sistemlerinin sağlıklı çalışmasını devam ettirmesine ihtiyaç duymaktadır. Gelinen noktada bilişim sistemlerinin düzgün ve istikrarlı çalışmasını tehdit eden birçok olay meydana gelmektedir. Literatürde felaket olarak adlandırılan bu olayların önüne geçebilmek adına kurum ve kuruluşların bilişim sistemleri özelinde almaları gereken birtakım tedbirler ve icra edilmesi gereken teknolojik uygulamalar bulunmaktadır. Bu tedbir ve uygulamaların tatbiki, etkin ve doğru bir felaket kurtarma yönetimi ile gerçekleştirilebilmektedir.

Bilişim sistemlerinin düzgün ve istikrarlı çalışmasını temin eden felaket kurtarma, iş sürekliliği disiplininin temel gereklerinden birini oluşturmaktadır. Aşağıda etkin ve doğru bir felaket kurtarma yönetimini uygulayabilmek noktasında tez boyunca yapılan incelemeler doğrultusunda edinilen bilgi ve tecrübeye dayanarak çözüm önerileri sıralanmıştır. Buna ek olarak bilişim sistemleri altyapısını haiz bir kamu kurumu olarak Radyo ve Televizyon Üst Kurulu özelinde bir felaket kurtarma değerlendirmesi yapılmıştır.

Çözüm Önerileri

- Kurum ve kuruluşların bilişim bölümleri tarafından, felaket kurtarma yönetimini icra etmek üzere felaket kurtarma yönetim ekibi ve felaket kurtarma operasyon ekibi üyeleri olası felaketler ortaya çıkmadan önce bilişim uzmanı personel arasından seçilmeli, bilişim sistemleri göz önüne alınarak yapılacak planlamalar ile ilgili personelin görev ve sorumlulukları netleştirilmelidir.
- Felaket kurtarma yönetim ve felaket kurtarma operasyon ekibi üyeleri sorumlu oldukları bilişim sistemleri ile ilgili iyi derecede eğitim almış ve yeterli tecrübeye sahip kişiler arasından, kurum ve kuruluşların bilişim bölümleri tarafından yeterli

sayıda seçilmelidir. Bilişim sistemlerinin hızlı değişimi karşısında, sorumlu personelin teorik ve pratik olarak güncel kalması sağlanmalıdır.

- Felaket kurtarma yönetim ve operasyon ekibi tarafından yapılacak çalışmalarda bilgi sistemleri ortam izleme araçları doğru yapılandırılmalı, güncellemeleri düzenli takip edilmeli ve iyi derecede eğitim almış uzman personel tarafından olağan dönem ve felaket dönemlerinde veri merkezi bilgi sistemlerinde olası meydana gelecek arıza, hata ve durumlar düzenli bir şekilde takip edilmelidir.
- Felaket kurtarma yönetim ve operasyon ekiplerince, kurum ve kuruluşlar açısından iş sürekliliğini etkileyecek afet ya da acil durum kaynaklı olası riskler belirlenerek risk değerlendirmesi yapılmalıdır. Olayın türüne bağlı olarak hangi önlemlerin alınacağı ve kaynakların gerekli olacağı konusunda strateji belirlenmelidir.
- Sanallaştırma teknolojisinin yönetimsel kolaylıklar, fiziksel karmaşa, hız konusunda getirmiş olduğu avantajlar ve olası felaket durumlarında meydana gelebilecek fiziksel kazaları elimine ederek olası felaketlerin vereceği zararları asgari düzeye indirme açısından sağlamış olduğu faydalar sayesinde bilişim sistemleri, teknik imkânlar ölçüsünde sanallaştırılarak söz konusu sistemlerin donanım bağımsız olması sağlanmalıdır.
- Kurumsal sunucu sistemleri sanallaştırılmalıdır.
- Kurumsal veri depolama sistemi (storage) altyapısı sanallaştırılmalıdır.
- Kurumsal veri iletişim ağı (network) altyapısı sanallaştırılmalıdır.
- Ana veri merkezinde meydana gelecek olası felaketlerde bilgi sistemlerinin ve iş sürekliliğinin sağlıklı çalışmasını temin etmek maksadı ile bilişim sistemlerinin coğrafi mekân yedekliliği sağlanmalıdır.
- Bilgi sistemleri coğrafi mekân yedekliliğini sağlamak, veri yedeklerinin tutulmasını sağlamak, birincil veri merkezine eşgüdümlü alternatif görev ifa etmek amacı ile ana veri merkezinin konumundan coğrafi olarak farklı bir konumda bulunmak üzere Felaket Kurtarma Merkezi-FKM niteliğine haiz ikincil bir veri merkezi kurulmalıdır.
- İkincil veri merkezi (Felaket kurtarma merkezi-FKM) veri iletişim ağı altyapısı, mimari, elektrik ve konsept dizaynları, enerji altyapısı, iklimlendirme sistemi, fiziksel güvenliği, yangın algılama ve söndürme sistemi, doğal afetlere karşı alınan önlemler, ortam izleme sistemi, yükseltilmiş döşeme sistemleri ve kablo kanalları

TÜBİTAK'ın 2017 yılında hazırlamış olduğu Felaket Kurtarma Merkezi Kurulumu Rehberi[510] dikkate alınarak tasarlanmalıdır.

- Felaket kurtarma yönetim ve operasyon ekiplerince, olası felaket durumlarında uygulanmak üzere, kurum ve kuruluşların sahip oldukları bilişim sistem ve uygulamaları baz alınarak bu sistem ve uygulamaların hangi noktaya dönülürse bunun ilgili kurum için azami tolere edilebilir olduğunun saptanması amacıyla Felaket Kurtarma Noktası (Recovery Point Objective) tablosu belirlenmelidir.
- Felaket kurtarma yönetim ve operasyon ekiplerince, olası felaket durumlarında uygulanmak üzere, kurum ve kuruluşların sahip oldukları bilişim sistem ve uygulamalarını baz alarak bu sistem ve uygulamaların azami tolere edilebilir yeniden ayağa kalkma sürelerinin saptanması amacıyla Felaket Kurtarma Süresi (Recovery Time Objective) tablosu belirlenmelidir.
- Felaket kurtarma yönetim ve operasyon ekiplerince, olası felaket durumlarında uygulanmak üzere, bilişim sistem ve uygulamalarının etki alanları ve felaket durumunda kurtarılma öncelikleri dikkate alınarak İş Etki Analizi tablosu belirlenmelidir.
- Felaket kurtarma yönetim ve operasyon ekiplerince, olası felaket durumlarında uygulanmak üzere, bilişim sistem ve uygulamalarının felaket kurtarma süresi ve felaket kurtarma noktası değerlerine ve İş Etki Analiz tablosundaki değerlere göre önceliklendirilmesiyle elde edilen Sistem Kurtarma Öncelik Listesi belirlenmelidir.
- Bilgi sistemlerinde sanal sunucu planlaması yapılırken kritik servislerin hizmet verdiği sunucu sistemlerinde yedekliliği sağlamak ve sunucu kümesi içerisindeki herhangi bir sunucunun olası felaketlerden etkilenerek çalışamaz duruma gelmesi karşısında yük devretmeyi aktif ederek bilgi sistemlerinin ve iş sürekliliğinin sürdürülebilirliğini temin etmek için sunucu kümeleme teknolojisi uygulanmalıdır.
- Olağan dönemde farazi felaket senaryoları hazırlanarak felaket kurtarma tatbikatları yapılmalıdır.
- Yedeklemeden sorumlu felaket kurtarma yönetim ve operasyon ekibi üyelerince, kurum ve kuruluşların bilişim sistem ve uygulamalarının önem derecesi göz

[510] TÜBİTAK (2017), *Felaket Kurtarma Merkezi Kurulumu Rehberi*, Ankara.

önünde tutularak kurumsal veri yedekleme politikası belirlenmelidir ve kurumsal veri yedekleme politikasına göre veri yedeklerinin günlük, haftalık, aylık olmak üzere hem ana veri merkezinde hem de ikincil veri merkezinde hatasız olarak alınmasının kontrolü, günlük yedekleme raporları ile sağlanmalıdır.

- Yedeklemeden sorumlu felaket kurtarma yönetim ve operasyon ekibi üyelerince, kurum ve kuruluşların bilişim sistem ve uygulamalarının önem derecesi göz önünde tutularak kurumsal veri geri yükleme politikası belirlenmelidir ve olağan dönemde gerçekleştirilecek veri geri yükleme testleri ile felaket durumunda hedeflenilen felaket kurtarma süresi ve felaket kurtarma noktası değerlerine ulaşmak için belirleyici role sahip yedekleme yazılımı, ana ve ikincil veri merkezleri arası veri iletişim ağı altyapısı hat hızı gibi etkenlerin seçimi doğru yapılmalıdır.
- Olası felaket durumlarında, bilişim sistemlerinin tekrardan işlevsel hâle gelmesi için yedeklemeden sorumlu felaket kurtarma yönetim ve operasyon ekibi üyelerince, kurum ve kuruluşların kurumsal veri yedekleme politikaları sonucunda alınmış olan veri yedekleri üzerinden veri geri yükleme süreçleri, sistem kurtarma öncelik listesine göre devreye alınarak gerekli sanal sunucu ve dosya düzeyinde geri yüklemeler/kazanımlar gerçekleştirilmelidir.

Radyo ve Televizyon Üst Kurulu Bağlamında Felaket Kurtarmanın Değerlendirilmesi ve Öneriler

Günümüzde özel sektörde ya da kamu sektöründe olması fark etmeksizin kurumsal yapıyı haiz kurum ve kuruluşlar gibi düzenleyici ve denetleyici bir kamu kurumu olan Radyo ve Televizyon Üst Kurulu da iş süreçlerini yürütürken bilişim sistemlerini geniş ölçüde kullanmaktadır. Bilişim sistemlerinin çalışmasında meydana gelecek muhtemel aksaklıklar, iş süreçlerinin kesintiye uğramasına sebebiyet verecektir. Bu itibarla; Radyo ve Televizyon Üst Kurulu, kurum bilişim sistemlerinin sağlıklı olarak çalışmasını temin etmek durumundadır. Kurum bilişim sistemlerinden sorumlu personel, felaket kurtarma yönetim ve operasyon ekibi olarak rol alıp felaket durumlarında harekete geçebilecektir. Felaket kurtarma ve yönetim ekip üyeleri

belirlenmeli, ekip üyelerinin rol ve sorumlulukları net olarak tanımlanmalıdır. Anılan ekiplerce farazi anlamda felaket kurtarma tatbikatları gerçekleştirilmesi felaketlere hazırlık aşamasında yerinde olacaktır.

Kurum bilişim sistemleri sorumlu personelce ortam izleme araçları ile izlenmektedir ve bu sayede kesinti ile arızalara karşı ivedi müdahale imkânı bulunmaktadır. Kurumun coğrafi konumu da dikkate alınarak kurum için risk değerlendirmesi yapılmalı ve olası felaketler belirlenmelidir. Olası felaket durumlarında felaket kurtarma yönetim ve operasyon ekiplerine felaket yönetiminde rehberlik etmek üzere tezin içerisinde hazırlanmış olan felaket kurtarma noktası, felaket kurtarma zamanı, iş etki analizi ve sistem kurtarma öncelik listesi tablolarından yola çıkılarak kurum bilişim sistemleri için söz konusu değerler belirlenmelidir.

Kurum sunucularının tamamına yakınının ve veri depolama sisteminin sanallaştırılmış olması felaket kurtarma anlamında fayda sağlayan uygulamalar olup olası felaketler karşısında kurumun elini güçlendirmektedir. Fiziksel sunucuların ikincil bir lokasyonda eş donanım yedekliliğinin sağlanması faydalı olacaktır. Bunun yanında ikincil bir veri merkezi kurularak felaket kurtarma merkezi olarak hizmet vermesi, felaket kurtarma anlamında doğru bir uygulama olacaktır.

Kurum bilişim sistemlerinde veri yedekleri günlük, haftalık ve aylık olarak alınmaktadır. Yedekler, yerinde (kurum içi) alındığı gibi kurum dışı ortama da gönderilmektedir. Yedekleme sistemi üzerinden kurum dışına veri yedeklerinin gönderilmesi; geri yükleme işlemleri aracılığı ile veri ve uygulama bazında normal çalışma seyrine dönülmesini mümkün kılmaktadır. İkincil veri merkezi ve donanım yedekliliği sağlanarak yedeklerin anlık alınması ve ikincil veri merkezine gönderilmesi, felaket kurtarma süresi ve felaket kurtarma noktası değerlerinin optimum düzeye gelmesine ve çok kısa süreler içinde bilişim sistemlerinin normal seyrine dönmesine olanak tanıyacaktır.

KAYNAKÇA

Yıldırım, Ali, Şimşek, Hasan (2013), *Sosyal Bilimlerde Nitel Araştırma Yöntemleri*, Seçkin Yayınları, Ankara.

Akıllı, Yasin (2016), *Sanal Sunucu Sistemlerinde Felaket Kurtarma Yönetimi ve Felaket Kurtarma Plan Önerisi*, İstanbul Aydın Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi, İstanbul.

Akpınar, Haldun (2009), *Enformasyon Teknolojilerinde İş Sürekliliği Yönetimi ve Felaket Planlaması*, İstanbul Teknik Üniversitesi Yayını, İstanbul.

Bahan, Chad (2003), *The Disaster Recovery Plan*, SANS Institute Press, ABD.

Brotherton, Heather M. (2011), *Data Center Recovery Best Practises:Before, During and After Disaster Recovery Execution*, Purdue University, Yüksek Lisans Tezi, Indiana.

Cresswell, John W. (2005), *Educational research: Planning, conducting, and evaluating quantitative*, Prentice Hall Upper Saddle River, New Jersey.

Garfinkel, Simson, Spafford, Gene, Schwartz, Alan (2003), *Practical UNIX and Internet security*, O'Reilly Media, Inc., ABD.

Gerace, Thomas, Jean, Raymond, Krob, Adam (2007), "Decentralized and centralized it support at Tulane University: a case study from a hybrid model", *SIGUCCS 07*, Proceedings of the 35th Annual ACM SIGUCCS Fall Conference, Florida ABD.

Hayes, Bob, Kotwica, Kathleen (2013), *Business Contiunity:Playbook*, Elsevier Inc, ABD, 2013.

Hinca, Martin (2006), *Business Contiunity and Disaster Recovery for IS*, Masarykova Univerzita Fakulta Informatiky, Lisans Tezi, Çek Cumhuriyeti.

Jayaraman, Arunkumar, Rayapudi, Parankumar (2012), *Comparative Study of Virtual Machine Software Packages with Real Operating System*, Blekinge Tekniska Högskolva, Yüksek Lisans Tezi, İsveç.

Jorrigala, Vyshnavi (2017), *Business Contiunity and Disaster Recovery Plan for Information Security Rebublic, St. Cloud State University*, Yüksek Lisans Tezi, Minnesota.

İnce, Kenan, İnce, Cemile, Topal, Ahmet, Çiçekli, M. Tahir, Adanur, Kerem ve Kuzu, Bünyamin (2020), "Bilişim Altyapı Sistemi Yenileme Çalışması: İnönü Üniversitesi Örneği", *Anatolian Journal of Computer Sciences*, Cilt 5, Sayı 1, s. 54-61.

Kazım Özdamar (2003), *Modern Bilimsel Araştırma Yöntemleri*, Kaan Kitabevi, Eskişehir.

Krane, N. Kevin, Kahn, Marc J., Markert, Ronald J., Whelton, Paul K., Traber, Peter G., Taylor, Ian L. (2017), "*Surviving Hurricane Katrina: Reconstructing the Educational Enterprise of Tulane University School of Medicine*", *Tulane University School of Medicine*, Cilt 82, Sayı:8, s. 757-762 .

Kulaklı, Atik, Aslan, Serpil (2010), "İşletmelerde Bilgi Teknolojilerindeki Gelişmelerin İşletme ve Yönetim Fonksiyonları Üzerine Etkileri", *Sosyal Bilimler Dergisi*, Cilt 4, Sayı 1, s. 1-16.

Lawson, John (2005), "A Look Back at a Disaster Plan: What Went Wrong and Right", *Information Technology Supplement*, Cilt 52, Sayı 16.

Lenk, A., Tai, S. (2014),"Cloud standby: disaster recovery of distributed systems in the cloud", European Conference on Service-Oriented and Cloud Computing, Eylül 2014, *Springer Berlin Heidelberg*, Berlin.

Yıldız, Mehtap (2005), *Araştırmalarda Kaynak Tarama Yöntemleri*, Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Somesekaram, Premathas (2017), *A Component-Based Business Contiunity and Disaster Recovery Framework*, Uppsala Universitet, Department Of Information Technology, Yüksek Lisans Tezi, İsveç.

Pritz, Florian (2016), *Concept of a Server Based Open Source Backup Process with an Emphasis on IT Security*, TU Viyana Faculty of Informatics, Lisans Tezi, Viyana.

Rittinghouse, John W., Ransome, James F. (2005), *Business Contiunity and Disaster Recovery for InfoSec Managers*, Elsevier Digital Press, Birleşik Krallık.

Roy, M. K., Dastidar, D.G. (1983), *Cobol Programming*, McGraw-Hill Education, ABD.

Snedaker, Susan (2007), *Business Contiunity and Disaster Recovery Planning For IT Professionals*, Syngress Publishing Inc., ABD.

TÜBİTAK (2017), *Felaket Kurtarma Merkezi Kurulumu Rehberi*, Ankara.

TÜRKSAT (2015), *Faaliyet Raporu*, Ankara.

Üzümcü, Özlem (2016), "Nitel Araştırma Yöntemine Sahip Tezlerin Bazı Değişkenler Açısından İncelenmesi", *Akademik Sosyal Araştırmalar Dergisi*, Cilt 4, Sayı 32, 2016, s. 327-340.

Vasak, Jaroslav (2017), *Analysis of Backup for Small and Medium-sized Enterprises (SME) in the Czech Rebublic*, Czech Technical University Faculty of Information Technology, Yüksek Lisans Tezi, Prag.

Yarrapothu, Sindhura (2015*), Effectiveness of Backup and Disaster Recovery in Cloud*, Blekinge Institute of Technology Faculty of Computing, Yüksek Lisans Tezi, İsveç.

Zrnec, Aljaz, Lavbič, Dejan (2011), "*Comparison of Cloud vs. Tape Backup Performance and Costs with Oracle Database", Journal of Infomation and Organizational Sciences*, Sayı:26, No:1, s. 135–142.

ELEKTRONİK KAYNAKLAR

https://www.imperva.com/learn/availability/disaster-recovery/ (05.10.2020)

https://www.vmware.com/topics/glossary/content/disaster-recovery (13.08.2020)

https://www.inap.com/blog/business-continuity/ (12.09.2020)

https://www.nakivo.com/blog/overview-disaster-recovery-sites/) (08.10.2020)

https://www.seguetech.com/three-stages-disaster-recovery-sites/ (10.10.2020)

https://www.barracuda.com/glossary/disaster-recovery (07.11.2020)

https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery (13.10.2020)

https://www.ibm.com/support/knowledgecenter/SSGSG7_7.1.0/com.ibm.itsm.srv.doc/c_tier3.html (12.06.2020)

http://www.clarecomputer.com/pdf/CCS_e-book_BusinessContinuity_DR.pdf (12.09.2020)

https://www.gartner.com/en/information-technology/glossary/bia-business-impact-analysis (23.10.2020)

https://www.mayerbrown.com/public_docs/events/bank_12Jun03_DisasterRecovery.pdf (04.09.2020)

https://scialert.net/fulltext/?doi=jai.2013.60.67 (06.08.2020)

https://www.gowhiteowl.com/blog/virtualization-benefits-disaster-recovery/ (13.07.2020)
https://www.vmware.com/topics/glossary/content/servervirtualization?SRC=WWW_US_GP_virtual-machine_SiteLink (03.12.2020)
https://www.vmware.com/topics/glossary/content/networkvirtualization?SRC=WWW_US_GP_virtual-machine_SiteLink (03.12.2020)
https://solutionsreview.com/backup-disaster-recovery/tape-based-disk-based-and-cloud-based-backup-how-do-you-choose/ (12.06.2020)
http://www.everspan.com/wpcontent/uploads/2016/04/ODA_Gen2_WhitePaper_20160408_English.pdf (14.07.2020)
http://support.unitrends.com/ikm/questions.php?questionid=980 (12.09.2020)
http://www.encyclopedia.com/computing/dictionariesthesauruses-pictures-and-press-releases/full-backup (18.06.2020)
http://www.techworld.com/storage/what-are-synthetic-backups-1149/ (03.10.2020)
http://www.webopedia.com/TERM/S/synthetic_backup.html (01.10.2020)
http://typesofbackup.com/local-backup/ (13.01.2021)
https://social.technet.microsoft.com/wiki/contents/articles/206.backup-and-restore-classification-ofscenarios.Aspx (17.11.2020)
http://searchdatabackup.techtarget.com/definition/image-based-backup (11.12.2020)
https://storageswiss.com/2014/12/16/what-is-hybrid-cloud-backup (09.10.2020)
http://www.availabilitydigest.com/public_articles/0510/virginia.pdf (03.09.2020)
http://www.cdc.gov/mmwr/preview/mmwrhtml/mm51spa6.htm (12.09.2020)
http://searchstorage.techtarget.com/tip/0,289483,sid5_gci808783,00.html (13.01.2021)
http://h71000.www7.hp.com/openvms/brochures/commerzbank/commerzbank.pdf?jumpid=reg_R1002_USEN (26.01.2021)
https://theengineeringmindset.com/data-center-hvac-cooling-systems/ (18.12.2020)
http://www2.openvms.org/kparris/Bootcamp_2010_Disasters_Part2_Organizations.pdf (12.02.2021)
www.egenera.com/1157984790/Link.htm (12.11.2020)
http://www.blackboard.com/CMSPages/GetFile.aspx?guid=39a0b112-221d-4d04-be80-f2024d16943a (23.12.2020)

https://www.vox.com/2015/8/23/9191907/hurricane-katrina (19.11.2020)
http://issue.com/thebooksmithgroup/docs/tulane (22.02.2021)
http://www.computerworld.com/s/article/print/314109/Tulane_University (07.01.2021)
http://espanol.siemon.com/sis/storage-area-networks/ (20.07.2020)
http://www.wvec.com/news/local/Northrop-Grumman-to-pay-for-computeroutageinvestigation-102796459.html (30.11.2020)
http://www.vita.virginia.gov/communications/publications/networknews/default.aspx?id=12906 (23.10.2020)
http://www.vita.virginia.gov/library/default.aspx?id=545 (26.10.2020)
https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=1252 (24.01.2021)
https://faq.cc.metu.edu.tr/tr/sss/felaket-kurtarma-merkezi-ve-surekliligi-nasil-saglanmaktadir (03.01.2021)
https://bidb.dpu.edu.tr/tr/index/slide/1130/sistem-odasi-felaket-kurtarma-merkezi-fkm-is-surekliligi-projesi (04.03.2021)

ÖZET

Günümüzde, kurumsal ölçekte çok büyük miktarda veri üretilmektedir. Üretilen bu verilere ihtiyaç olduğu anda ulaşılabilmesi ve üzerinde işlemler yapılabilmesi için bu verilerin çok iyi bir şekilde korunması gerekmektedir. Teknolojinin gelişmesiyle ve buna paralel olarak kullanılan verinin gittikçe artmasıyla, birçok kurum ve kuruluş kendileri için hayati derecede önem taşıyan operasyonların ve sahip oldukları verilerin muhafaza edilmesini bilişim sistemleri yoluyla gerçekleştirmektedir.

Bilişim sistemi tabanlı, iş süreçlerini sekteye uğratan ya da sistemlere erişilmesini engelleyen olaylar; felaket olarak adlandırılmaktadır. Bilişim sistemlerinin, her an felaketlere maruz kalma olasılığı bulunmaktadır. Kurum ve kuruluşların felaketlerle karşılaşmaları hâlinde iş sürekliliklerinin sağlıklı bir şekilde devam etmesi için etkili bir felaket kurtarma yönetimini gerçekleştirme noktasında kurumsal farkındalık ve hazırlık gerekmektedir.

Bu çalışmanın amacı, kurum ve kuruluşlar özelinde felaket kurtarma ve iş sürekliliği kavramları konusunda farkındalık oluşturmaktır. İş sürekliliğinin bir parçası olmakla birlikte nihai hedefi bilişim sistemlerinin sıfır kesinti ile çalışma devamlılığını temin etmek olan felaket kurtarma yönetimi konusunda yapılması gereken hazırlıklar ve tedbirlere yer verilecektir. Aynı zamanda felaket kurtarma konusunda ülkemizde ve dünyada gerçekleştirilmiş uygulamalara ve örneklere de yer verilecektir.

Anahtar Kelimeler: Felaket kurtarma, bilişim sistemleri, iş sürekliliği.

ARŞİV Kayıt Bilgileri

Tezin Adı	Bilgi İşlem Merkezlerinde Kurumların İş Sürekliliği Açısından Önem Arz Eden Felaket Kurtarmanın İncelenmesi ve Çözüm Önerileri
Tezin Yazarı	Ahmet Can ÖZDEMİR
Tezin Danışmanı	İbrahim ESER
Tezin Konumu	Uzmanlık Tezi
Tezin Tarihi	Nisan 2021
Tezin Alanı	Bilişim Teknolojileri
Tezin Yeri	RTÜK – ANKARA
Anahtar Kelimeler	Felaket kurtarma, bilişim sistemleri, iş sürekliliği.

ABSTRACT

Today, a huge amount of data is produced on an institutional scale. These data must be well protected so that these data can be accessed when needed and can be processed. With the development of technology and the increasing amount of data used in parallel with this, many institutions and organizations are using information systems to preserve the operations that are vitally important to them and the data they have.

Information system-based events that interrupt business processes or prevent access to systems; It is called a disaster. Information systems are likely to be exposed to disasters at any time. In the event that institutions and organizations encounter disasters, awareness and preparation are required to realize an effective disaster recovery management so that their business continuity continues in a healthy way.

The purpose of this study is to raise awareness about disaster recovery and business continuity concepts specific to institutions and organizations. With being a part of business contiunity, the necessary preparations and measures will be included in disaster recovery management, whose ultimate goal is to ensure the continuity of information systems with zero interruption. At the same time, practices and examples of disaster recovery in our country and in the world will be included.

Keywords: Disaster recovery, information systems, business contiunity.

ÖZGEÇMİŞ

Ahmet Can ÖZDEMİR, 1991 yılında Mersin'in Tarsus ilçesinde dünyaya gelmiştir. İlkokul, ortaokul ve liseyi Tarsus'ta tamamlamıştır. Ardından Sakarya Üniversitesi Bilgisayar ve Bilişim Bilimleri Fakültesi Bilgisayar Mühendisliği bölümünden 2015 yılında mezun olmuştur. Bir süre Millî Eğitim Bakanlığına bağlı Kasım Ekenler Mesleki ve Teknik Anadolu Lisesinde öğretmenlik görevini ifa etmiştir. Ardından Radyo ve Televizyon Üst Kurulunun açmış olduğu yarışma sınavında başarılı bulunarak 2018 yılı şubat ayında Üst Kurul Uzman Yardımcısı olarak göreve başlamıştır.

Evli olan Ahmet Can ÖZDEMİR, iyi derecede İngilizce bilmektedir.