

FEN BİLİMLERİ ENSTİTÜSÜ
BİLİŞİM SİSTEMLERİ ANABİLİM DALI



YENİ NESİL VERİ MERKEZİ TASARIMI VE KURULUMU
AŞAMASINDAKİ GEREKSİNİMLERİ

YÜKSEK LİSANS TEZİ

ONUR MORAL

tarafından

YÜKSEK LİSANS

derecesi şartını sağlamak için hazırlanmıştır.

Haziran 2016

Program: Bilişim Sistemleri

YENİ NESİL VERİ MERKEZİ TASARIMI VE KURULUMU AŞAMASINDAKİ
GEREKSİNİMLERİ

YÜKSEK LİSANS TEZİ

ONUR MORAL

tarafından

OKAN ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Bilişim Sistemleri Anabilim Dalına

YÜKSEK LİSANS

derecesi şartını sağlamak için sunulmuştur.

Onaylayan Jüri:

Prof. Dr. Ahmet Faik KAŞLI
Danışman

Prof. Dr. Ahmet Mesut RAZBONYALI
Üye

Yrd. Doç. Dr. Nurşen TOPÇUBAŞI
Üye

Haziran 2016

Program: Bilişim Sistemleri

KISA ÖZET

Bu tez çalışması ile veri merkezleri ile ilgili doğru bilinen yanlışların düzeltilmesi, bilinen doğruların kaynakları ile birlikte açıklanması, bilgi teknolojileri ile ilgili standartların incelenerek veri merkezleri için ihtiyaç olan standartların belirlenmesi, ihtiyaç analizlerinin doğru yapılması ve işletmelerin veri merkezi edinim süreçlerinde dönüşü olmayan hatalara düşmelerinin engellenmesi hedeflenmektedir. Özellikle veri merkezi kurulumu, veri merkezi yer seçimi, yönetimi ve sürdürülebilir olarak kullanımı gibi konularda yeterli seviyede bulunmayan Türkçe kaynak ihtiyacına katkıda bulunmak amaçlanmaktadır.

Bu tezde veri merkezlerinin tarihi gelişimi, türleri belirtilmekte, veri merkezleri kapsamında olması ve dikkat edilmesi gereken; sanallaştırma teknolojisi, veri merkezlerinde kullanılan standartlar ve bu standartların denetlenmesi, veri merkezi yer seçimi, tasarımı ve altyapısı, veri merkezi sürekliliği, bakımı ve tatbikatları anlatılarak bu gerekliliklerin uygulandığı veri merkezleri örnek olarak verilmektedir.

İşletmelerin iş hacimleri ve bilgi sistem ihtiyaçları doğrultusunda sınıflandırmaları yapılmış, yapılan bu sınıflama doğrultusunda her sınıf için gerekli veri merkezi çözümlerinin bileşenleri ve standartları belirlenmiştir.

Anahtar Kelimeler: Veri Merkezi, Veri Merkezi Planlama, Veri Merkezi Tasarımı, Veri Merkezi Verimliliği, Veri Merkezi İş Sürekliliği, Veri Merkezi Standartları.

ABSTRACT

The thesis objectives are delete wrong information in ideas and teach correct facts, observe IT standards and decide to data center standardize, analyze of data center necessities, prevent the worst situation of company. Especially, the thesis provides article in Turkish regarding data center main subjects.

In the thesis, data center development progress, data center types, virtualization, standardize and audits, location choosing for data center, data center design and infrastructure, backup and business continuity and also practice and maintenances of data center are mentioned as very detail in the thesis in professional frame.

Some real data centers serve as model in this thesis.

Companies are classified in the thesis according their business load and make a decision suitable data center necessary for the companies.

Keywords: Data Center, Data Center Planning, Data Center Design, Data Center Efficiency and Optimization, Data Center Business Continuity, Data Center Standards.

ARMAĞAN

Gösterdikleri sabır, destek ve verdikleri yüksek moral'den dolayı tezimi öncelikle eşim Alev Moral'a, doğmak üzere olan kızım Nur Moral'a, bu günlere gelmemi sağlayan annem Aynur Moral ve babam Vural Moral'a, ablam Asuman Ülger ve yeğenlerime armağan ediyorum.

Onur Moral



TEŞEKKÜR

Tezli yüksek lisans yapmam konusunda beni yönlendiren ve yaklaşık 1 yıl boyunca tez çalışmamda desteklerini esirgemeyen Prof. Dr. Ahmet Faik Kaşlı ve bilimsel araştırma teknikleri konusunda bilgi ve tecrübelerini benimle paylaşan Öğr. Gör. Feridun Özçakır'a sonsuz teşekkürler.

Onur Moral



İÇİNDEKİLER

TABLO LİSTESİ.....	ix
ŞEKİL LİSTESİ.....	x
KISALTMALAR.....	xii
I. GİRİŞ.....	1
1.1. Tezin Amacı	3
1.2. Akademik Çalışmalar	4
II. GENEL KISIMLAR	6
2.1. Veri Merkezi Tarihi Gelişimi	6
2.2. Veri Merkezi Türleri	8
2.2.1. İşletme içi veri merkezleri	8
2.2.2. Bulut bilişim.....	9
2.3. Veri Merkezi Sanallaştırma.....	12
2.3.1. Sanallaştırma türleri	13
2.3.2. Sanallaştırmanın faydaları	14
2.4. Veri Merkezi Standartları Ve Denetleme.....	15
2.4.1. ISO sertifikaları.....	17
2.4.1.1. ISO 31000 risk yönetimi.....	17
2.4.1.2. ISO 22301 iş sürekliliği yönetim sistemi	18
2.4.1.3. ISO 27001 bilgi güvenliği yönetim sistemleri.....	18
2.4.1.4. ISO 9001 kalite yönetim sistemleri	20

2.4.1.5.	ISO 50001 enerji yönetim sistemleri	20
2.4.2.	Uptime Institute (Veri Merkezi Sürekliliği)	21
2.4.2.1.	Tier 1 - basit sistem	21
2.4.2.2.	Tier 2 - yedekli sistem	22
2.4.2.3.	Tier 3 - eşzamanlı bakım	22
2.4.2.4.	Tier 4 - hata toleransı	23
2.4.3.	LEED sertifikası	25
2.4.4.	ASHRAE standardı	26
2.4.5.	PCI DSS standardı	26
2.4.6.	SAS 70/SSAE-16	28
2.4.7.	ANSI/TIA-942-A, CENELEC EN 50173-5	29
2.4.8.	ANSI/BICSI-002	30
2.5.	Veri Merkezi Yer Seçimi	31
2.5.1.	Türkiye’de yer seçimi	33
2.6.	Veri Merkezi Tasarımı Ve Altyapısının Hazırlanması	36
2.6.1.	Veri merkezi enerji altyapısı ve verimliliği	36
2.6.1.1.	PUE’nin faydaları	39
2.6.1.2.	PUE ölçme seviyeleri	40
2.6.1.3.	Güç ve enerji sistemleri	40
2.6.1.4.	Enerji yedekliliği	41

2.6.2.	Kablolama ve ağ altyapısı	44
2.6.2.1.	Kablo bağlantı düzenleri.....	48
2.6.2.2.	Kablo türleri.....	50
2.6.3.	İklimlendirme sistemleri	53
2.6.3.1.	Başarılı bir iklimlendirme için dikkat edilecek hususlar	56
2.6.3.2.	İklimlendirme yöntemleri	57
2.6.4.	Yangın önleme altyapısı	59
2.6.4.1.	Veri merkezi yangın risk grupları.....	60
2.6.4.2.	Yangın önleme sistemleri	61
2.6.5.	Veri merkezi izleme sistemleri	64
2.6.6.	Veri merkezi güvenliği ve erişimi.....	65
2.6.6.1.	Siber güvenlik.....	66
2.6.6.2.	Fiziksel güvenlik.....	70
2.7.	Yedeklilik Ve İş Sürekliliği.....	71
2.7.1.	BT ekipmanlarının yedeklenmesi	72
2.7.2.	Verinin yedeklenmesi	73
2.7.2.1.	Yedekleme türleri	74
2.7.3.	Felaketten kurtarma merkezleri	76
2.7.3.1.	Önemli kavramlar	78
2.8.	Veri Merkezi Bakımı Ve Tatbikatlar	81

2.8.1.	Veri merkezi bakımı	81
2.8.2.	Veri merkezi tatbikatı	83
2.9.	Örnek Veri Merkezleri	84
2.9.1.	Switch SuperNAP veri merkezleri.....	84
2.9.2.	Utah veri merkezi.....	86
2.9.3.	Google veri merkezleri	88
2.9.4.	Microsoft veri merkezleri	90
III.	BULGULAR.....	91
3.1.	Küçük Ölçekli İşletmeler İçin Veri Merkezi Modeli	91
3.2.	Orta Ölçekli İşletmeler İçin Veri Merkezi Modeli.....	93
3.3.	Büyük Ölçekli İşletmeler İçin Veri Merkezi Modeli	95
IV.	TARTIŞMA VE SONUÇ	98
	ÖZGEÇMİŞ	117

TABLO LİSTESİ

Tablo 2.1. Uptime Institute Tier Karşılaştırmaları. (Turner, Seader, & Renaud 2008)	24
Tablo 2.2. PCI DSS Şartları. (PCI Security Standarts Council, 2010)	27
Tablo 2.3. Kart Sahibi Veri Yapısı. (PCI Security Standarts Council, 2010).....	28
Tablo 2.4. Türkiyede Görülen Afetler. (Gökçe, Özden , & Demir, 2008).....	34
Tablo 2.5. OSI Katmanları. (Cisco Systems Inc., 1998).....	46
Tablo 2.6. Kablo Karşılaştırması. (Cisco System Inc., 2003; HP Invent, 2006)	53
Tablo 2.7. ASHRAE 2008 Yönergeleri. (ASHRAE, 2011)	55
Tablo 2.8. ASHRAE 2004 ve 2008 Yönergeleri Karşılaştırması. (ASHRAE, 2011) ..	55
Tablo 3.1. İşletme Ölçeklerine Göre Veri Merkezi Özellikleri.	92

ŞEKİL LİSTESİ

Şekil 2.1. Bulut Bilişim.....	11
Şekil 2.2. Sanallaştırma.....	13
Şekil 2.3. ISO 27001 Süreçleri. (ISO, 2013)	19
Şekil 2.4. Dünyada Doğal Felaketlerin Görülme Durumları. (Gesellschaft, 2013).....	33
Şekil 2.5. Türkiye Deprem Haritası. (Bülent Özmen, 1997)	35
Şekil 2.6. Dual Bus Enerji Tasarımı. (Loucks & McCluer, 2012).....	42
Şekil 2.7. İzole Edilmiş Enerji Tasarımı. (Loucks & McCluer, 2012)	43
Şekil 2.8. Switch. (Cisco Systems Inc., 2015)	45
Şekil 2.9. Router. (Cisco Systems Inc., 2015)	45
Şekil 2.10. OSI Veri Akışı. (Cisco Systems Inc., 1998).....	47
Şekil 2.11. Düzenlenmemiş Kablo Altyapısı. (DiMinico, 2006).....	48
Şekil 2.12. Düzenlenmiş Kablo Altyapısı. (DiMinico, 2006).....	48
Şekil 2.13. Düz Bağlantı. (Lammle, 2007)	49
Şekil 2.14. Çapraz Bağlantı. (Lammle, 2007)	49
Şekil 2.15. Sarmal Bağlantı. (Lammle, 2007)	49
Şekil 2.16. UTP Kablo. (Eko Kablo, 2015)	51
Şekil 2.17. STP Kablo. (BWorks, 2015).....	51
Şekil 2.18. Koaksiyel Kablo. (Miratec, 2009)	52
Şekil 2.19. Fiber Kablo. (Kreasis, 2014)	52
Şekil 2.20. Sıcak Ve Soğuk Hava Koridorları. (Akın & Ketenci, 2010).....	59
Şekil 2.21. Yüksek Hacimli Sabit Tüp.....	62
Şekil 2.22. Taşınabilir Tüp.....	63
Şekil 2.23. Su Püskürtme Sistemi. (Üçler Yangın, 2011).....	64

Şekil 2.24. Sıcaklık Sensörü.	64
Şekil 2.25. Sensör Kumandası.	65
Şekil 2.26. Yıllara Göre Uygulama Güvenlik Zaafiyetleri. (McAfee, 2014)	68
Şekil 2.27. Ağ Atak Yöntemleri. (McAfee, 2014).....	68
Şekil 2.28. Yıllara Göre Zararlı Yazılım Grafiği. (McAfee, 2014)	69
Şekil 2.29. Şifreleme Atağı. (McAfee, 2014)	69
Şekil 2.30. Mail Trafiği. (McAfee, 2014).....	70
Şekil 2.31. Kart Ve Parmak Okuyucu.....	70
Şekil 2.32. Kamera.....	71
Şekil 2.33. Felaket Nedenleri ve Görülme Oranları. (Higgins, 2011)	78
Şekil 2.34. Felaketten Kurtarma Zaman Çizelgesi. (Snedaker, 2007).....	80
Şekil 2.35. SuperNAP Veri Merkezi. (SuperNap, 2015).....	86
Şekil 2.36. NSA Veri Merkezi. (NSA, 2015)	87
Şekil 2.37. Google Veri Merkezi. (Google Inc., 2014).....	89
Şekil 2.38. Microsoft Veri Merkezi. (Microsoft Corp, 2015).....	90

KISALTMALAR

BT	Bilgi Teknolojileri.
SLA	Service Level Agreement.
ISO	International Organization For Standardization.
UPS	Uninterruptible Power Supply.
LEED	Leadership In Energy And Environmental Design.
ASHRAE	The American Society Of Heating, Refrigerating And Air Conditioning Engineers.
TGG	The Green Grid.
PUE	Power Usage Effectiveness.
DCIE	Data Center Infrastructure Efficiency.
PDU	Power Distribution Unit.
PSU	Power Supply Unit.
AC	Alternating Current.
DC	Direct Current.
kWh	Kilowatt-Hour.
kW	Kilowatt.
kVA	Kilo Volt Amper.

MW	Megawatt.
MVA	Mega Volt Amper.
NREL	National Renewable Energy Laboratory.
LBNL	Lawrence Berkeley National Laboratory.
UTP	Unshielded Twisted Pair.
STP	Shielded Twisted Pair.
RH	Relative Humidity.
F	Fahrenheit.
CRAC	Computer Room Air Conditioning.
CRAH	Computer Room Air Handler.
AWG	American Wire Gauge.
RJ	Registered Jack.
SC	Subscriber Connector.
ST	Straight Type.
LED	Light Emitting Diode.
LAN	Local Area Network.
NFPA	National Fire Protection Association.
IGFSS	Inert Gas Fire Suppression System.

IPS	Intrusion Prevention Systems.
SSL	Secure Socket Layer.
ISP	Internet Service Provider.
RPO	Recovery Point Objective.
MTD	Maximum Tolerable Downtime.
WRT	Work Recovery Time.
RTO	Recovery Time Objective.
PCI DSS	Payment Card Industry Data Security Standard.
NOC	Network Operation Center.
AES	Advanced Encryption Standard.
NSA	National Security Agency.
OHSAS	Occupational Health And Safety Assessment Series.
EPA	Environmental Protection Agency.
FISMA	Federal Information Security Management.
SOC	Service Organization Controls.
PAE	Preliminary Energy Use Analysis.
ENI	External Network Interface.
MD	Main Distributor.

ZD	Zone Distributor.
LDP	Local Distribution Point.
VMM	Virtual Machine Monitor.
SLA	Service Level Agreement.



I. GİRİŞ

Türk Dil Kurumuna göre veri; *olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimidir.* (Türk Dil Kurumu, 2006) Veriler tek başına bir anlam ifade etmemektedir, enformasyonun ham maddesi olarak ta ifade edilebilir. Örneğin bir kişinin adı, yaşı, doğum tarihi ve mesleği tek başlarına birşey ifade etmezler. Veri tek başına anlam ifade etmese de bilgi sürecinin ham maddesi olması nedeniyle büyük öneme sahiptir. Süreç dahilinde ikinci aşama olarak verinin düzenlenip, biraraya getirilip anlam katılması ile enformasyon oluşturulur. Enformasyonun yorumlanıp anlam katılarak kullanılabilir hale getirilmesi ile de bilgi oluşturulur. (Odabaş, 2008)

İşletmeler üretim veya hizmet sektöründe farketmeksizin iş süreçlerinin başlangıcından sonuçlanıp müşteriye teslim edilene kadar geçen bütün süreçte veriye ihtiyaç duyarlar. Ham madde temininden yönetimine, işlenip ürüne çevrilmesinden pazara sunulmasına kadar doğru veriye sahip olmak zorundadırlar. Bu döngü hem hizmet hemde üretim süreçlerinin vazgeçilmez parçasıdır. Veriye işletmelerin farklı seviyelerinde farklı şekillerde ihtiyaçları vardır. İşletme iş süreçlerinin giriş halkası olan personelden stratejik karar almak zorunda olan üst düzey yönetime kadar herkes ihtiyacı olan veriye sahip olmak zorundadır veya istenilen anda erişebilmeleri gerekir. İşletmeler küreselleşme, farklı pazarlara açılma, doğru şekilde rekabet edebilme, hayatlarını sürdürebilmek ve varlık değerlerini artırabilmek gibi bütün süreçlerinde veriye ihtiyaç duyarlar. Sahip oldukları markalarına, güçlerine ve itibarlarına sahip oldukları doğru veriler sayesinde ulaşabilmektedirler.

Veri merkezleri; işletmelerin mali, itibar ve marka anlamında en değerli varlıkları olan verilerini gizlilik, bütünlük ve erişebilirlik ilkeleri ile saklamaları, korumaları ve istediklerinde hızlı ve güvenli bir şekilde erişmelerine imkan veren bilgi teknolojileri ekipmanlarına ev sahipliği yapan ve gerekli şartları sağlayan veri işleme ve depolama tesisleri veya merkezleri olarak tanımlanabilir.

Genel olarak benzer şekilde tanımlanan veri merkezlerini Gartner “*bilgi teknolojileri sistemlerine, veri depolama aygıtlarına, sunucular ve verilere ev sahipliği yapan ve koruyan gelişmiş işlem merkezleri*” olarak tanımlamaktadır. (Gartner Inc., 2016)

Veri merkezleri sunucular, depolama aygıtları, ağ cihazları, güvenlik cihazları, yedekleme cihazları gibi veriye erişimi sağlayan bileşenleri barındırmaktadır.

Bu cihazlar veri merkezi dışında barındırılabilir mi?

Veri merkezi bileşenleri olan altyapı cihazlarının sağlıklı çalışabilmeleri için gerekli oda şartlarının sağlandığı, izleme, güvenlik ve sürekliliğin yüksek seviyelerde olduğu, doğal afetlere dayanıklı tesislerde konumlandırılması gerekmektedir. Veri merkezleri enerji sistemleri, iklimlendirme sistemleri, yangından koruma sistemleri ve ortam izleme sistemleri gibi bir çok otomasyonla desteklenmektedir. Bu özellikler veri merkezlerini veri merkezi yapan değerlerdir. Varlığının devamını sağlamak ve varlık değerini artırmak amacıyla olan işletmelerin kesinlikle verilerinin riske atmamaları gerekmektedir. işletmeler bu şartları sağlayan kendi veri merkezlerini kurabilirler, fakat bu işlem hem maliyet hemde ayrı uzmanlık gerektirmektedir. Dolayısıyla günümüzde işi uzmanına yaptırmak mantığıyla işletmeler verilerinin değerine göre bu hizmeti belirli SLA (Hizmet Seviyesi Anlaşması) seviyelerinde profesyonel olarak

almayı tercih ediyorlar. Her iki durumda da veri merkezleri işletmelerin hayatlarını devam ettirebilmeleri için vazgeçilmez en önemli varlıklarındandır.

Yer sağlayıcı olabilmek yani veri merkezi hizmeti verebilmek için ülkelere göre farklı zorunluluklar vardır. Veri merkezi hizmeti verenler kanun ve yönetmeliklere uygun hizmet vermek zorundadırlar. Türkiye’de yer sağlayıcı olarak hizmet sunan veri merkezleri BTK tarafından düzenlenen ve düzenlendikten sonra 5 yıl süreyle geçerli olan faaliyet belgesini almak zorundalar. (Telekomünikasyon İletişim Başkanlığı, 2007)

1.1. Tezin Amacı

Geçmişte ve günümüzde ihtiyacımız olan gelecekte de devam edecek ihtiyaçtan dolayı veri merkezlerinin tasarımından, yapılışı ve yönetimine kadar bütün aşamalar hem veri merkezi yöneticileri hemde kullanan işletmeler tarafından iyi bilinmelidir. Gerek veri merkezi yöneticileri gerekse kullanan işletmelerin yaptıkları yanlış tercihler geri dönüşü olmayan hatalara neden olabilir. Bu sorunu ortadan kaldırmak veri merkezinin çıkış noktası olan doğru verilere sahip olmaktan geçer. Veri merkezine ihtiyacı olan işletmeler bu ihtiyaçlarını ilk olarak doğru belirlemeleri, iyi ölçeklendirmeleri ve farkındalıklarını artırmaları gerekir. İhtiyacının tam olarak ne olduğunu belirleyen işletme bu ihtiyacı karşılayacak veri merkezini seçerken bir takım standartların ve sertifikaların neler olduğunu ve bunların ne ifade ettiğini iyi bilmesi olası hatalara düşmesini engelleyecektir. Bu noktada gerekli sertifikasyonlara sahip olmayan veri merkezlerinden uzak durmak gerekir veya bu sertifikalar olmadan da veri merkezinin seviyesini belirleyebilmek için gerekli bilgiye sahip olmak ta yeterli olabilir.

Bu noktada sağlıklı veri merkezi yapısında;

- Neler olması gerekir?
- Nasıl yönetilmesi gerekir?
- Güvenliği nasıl sağlanmalı?
- Yer seçiminde hangi kriterler önemlidir?
- Veri merkezi sürekliliği ve yedekliliği nasıl sağlanır?

sorularının cevaplarını iyi bilmek ileride yaşanacak problemleri engellemek anlamına gelir. Günümüzde en çok yapılan hatalar tam olarak bu bilgilere sahip olmamaktan kaynaklanmaktadır. Bu durumun önüne geçmekte hem veri merkezi hizmeti verenlere hemde veri merkezi hizmeti alanlara düşmektedir.

1.2. Akademik Çalışmalar

Veri merkezi hakkında farklı veya benzer konularda yapılmış diğer akademik çalışmaları incelemek konunun farklı açıdan hangi özellikleri ile değerlendirildiğini tespit etmek, çalışmaların farklılıklarını veya benzerliklerini karşılaştırtırıp daha iyi kavraya bilmek adına fayda sağlayacaktır. Bu amaçla Ecir Uğur Küçüksille ve Hüyenin Taner Gökmen'in Veri Merkezi Tasarımı (Gökmen & Küçüksille, 2013), Uğur Yüzgeç ve Arif Günel'in Üniversitelere Yönelik Bir Veri Merkezinin İklimlendirme Planlaması (Yüzgeç & Günel, 2014), Derya Çavdar ve Fatih Alagöz'ün Yeşil Veri Merkezlerinde Enerji Verimliliği (Çavdar & Alagöz, 2013), Luiz Andre Barroso, Jimmy Clidas ve Urs Hölzle'nin The Datacenter as a Computer (Barroso, Clidas, & Hölzle, 2013), Kejiang Ye, Dawei Huang, Xiaohong Jiang, Huajun Chen ve Shuang Wu'nun Virtual Machine Based Energy-Efficient Data Center Architecture

for Cloud Computing: A Performance Perspective (Ye, Huang, Jiang, Chen, & Wu, 2010), Yanpei Chen, Laura Keys, Randy H. Katz'ın Towards Energy Efficient MapReduce (Chen, Keys, & Katz, 2009), Taşkın Kavzoğlu ve Emrehan Kutluğ Şahin'in Bulut Bilişim Teknolojisi ve Bulut CBS Uygulamaları (Kavzoğlu & Şahin, 2012), Haldun Akpınar'ın İş Sürekliliği ve Felaket Planlaması (Akpınar, 2011), Prashant Baweja'nın Refining Your Criteria for Data Center Site Selection (Baweja, 2013), Luiz André Barroso, Jimmy Clidaras ve Urs Hölzle'nin The Datacenter as a Computer (Barroso, Clidaras, & Hölzle, 2013), Yanpei Chen, Laura Keys ve Randy H. Katz'ın Towards Energy Efficient MapReduce (Chen, Keys, & Katz, 2009), Oktay Ergünay'ın Türkiye'nin Afet Profili (Ergünay, 2008) çalışmaları incelenebilir.

II. GENEL KISIMLAR

2.1. Veri Merkezi Tarihi Gelişimi

Veri merkezleri son yıllarda daha çok dikkat çekmeye başlasalar da veri merkezi ihtiyacının oluşması ve veri merkezlerinin kurulması esasen bilgisayar ihtiyacının doğmasından ve kullanılmaya başlamasından daha eski tarihlere dayanmaktadır. 1960'lı yıllarda oda boyutundaki cihazlar onlara özel, kontrollü sistem odası olarak tanımlanan odalarda tutulurlardı. Bilgisayar öncesi bu sistemlerin bedeli oldukça yüksekti. Dolayısıyla sadece askeri ve kamu alanında kendilerine özel kontrollü erişime izin verilen odalarda kullanılırdı. Bu cihazlar çalışma sırasında ısı üretikleri için odaların soğutulma ihtiyacı ortaya çıktı. Zaman içerisinde cihazların sayılarının artması, bunların birbirine bağlanması ve düzenlenmesi gibi ihtiyaçlar oluştu. Esasen bugün kabinetlere cihazların yerleştirilmesi, bunların birbirine bağlanması ve düzenlenmesi benzer bir durumdur. 1980 yıllarında bilgisayar dünyası gelişmeye ve ilerlemeye başladı, bilgisayarlar büyük odalarda değil her yere kurulabilir boyutlara dönüştü. Teknolojinin gelişim süreci incelediğinde rahatça bilgisayarlardan önce sistem odalarının varlığı görülmektedir. 1990 yıllarında sunucu – istemci ağ yapıları standartlaştı, sistem odalarının bu sunuculara ev sahipliği yapmaya başlamaları ile veri merkezleri gelişimi de başlamış oldu. Zaman içerisinde internetin gelişimi ile işletmeler 7x24 işlem yapabilecek sistemler kurmaya başladılar. İnternetin hızla yayılması, yapılan işlerin kapasitelerinin artması, bu işlemleri yapacak daha güçlü internet altyapısını destekleyen cihazların ihtiyacını ortaya çıkardı ve bu doğrultu da daha büyük, daha düzenli ve daha güvenli veri merkezlerine ihtiyaç duyuldu. O

dönemin veri merkezlerinin yüksek bedelli çözümler sunması bazı firmaların kendilerine özel daha küçük veri merkezleri kurmalarına neden oldu. (Nutt, 2008)

Bilgisayar verileri ve ağları gün geçtikçe büyümeye devam ettiği için daha büyük ve profesyonel veri merkezleri dünya genelinde artmaktadır. Bu artış küreselleşme anlamında olumlu yorumlansa da bazende enerji tüketimi gibi olumsuz sonuçlar doğurabilmektedir. Günümüz veri merkezi gereksinimleri, veri merkezi yöneticilerini getirdiği nokta da daha yaratıcı düşünme zorunluluğunu ortaya çıkarmaktadır. (Casey, 2014)

Örneğin; Google'ın "Yüzen Veri Merkezi" patentini alması veri merkezleri gelişiminin ulaştığı noktayı göstermektedir. Buradaki amaç okyanus dalgalarıyla veri merkezine enerji üretmek ve aynı zamanda okyanus suyuyla sistemlerin ihtiyacı olan soğutmayı sağlamaktır. (Miller, 2008)

Veri merkezleri bugün hem donanımsal hemde yazılımsal daha verimli, esnek, modern, güvenilir, kontrollü ve çok büyük iş yüklerine hizmet edebilecek hale geldi. Bu konuda donanım üreticilerinin yanı sıra sanallaştırma teknolojilerinin de katkısı oldu. Veri merkezi yöneticileri özel durumlar dışında avantajlarından dolayı sanallaştırma teknolojilerini tercih etmeye başladılar. Sanallaştırma; sunucudan, istemci bilgisayarlara, ağ sanallaştırmadan depolama aygıtlarına kadar birçok fiziksel ortamın sanallaştırılmasına imkan sağlamasıyla kullanımının önemli oranda artmasına neden olmaktadır. Sanallaştırma kullanımının artışı sonucu olarakta bulut bişim hayatımızda önemli bir yere ulaştı. Birçok firma ortak veri merkezlerini kullanmaya başladılar. Bu gibi nedenler veri merkezi yöneticilerinin sürekli geliştirme yapma ihtiyacını ortaya çıkartmaktadır.

2.2. Veri Merkezi Türleri

Veri merkezleri kapasitelerine, yapılacak işlem, verilecek hizmetlere göre farklılık gösterebilir. Bu noktada ihtiyaca göre kurum ve kuruluşlar kendi veri merkezlerini kurabilir veya profesyonel bir veri merkezinden hizmet alabilirler. Her iki durumda da bazı olumlu ve olumsuz sonuçlar söz konusudur. Bu doğrultuda veri merkezleri işletme içi ve bulut bilişim olarak sınıflandırılabilir.

2.2.1. İşletme içi veri merkezleri

Küçük çaplı, çok fazla ve kritik veri içermeyen, zamansal işlem yapmayan işletmeler profesyonel hizmet almak yerine işletmelerine kendi basit yapılı veri merkezlerini kurabilirler. Bu tip veri merkezlerine işletme içi veri merkezleri denir. İşletme içi veri merkezi kurulmasına karar verirken önemli olan işletme ihtiyaçlarının doğru şekilde belirlenmesi ve bu ihtiyaçların yerine getirilebilmesi için gerekli veri merkezi altyapı maliyetlerinin gerektirdiği kadar bütçeye sahip olup olmamasına bağlıdır. İşletme içi veri merkezleri profesyonel olarak tasarlandığında enerji, soğutma, ortam izleme, yangından koruma ve güvenlik gibi altyapı maliyetlerden dolayı yüksek bütçelere ihtiyaç duyulur. Ayrıca veri merkezinin işletilmesi, kapasitenin planlaması ve sorumluluk alma maliyetleri ayrı hesaplanmalıdır, çünkü ilerleyen süreçte bu maliyetler gizli risk olarak ortaya çıkmaktadır. Son zamanlarda işletme içi veri merkezleri yerlerini bulut tabanlı veri merkezlerine bıraktı, çoğu işletme veri merkezi hizmetlerini bulut üzerinden almaya başladılar. (Turner, 2013)

Fakat bazı kurum ve kuruluşlar özel bağlayıcı nedenlerden dolayı bulut bilişimin sadece belirli türlerini kullanabilirler veya kendi özel gerekliliklerinden dolayı kendi veri merkezlerini yerel olarak kurma kararı alabilirler. Örneğin devlet kurumları kendi

bünyelerinde kurdukları veri merkezlerini kullanabildikleri gibi bulut bilişimde sadece kendi özel veya topluluk bulutlarını tercih edebilmek gibi zorunluluklarla karşılaşmaktadırlar. (Ergin, Gerede, & Korkmaz, 2012)

2.2.2. Bulut bilişim

Bulut bilişim en az çaba ve maliyet ile servis sağlayıcı desteğini alarak internet üzerinden sistem kaynaklarının (sunucu, depolama, ağ) kullanılması amacıyla tasarlanmış altyapılardır. Bulut bilişim maliyet ve yönetim gibi avantajlar sağlamanın yanı sıra bazı modellerinde paylaşımlı kaynak kullanımı, sistemlerin başkaları tarafından yönetilmesi, zorunluluklar, bağımlılık, erişebilirlik gibi ortaya çıkan nedenler bulutun bir handikapı olarak görülmektedir. (Uzuner, 2010).

Verilerin bütünlüğü, gizliliği ve güvenliğinin önemli olduğu durumda işletmeler aldıkları bulut hizmetlerini gözetim altında tutmak ve sözleşmeler aracılığıyla kendilerini güven altına almak zorundadır. İlk bulut sağlayıcı hizmetini Amazon firması kitaplarla ilgili yaptığı uygulamayı hizmete alarak yapmıştır. Günümüzde internet hizmet sağlayıcılar (ISP), Salesforce, Microsoft, Oracle ve Google gibi firmalar bulut bilişim konusunda önemli altyapı hizmetleri sunmaktadır. Bulut bilişim verdiği hizmetin şekli, kapasitesi, yönetimi, gizlilik dereceleri ve çalışma mantığı bakımından genel, özel, topluluk ve karma olmak üzere farklı türlerde hizmet sunmaktadır. (Shroff, 2010)

Genel bulut (public); işletmenin kendi bünyesinde barındırılmaz, servis sağlayıcı tarafından kaynakların internetten erişime açılmasıyla oluşur. İşletmenin genel bulut altyapı sistemlerinde yönetim hakkı yoktur. Kullanılan altyapının nerede olduğu ve kim tarafından yönetildiği genellikle bilinmemektedir. Bu yöntemde herhangi bir

donanım, yazılım alınması gerekmediği gibi altyapı yönetim maliyetide yoktur. (Keith Jeffery, 2010; Peter Mell, 2011)

Google'nin harita hizmetleri, Google drive, Amazon'un kitaplar için geliştirdiği uygulama hizmetleri, Microsoft'un mail veya OneDrive gibi verdiği hizmetler, Dropbox ve birçok alış veriş hizmeti sunan web siteleri genel buluta örnek olarak verilebilir.

Özel bulut (private, co-location); işletmenin kendi bünyesinde bulundurulabileceği gibi işletme dışında da barınmasına izin verilen işletmeye özel ve işletmenin bütün altyapıyı yönetmesine imkan veren bulut türüdür (Keith Jeffery, 2010; Peter Mell, 2011).

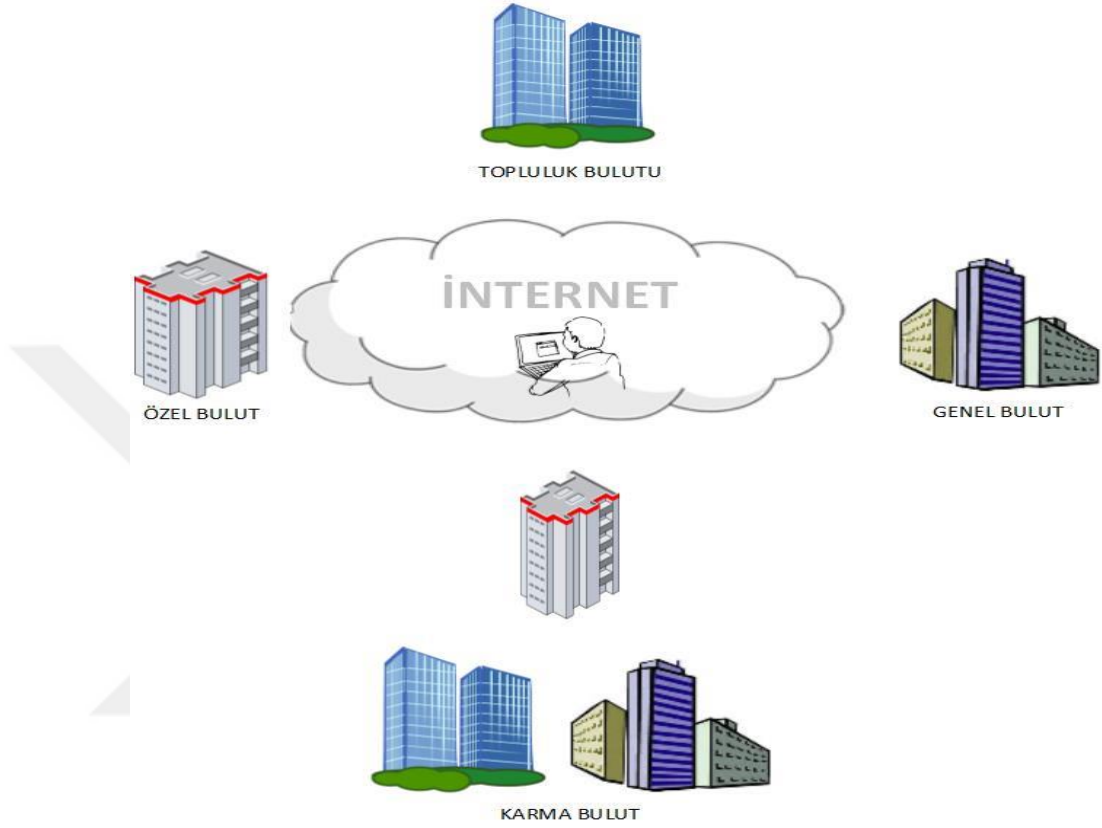
Örneğin herhangi bir işletmenin kendi sistemleri için barındırma hizmeti aldığı veri merkezindeki, kendilerine ait yönettikleri sistemler özel bulutu temsil eder.

Topluluk bulutu (Community); bulut altyapısının güvenlik, politika, gizlilik gibi değerleri benzer olan ve birlikte hareket eden kurum veya kuruluşlara paylaştırılmış sistemlerdir (Keith Jeffery, 2010; Peter Mell, 2011).

Topluluk bulutu için E-devlet uygulaması örnek olarak gösterilebilir.

Karma (hybrid); bu model iki veya daha fazla bulut altyapısının özelliklerini bünyesinde barındıran birlikte kullanılmasına izin veren karmaşık ve bütünleşik bir yöntemdir. Özel bulut altyapısı kullanılırken bir taraftan da genel buluta ait bazı hizmetlerle entegre olup kullanabilmek örnek olarak verilebilir. (Keith Jeffery, 2010; Peter Mell, 2011)

Özel bulut üzerinde çalışan araç takip uygulamasının Google'nin genel bulut hizmeti olarak sunduğu harita uygulamasını kullanması karma bulut olarak örneklendirilebilir.



Şekil 2.1. Bulut Bilişim.

Bulut bilişim farklı türlerde hizmet sağlayabildiği gibi hizmet olarak da farklı imkanlar sunabilmektedir.

Yazılım tabanlı hizmet (Software as a service); donanım maliyetlerinden kurtulmak amacıyla sadece uygulama bazlı verilen hizmettir. Uygulamalar buluttaki sunucularda çalışır ve başkaları tarafından yönetilir. (Peter Mell, 2011; Keith Jeffery, 2010)

Platform tabanlı hizmet (Platform as a service); yazılımın geliştirilip kullanılmasına imkan veren ortamın sunulduğu yöntemdir. Bu yöntemde güvenlikten hem işletme hemde hizmet sağlayıcı sorumludur. Bu sayede donanım ve yazılım geliştirme

ortamlarının satın alma maliyeti ortadan kalkmaktadır. (Peter Mell, 2011; Keith Jeffery, 2010)

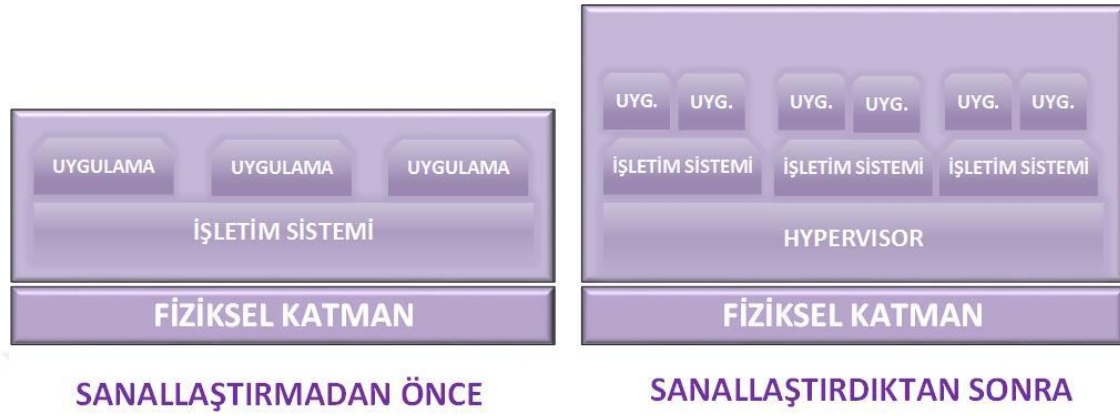
Altyapı hizmeti (Infrastructure as a service); sistemlerin geliştirilip kullanılması için gereken bütün altyapı hizmetlerinin sağlandığı yöntemdir. Müşteriye bulut bilişimin temel altyapısını yönetmesine izin vermemekle birlikte işletim sistemine müdahale etme, herhangi uygulama kurulup kullanılmasına, seçilen bazı bileşenlerin (sunucu, depolama, ağ) limitli olarak kontrol edilmesi ve yönetilmesine izin verir. (Peter Mell, 2011; Keith Jeffery, 2010)

2.3. Veri Merkezi Sanallaştırma

Sanallaştırma bilgi teknolojileri altyapılarına yeni bir bakış açısı getiren en önemli geliştirmelerdendir. Özellikle kurulum, yönetim, bakım, entegrasyon, iş sürekliliği, optimizasyon, maliyet ve bütçeleme gibi konular için veri merkezlerinde kullanılan anahtar çözümdür. (Kuma, Roberts, & Kawalek, 2010; VMware Inc., 2006)

Sanallaştırma fiziksel ekipman kaynaklarının mantıksal olarak ayrıştırılıp birden fazla sunucunun aynı kaynakları paylaşmasını sağlayan yazılım tabanlı sistemlerdir. Bu sistemler kullanıcı ile donanım arasında (Sunucu, depolama, ağ cihazları vb.) bir katman oluşturarak kullanıcının doğrudan fiziksel sistem kaynaklarına erişmesini engeller. Bu katman kullanıcı taleplerini alarak uygun bir şekilde donanıma ileten, sanallaştırmanın çekirdeği olarak adlandırılan Hypervisor veya VMM (Virtual Machine Monitor) olarak adlandırılan mantıksal bir katmandır. Daha basit anlamıyla sanallaştırma; misafir olarak isimlendirilen birden fazla işletim sisteminin aynı fiziksel

ekipman kaynaklarını paylaşılarak çalışmasını ifade eder. (VMware Inc., 2006; Santana, 2014)



Şekil 2.2. Sanallaştırma.

2.3.1. Sanallaştırma türleri

Santana, Kuma ve arkadaşlarına göre; bütün sanallaştırma türlerinin kendine ait kullanım alanları ve özellikleri vardır. Bütün türler birlikte kullanılabilirdiği gibi bazı durumlarda sadece belli başlı türlerde de sanallaştırma yapılabilir. Aşağıdaki sanallaştırma türleri işletmelerde kullanılmaktadır. (Santana, 2014; Kuma, Roberts, & Kawalek, 2010)

Sunucu sanallaştırma; birden fazla fiziksel sunucuyu sanallaştırarak daha az fiziksel sunucu üzerinden çalışmasını sağlayan sanallaştırmadır. Örneğin 5 fiziksel sunucunun sanallaştırılarak 1 fiziksel sunucu üzerinde misafir yani sanal olarak çalışmasını sağlamaktadır.

Depolama sanallaştırma; verilerin sanallaştırılmış bir dosya içinde tutulmasını ifade eder.

Ağ sanallaştırma; ağ bileşenlerinin sanallaştırılıp tıpkı fiziksel ağ ile bağlantı yapılmış gibi çalışmasını sağlayan sanallaştırma türüdür. Daha az ekipman ile daha fazla sanal ağ kurup çalışmasına izin verir.

Masaüstü ve laptop sanallaştırma; bilgisayarların sanallaştırılarak veri merkezine taşınması ve sonrasında son kullanıcıların ağ veya internet üzerinden bu kaynaklara erişerek kullanılmasını sağlayan sanallaştırma türüdür. Özellikle laptoplar için güvenli ortam sağlamaktadır.

Uygulama sanallaştırması; uygulamaların bilgisayarlara kurulmadan sunucu üzerinden çalıştırılıp fakat bilgisayara kurulmuş gibi kullanılabilmesine imkan sağlayan sanallaştırma türüdür.

2.3.2. Sanallaştırmanın faydaları

Literatürdeki birden fazla kaynağa göre sanallaştırmanın faydaları aşağıdaki şekilde listelenebilir (Santana, 2014; Kuma, Roberts, & Kawalek, 2010; VMware Inc., 2006; Bouley, 2010).

- Veri merkezi ölçeklendirme, raporlama, optimizasyon, yük dengeleme ve esneklik gibi konularda fayda sağlar,
- Otomasyon ve standartlaşmanın kolay bir şekilde yapılmasını sağlar,
- Veri merkezinde ihtiyaç duyulan fiziksel ekipmanların sayısını azaltır,
- Daha az fiziksel ekipman ile hizmet verebilmesi özelliği yerden kazanç sağlarken iklimlendirme ve enerji tasarrufundan da büyük oranda kazanç sağlar. Bu kazanç daha az altyapı ile daha kaliteli hizmet verilmesine imkan sağlar,

- Sistem kaynaklarının yüksek verimlilikle kullanılmasını sağlar. Atıl kaynak oluşmasını engeller,
- Gereksiz yatırımların yapılmasını engeller, yapılan yatırımların tam anlamıyla kullanılmasını sağlar,
- İhtiyaç halinde çok hızlı şekilde kaynak oluşturulmasına imkan sağlar,
- Donanım maliyetlerini önemli oranda düşürür,
- Yönetim kolaylığı sağlar. Bir noktadan birden çok sunucu ve diğer bileşenlerin yönetilmesini ve izlenmesini sağlar. Bu sayede gereksiz iş gücü kaybını engeller,
- İş sürekliliği konusunda çok önemli rol oynar,
- Sanallaştırma sistemlerinin donanım bağımsız olması istediğimiz ekipman ile çalışmamıza imkan sağlar,
- Yüksek oranda konsolidasyon yapılabilmesi veri merkezinin daha çevreci olmasını sağlar.

2.4. Veri Merkezi Standartları Ve Denetleme

Veri merkezleri belirli standartlara sahip olmak ve güven vermek zorundadırlar. Bu standartlar dünya çapında kabul görmüş ISO, Uptime Institute, LEED, ASHRAE gibi bazı enstitüler ve yetkili kurumlar tarafından belirlenen standartlardır. Standartların amacı uluslararası alanda değer kazanmak, veri merkezinin seviyelerini belirlemek ve bu sertifikalarla ihtiyaç sahibine veri merkezinin hangi seviyede hizmet sunabildiği bilgisini doğru şekilde vermektir. Sertifika ve standartlardaki en temel amaç yürütülen operasyonlarda aksaklık olmaması adına iş sürekliliğini ve güvenliğini verimli şekilde sağlamaktır. Bu amaç doğrultusunda işletmeler veri merkezleri yatırımlarını yaparken

ihtiyaları olan seviye ile veri merkezinin sunduėu seviyeyi karřılařtırmak ve gven duymak iin bu sertifikalara ihtiya duyarlar. Kaynak planlaması, gvenlik, enerji tk etimi, iř srekliliėi konuları zerine alıřan birok kurum ve kuruluř olduėu gibi onların hazırladıkları standartlar ve sertifikalar da vardır. Bu sertifikaları almanın nemli olduėu kadar aldıktan sonra da standartları saėlamak adına devamlılıėını kaybetmemek gerekir. Bu nokta da hem devamlılıėı saėlamak hem de sertifika saėlayıcıların verdikleri sertifikaların gereėinin yerine getirilip getirilmediėini kontrol etme ihtiyaı denetleme kavramı ortaya ıkarmaktadır. Denetleme yanlıř yorumlandıėı iin iř hayatında kaınılan bir sretir, fakat profesyonel alıřma hayatında denetlenme esnasında ve sonucuna gre durumdan avantaj saėlamak gerekmektedir. Bu anlamda denetlenme kaınılacak deėil dersler ıkartılacak bir olgudur. nk denetleme sonucunda; yapılan hatalar, eksikler veya yapılan iřin ne kadar doėru olduėu rapor halinde dersler ıkartılabilecek řekilde sunulmaktadır. Denetleme kapsamında olan veri merkezlerinde i ve dıř denetleme olarak iki farklı řekilde denetleme yapılmaktadır. Veri merkezleri sahip oldukları standartlara baėlı olarak dzenli olarak denetlenmek zorundadırlar. İ deneti mmkn olduėu kadar uluslararası alanda kabul gren řekilde denetleme yaptıėı gibi iřletme i dinamiklerini iyi bildiėi iin bu doėrultuda da iřletmeye zel yntemler geliřtirebilir. Dıř denetiler yapılacak denetlemenin konusuna gre genellikle o konunun uluslararası standartlarını kullanarak baėımsız denetleme yaparlar. rneėin bazı sektrlerde hizmet veren veri merkezleri kendi standartlarına gre denetlenmektedir. Kredi kartı iřlemleri gerekleřtiren tesisler PCI DSS standardına ve ISO denetlemeleride ISO standartlarına gre baėımsız denetiler tarafından denetlenirler. Bunların dıřında onlarca uluslararası

ve ülkelere özel veri merkezi standartları ve onları denetleyen birimler de mevcuttur.

(Eagle, 2013)

Veri merkezlerinin güvenlik, verimlilik ve süreklilik gibi konularda denetlenmesi gerekir fakat hangi standarda göre denetlendiği önemlidir.

Bu standartları aşağıdaki gibi özetleyebiliriz;

2.4.1. ISO sertifikaları

ISO dünyanın en büyük uluslararası standart geliştiren ve yayınlayan kuruluşları arasına girmektedir. ISO geliştirdiği standartlarla tesislerin güvenliliğini, sürekliliğini ve kalitesini en iyi hale getirip denetlemeyi amaçlar. Bu amaçlarla geliştirdiği sayısız sertifikadan bahsetmek mümkündür. ISO'nun genel amacı işletmeleri korumaktır, bu amaçla veri merkezlerini de kapsaması gerekmektedir. Bu anlamda veri merkezleri ile ilgili olan ISO belgerinin bazılarını aşağıdaki şekilde özetleyebiliriz.

2.4.1.1. ISO 31000 risk yönetimi

İşletmeler hayatları boyunca belirsiz risklerle karşılaşmakta bazen bu riskleri aşabildikleri gibi bazende bu süreçte büyük zararlar yaşayabilmektedirler. Bu riskler bazen işletme içinden bazende işletme dışından kaynaklı olabilmektedir. İşletmeler riski genellikle belirli bir seviyeye kadar yönetebilmekte devamında ise büyük problemler yaşamaktadırlar. Bu noktada risk yönetim kavramı devreye girmektedir ve bu kavram ISO tarafından belirli kriterlerle desteklenerek, henüz belirlenemeyen risklerden zarar görmeyi ortadan kaldırma noktasında destekçi olmaktadır. İşletmelerin hayatlarını sürdürebilmelerinde önemli rol oynayan veri merkezleri bu özelliği ile risk yönetimi kapsamına girmektedir. Veri merkezlerindeki riskleri önceden tanımlamak,

seviyelerini belirlemek, analiz etmek ve iyileştirme çalışmaları yapmak işletmelerin yaşam sürecinde veri merkezlerinden kaynaklı risklerden arınmak anlamına gelmektedir. (ISO, 2011)

2.4.1.2. ISO 22301 iş sürekliliği yönetim sistemi

İşletmelerin yönetmek zorunda oldukları süreçlerden biride iş sürekliliğidir, bu sürecin kesintiye uğraması işletmelerin para kaybetmesinden itibar kaybetmesine kadar olumsuz şekilde sonuçlanabilir. İşletmelerin her zaman iş sürekliliğine ihtiyaçları vardır. Bu yüzden olağan üstü durumlar gerçekleşmeden önce tedbirler alınır, gerçekleşme anında da yapılacak işler ve bu işlerden kimin ne kadar sorumlu olacağı önceden belirlenir. ISO 22301 gelecekte oluşabilecek doğal afet, terörizm, teknoloji hataları, çevreyle ilgili olaylar veya beklenmeyen olağan üstü diğer tehditlerle karşılaşıldığında işletmenin hayatını devam ettirmek ve zarar görmesini engellemek adına hazır olmak için standart geliştirmektir. İş sürekliliğine özen gösteren veri merkezleri ISO 22301 standardından faydalanmaktadır. (Gasirowski, 2012)

2.4.1.3. ISO 27001 bilgi güvenliği yönetim sistemleri

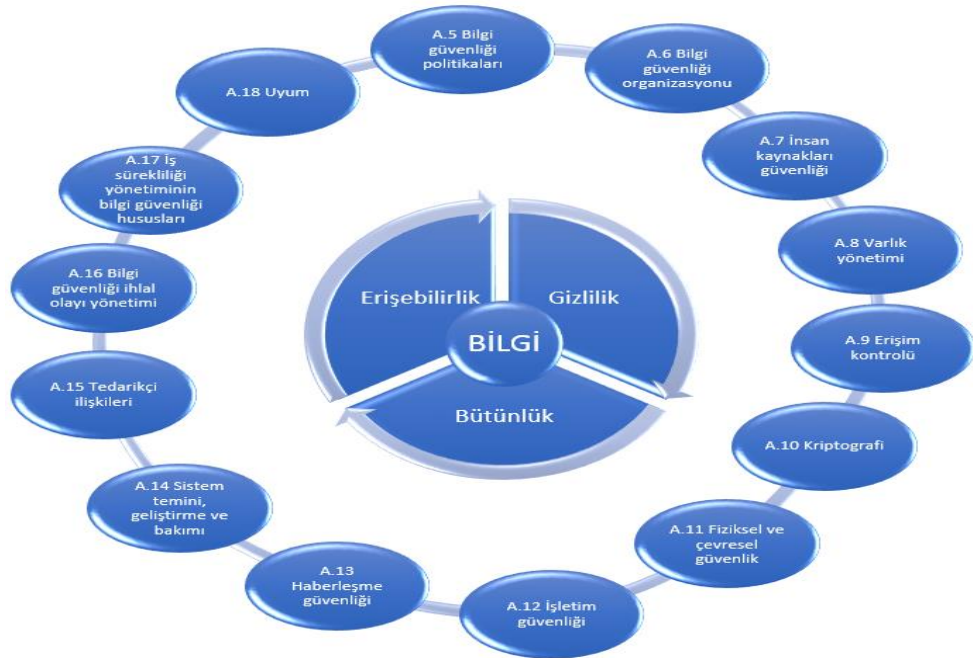
ISO 27001, ISO nun en kapsamlı sertifikalarından bir tanesidir, bu sertifikanın kapsamı aşağıda yer almaktadır. (ISO, 2013)

Diğer ISO sertifikalarında olduğu gibi kendi kapsamındaki sistemin kurulmasından, güvenliğinden, devamlılığından, geliştirilmesi ve denetlenmesinden sorumludur. Bütün bunları yaparken gizlilik, bütünlük ve erişilebilirlik durumlarını göz önüne alarak değerlendirir. ISO 27001 güvenlik üzerine oluşturulan bir standart olmasının yanı sıra bütünlük ve erişilebilirlik kapsamında kaynak yönetimi, sistemlerin izlenmesi,

envanter yönetimi, envanteri oluşturan ekipmanların bakımlarının yapılması, değişim yönetiminin yapılması, olayların yönetilmesi, iş sürekliliği, risk yönetimi gibi bir çok kavramı kapsamına almaktadır. Bu kapsamlarıyla veri merkezlerinde ihtiyaç haline gelen sertifikalardan birisi olmuştur.

ISO 27001'e sahip olmak isteyen veri merkezleri ilk aşamada ve her yıl düzenli olarak yetkilendirilmiş denetçiler tarafından denetlenmektedir. Bu denetçiler de yetkili müfettişler tarafından ayrıca denetlenmektedir.

Bazı işletmeler ortak iş yapma, proje geliştirme gibi süreçleri yürüteceği çözüm ortaklarının da bu belgeye sahip olmasını ön koşul olarak belirtebilmektedir. ISO 27001 sertifikasını almak ve aldıktan sonra yıllık yapılan denetlemelerin başarıyla sonuçlanması için bir takım gerekliliklerin ve süreçlerin yerine getirilmesi gerekir.



Şekil 2.3. ISO 27001 Süreçleri. (ISO, 2013)

2.4.1.4. ISO 9001 kalite yönetim sistemleri

ISO 9001 müşteri taleplerini en iyi şekilde karşılayabilmek amacıyla oluşturulan ve kaliteyi artırmak adına her sürecin döküman haline getirilip devamlılığının sağlanması için oluşturulmuş sistemdir. ISO 9001 üretim, hizmet, satış gibi her türlü sektörde faaliyet gösteren yapılarda uygulanabilir. ISO 9001 sertifikası işletmenin her türlü kalite sistemine önemli derecede değer verdiğini gösteren bir belgedir. Bu anlamda müşteriler bu sertifikaya sahip olan veri merkezlerine kalite anlamında güvenilmesi gerektiğini bilirler. Kalite standardının geniş amacı yönetim katmanının iyileştirilmesi, planlama, sorunların çözülmesi, çözümlerin uygulanması ve kontrol edilmesi, işletme ve tesislerin müşteri gözünde saygınlığının artırılması ve bütün bunların devam ettirilmesidir. Her tesise ve işletme türüne uygulanabilmesi nedeniyle veri merkezlerini de kapsamına almaktadır. (ISO, 2009)

2.4.1.5. ISO 50001 enerji yönetim sistemleri

Enerji kullanımı organizasyonlarda büyük maliyet kalemi olarak karşımıza çıkmaktadır. Özellikle enerjinin çok fazla tüketildiği ve önemli olduğu veri merkezi gibi tesislerde enerji konusuna değinmemek mümkün değildir. Bu noktada ISO 50001 enerjiyi verimli kullanmak adına devreye girmektedir. Enerji tüketim ölçümlerinin yapılması, raporlanması, maliyetlerini azaltmak, doğayı korumak ve devamlılığını sağlamak amaçlanmıştır. Büyük ve küçük ölçekli bütün organizasyonlarda uygulanabilir. (ISO, 2011)

2.4.2. Uptime Institute (Veri Merkezi Sürekliliği)

Uptime Institute veri merkezi sürekliliği için standartlar geliştirilen bir kuruluştur. “Tier Classification System” (Seviye Sınıflandırma Sistemi) ile çığır açan Uptime Institute Tier 1, Tier 2, Tier 3 ve Tier 4 olarak 4 farklı şekilde yayınlanan standart ve sertifikaları uluslararası alanda kabul görmüş ve günümüzde veri merkezlerinin varsayılan sertifikaları haline gelmiştir. Uptime Institute’in bu sertifikaları oluşturmaktaki amacı işletmelerin yaşam döngüsünün en büyük parçalarından olan veri merkezlerinin sürekliliğini, yedekliliğini sağlamak ve bunları farklı ihtiyaç gruplarına göre yapmaktır. Bu yüzden de dört farklı seviyede sertifika yayınlayarak esneklik göstermektedir. Uptime; enerji sağlama, iklimlendirme, ortam izleme, güvenlik, yangından koruma, kablolama gibi bir çok sisteme değinerek bu sistemlerin sürekliliğini değerlendirmektedir. Veri merkezlerinin maliyet ve güvenilirlik seviyeleri Tier seviyelerine göre değişmektedir. (Neudorfer, 2012)

2.4.2.1. Tier 1 - basit sistem

Bu seviye çok büyük öneme sahip olmayan yapılarda, bilgi teknolojileri sistemleri için çalışma ortamlarından ayrıştırılmış rezerve bir oda söz konusudur. Bu sistem odaları sistemin anlık veya kısa süreli enerji kesintilerinden ve dalgalanmalarından korumak amacıyla bir adet UPS cihazıyla desteklenir. Uzun süreli enerji kesintilerinde UPS’e enerji iletmek amacıyla bir adet jeneratör bulunmaktadır. Sistem altyapısında herhangi bir yedeklilik söz konusu olmadığı için planlı bir çalışma yapılacağı zaman sistemin önceden güvenli bir şekilde kapatılması gerekmektedir. Plansız oluşan kesintilerde ise bilgisayar sistemlerinin kesintiye uğraması söz konusudur. (Diaz, 2014; Turner, Seader, & Renaud, 2008)

Tier 1 seviyesinde bakım veya planlanmayan problemlerden dolayı yıllık 28.8 saat kesinti yaşanabileceği yani sistemde %99.67 oranında devamlılık olacağı öngörülmektedir. (Turner, Seader, & Renaud, 2008)

2.4.2.2. Tier 2 - yedekli sistem

Tier 2 de Tier 1' e ilave olarak sistem kesintilerini engellemek amacıyla enerji ve soğutma sistemleri yedekli olarak çalışmaktadır. Bu sayede bakım yapılacağı zaman bilgisayar sistemleri etkilenmeden işlem yapılabilir. Dezavantajı yedekli bu sistemlerin enerji dağıtımları tek kanaldan yapılmaktadır, bu nedenle enerji dağıtım kanalında oluşan problem sistemi etkileyecektir. (Diaz, 2014; Turner, Seader, & Renaud, 2008)

Tier 2 seviyesinde bakım veya plansız olaylardan dolayı yıllık 22 saat kesinti yaşanabileceği farklı bir ifade ile sistemde %99.75 oranında kesinti olmayacağı öngörülmektedir. (Turner, Seader, & Renaud, 2008)

Örnek veri merkezleri; Edicom Business Center, AB Network, S.A. Primary Data Center, Hewlett-Packard Centroamerica Datacenter Services. (Uptime Institute, 2016)

2.4.2.3. Tier 3 - eşzamanlı bakım

Tier 3 de ilave olarak veri merkezi bileşenlerinde değişiklik veya bakım gibi çalışmalarda bilgisayar sistemlerinin kapanmasına gerek kalmadan sistemin devam edebilmesi için enerji, yedekli dağıtım kanallarıyla otomatik enerji taransferi yapan anahtarlar sayesinde dağıtılmaktadır. UPS ile bilgisayar bileşenleri birden fazla bağlantıyla birbirine bağlanmaktadır. Bu sayede bilgisayar sistemleri oluşan bir

aksaklıktan etkilenmemektedir. Genellikle büyük sorumlulukları olan veri merkezlerinde kullanılır. (Diaz, 2014; Turner, Seader, & Renaud, 2008)

Tier 3 seviyesinde bakım zamanlarında yedeklilik sayesinde sistemi kapatmak gerekmediğinden sadece beklenmeyen problemlerde kesinti yaşanabilmektedir. Bu durum yıllık 1.6 saat kesinti yaşanabileceği, sistemde %99.98 oranında süreklilik olacağını göstermektedir. (Turner, Seader, & Renaud, 2008)

Örnek veri merkezleri; TURKCELL Gebze veri merkezi, Turksat Konya veri merkezi, Turk Telekom Gayrettepe veri merkezi, Türkiye Finans Katılım Bankası veri merkezi, Samsung SDS ICT, Fujitsu Services, Huawei Technologies Co., LTD K3 Cloud Container. (Uptime Institute, 2016)

2.4.2.4. Tier 4 - hata toleransı

Tier 3'ün üzerinde bütün altyapı hata toleransı mantığı ile tasarlanmıştır. Başka bir ifade ile bütün tier seviyelerini kapsayan ilaveten hata toleransının en yüksek şekilde planlanmasıyla oluşan seviyedir. Bu seviyede birden fazla enerji üreticisinden yedekli olarak enerji temin edilir. Birden fazla ve fiziksel olarak birbirinden ayrılmış ve ayrılan sistemlerin kendi içinde yedeği olan sistemler söz konusudur ve bu sistemler bilgisayar sistemlerine (sunucu, depolama, ağ bileşenleri) birden fazla bağlantı yoluyla yedekli olarak bağlanıp desteklenmektedir. Yedeklenen bütün sistemlerin arasındaki geçişler otomatik olarak gerçekleşmektedir. Çok yüksek yatırımlar gerektirdiğinden genellikle üst düzey seviyede işlem yapan veri merkezleri tercih etmektedir. (Diaz, 2014)

Tier 4 seviyesinde gerçek anlamda yedeklilik söz konusu olduğu için bakım zamanlarında kesinti yaşanmamaktadır, beklenmeyen problemlerden dolayı yıllık 0,8

saat kesinti yaşanabileceği ve sistemin %99.99 oranında devamlılığı söz konusudur.

(Turner, Seader, & Renaud, 2008)

Örnek veri merkezleri; Switch SUPERNAP, Standard Bank Data Centre, Vodafone Shared Service Limited Data Center-A (Uptime Institute, 2016)

Tablo 2.1. Uptime Institute Tier Karşılaştırmaları. (Turner, Seader, & Renaud, 2008)

	Tier I	Tier II	Tier III	Tier IV
Bina Türü	Bağımlı	Bağımlı	Bağımsız	Bağımsız
Destek Vardiyası	Yok	1 vardiya	1'den fazla vardiya	24 saat destek
Kabinet Başına Standart Enerji	< 1 kW	1-2 kW	1-2 kW	1-3 kW
Kabinet Başına En Fazla Enerji	< 1 kW	1-2 kW	> 3 kW	> 4 kW
Yükseltilmiş Zemin Yüksekliği	12"	18"	30-36"	30-42"
BT Yükünü Destekleyen Bileşenlerin Kapasitesi	N	N + 1	N + 1	N + herhangi hata
Yedeklilik	Yok	Var	Var	Var
Dağıtım Kanalları	1	1	1 aktif, 1 alternatif	2 eş zamanlı aktif
Eş Zamanlı Bakım	Hayır	Hayır	Evet	Evet
Beklenen Kesinti Süresi	28,8 saat	22 saat	1,6 saat	0,8 saat
Süreklilik Oranı	% 99,67	% 99,75	% 99,98	% 99,99
İlk Kurulum Tarihi	1965	1970	1985	1995

Uluslararası alanda geçerlilik gösteren ve kapasite, yedeklilik, hata toleransı konularına odaklanan Uptime'ın sahip olduğu 4 farklı sertifikasyon için farklı

zorunluluklar vardır. Tier sertifikalarına sahip olmak için bu zorunlulukların yerine getirilmesi gerekir.

2.4.3. LEED sertifikası

LEED 1992 yılında U.S. Green Bulding Council tarafından tasarlandı. LEED enerji ve kaynak kullanımını, tasarrufu ve düşük maliyetle daha değerli tesisler oluşturmak konularında fayda sağladığı gibi çevreyi korumayı da amaçlamaktadır. Hedef noktası sadece veri merkezi olmamakla beraber okul, ev, hastane, işletme ve depo gibi tesislerde de uygulanabilir. LEED sertifikasını alabilmek için belirli kriterlerde belirli puanları alabilmek gerekmektedir. Bu kriterler sürdürülebilirlik, enerji, malzeme ve kaynak yönetimi, tesis içindeki kalite olarak gruplanabilir. Bu kriterler ışığında verilen LEED sertifikasında, Certified (40-49 puan) , Silver (50-59 puan), Gold (60-79 puan) ve Platinum (80 ve üzeri puan) olmak üzere 4 farklı seviye vardır. Alınabilecek en iyi seviyedeki sertifika Platinum'dur. LEED yapısı bakımından esneklik gösterebilir; bir tesisin belirli bir kısmına, yeni tesis inşaatlarına ve mevcut binalara uygulanabilir. (Coyle, 2014; Green Building Education Services, 2011)

Google okyanus dalgalarıyla hem enerji üretip hem de soğutma sağlaması bu kategorideki en iyi örneklerdendir (Miller, 2008).

Enerji kullanımı, tasarrufu ve çevre gibi konulara yoğunlaşan LEED sertifikasına sahip olmak ve denetlemesinden başarıyla çıkabilmek için tesis inşaatlarından kaynaklı kirliliği engellemek, tesisin su kullanımının ölçülmesi ve su kullanımını düşürmek, tesisin enerji kullanımının ölçeklendirilip en az enerji tüketimini sağlamak, atıkların yönetimi ve planlanması mümkünse geri dönüşümlerinin sağlanması, tesisin hava

kalitesinin artırılması gibi zorunlukların yerine getirilmesi gerekmektedir. (LEED, 2014)

2.4.4. ASHRAE standardı

ASHRAE birtakım özellikleriyle LEED'e benzerlik göstermektedir. Kapsam olarak bina sistemleri, enerji verimliliği, tesis içi hava kalitesi ve soğutma gibi konulara odaklanarak bunların üzerine uluslararası kabul görmüş standartlar geliştirmektedir. (ASHRAE, 2016)

ASHRAE denetlemelerinde PEA' yi ön şart olarak belirlemektedir.

PEA denetlemelerden bir önceki aşamadır, analiz yapılırken geçmiş verilerden yararlanılır, yapıyı en verimli seviyeye çıkarmayı hedefler ve enerji maliyetlerini düzenler. Yapılan bu çalışmalar ASRAE'nin yaptığı enerji maliyetleri, enerji verimliliği, detaylı enerji hesaplamaları ve finansal analizler gibi denetleme konularına bilgi sağlar. (Hunn, ve diğerleri, 2011)

2.4.5. PCI DSS standardı

Yıllık olarak düzenli yapılan PCI DSS denetlemeleri kart sahiplerinin verilerini korumak için geliştirilmiş bir standarttır. Bu güvenlik standardı American Express, Discover Financial Services, JCB International, MasterCard Worldwide ve Visa Inc. tarafından kurulan PCI Security Standards Council tarafından yönetilmektedir. PCI standardı üretici, uygulama geliştirici, satıcı ve hizmet sağlayıcılara yani zincirin bütün halkalarına uygulanmaktadır. Bu kapsama giren veri merkezleri PCI zorunluluklarına yerine getirmekle mükelleftir. PCI DSS veri güvenliği standardına erişebilmek için altı ana başlık altında 12 şartı sağlamak gerekir. (PCI Security Standarts Council, 2010)

Tablo 2.2. PCI DSS Şartları. (PCI Security Standarts Council, 2010)

Network Güvenliği	▪ Güvenlik duvarı yönetimini kart verisini koruyacak şekilde planlamak, ▪ Üreticilerin belirlediği standart şifre ve diğer güvenlik parametrelerini değiştirmek yani varsayılan şifreleri kullanmamak,
Kart Bilgilerini Koruma	▪ Kayıt altına alınan kart bilgilerini korumak, ▪ Ağ ve internet ortamında kart bilgileri transferini şifreli yapmak,
Güvenlik Açıklarının Yönetilmesi	▪ Antivirüs ve diğer uygulamaların güvenlik güncellemelerini düzenli yapmak, ▪ Güvenlik sistemleri ve uygulamalarını sürekli geliştirmek ve bakımlarını yapmak,
Güvenli Erişim Kontrollerinin Uygulanması	▪ Kart sahibinin bilgilerine erişimleri engellemek, ▪ Her bilgisayar kullanıcısına kendine özel kullanıcı hesabı vermek, ▪ Kart sahibinin verisine fiziksel erişimi engellemek,
Düzenli İzleme Ve Test	▪ Ağ kaynaklarına ve kart bilgilerine erişimleri izleyip kayıt altına almak, ▪ Güvenlik sistemlerinin düzenli olarak test ve tatbikat yapılması,
Bilgi Güvenliği Politikalarını Uygulamak	▪ Bilgi güvenliği politikalarını bütün personele uygulamak.

Güvenliği sağlanan veri; kart sahibi verisi ve kimlik doğrulama verileri olarak iki parçadan oluşur. (PCI Security Standarts Council, 2010)

Tablo 2.3. Kart Sahibi Veri Yapısı. (PCI Security Standarts Council, 2010)

Veriler	Veri Elemanları	Kayıt İzni
Kart Sahibi Verisi	Hesap Numarası	Evet
	Kart Sahibi Adı	Evet
	Hizmet Kodu	Evet
	Sona Erme Tarihi	Evet
Hassas Doğrulama Verisi	Manyetik Şerit Verisi	Hayır
	CAV2/CVC2/CVV2/CID	Hayır
	PIN Kodu	Hayır

2.4.6. SAS 70/SSAE-16

American Institute of Certified Public Accountants tarafından geliştirilen SAS 70 ve SSAE16'nın kendine ait özellikleri vardır. SAS 70 finansal raporları denetleyen ve bunun gerekliliği kadar da servis sağlayıcıları denetleyen bir standarttır. İki şekilde raporlama yapar. Birincisi denetçinin açıklamaları ve fikirlerini içeren finansal rapordur, ikincisi ise açıklama ve fikirlerin verimliliği test ve kontrol edilir. Bundan dolayı ikinci tür daha faydalıdır. SAS 70 daha çok finansal konulara odaklandığı için güzellik, güvenlik ve hizmet sağlayıcılarının diğer detaylarını tam olarak kontrol etmemektedir. Sadece erişim kontrolleri ve yatırım gibi kontrolleri yapmaktadır. SAS 70' in bir takım yetersizliklerinden dolayı SSAE 16 geliştirildi. SSAE 16 üç farklı raporlama sunmaktadır. SOC 1, SAS 70 ile aynı kapsam sahip olduğu için ona göre hizmet vermektedir. SOC 2, finansal konulara ilave olarak güvenlik, süreklilik,

bütünlük ve gizlilik konularında içermektedir. SOC 3 ise SOC 2 den farklı olarak biraz daha kısa raporlar sunmaktadır. (Peirce, 2011; AICPA, 2010)

2.4.7. ANSI/TIA-942-A, CENELEC EN 50173-5

Veri merkezlerinin güvenilir olmasını sağlayan konulardan biriside kablolama yapısıdır. Bu gerekliliklerden dolayı bir takım standartlar geliştirilmiştir. Birinci standart 2005 yılında yayınlanan TIA-942 standardıdır. TIA-942 veri merkezinin hangi bölümünde nasıl kablolama yapılması gerektiği ile alakalı standarttır. Telekomünikasyon kablolamasının ötesinde enerji ve iklimlendirme kablolaması ile de ilgilenmektedir. Bir sonraki standart ise 2007 yılında yayınlanan CENELEC EN50173-5 avrupa standardıdır. Bu standart özellikleriyle TIA-942' ye büyük oranda benzerlik göstermektedir. Her iki standart ta kablolama yapısını benzer şekilde özetlemektedir. TIA-942 yapısında servis sağlayıcıdan gelen bağlantılar merkezi dağıtım noktasında toplanır ve ilgili dağıtım alanlarına transfer edilip bu alanlardan ilgili ekipmanlara gerekli bağlantılar yapılır. CENELEC EN50173-5 standardı da yapıyı benzer şekilde tanımlamaktadır. Birbirinden farklı olan bu standartlar ilgili kurumlar tarafından veri merkezleri telekomünikasyon altyapısını standart hale getirmek ve kablolama konularını düzenlemek amacıyla geliştirildi. Bu standartlar kablolamanın nasıl yapılacağı ve LAN, WAN ve SAN kablolamalarının yapısal özellikleri hakkında bilgi verirken hangi iş için ne tür kablo kullanılması gerektiği hakkında da yönlendirme yapmaktadır. Bu standartlar kablolamaların genellikle iklimlendirmeye engel olmayacak şekilde kabinlerin üzerinden tavan tepsileri içinden yapılmasını tavsiye eder. (Kepekci, 2011)

2.4.8. ANSI/BICSI-002

BISCI uluslararası genel kabul görmüş standartlar ve yayınlar sunan profesyonel bir gruptur. Bu yayınlar genel olarak bilgi iletişimi ve teknoloji sistemlerinin tasarlanmasıyla ilgili olarak değerli kaynak durumundadır. Bu standartlardan BISCI 002 Veri Merkezleri Tasarım ve Kurulumu için klavuz oluşturur. Bu standart ilk defa 18 Haziran 2010 tarihinde “BICSI 002-2010, Data Center Design and Implementation Best Practices” olarak yayınlandı. Akabinde 15 Mart 2011 tarihinde özellikle elektrik ve telekomünikasyon konularında yenileme geçirerek ikinci defa “ANSI/BICSI 002-2011, Data Center Design and Implementation Best Practices” adıyla yayınlanmış oldu. Son olarakta 09 Aralık 2014 yılında “ANSI/BICSI 002-2014, Data Center Design and Implementation Best Practices” adı ile yeni halini aldı. BISCI standartları belirli aralıklarla gözden geçirilerek düzenlemeler gerçekleştirilir. Bu standart veri merkezi mühendislerine ve mimarlarına klavuzluk yapacak düzeydedir. Aynı şekilde veri merkezi sahipleri, veri merkezi kullanıcıları ve danışmanları tarafından da kullanılabilir seviyededir. Bu standart zorunlu ve tavsiye olmak üzere iki farklı kategoride klavuzluk yapmaktadır. Zorunlu kategorisinde genellikle koruma, performans, yönetim ve uyumluluk konuları yer almaktadır. Tavsiye kategorisinde ise başarıya ulaşmak için gereken diğer veri merkezi konularını kapsamaktadır. Bu anlamda BISCI-002 kapasite planlama, tesis yeri seçimi, enerji sistemleri, yangın koruma, güvenlik, telekomünikasyon, iş sürekliliği, risk yönetimi, veri merkezi operasyonlarının yönetimi, iklimlendirme ve veri merkezi bakımı gibi konuları kapsamına almaktadır. (BICSI, 2014)

2.5. Veri Merkezi Yer Seçimi

Veri merkezi konumlandırma bütün çalışmaların en temelini oluşturmaktadır, dolayısıyla temelin sağlıklı şekilde inşa edilmesi gerekmektedir. Aksi taktirde yapılacak bir hata yüksek maliyet ve çabalarla yapılan bütün çalışmaların her an risk içinde olmasına neden olabilir. Dünya üzerinde bütün bölgeler bulundukları iklim şartları, doğal afetler, terör, yangın, patlama, teknoloji altyapıları bakımından farklılıklar gösterir. Veri merkezi inşa edilmeden önce titizlikle değerlendirilmesi gereken en önemli konu bölge ve arazinin bu iş için uygun verimlilikte olup olmamasıdır. Bunların yanı sıra veri merkezi seçiminde tesise enerji sağlama, tesisin yakın çevresinde iş yapan diğer tesislerin faaliyet alanları, hava alanı, trafik bölgeleri, deniz ve göllere yakınlığı yani yakın çevrede gelişen bütün olayların yer seçimi yapılırken hassasiyetle değerlendirilmesi gerekir. Yapılan en büyük hata işletmelerin veri merkezi seçimlerinde maliyet konusuna öncelik vermeleridir. Maliyet önemli bir konu olsada asıl önemli olan veri merkezinde barındırılan varlıkların maddi ve manevi değerleridir. Bu değerler para kaybından itibar kaybına kadar uzayabilmektedir. (Baweja, 2013; Gigerich, 2012)

Zenium Technology Partners tarafından Türkiye, İngiltere ve Almanya’da yapılan Büyüme, Risk ve Bulut Yönetimi Araştırması göstermiştir ki yapılan araştırma kapsamındaki veri merkezlerinin %45’i su baskınlarına, %43’ü depreme karşı dayanıklıdır, %60’ı ise risklerden uzak yerlere inşa edilmiştir. Aynı araştırmaya göre işletmelerin yarısı yaşanan doğal afetlerden etkilenmektedir. Bu durum hala bazı veri merkezlerinin doğal afetlere karşı yeteri kadar güvenli olmadığını gösteriyor. Özellikle %65’lik oran ile Türkiye’nin bu konuda en çok etkilenen ülke olduğu ortaya çıkmıştır.

Bu sonuç veri merkezi kurulurken yer seçimi hatalarından ve veri merkezi inşaatına kadar gerekli özenin gösterilmemesinin sonucu olarak değerlendirilmektedir. (Zenium Technology, 2015)

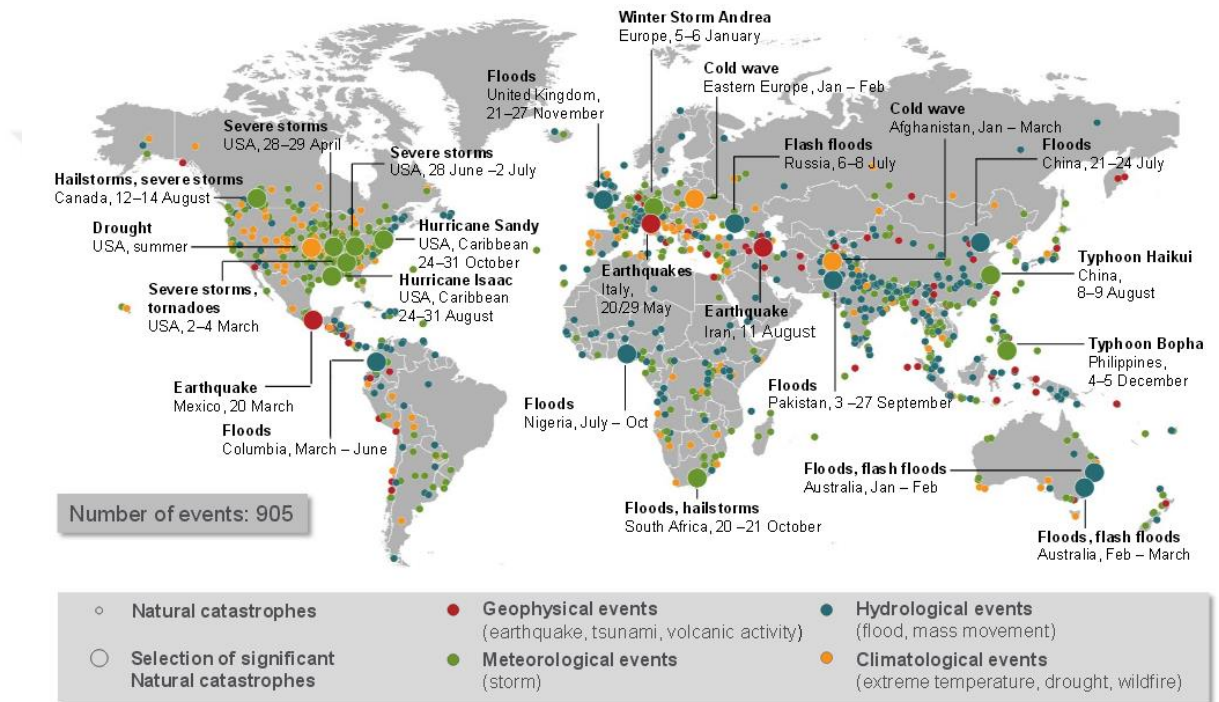
Kurulum yeri seçerken etki eden bütün iç ve dış etkenlerin değerlendirilmesi gerekmektedir, “veri merkezinin konumlandırılacağı yer ile ilgili oluşabilecek felaket yüzdesi %68 civarındadır. (Alkan & Coşar, 2014; Ergünay, 2008)

Veri merkezleri için yapılan teknolojik işlemler kadar yer seçimi yapılırken o coğrafyada görülen doğal afetlerin ve ne sıklıkla görüldüğünün de göz önünde tutulması önemlidir. Bu problemlerin yaşandığı yerlerde veri merkezi kurulmaz veya gerekli tedbirler önceden alınır. Aksi taktirde veri merkezi farkında olunmayan gizli risklere sahip olur ve beklenmedik zamanda gizli risk olarak tanımlanan durum açık problem olarak veri merkezini tehlikeye sokar.

Veri merkezi yeri seçerken özellikle aşağıdaki ana konulara dikkat edilmesi gerekmektedir; (Gilly, 2012)

- Veri merkezi boyutu ve işletme maliyeti,
- Veri merkezi ve zeminin sağlamlığı,
- Bölgede yaşanan doğal afetler (deprem, sel, heyelan, kasırga, hortum, tsunami, yanardağ patlamaları, çığ, vb.) ve alınabilecek tedbirler,
- Çevresel faktörler (deniz, göl, trafik gibi faktörlere yakınlık),
- Bölgede faaliyet gösteren diğer işletmelerin faaliyet alanları,
- Bölgede teknolojiye kaynaklı problemler (internet altyapısı),
- Bölgede insandan kaynaklı (terörizm, grev, hırsızlık, yangın) problemler,
- Enerji ve iletişim ağının kusursuz sağlanması,

- Elektrik, soğutma, veri iletişimi vb. maliyetlerin hesaplanması,
- İhtiyaç halinde veri merkezinin büyümesine olanak sağlaması,
- Büyüyen hacime göre elektrik ve veri iletişim değerlerinin artmasına imkan vermesi,
- Ziyaretçilerin kolay ulaşım sağlaması.



Şekil 2.4. Dünyada Doğal Felaketlerin Görülme Durumları. (Gesellschaft, 2013)

2.5.1. Türkiye’de yer seçimi

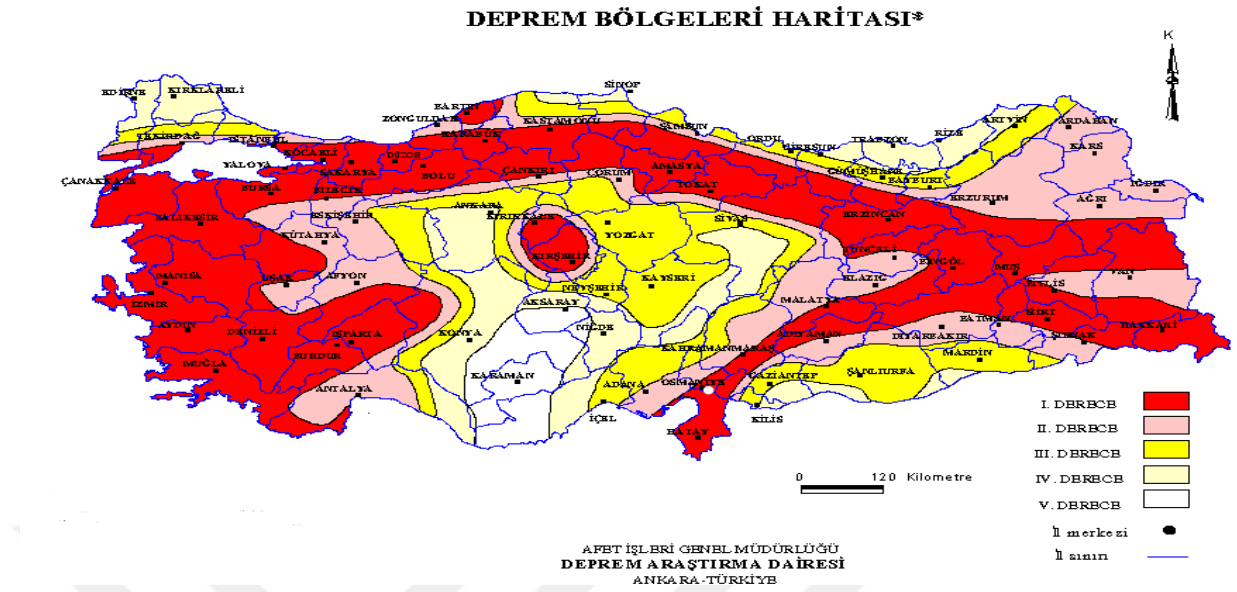
Bütün dünyada olduğu gibi Türkiye’de de veri merkezi yer seçimi yapılırken aynı konulara dikkat edilir. Türkiye bulunduğu jeolojik ve jeomorfolojik yapısı nedeni ile deprem, sel ve heyelan gibi doğal afetler görülmektedir. Önemli oranda görülen bu olaylar can ve mal kaybına neden olacak düzeydedir. Afetlerden etkilenme oranına göre dağılım yapıldığında %55’lik oranla deprem başta gelmektedir, sonrasında %21 heyelan, %8 su baskını, %7 kaya düşmesi, %4 çoklu afetler, %3 diğer afetler ve %2

çığ olarak sıralayabiliriz. Doğal afetler gerçekleşmeden önce, gerçekleşme sırasında ve sonrasında yapılması gereken bir çok işlem vardır. Türkiyede görülen afet sayıları ve etkileri aşağıdaki tabloda verildiği gibidir. (Gökçe, Özden , & Demir, 2008)

Tablo 2.4. Türkiyede Görülen Afetler. (Gökçe, Özden , & Demir, 2008)

Afetler	Afet Olay Sayısı	Etkilenen Toplam Afetzedede Sayısı
Deprem	5318	158241
Heyelan	13494	59345
Su Baskını	4067	22157
Kaya Düşmesi	2956	19422
Çoklu Afetler	2024	12210
Diğer Afetler	1175	9237
Çığ	731	4384

Deprem; Türkiye'nin %66'sı 1'inci ve 2'inci derece deprem kuşaklarında bulunmaktadır. Türkiye'de yaşanan olay sayısına bakıldığında %18'lik paya sahip olan deprem etkisi bakımından %55'lik bir orana sahiptir. Bu özelliği ile deprem bölgesi özelliğini koruyan Türkiye veri merkezi kurulumu açısından incelendiğinde; karadeniz, doğu anadolu ve ege bölgeleri deprem felaketinin birinci derece yoğunlukta görüldüğü bölgeler olarak tespit edilmektedir. (Gökçe, Özden , & Demir, 2008)



Şekil 2.5. Türkiye Deprem Haritası. (Bülent Özmen, 1997)

Heyelan; Özellikle karadeniz, iç ve doğu anadolu bölgelerinde görülen heyelan olay sayısı bakımından %45'lik oran ile ilk sırada olmasında rağmen etki ve zarar bakımından %21'lik oran ile depremde sonra gelmektedir. Çoğunlukla karadeniz bölgesinde görülse de hemen hemen bütün illerin heyelandan belirli seviyelerde etkilendiği kayıt altına alınmıştır. (Gökçe, Özden , & Demir, 2008)

Su baskını; Türkiye’de sık karşılaşılan olaylardan birisi de su baskınlarıdır. Bölgenin meteorolojik özellikleri ve insandan kaynaklı altyapı problemleri nedeni ile etki eden afetlerdendir. (Gökçe, Özden , & Demir, 2008)

Deprem, heyelan ve su baskınının yoğun olmasının dışında çığ, kaya düşmesi, çoklu afetler ve diğer afetlere maruz kalan Türkiye’de problem yaşamamak ve bir çözüme sahip olmak adına; oluşabilecek felaket türleri tespit edilip bu felaketlere karşı tedbirler alınarak hazırlıklar yapılır.

Veri merkezleri; felaket risk analizleri yapılmış (doğal afetler ve insan kaynaklı felaketler), ulaşım ve bilgi teknolojileri altyapısı bakımından incelenmiş, risk kuşaklarına sahip olmayan yerlere veya gerekli tedbirlerin alınmış olduğu alanlara kurulur.

2.6. Veri Merkezi Tasarımı Ve Altyapısının Hazırlanması

Veri merkezi altyapısı incelenirken öncelikle altyapının ne anlama geldiği ve kapsamı değerlendirilir. Altyapı; bütün operasyonel süreçlerin yürütülebilmesi için önceden oluşturulmuş temel olarak tanımlanabilir. Temel olarak tanımlanmasının nedeni veri merkezinin işlevini yerine getirebilmesi için kurulması ve yönetilmesi gereken uygulama, platform ve hizmetlerin üzerine inşa edildiği yapı olmasından kaynaklanmaktadır. Veri merkezi altyapısının en önemli bileşenleri enerji altyapısı, kablolama ve ağ altyapısı, iklimlendirme altyapısı, yangından koruma sistemleri, ortam izleme sistemleri, güvenlik altyapısı ve diğer BT ekipmanları (sunucu, depolama, güvenlik duvarı, ağ cihazları, sanallaştırma) olarak sınıflandırılabilir.

2.6.1. Veri merkezi enerji altyapısı ve verimliliği

Veri merkezleri kurulum esnasında sistem devamlılığı, güvenlik, kapasite gibi konularla birlikte enerji kullanım ve verimliliği de dikkat edilmesi gereken hususlardır. Tasarım hataları veya konum seçiminde yapılan hatalar enerji tüketimi ve maliyetini artıran konular arasındadır. Bu durumlardan dolayı veri merkezlerindeki enerji tüketimi bilgi teknolojilerinin önemli bir gider kaynağı haline gelmiştir ve dolayısıyla enerji optimizasyonu günümüzde zorunlu konuların arasına girmiştir. (Rasmussen, 2001)

Enerji tüketimini azaltmak veya başka bir ifadeyle enerji verimliliğini sağlamak için öncelikle enerjiyi neyin, nasıl tükettiği tespit edilir. Enerji tüketimi üzerinde çalışırken üç farklı kanaldan inceleme yapılır.

- Enerjinin BT ekipmanları (sunucu, depolama aygıtları, ağ cihazları, bilgisayarlar, vb.) ve veri merkezi tesisinin kullandığı sistemler (güç sistemleri, soğutma ve aydınlatma gibi.) arasında nasıl dağıtıldığının incelenmesi,
- Enerjinin diğer BT ekipmanlarının bileşenleri (işlemci, ram, disk) arasında nasıl dağıtıldığı ve tüketildiği,
- Enerjinin BT kaynakları için nasıl ayrıldığı, ayrılan bu kaynağın ne kadarının kullanıldığı ve ne kadarının kullanılmadığıdır.

Veri merkezlerinde enerji tüketimi önemli ölçüde soğutma sistemleri tarafından yapılmaktadır. Tasarımların yanlış yapılması, sunucuların ve diğer cihazların düzgün ve planlı şekilde yerleştirilmemesi soğutma için harcanan enerji tüketimini artırmaktadır. Bu noktada enerji verimliliğinin sağlanması için standartlar ve standartların belirleyicileri ortaya çıkmaktadır. Bu belirleyicilerin en önemlilerinden birisi de The Green Grid'dir. The Green Grid dünya çapında, bilgi teknolojileri ve veri merkezi enerji kaynaklarının verimli kullanılması üzerine standartlar geliştirmekte olan bağımsız yetkili bir kuruluştur. Veri merkezi enerji verimliliğinin belirlenmesinde ve sınıflandırılmasında kullanılan TGG tarafından yayınlanan 2 ölçü vardır. Bu ölçüler sistemlerin ne kadar verimli olduğunu gösterdiği için önemlidir. Ayrıca ölçeklendirme ve geliştirme çalışmaları içinde önemli değerler olarak karşımıza çıkmaktadırlar. TGG'nin yayınladığı metriklerin birincisi güç kullanım verimliliği (PUE), ikincisi veri merkezi altyapı verimliliğidir (DCIE). The Green Grid bu iki metriği yayınladıktan sonra PUE, DCIE' den daha fazla kullanılmaya başladı dolayısıyla TGG altyapı enerji

verimliliğini ölçeklendirebilmek için de veri merkezlerinde PUE'yi kullanır hale geldi. PUE şuanda bilgi teknolojileri ekipmanlarının tükettiği enerji bilgisini alıp ölçeklendiren ve veri merkezi içerisine giren enerjinin ne kadar verimli kullanıldığını gösteren en iyi çözümdür. Formül ile açıklamak gerekirse toplam tesis enerjisinin BT ekipman enerjilerine bölümü PUE'yi, tam tersi BT ekipman enerjisinin toplam tesis enerjisine bölümü de DCIE'yi vermektedir. (Avelar, Azevedo, & French, 2012)

$$“PUE= \text{Toplam Tesis Enerjisi} / \text{BT Ekipman Enerjisi}” \quad (7.1)$$

$$“DCIE= \text{BT Ekipman Enerjisi} / \text{Toplam Tesis Enerjisi}” \quad (7.2)$$

“Toplam Tesis Enerjisi; soğutma, güç ekipmanları, aydınlatma, BT ekipmanları”

“BT Ekipmanları; sunucu, depolama aygıtları, ağ cihazları, yönlendiriciler, vb....”

BT ekipmanları enerjisi bütün BT ekipmanlarını kapsamaktadır. Örneğin; Sunucu, depolama aygıtları, yönlendiriciler, bağlantı cihazları, ekran ve bilgisayarlar. BT enerjisi kWh türünden ölçülmektedir, tavsiye edilen ölçüm PDU çıkışlarından veya mümkün değil ise UPS çıkışlarından yapılmaktadır. Toplam tesis enerjisi ise bütün BT ekipmanları ile beraber bu ekipmanları destekleyen / hizmet veren elektrik sistemlerinin bileşenleri (UPS, elektrik panosu, jenaratorler, PDU, bataryalar), iklimlendirme sistemlerinin bileşenleri (klima, soğutucular, pompa, bilgisayar odaları hava tahliye ve çevirme üniteleri) ve diğer bileşenler (lamba) gibi herşeyi kapsamaktadır. (Avelar, Azevedo, & French, 2012)

PUE bütün tesise uygulanabildiği gibi çok büyük tesislerde sadece tesis içerisindeki veri merkezine de uygulanabilir.

PUE değerleri 1.0'dan başlayarak artabilmektedir. Değerin 1.0 olması verimliliğin %100 olduğunu göstermektedir, ulaşılması istenen değer de budur. Çoğu veri merkezinin elde ettiği PUE değeri genellikle 3.0 veya daha yüksektir. Fakat 1.6 veya daha iyi değerler verimliliğin yüksek olduğu anlamına gelmektedir. (Avelar, Azevedo, & French, 2012)

Nadiren de olsa PUE değerinin 1.0'ın altında olduğu durumlar gözlemlenmektedir, bu normal bir durum olmadığı için National Renewable Energy Laboratory (NREL) ve Lawrence Berkeley National Laboratory (LBNL) beraber geliştirme çalışmaları yapmaktadır. TGG bu çalışmalar ile ilgili gerekli desteği vermektedir. (Patterson, 2010)

2.6.1.1. PUE'nin faydaları

PUE'nin faydalarını aşağıdaki şekilde özetleyebiliriz. (Avelar, Azevedo, & French, 2012)

- Enerji riskinden oluşabilecek problemleri ortadan kaldırarak işlem verimliliğini artırır,
- Diğer veri merkezleriyle karşılaştırıp analiz yapmayı sağlar,
- Veri merkezi yöneticilerinin zaman içerisinde tasarım ve süreçlerle ilgili geliştirme yapmalarına imkanı verir,
- İlave BT bileşenleri için yeniden enerji tasarlamasıyla ilgili bilgi verir,
- Yeni veri merkezi için tasarım hedeflerini ve modelleri oluşturur.

2.6.1.2. PUE ölçme seviyeleri

Pue'nin kullandığı üç farklı ölçme seviyesi vardır. (Avelar, Azevedo, & French, 2012)

Seviye 1; basit ölçme olarak isimlendirilir, BT yükü UPS'lerin ön tarafında bulunan ekrandan bakılarak ölçülür. Bu seviyede bu ölçüm en az ayda birkere yapılır daha sık yapılmasında tavsiye edilir.

Seviye 2; orta derece ölçme olarak tarif edilir. BT yükü veri merkezlerindeki PDU'ların önündeki panele bakarak ölçülür, ölçüm en az günde birkere yapılır ve daha sık yapılması da tavsiye edilir.

Seviye 3; ileri derece de ölçme olarak tanımlanır. BT yükü veri merkezindeki ekipmanlardan bireysel olarak ölçülür. Gelen enerji ölçümü bu iş için kullanılan uygulamalar tarafından yapılır. Güç ölçümü 15 dakikada bir veya daha sık sürelerde yapılabilirdiği gibi eş zamanlı olarakta yapılabilir.

2.6.1.3. Güç ve enerji sistemleri

Güç ve enerji sistemleri bilgi teknoloji altyapılarının sürekliliği için gerekli en önemli parçalardandır. Bu parçaların görevi sistemlere enerji sağlamanın yanı sıra akım düzensizliklerini ve kesintilerini bilgi teknolojileri sistemlerine hissettirmemektir. Bu sistemler; kesintisiz güç kaynakları, regülatörler, güç dağıtım üniteleri, güç kaynağı üniteleri ve jenaratörler olarak belirtilir. (Loucks & McCluer, 2012)

Kesintisiz güç kaynağı (UPS); UPS'ler şebekeden gelen alternatif akımı (AC) doğru akıma (DC) çevirerek bataryaları şarj eder, bataryalar ise akımı sistemin ihtiyacı olan şekilde aktarır. Kesintisiz güç kaynağı olarak tabir edilen UPS'ler üzerlerindeki bataryalar sayesinde enerji kesintilerini besleme süreleri kadar tolere edebilirken aynı zamanda elektrik dalgalanmalarına karşıda kritik BT sistemlerini korumaktadır.

Besleme süresi UPS'in sahip olduğu akülere ve enerjiyi tüketen sistemin tükettiği enerji miktarına bağlı olarak değişmektedir.

Regülatör; şehir şebekesinde dalgalanmalar yaşayan alternatif akımın hassas cihazlara zarar vermemesi için sabitlenmesini sağlayan cihazlardır.

Güç dağıtım üniteleri (PDU); ihtiyaç duyulan enerjiyi kritik BT sistemlerinin olduğu kabinette dağıtmayı sağlar. PDU'lar üzerinden enerji ölçümleri yapılabilir ve kontrol edilebilir. Bu ölçümler geçmişe yönelik veya eş zamanlı olarak yapılabilir, bu yüzden anlık olarak gerekli enerji ihtiyacını sağlayıp sağlayamadığını tespit edilebilir ve elde edilen bilgilerle gelecek için planlama yapılmasına destek olur.

Güç kaynağı ünitesi (PSU); PSU gelen voltajı düzenleyerek donanımların ihtiyacı olan 12V çıkış voltajına çevirir.

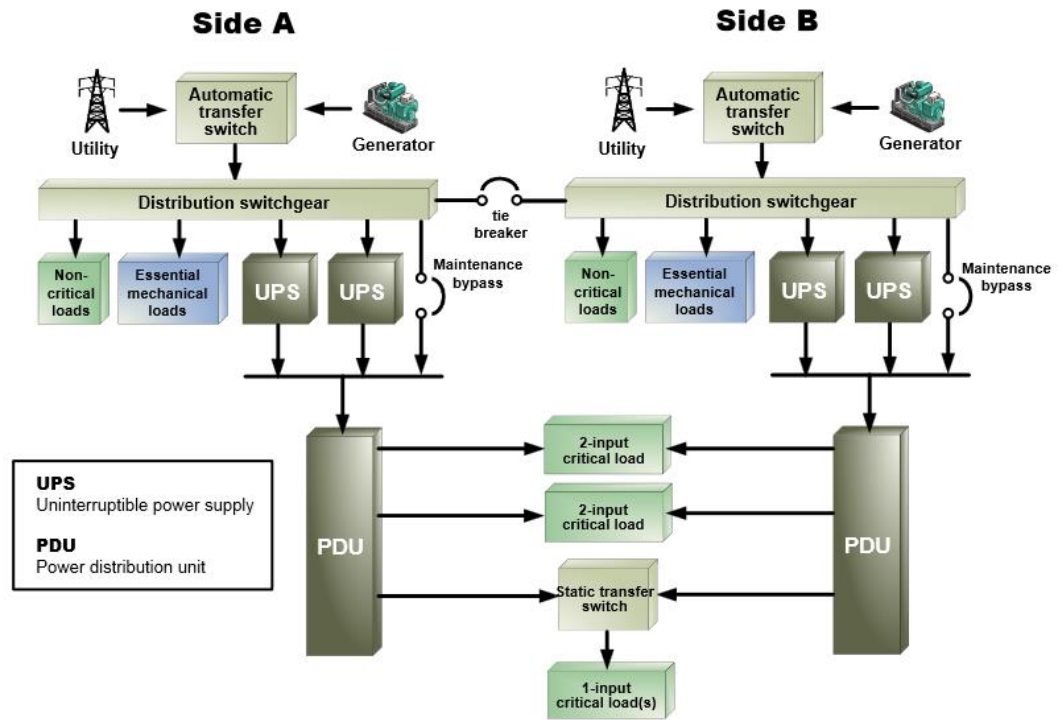
Jenaratör; jenaratörler AC (alternatif akım) yani şehir elektriği üreten cihazlardır. Bazı jenaratörler diğerleriyle paralel bağlanarak beraber çalışabilirler. Jenaratörler taşınabilir veya sabit olabilmekle beraber kW (kilowatt) / kVA (kilo volt amper) veya MW (megawatt) / MVA (mega volt amper) olarak güçlerine görede ayrılabilir. Jenaratörlerin yedeklemesi yapılırken birbirinden ayrı ve paralel veya birbirine seri şekilde bağlanarak yapılabilir.

2.6.1.4. Enerji yedekliliği

Planlı bakım çalışmaları veya beklenmeyen kesintilere karşı enerji altyapılarının yedekliliği sağlanır. Bu amaçla enerji altyapılarının yedekliliği A-B sistemi veya izole edilmiş yedekli sistemler olarak sağlanabilir. (Loucks & McCluer, 2012)

A-B (“Dual bus”) sistem;

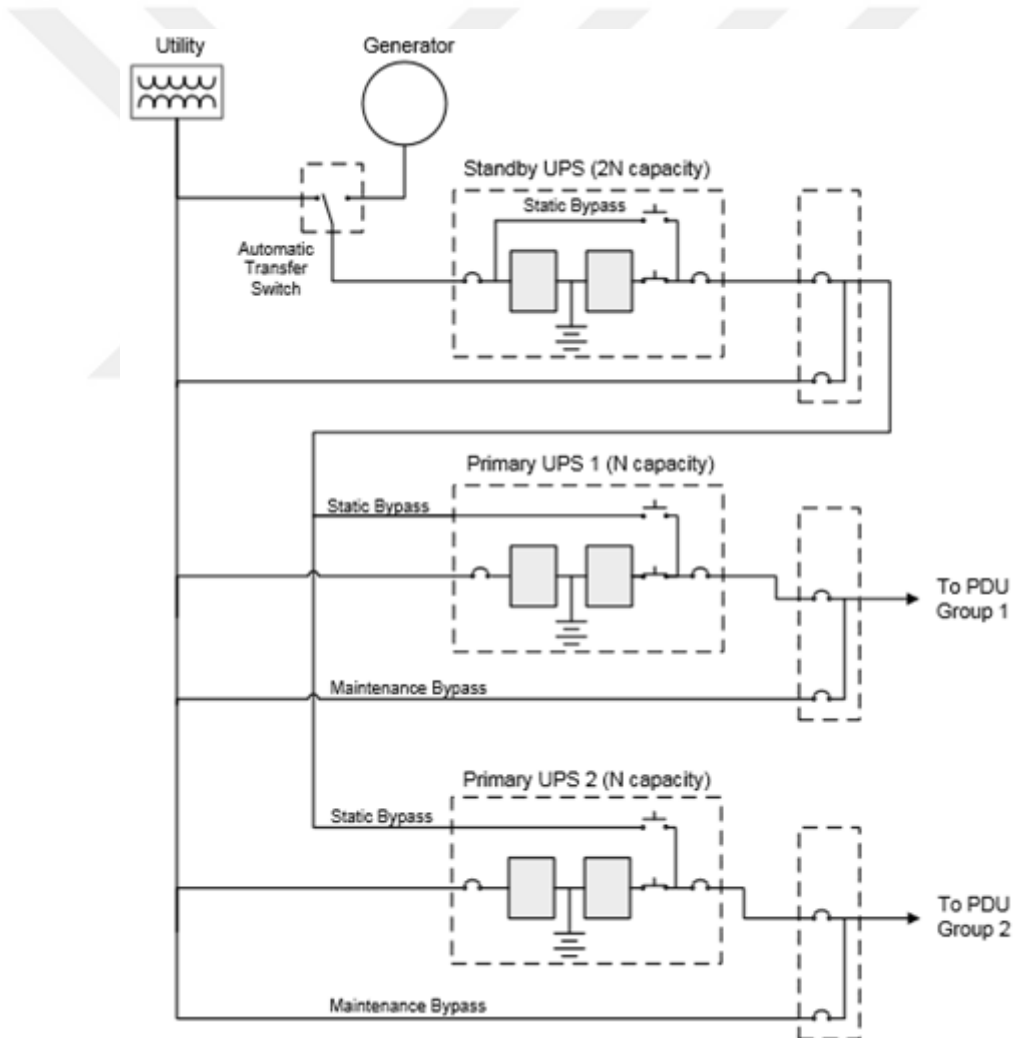
A-B güç sisteminde; enerji sistemlere A ve B olarak iki farklı kanaldan iletilir. Her kanal yedekli olarak birden fazla UPS ile UPS’ler ise enerji kesintisi halinde yeteri kadar elektrik üretebilecek şekilde konumlandırılmış jeneratörlerle desteklenir. Enerjiye ihtiyaç duyan kritik sistemler enerjinin bir kısmını A kanalından bir kısmını da B kanalından alacak ve enerji yükü yaklaşık %50 oranında paylaşılacak şekilde tasarlanır. Böylece yük dengeli olarak ikiye bölünmüş olur. Aynı zamanda her iki kanalda tek başına bütün enerji tüketen cihazları destekleyebilecek şekilde planlanır. Böylece kanallardan birinde problem olsa dahi diğer kanal tek başına bütün sistem için gereken enerjiyi sağlar. Bu sayede güç yedekliliği ideal seviyede sağlanmış olur.



Şekil 2.6. Dual Bus Enerji Tasarımı. (Loucks & McCluer, 2012)

İzole edilmiş yedekli sistem;

İzole edilmiş yedekli sistem de enerji farklı iki PDU grubundan farklı UPS grupları ile desteklenmektedir. Bir adet UPS grubu gerektiğinde ana UPS gruplarının yerine geçmek için bekleme modunda hazır konumdadır. Yedek olarak hazır konumda bekleyen grup ana grupların yerine geçebilecek kapasitede tasarlanır. Bu sistemde elektrik kesintisi durumunda bütün UPS'ler ortak jeneratörün ürettiği enerji ile desteklenir.



Şekil 2.7. İzole Edilmiş Enerji Tasarımı. (Loucks & McCluer, 2012)

Jeneratör ve UPS'ler veri merkezlerine enerji sağlayan cihazlar olsada amaçları ve çalışma şekilleri birbirinden farklıdır. UPS'ler kesintisiz güç kaynakları olarak çalışan cihazlardır, elektrik kesintilerinde veya şebekede meydana gelecek dalgalanmalarda sürekli devrede kalarak sistem kesintisini engeller ve sistemi korur. Sistem kesintisini engelleme süresi besleme süresi olarak adlandırılır. Besleme süresi; elektrik kesintisi yaşandığında UPS'lerin mevcut akülerinin sistem için gereken enerjiyi sağlayabileceği süredir. Bu noktada UPS sistemlerinde 2 önemli noktadan bahsedilebilir. Birincisi veri merkezimizin tükettiği enerjinin iyi hesaplanıp bu enerjiyi destekleyebilecek UPS akü gruplarına sahip olmak, ikinciside UPS'lerin uygun şartlardaki odalarda yedekli olarak çalışmasını sağlamaktır.

Jenaratörler ise UPS'lerden farklı olarak yakıt kullanarak elektrik üretilip sistemin ihtiyaç duyduğu enerjiyi sağlamak amacıyla kullanılırlar. Diğer fark ise Jeneratörler sürekli aktif değildir, elektrik kesintisi yaşandığında devreye girdikleri için birkaç saniyelik elektrik kesinti söz konusudur. Bu noktada kesintiden hiç etkilenmemek için jeneratör ve UPS'ler birlikte çalıştırılır. İdeal jeneratör konumlandırması veri merkezlerinin dışında cihazların ihtiyaç duydukları ortamda yedekli olarak yapılır.

2.6.2. Kablolama ve ağ altyapısı

Bilgi teknolojileri ekipmanlarının kendi aralarında düzenli iletişim kurabilmeleri için aynı standartları kullanmaları gerekmektedir. Bilgi teknolojileri iletişimi kablolama ve ağ cihazları (switch ve router) gibi ağ altyapı bileşenleri aracılığı ile sağlanır. (Cisco Systems Inc., 2015)

Switch; bilgisayar, printer, sunucu, vb. ekipmanların bir birine bağlanabilmesi, bir birinin kaynaklarına erişebilmesi ve veri alış verişinin verimli bir şekilde yapılması

için köprü ve kontrol görevini yerine getirerek ağ ortamını oluşturmak için kullanılan anahtar cihazlardır. Switchler yönetilebilen veya yönetilemeyen olmak üzere ikiye ayrılır. Yönetilemeyen switchler genellikle ev ortamında kullanılan basit yapıdır, yönetilebilenler ise profesyonel iş ortamında (veri merkezleri, iş yerleri, vb.) bazı kontrollerin, ayarlamaların ve izlemelerin yapılabilirdiği gelişmiş cihazlardır.



Şekil 2.8. Switch. (Cisco Systems Inc., 2015)

Router; switchler ağ ortamı oluşturmak için kullanılır fakat oluşturulmuş farklı ağ ortamlarının bir birine bağlanması gerekebilir. Tam bu noktada ağ yapılarında farklı ağlar arasında iletişim ihtiyacını karşılamak için router kullanılır. Ayrıca bilgisayar, vb. cihazların internete erişmesi içinde router'a ihtiyaç vardır. Bu noktada internet te farklı bir ağ olarak tanımlanır.



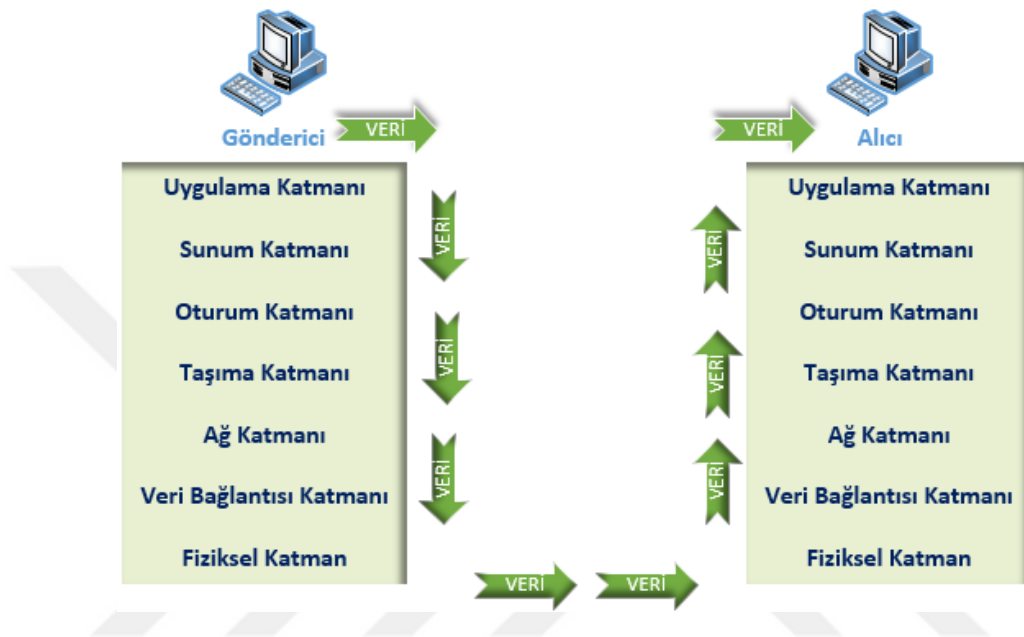
Şekil 2.9. Router. (Cisco Systems Inc., 2015)

Switch ve routerlara bağlı cihazların sağlıklı iletişim kurmaları için aynı protokolleri kullanmaları gerekir. Bu noktada ISO tarafından geliştirilen OSI modeli düzenli iletişim kurulması amacıyla geliştirilmiştir. Uygulama, sunum, oturum, ulaşım, ağ, veri bağlantısı ve fiziksel olmak üzere yedi katmandan oluşan OSI modelinin her katmanda kendi fonksiyonlarına göre kendine özel protokol ve standartları vardır. (Cisco Systems Inc., 1998; Microsoft Corporation, 2014; Lammle, 2007; Lammle, 2000)

Tablo 2.5. OSI Katmanları. (Cisco Systems Inc., 1998)

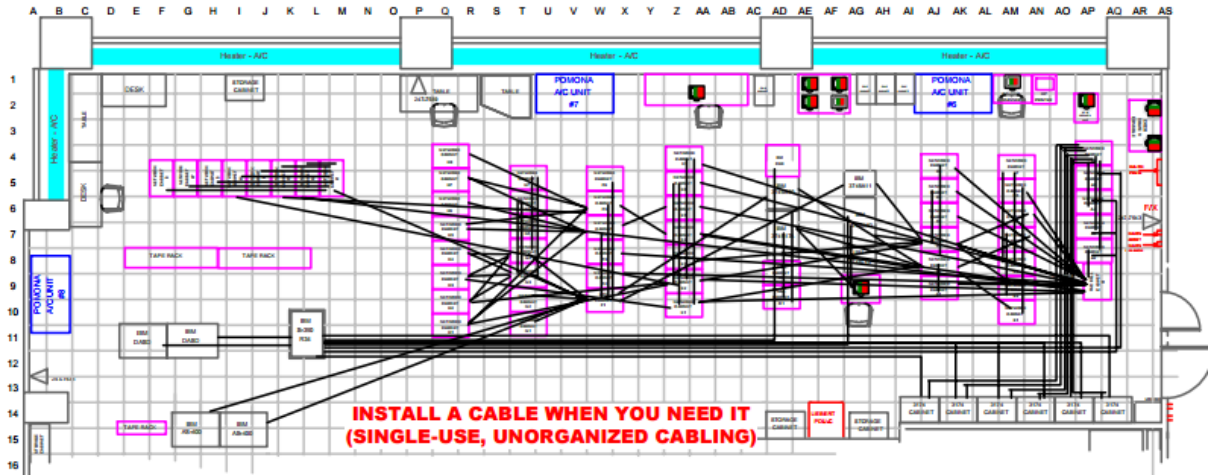
Katman	Açıklama	Protokol / Standart
7-Uygulama katmanı	Kullanıcıların uygulamaları çalıştırdığı son katmandır.	HTTP, FTP, SMTP, Telnet, SNMP, SSL, SSH.
6-Sunum katmanı	Verinin hangi biçimde sunulacağını belirlenip anlamlı hale getirildiği katmandır. Bu sayede gönderilen veri hedef bilgisayar tarafından anlaşılır hale gelir.	ASCII, JPEG, DOC, MPEG, DIVX.
5-Oturum katmanı	Bilgisayarlar arasında oturum açan ve kapatan katmandır. Aynı anda farklı bilgisayarlardan bağlanabilmeyi veya farklı oturumların bir biriyle karışmasına engel olarak aynı bilgisayarda birden fazla uygulama çalıştırmayı sağlar.	NetBIOS, NFS, SQL, SMB, RPC.
4-Taşıma katmanı	Veriyi hedefe iletmeyi sağlayan, bozularak iletildi ise tekrar iletilmesinin sağlandığı katmandır.	TCP, UDP.
3-Ağ katmanı	Verinin en kısa yoldan doğru hedefe gitmesini sağlayan katmandır.	IP, ARP, ICMP, IGMP, Router.
2-Veri bağlantısı katmanı	Ağ katmanından gelen mesajları MAC adreslerini kullanarak LAN üzerinden mesajların doğru cihazlara iletilmesinden sorumlu olan katmandır.	ATM, PPP, Frame relay, Ethernet, Wi-Fi, Switch.
1-Fiziksel katman	Verinin sayısal değerlere dönüştürülüp veri aktarımının yapıldığı katmandır.	Kablolar, RJ45, RS-232, Hub.

OSI katmanlarında veri transferi kaynaktaki uygulama katmanından başlar aradaki bütün katmanlarda işlemler sırayla başarılı bir şekilde tamamlandıktan sonra hedefteki uygulama katmanında sonlanır.

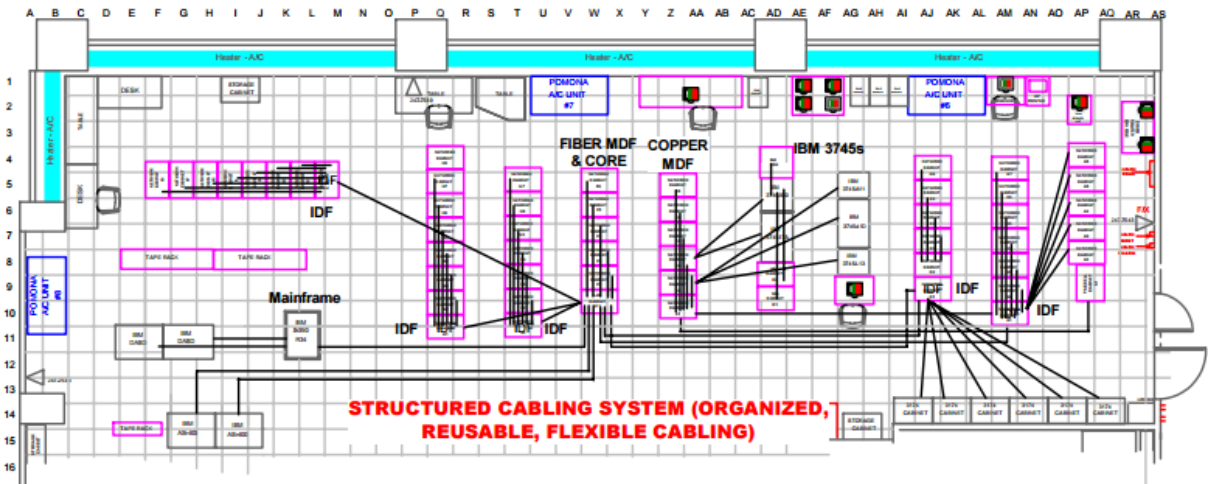


Şekil 2.10. OSI Veri Akışı. (Cisco Systems Inc., 1998)

Kablolama altyapısı da bilgisayar ağlarını oluşturmak için ağ cihazları ve kullanılan protokoller kadar önemlidir. Düzensiz yapılan kablolama altyapısından dolayı bütün ağ ortamı zaman içinde zarar görür ve oluşan problemlerin çözülmesi de kablo karmaşasından dolayı uzun sürer. Bunu engellemek amacıyla ANSI/TIA-942-A, ANSI/BICSI-002, CENELEC EN 50173-5 gibi standartlar geliştirildi. (Jew, 2012) Kablolama aynı kabinetteki cihazları birbirine bağlamak için, kabinetten başka kabinete bağlantı vermek için veya ISP hattını bağlamak amacı ile yapılabilir.



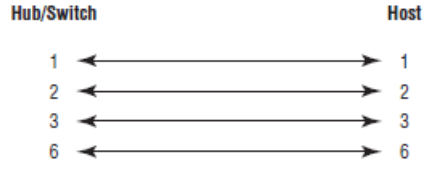
Şekil 2.11. Düzenlenmemiş Kablo Altyapısı. (DiMinico, 2006)



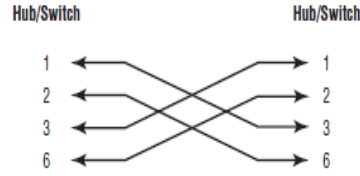
Şekil 2.12. Düzenlenmiş Kablo Altyapısı. (DiMinico, 2006)

2.6.2.1. Kablo bağlantı düzenleri

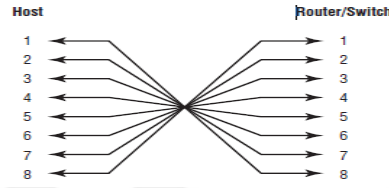
Kablolama şekilleri düz bağlantı yöntemiyle; Switch'den fiziksel sunucuya veya Switch'den Router'a, çapraz bağlantı yöntemiyle; Switch'den Switch'e, fiziksel sunucudan fiziksel sunucuya veya Router'dan fiziksel sunucuya şeklinde olabilir. Sarmal kablo yöntemi ise network cihazlarının yönetilmesi için seri bağlantı şeklinde yapılır. (Lammle, 2007; Lammle, 2000)



Şekil 2.13. Düz Bağlantı. (Lammle, 2007)



Şekil 2.14. Çapraz Bağlantı. (Lammle, 2007)



Şekil 2.15. Sarmal Bağlantı. (Lammle, 2007)

Veri kablosundan iletilen verinin zarar görmemesi, özellikle manyetik enerjiden etkilenmemesi için enerji ve veri kabloları birbirinden farklı kanallardan ve koruyucu düzeneklerle ayrılmaktadır. Örneğin veri kabloları genellikle kabinetlerin üzerinde onlar için ayarlanmış tepsilerin içinden geçirilirken enerji kabloları ise yükseltilmiş zeminin altında onlar için ayarlanmış tepsiler içinde düzenlenmektedir. Kablolamanın düzenli olması kadar sistemin stabil ve performanslı çalışması için ihtiyaç duyulan bant genişliğini ve kablo mesafesini de iyi hesaplamak gerekmektedir. Hesaplanan değerlere göre hangi tür kablonun kullanılacağına karar verilebilir. (Jew, 2012)

2.6.2.2. Kablo türleri

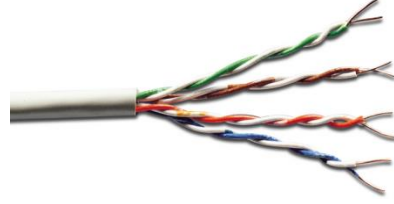
Veri merkezlerinde genellikle çift bükümlü kablo, koaksiyel kablo veya fiber optik kablo türleri kullanılmaktadır (Cisco System Inc., 2003; HP Inc., 1998).

Çift bükümlü kablo; veri merkezlerinde veri iletişimi için çok yaygın kullanılan kablo türüdür. Kablonun çift bükümlü olması kablodan iletilen verinin bozulmasını engellemektedir. Veri transferi sırasında her bir kablonun etraflarında ufak bir manyetik alan oluşur, kabloların bir birine sarılmış olması bir birinin etrafında oluşan manyetik enerjiyi yok ederek verinin bozulmasını engeller. Bu şekilde çalışan bükümlü kablolar UTP ve STP olarak iki sınıfa ayrılır.

UTP (Unshielded Twisted Pair) kablo; en çok kullanılan bükümlü ve dört çift telden oluşan veri kablosudur, UTP kablolar en fazla 100 m mesafeye kadar veri iletimi yapabilir, daha uzun mesafelerde kullanılabilmesi için en fazla her 100 m’de bir tekrarlayıcı cihazlar konumlandırılır. 100 m’den daha uzun mesafede bağlantı yapılması gerekiyorsa tekrarlayıcılar yerine daha uzak mesafelere kadar veri iletebilen kablolar kullanılması veri iletimi için daha doğru olmaktadır. UTP kabloların üzerinden geçireceği verinin iletim hızı 10 ile 1000 Mbps aralığında olabilmektedir.

En çok kullanılan UTP kablo türleri telefon iletişimi için Cat1 (kategori 1), 4 Mbps hızındaki veri iletimi için Cat2, 10BASE-T ağlarda 10 Mbps hızındaki veri iletimi için Cat3, Token Rings networkler de 16 Mbps veri iletim hızı için Cat4, 100 Mbps veri transferi için Cat5, 1000 Mbps yani 1 Gbps değerlerinde veri iletimi için Cat5e kablo türü kullanılır. Günümüzde yaygın olarak AWG’nin (American wire gauge) desteklediği 1 Gbps hızındaki dört çift sarmal olan Cat6 kablo kullanılmaktadır. Gerekli performaslara ulaşabilmek için bilgisayarlarda kullanılan bağlantı kartlarında

gerekli desteđi sađlaması gerekmektedir. Bilgisayar veya diđer ađ cihazlarının bađlantıları iin genellikle RJ-45 konnektr kullanılır. Kablonun ince yapısı kullanımı ve ucuz olması da satınalma aısından avantajlar sađlarken, ok uzun mesafelerde kullanılamaması dezavantajı olarak ortaya ıkmaktadır. (Microsoft Inc., 2015),



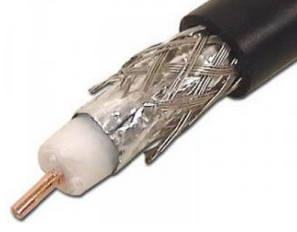
Şekil 2.16. UTP Kablo. (Eko Kablo, 2015)

STP (Shilded Twisted Pair) kablo; metal folyo ile sarılarak koruma altına alınan kablo, oluşan manyetik alanlara karşı iletilen verinin bozulmaması iin daha iyi koruma sađlar. STP kablolar 10 Mbps ile 100 Mbps veri iletim hıza ulaşabilirken UTP’de olduđu gibi 100 m mesafeye kadar veri iletimi sađlayabilirler. UTP kablo da olduđu gibi aynı RJ-45 konnektr kullanılır. STP kablo yapısı nedeniyle maliyeti daha yksek ve kullanımı daha zordur. Bu nedenlerden dolayı ok fazla tercih edilmemektedir.



Şekil 2.17. STP Kablo. (BWorks, 2015)

Koaksiyel kablo; koaksiyel kablo genellikle ses, video iletimi veya “Bus Topolojiye” sahip networklerde veri transferi iin kullanılır. Veri transferinde 10 Mbps – 100 Mbps veri hızına ulaşabilirken 500 m mesafeye kadar kullanılabilir. (BWorks, 2015)



Şekil 2.18. Koaksiyel Kablo. (Miratec, 2009)

Fiber optik kablo; fiber optik kablolar genellikle çok hafif bir plastik kaplamayla koruma altına alınırlar. Bu kaplama içerideki veri iletiminin yapıldığı cam tüpü çevreleyerek zarar görmesini engellemektedir. Fiber optik kablo diğer kabloların içerisinde veri iletimini en hızlı ve en uzak noktalara yapabilen kablo türüdür. Dolayısıyla maliyeti diğerlerine göre daha yüksektir. Single ve multi olmak üzere iki tür fiber optik kablo vardır. Single mod lazer şeklinde çalışır. 10 km den daha uzak mesafelerde kullanılır. Bu özelliği nedeni ile maliyeti multi mod'dan daha yüksektir. Multi mod LED şeklinde çalışır ve en fazla 2 km mesafeye kadar veri transferi yapabilir ve 1 Gbps' ın üzerinde veri transfer hızı sağlar. Bütün fiber optik yapılarda çalışma mantığı ışık iletimi şeklindedir. Bağlantı yapabilmek için SC (Subscriber Connector) ve ST (Straight Tip) olarak iki farklı konnektör kullanır. Günümüzde büyüyen veri boyutları ve veri iletim hızının önemli hale gelmesinden dolayı veri merkezlerinde çok kullanılan kablo türü olmuştur.



Şekil 2.19. Fiber Kablo. (Kreasis, 2014)

Tablo 2.6. Kablo Karşılaştırması. (Cisco System Inc., 2003; HP Invent, 2006)

Kablo Türü	En Fazla Mesafe	En Fazla Hız	Avantaj	Dezavantaj
UTP	100 m	1000 Mbps / 1 Gbps	Kolay ve geniş kullanım alanı.	Çok uzun mesafelerde kullanılamaz.
STP	100 m	100 Mbps	Veri bozulmalarına karşı daha gelişmiş koruma özelliği.	Kullanım zorluğu ve çalışma mesafesi.
Koaksiyel	500 m	100 Mbps	Kullanım mesafesi.	Hız limiti.
Fiber Optik	10 km üzeri	100 Gbps	Daha güvenli, daha uzak mesafelere daha hızlı veri transferi.	Maliyet.

2.6.3. İklimlendirme sistemleri

İklimlendirme; veri merkezlerinde havanın temizlenmesi, sıcaklık, soğukluk, nem gibi değerlerin yönetilmesi ve hava akışının sağlanması amacıyla dünya standartları kapsamında ölçeklendirilen bir süreç olarak tanımlanabilir. Genellikle yapılan hataların önüne geçmek için bu dünya standartlarının iyi bilinmesi gerekiyor. Hataların başında veri merkezlerinin soğutulması gelmektedir. Veri merkezinin kontrollü soğutulmasının yanısıra iklimlendirilmeye de ihtiyacı vardır. Çünkü veri merkezlerinde hizmet veren sunucu, depolama aygıtları, yedekleme cihazları, ağ bileşenleri gibi BT ekipmanlarının, üreticilerin belirlediği değerlerde soğutması ile beraber sıcaklık, nem, hava akışı ve havanın temizlenmesine de ihtiyaçları vardır. Sürekli çalışan bu ekipmanların ürettikleri ısı ve genişleyen iş hacmi, artan ekipman sayıları nedeni ile iklimlendirilmiş hava şartlarının bozulma eğiliminde olması sürecin hassasiyetle değerlendirilmesi gereken bir konu olduğunu göstermektedir. Cihazların

ihtiyacı olan oda şartları sağlanmazsa bu cihazlar kendi ısıttıkları havayla beraber hata vermeye ve iş sürekliliğini etkilemeye başlarlar. Veri merkezinde çalışan ekipmanlar verimli şekilde çalışabilmek için gerekli oda şartlarına ihtiyaç duyarlar. İklimlendirme sistemlerinde soğuk ve sıcak hava değerlendirmeleri genellikle BTU/h, ton/d cinsinden ölçülür. BTU küçük, orta ve büyük çapta sistemler için, ton ise büyük sistemler için iklimlendirme kapasitesini tanımlamak amacı ile kullanılan ölçü birimidir. 1 ton iklimlendirme bir saat içerisinde ortamdan çekilebilecek 12000 BTU'ya karşılık gelmektedir. (McDowall, 2006)

Başarılı bir iklimlendirme için ASHRAE tarafından 2004 yılında yayınlanan “Thermal Guidelines for Data Processing Environments” (Veri İşleme Birimleri İçin Isı Önerileri) 2008 yılında kuru sıcaklık, nem ve yoğunlaşma değerlerini tekrar güncellemiştir. Bu güncellemeler üreticilerden gelen bilgiler, testler ve değerlendirmeler ışığında yapıldığı için ASHRAE standartlarına dikkat ederek iklimlendirmenin sağlanması çok önemlidir. Bu değerler veri merkezi verimliliğini en üst seviyeye çıkarmak için planlandığı gibi aynı zamanda iklimlendirme maliyetlerini de düşürmektedir. ASHRAE iklimlendirme ortamlarını 4 farklı sınıfta incelemektedir. Birinci sınıf; zamana bağlı işlerin gelişmiş BT bileşenleriyle yapıldığı ve çok önemli ortam kontrollerinin olduğu veri merkezleridir. İkinci sınıf; veri merkezinden ziyade BT cihazları için ayrılmış bir oda veya ofis ortamıdır, bu ortamda daha düşük hacimli işler yapılır ve yapılan ortam kontrolleri birinci sınıf kadar önemli değildir. Üçüncü sınıf ortam; ofis ve ev ortamlarını ifade etmektedir. Dolayısıyla gelişmiş BT cihazlarının yerine bilgisayarlar, laptop ve yazıcı gibi aygıtlar söz konusudur. Düşük seviyede ortam kontrolleri yapılmaktadır. Dördüncü sınıf ise satış noktaları olarak ifade edilir, herhangi bir ortam kontrolü yapılmamaktadır. Dolayısıyla veri merkezleri

iklimlendirme değerleri birinci sınıfa göre ele alınır. Aşağıdaki tablolarda sınıflara göre iklimlendirme değerleri ve versiyonlar arası karşılaştırma verileri verilmektedir. (ASHRAE, 2011)

Tablo 2.7. ASHRAE 2008 Yönergeleri. (ASHRAE, 2011)

Sınıf	Çalışan Ekipmanlar				Kapalı Konumdaki Ekipmanlar	
	Kuru Sıcaklık (°C)		Nem Oranı (%)		Kuru Sıcaklık (°C)	Nem Oranı (%)
	İzin Verilen	Önerilen	İzin Verilen	Önerilen		
1	15 - 32	18 - 27	20 - 80	60	5 - 45	8 - 80
2	13 - 58	18 - 27	20 - 80	60	5 - 45	8 - 80
3	5 - 35	-	8 - 80	-	5 - 45	8 - 80
4	5 - 40	-	8 - 80	-	5 - 45	8 - 80

Tablo 2.8. ASHRAE 2004 ve 2008 Yönergeleri Karşılaştırması. (ASHRAE, 2011)

	2004 Yılı Değerleri	2008 Yılı Değerleri
En Düşük Sıcaklık (°C)	20	18
En Yüksek Sıcaklık (°C)	25	27
En Düşük Nem (%)	40	60
En Yüksek Nem (%)	55	60

ASHRAE'nin bu değerleri yayınlarken BT bileşenleri üreticilerinin yayınlamış olduğu değerleri ölçü olarak alması, çok fazla sayıda üretici olması, bütün ekipmanların çalışma ortamı değerlerinin ortak en verimli değerde düzenlenmesinin gerekliliği ve veri merkezlerinin çok çeşitli üreticilerin cihazlarına ev sahipliği yaptığı gerçeği ile ASHRAE'nin belirlediği değerlerin çok önemli olduğu anlaşılmaktadır. (ASHRAE, 2011)

2.6.3.1. Başarılı bir iklimlendirme için dikkat edilecek hususlar

Veri merkezlerinde verimli bir iklimlendirme yapabilmek için gereken unsurlar aşağıdaki şekilde özetlenebilir. (Emerson Electric Co., 2007)

- Veri merkezinin zemin ve duvarları dış ortamdan yalıtılarak dışarıdan herhangi şekilde ısı veya hava akışı engellenir, aynı şekilde içerideki havanın kontrolsüz şekilde dışarıya çıkmasına izin verilmez,
- BT ekipmanlarına ev sahipliği yapan kabinetler soğuk ve sıcak havanın birbirine karışmasını engelleyecek şekilde yerleştirilir. Kabinetler soğuk hava koridorundan soğutulmuş havayı çekecek, kabinet içindeki cihazların ürettikleri sıcak havayı da sıcak hava koridoruna doğru transfer edecek şekilde tasarlanır,
- Kabinet içinde, etrafında veya yükseltilmiş zeminin altından yapılan kablolama işlemleri hava akışını engellemeyecek şekilde düzenlenir. Yükseltilmiş zeminin altından çok fazla kablolama yapılması ihtimali ile özellikle zeminden soğutmalı sistemlere engel olmaması açısından zemin yüksekliği en az 2,4 m yüksekliğinde tasarlanır, (Bouley & Brey, 2009)
- CRAC / CRAH (Computer Room Air Conditioner / Computer Room Air Handler) üniteleri sıcak hava koridorundan yükselen sıcak havayı kolay çekecek şekilde tasarlanmalıdır. Örneğin üniteler sıcak hava koridorlarının başında konumlandırılır veya ısınan havayı kolay çekebilmesi için tasarımlar geliştirilir,
- Kabinet sayıları ve yoğunluğu, tesis büyüklüğü ve iklimlendirilecek alan dikkate alınır.

2.6.3.2. İklimlendirme yöntemleri

Veri merkezi iklimlendirmesi için 10'dan fazla yöntem vardır ama en uzun tecrübe edilmiş ve en yaygın olarak kullanılan yöntemler CRAC, CRAH, CRAC/CRAH daraltılmış alan ve kabinet soğutma olarak özetlenebilir. Soğutma sistemleri temel olarak kabinet, koridor ve tesis seviyesinde olmak üzere kategorize edilirken yeni nesil veri merkezlerinde genel olarak CRAC veya CRAH daraltılmış alan sistemi tercih edilmektedir. (Kennedy, 2009)

CRAC/CRAH daraltılmış alan; CRAC şuanki veri merkezlerinde sık kullanılan yöntemlerden birisidir. Doğrudan genişleyen soğutucu gaz aracılığı ile soğutma gerçekleşir. Bu sistemin soğutma kapasitesi yaklaşık olarak 30 tondur, veri merkezi soğutma planlaması bu kapasiteye göre yapılır. Soğutmanın yanında nem oranını da ayarlayabildiğinden gerçek bir iklimlendirme sağlamaktadır. (Kennedy, 2009)

Dış ünite olarak nitelendirilen yoğunlaştırıcılar (Condensing unit) soğutma sistemlerinde ısınan havanın yer değiştirmesi, dışarıya atılmasından özetle hava dolaşımının yapılmasından sorumlu ünitelerdir. Ufak ünitelerde sadece soğutucu vardır, hava akımını yer çekimi gücüyle yaparlar. Genellikle kullanılan model büyük olan yani içerisindeki motor ve fanlar yardımıyla hava akımını sağlayan modellerdir. Dış üniteler hava dolaşımını kolay yapabilecek şekilde açık ortamlara yerleştirilir. (ASHRAE Inc., 2012)

Bu yapıdaki soğutma sistemlerinde veri merkezinin hava dağılımı görevini CRAC ünitesi üstlenmektedir. Ünite ortamdaki sıcak havayı soğutmak için çekip soğutulan havanın tekrar zeminden veri merkezine dağıtılmasından ve gerekli nem değerlerinin

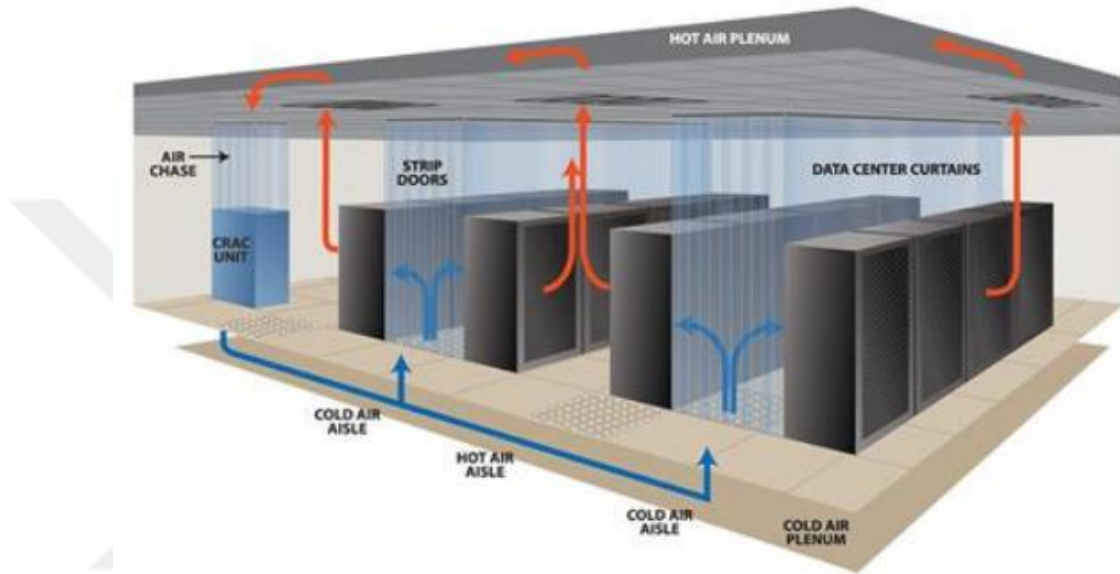
sağlanmasından sorumludur. Böylece veri merkezinin ihtiyacı olan hava akımı ve oda şartları sağlanmış olur. (Rasmussen, 2003; Smith, 2013)

CRAH soğutma sistemi ise diğer sık kullanılan yöntemdir. Bu yöntemde soğutma işlemi doğrudan genişleyen gaz yerine soğutulmuş su ile yapılmaktadır. 1000 ton'a kadar soğutma yapılabildiği için CRAC'a göre daha büyük alanlara uygulanabilir. Soğutmayla beraber veri merkezinin nem oranını da düzenleyerek gerekli oda şartlarını sağlamaktadır. (Kennedy, 2009)

Akan su soğutmayı iki şekilde yapar ; buharlaştırıcıdan (evaporator) geçen su ısısını bırakarak tekrar soğuk hale gelir, bu olay “Chilled Water (Soğutulmuş su)” olarak adlandırılır. Su dolaşımını yoğunlaştırıcıdan (condenser) yaparak soğutuluyorsa bu süreç “Condenser Water (Yoğunlaştırılan su)” olarak isimlendirilir. Ton olarak hesaplanan chiller kapasitesi standart olarak saatte 12,000 BTU sıcak enerjiyi çekebilir. Genel olarak 1-3 ton kapasitelerinde olmakla beraber genişleyen büyük yapılarda 10,000 ton kapasitesinde çıkabilmektedir. Chiller kapasitesiyle soğutulacak alan kapasitesi iyi hesaplanmalıdır. Gerekli soğutma kapasitesini sağlamak için birden fazla chiller beraber çalıştırılabilir. (McDowall, 2006)

CRAC ve CRAH sistemlerinin kullanılabildiği “Daraltılmış Alan Soğutma Sistemi” son yıllarda kullanılmaya başlayan ve giderek artan yöntemdir. Soğuk ve sıcak hava koridorları oluşturulur, kabinetlerin yerleştirilmesi ve veri merkezinin bunu destekleyecek şekilde tasarlanması gerekir. Çünkü amaç veri merkezindeki sıcak ve soğuk havanın bir birine karışmasını engellemektir. CRAC/CRAH üniteleri soğuk havayı yükseltilmiş zemine iletir, iletilen hava soğuk hava koridorlarında kabinetlerin önündeki ızgaralardan yükselir. Yükselen soğuk hava kabinetlerdeki ekipmanların

fanlarıyla emilerek kabinetlerin arkasına yani sıcak hava koridoruna iletilir. Isınan hava doğal yapısı gereği yükselir ve yükselen hava CRAC/CRAH üniteleri tarafından tekrar çekilir. Sıcak ve soğuk havanın birbirine karışmaması enerji tüketimini de düşürmektedir. (Kennedy, 2009)



Şekil 2.20. Sıcak Ve Soğuk Hava Koridorları. (Akın & Ketenci, 2010)

2.6.4. Yangın önleme altyapısı

Yangın hem çevreye hem de canlı hayatına zarar veren bazen kaza bazen de eğitimsizlik ve bilinçsizlik gibi nedenlerden kaynaklanan felaketlerdendir. Bu nedenle hem kendi sağlığımızı hemde çevreyi bu felakete karşı korumak zorundayız. Veri merkezlerinde de yangın koruma sistemleri insan hayatını, veriyi ve çevreyi koruyan önemli konular arasındadır. Yangın koruma sistemleri her zaman ihtiyaç olmayan fakat ihtiyaç halinde de büyük önem kazanan sistemlerdir. Bu nedenle yangın olasılığına karşı her zaman tedbirler alınır ve yangın esnasında ne yapılması gerektiği konusunda insanlar bilinçlendirilir. Veri merkezlerindeki yangın olayı, veri merkezinden kaynaklı yani doğrudan veya veri merkezi dışındaki etmenlerden dolayı

olarak gerçekleşebilir. Yangını söndürmek çok önemlidir, fakat asıl amaç yangının oluşmasını engellemektir.

2.6.4.1. Veri merkezi yangın risk grupları

Yangına karşı tedbirler almadan önce önemli adımlarından biri de önce nelerin yangın kaynağı olabileceğini belirlemektir. Veri merkezlerinde yangına karşı alınacak birinci tedbir veri merkezlerinde BT ekipmanları veya destekleyici bileşenlerin dışında herhangi bir ekipman konumlandırılmamasıdır. Böylece veri merkezleri sadece yangın riski düşük olan BT ekipmanları, kablolar, iklimlendirme ve enerji sistemlerine ev sahipliği yapmış olur. Veri merkezi yangın risk grupları aşağıdaki şekilde özetlenebilir. (Hurley, 2013)

BT ekipmanları; BT ekipmanlarından kaynaklı olarak yangın çıkma riski bu ekipmanların düşük enerjiyle çalışması nedeniyle düşüktür. Birtakım bileşenler çalıştıkları süre içerisinde ısınmaya neden olurlar, fakat onlarda kendilerine özel soğutucular ile soğutulmaktadır. Soğutucularda problem olsa bile bileşenlerin sıcaklıkları dahili sıcaklık ölçerler tarafından ölçülür ve üreticilerin belirlediği yüksek derecelere ulaştığında sistemler otomatik olarak kapanarak olası bir yangını engeller. Sıcaklık değerleri belirli seviyeye ulaştığında ilgili sorumlulara otomatik bilgi veren sistemler aracılığıyla bilgi verilerek olası problemlerin önüne geçilir.

Kablolar; veri merkezlerinde veri ve enerji transferi olmak üzere iletim yapan iki tip kablo kullanılır. Veri transferi yapan kablolarda yüksek derecede ısınma oluşmadığı için bunlardan kaynaklı yangın riski yoktur. Enerji taşıyan kablolar veri kablolarına göre yükleri nedeniyle ısınmaya ve yangına daha elverişlidir. Bu yüzden özellikle enerji kabloları için önlemler alınır ve tasarımlar yapılır. Yükseltilmiş zemin altından

yapılan kabloların yangın riskini oluşturmayacak şekilde tasarlanır. Yangın olayının gerçekleşmesi anında ise yangın söndürücülerin yükseltilmiş zeminin altına temas etmesi için gerekli tedbirler önceden alınır.

İklimlendirme sistemleri; iklimlendirme sistemlerinin veri merkezlerindeki havayı çekmek için harcadıkları yüksek enerji ve hava dolaşımını sağlamak için kullanılan yüksek seviyeli motorlar yüksek derecelerde ısınmaya neden olur.

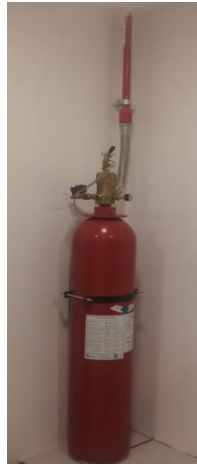
Enerji sistemleri; enerji sistemleri veri merkezlerinin içinde bulundurulmaları dahi besleyici üniteler olarak risk grubuna dahil olurlar. Jeneratör, UPS, elektrik panoları gibi enerji üretimi, depolanması veya transferini yapan ekipmanlar yoğun enerjiden dolayı aşırı ısınmaya maruz kalabilirler. Isınmayı kontrol altına almak ve enerji sistemlerinin ısınmasını engellemek amacıyla gerekli iklimlendirme şartlarının sağlanması yangın riskini ortadan kaldırmaktadır.

2.6.4.2. Yangın önleme sistemleri

Genel kabul görmüş ve NFPA (National Fire Protection Association) tarafından desteklenip yayınlanmış bazı yangın koruma standartları vardır. Özellikle NFPA veri merkezlerini ve BT ekipmanlarını yangına karşı korumak için olması gereken en az gereklilikleri ile ilgili standart 75'i. Ses, video, veri transferleri gibi hizmetlerin sunulduğu telekomünikasyon tesisleri için de standart 76'yı geliştirdi. Yangın önleme sistemleri durağan gaz, taşınabilir püskürtme tüpü ve su püskürtme sistemi olarak gruplanabilir. (Hart, 2011)

Durağan gaz sistemi; kritik sistemlerin olduğu ortamlarda tavsiye edilen yöntemdir. BT ekipmanlarına zarar vermez, bu gazla maruz kalan ekipmanlar hizmet vermeye

devam ederler. Kablolama ve iklimlendirme için kullanılan yükseltilmiş zeminlere dikkat edilmesi gerekir, gerektiğinde ortama iletilen gazın yükseltilmiş zemine erişebilmesi için tasarımlar geliştirilir. IGFS (Inert Gas Fire Suppression System) olarak isimlendirilen bu sistem nitrojen, argon veya ikisinin karışımını birden içerebilir. Gazlar hareketsiz olarak büyük tüplerde tutulur. Bu sistem çok hızlı şekilde havadaki oksijenin değerini %13-15'e düşürerek yangını söndürür. Yanmanın gerçekleşmesi için havadaki oksijen değerinin en az %16 olması gerekmektedir. Düşürülen oksijen değeri insan yaşam faaliyetlerinin devam etmesi için yeterli olduğundan bu sistem insana zarar vermediği gibi çevreye ve elektronik ekipmanlara da zarar vermemektedir. Dolayısıyla veri merkezlerinde genel olarak tercih edilen söndürme sistemidir. Bu sistemlerin içinde FM-200 en yaygın kullanılan gaz sistemidir. (NFPA, 2003; Rawson & Green, 2012)



Şekil 2.21. Yüksek Hacimli Sabit Tüp.

Taşınabilir püskürtme tüpü; taşınabilir tüpler karbondioksit veya halojen olmak üzere iki türe sahiptir. Halojen tür elektronik ekipmanlara zarar vermediği için veri merkezlerinde kullanılabilir. Söndürme kapasiteleri çok büyük olmadığı için ufak çaplı yangınlarda kullanılması uygundur. (NFPA, 2003)



Şekil 2.22. Taşınabilir Tüp.

Su püskürtme sistemi; genel olarak ele alındığında, su püskürtme sisteminde bir depo içinde bekletilen su ihtiyaç halinde otomatik olarak pompalar vasıtasıyla ilgili alanlara püskürtülür bu çalışma mantığına göre veri merkezlerinin bulunduğu binalar su püskürtme sistemiyle koruma altına alınabilir ancak BT ekipmanlarının olduğu veri merkezlerinde su püskürtme sistemi kullanılmamaktadır. Çünkü amaç sadece yangını engellemek veya söndürmek değil yangın söndürme işlemi tamamlandığında BT ekipmanlarının hala hizmet verebilir ve veriye ulaşılabilir durumda olmasını sağlamaktır. Veri merkezleri bulundukları bina içindeki diğer ortamlardan yeteri kadar yalıtılmış ve yangına yüksek seviyede dayanaklı yangın kapısı, ısı geçirmez ve yanmaz duvarlar gibi yapı malzemeleriyle inşa edilmiş olmaları gerekir. Bu söndürme sistemi veri merkezlerinin içinde kullanılsa da veri merkezi alanlarını korumak amacıyla etrafında veya veri merkezlerinin olduğu binaların ofis vb. alanlarında kullanılmaktadır. (NFPA, 2003)



Şekil 2.23. Su Püskürtme Sistemi. (Üçler Yangın, 2011)

Yangın söndürme sistemleri ortamdaki sensörler aracılığı ile otomatik olarak devreye alınabilir veya sensörler sadece uyarı vermesi için ayarlanıp gerek duyulursa sistemler manuel olarak devreye alınabilir. Bu sistemlere ne zaman ihtiyaç duyulacağı önceden bilinemediği için tercih edilen yöntem sistemin otomatik olarak devreye girmesidir.

2.6.5. Veri merkezi izleme sistemleri

Veri merkezi altyapısı hazırlanıp kurulumların yapılmasıyla devreye alınan bütün ekipmanların olası bir probleme karşı anlık olarak izlenmesi gerekmektedir. Yapılan bu işlem BT ekipmanlarındaki performans kaybı, sistem kesinti, yangın ve su baskını gibi olası birçok problemi engelleyecektir. Bütün ekipmanlar bireysel olarak izlene bildiği gibi veri merkezi ortamında özellikle ısı, nem, duman ve hava kirliliği, su baskını, enerji giriş-çıkış voltajları sensörler aracılığı ile izlenmektedir.



Şekil 2.24. Sıcaklık Sensörü.



Şekil 2.25. Sensör Kumandası.

Veri merkezi izleme süreci ortamdan bilgi toplama, toplanan bilginin atanmış varsayılan değerlerle karşılaştırılması ve çıkan sonuca göre otomatik uyarı sisteminin ilgililere bilgi verilmesi şeklinde olabildiği gibi kritik veri merkezlerinde ilgili kişilerin, bütün değerleri eş zamanlı olarak ekrandan takip etmesi şeklinde de yapılmaktadır.

BT ekipmanları (sunucu, depolama ve ağ cihazları), iklimlendirme, yangın koruma ve enerji cihazlarının üreticileri kendi ürettikleri izleme uygulamaları aracılığı ile anlık olarak izlenebilir veya uyarı ayarlarında otomatik bildirim yapılması için mail, sms gibi bilgiler girilerek olağan dışı bir olay gerçekleştiğinde ilgili kişilere bilgi vermesi sağlanabilir. Geniş uygulama aralığı olduğu düşünüldüğünde bütün ekipmanların izleme kayıtları merkezileştirilip tek noktadan izlenip raporlaması daha verimli olmaktadır. Aynı anda bir veya daha fazla veri merkezinin birlikte izlenebileceği düşünüldüğünde merkezileştirilmesi daha büyük önem kazanmaktadır.

2.6.6. Veri merkezi güvenliği ve erişimi

Güvenlik; veri merkezini bilinçli veya farkında olmadan zarar verebilecek herkese karşı alınacak tedbirler bütünüdür, sürecidir. Süreçtir çünkü güvenlik sadece ürün

değildir veya sadece ürünlerle sağlanacak bir hizmet değildir. Veri merkezlerinin kurulması, iş sürekliliği için bütün ekipmanların yedekli olması, istenilen işlerin istenildiği gibi çok kısa sürede tamamlanabilmesi istenilen ama tam anlamıyla yeterli olmayan konulardır. Bütün bu süreçlerin başladığı gibi devam etmesi, en değerli varlık verinin her zaman erişilebilir ve hızlı işlenebilir olması aynı zamanda bu sürecin güvenliğine bağlıdır. Bilgi güvenliğini üç ana konuda ele alabiliriz. Verinin gizliliği ve bütünlüğü erişilebilirliği gibi çok önemlidir. Gizlilik verinin işletme içi veya işletme dışı yetkisiz kişilerce erişilmesini engellemektir. Bütünlük verinin yetkisiz kişilerce bozulması, değiştirilmesi veya silinmesine engel olmaktır. Erişebilirlik özelliği ise veriye ihtiyaç olduğu her an kullanabilmek amacıyla erişmek olarak tanımlanır. (Önel & Dinçkan, 2007)

İşletmeler verilerini yeteri kadar önem vererek korumak zorundadır ve bu zorunluluk sürecin en başından sonuna kadar gereklidir. Güvenlik zaafiyetinden dolayı verilerin yok olması veya başkalarının eline geçmesi itibar kaybı, para kaybı, müşteri kaybı gibi çok büyük zararlar doğurabilir. Bu yüzden bu sürecin hassasiyetle yönetilmesi gerekir. Bunun için kullanılan zarar verici yöntemlerin iyi bilinmesi ve bunlara göre önlemler alınması gerekir. Veri merkezlerinde güvenlik konusu siber güvenlik ve fiziksel güvenlik olarak iki alanda incelenebilir.

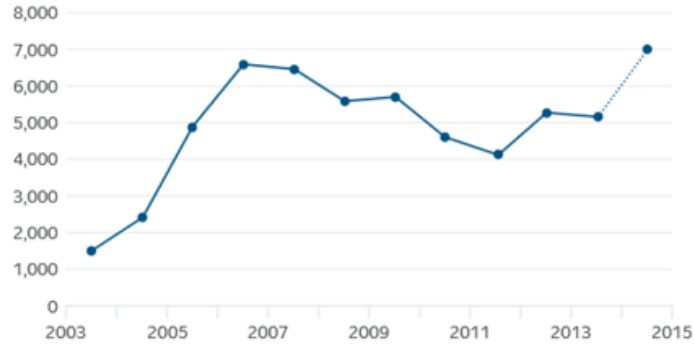
2.6.6.1. Siber güvenlik

Güvenlik önlemleri almak için öncelikle ne tür siber atakların yapıldığını kimler tarafından yapıldığını iyi bilmek gerekir. Yapılması gerekenlerden biriside sadece dışarıdan gelecek zararlara karşı değil işletme içi çalışanlara karşıda tedbirler almaktır. Dolayısıyla sağlanan güvenlik içeriye ve dışarıya doğru çift taraflı sağlanmalıdır.

Güvenlik ihlali bilinçli yapıldığı gibi bazı kişilerin farkında olmadan da yapabildikleri bir zaafiyettir. Bu yüzden veri güvenliği farkındalığı çok önemlidir. Veri merkezi sistemlerine atak yapan kişiler hacker olarak isimlendirilir ve bunlar beyaz şapkalı, gri şapkalı ve siyah şapkalı olarak sınıflandırılır. Beyaz şapkalılar erişim sağladıkları sistemleri dinleyerek güvenlik açıklarını tespit eder ve ilgili kişilere bilgi verir. Siyah şapka da ise amaç işletme verilerini ele geçirmek ve erişim sağlanan sisteme zarar vermektir. Gri şapkalı olanlar ise iyi ve kötü arasında kalmış iki tarafta da görev alabilen hackerlardır. Bütün atak yapan kişiler benzer yöntemler ve uygulamaları kullanarak saldırılarını gerçekleştirirler. Genellikle ağ tarama, sistem atağı, zararlı yazılımlar (trojan, backdoor, malware, ransomware, botnet, malicious, diğer virüsler), spam mail, ortam dinleme, DDOS, sosyal mühendislik, SQL atakları, araya girme, web sunucu, kablosuz ağlar, bellek taşıma gibi ataklar yapılır. (EC-Council, 2010)

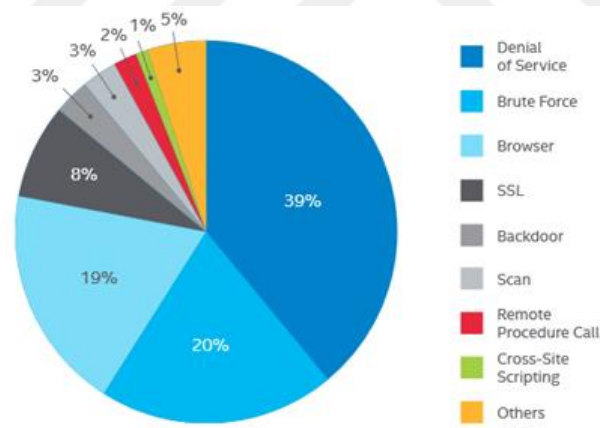
Artan internet suçlarıyla beraber sayısız güvenlik ürünü (güvenlik duvarı, IPS, antivirüs, internet filtre uygulamaları, vb.) piyasada kullanılmaya başlandı. Bu şekilde birçok işletme kendini güvenlik altına aldı, fakat güvenlik insan faktörünün en zayıf halka olarak önemli rol aldığı bir süreçtir. Dolayısıyla güvenlik ürünlerine yapılan yatırımlar kadar insana da yatırım yapıp farkındalığın sağlanmış olması çok önemlidir. Aksi taktirde yüksek maliyetler gerekiren güvenlik ürünü yatırımları aslında amacına hiçbir zaman ulaşamaz. (Simon & Mitnick, 2003)

Artan iş hacimleri ve iş türleri değişik uygulamalara ihtiyaç duyulmasına neden olmuş ve zaman içinde geliştirilen uygulamalarında kendi içlerinde güvenlik açıklıkları olduğu görülmüştür. Bu açıklar sürekli kontrol edilip gerekli tedbirler alındığı sürece güvenlik sağlanabilir.



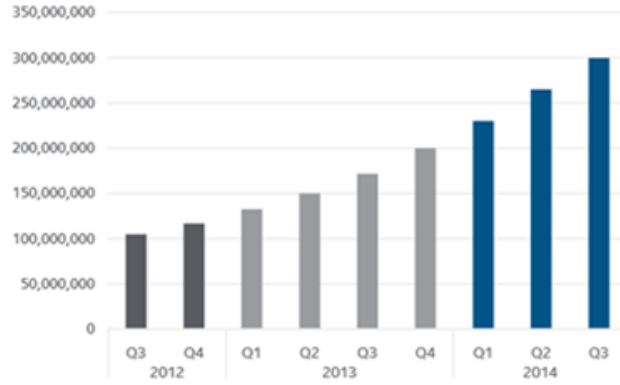
Şekil 2.26. Yıllara Göre Uygulama Güvenlik Zaafiyetleri. (McAfee, 2014)

Günümüzde güvenli olarak gördüğümüz birtakım uygulamalar, sistemler, standart protokoller zaman içerisinde üzerlerinde çalışılıp güvenlik zaafiyetleri tespit edildikten sonra artık güvenilmez hale gelebilirler. Dolayısıyla günümüzde güvenli olan bir hizmet, uygulama, cihaz vb. gelecekte artık güvenli olmayabilir.



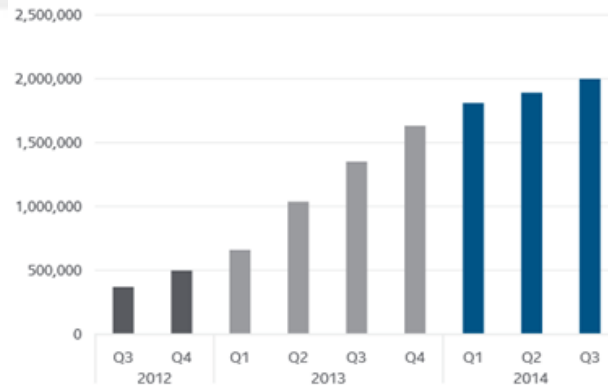
Şekil 2.27. Ağ Atak Yöntemleri. (McAfee, 2014)

Sistemlerden veri çalmak için bazen standart bilinen atak yöntemlerinin uygulanmasının yanı sıra ileri düzey programlama ve sistem bilgisine sahip hackerlar zararlı uygulamalar geliştirerek sisteme zarar verebilir veya sahip olunan verileri çalabilirler, bu yöntemde çok kullanılan yöntemlerden birisidir.



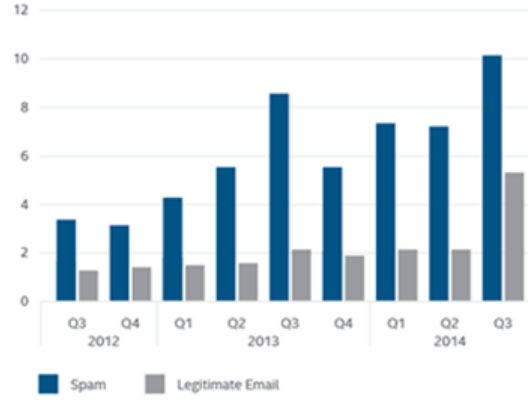
Şekil 2.28. Yıllara Göre Zararlı Yazılım Grafiği. (McAfee, 2014)

Kötü niyetli kişiler işletmelerin verilerini bozmanın dışında bu verilerin çalınması üzerine yoğunlaşarak bu vasıta ile işletmelerden para talep etmeleri de yaygın olarak kullanılan yöntemlerden biridir. Özellikle son günlerde ransomware olarak isimlendirilen şifreleme atağı bunun en büyük örneği olmuştur.



Şekil 2.29. Şifreleme Atağı. (McAfee, 2014)

İşletmeler işleyişlerinin büyük kısmını mailler üzerinden sağlamaktadırlar. Bu yoğunlukta kullanıma sahip mailler de güvenlik zaafiyetleri için kullanılabilir hale geldi. Dolayısıyla yıllık mail trafiğinin çok küçük kısmı gerçek maildir. Gelen mailleri açmadan önce göndericinin gerçek olduğuna dikkat etmek bilgi güvenliği farkındalığı yüksek bir harekettir.



Şekil 2.30. Mail Trafiği. (McAfee, 2014)

2.6.6.2. Fiziksel güvenlik

Siber atakların dışında veri merkezlerine fiziksel olarak erişebilecek kişilerde sınırlandırılmaktadır. Veri merkezine erişim için gerekli yetkiler sadece belirli yetkinliğe sahip insanlara verilir, konu hakkında yeterli bilgiye sahip olmayan kişilerin erişim sağlaması ve farkındalığın eksikliği sonucunda yapılan ufak bir hata çok ağır şekilde geri dönebilir. Yapılan veri merkezi erişimleri kayıt altına alınır ve yetkisiz erişimlere izin verilmez. Veri merkezlerine erişim genellikle yetkilendirilmiş kişiler için iris tarama veya parmak izi okuyucu cihazlar ile yapılır. Bu sayede sisteme daha önce tanımlanmış kişilerin ne zaman giriş-çıkış yaptıkları kayıt altına alınmaktadır.



Şekil 2.31. Kart Ve Parmak Okuyucu.

Veri merkezine erişim yapan kişilerin ne amaçla veri merkezlerine giriş yapacakları ilgili formlar ile imzalı olarak kayıt altına alınmaktadır. Veri merkezine erişen yetkili veya yetkili kişi nezaretinde erişen kişilerin içeride yaptığı bütün aktiviteler veri merkezini her açıdan izleyen kameralar ile kayıt altına alınmaktadır.



Şekil 2.32. Kamera.

2.7. Yedeklilik Ve İş Sürekliliği

Bilginin en değerli varlık olarak karşımıza çıktığı tarihten günümüze kadar bilgiye ulaşmak ta, kendisi kadar değerli olmuştur. Firmaların faaliyet gösterdikleri alanlara göre bu önem derecesi değişiklik göstermekle birlikte vazgeçilmezleri olmuştur. Herhangi bir felaketten dolayı veri merkezlerinin verdikleri hizmetlerinin kesintiye uğraması veya sahip oldukları verilerinin zarar görmesi karşılabilecek problemler arasındadır. İş sürekliliği; veriye sadece felaket anında erişememe veya planlı bakımlardan kaynaklı kesintiler olarak düşünülemez. Sahip olunan verinin bozulması, silinmesi veya çalınması da iş sürekliliğini kesintiye uğratan önemli konulardır. Dolayısıyla iş sürekliliğinde iki temel konu vardır. Birincisi herhangi bir nedenden dolayı sisteme erişememekten kaynaklı, ikincisi de sisteme erişim ile ilgili bir problem olmayıp erişilen sistemde verinin yok olması veya bozulmasıdır. Bu durumlara göre iş sürekliliği için dikkat edilmesi gereken bazı hususlar vardır. Bu hususlara ne seviyede dikkat edildiği veya bu hususların detaylarının ne kadar bilindiği önemlidir. İş sürekliliği noktasında bilgi teknolojileri en önemli birimlerden biridir. Fakat iş

sürekliliğini sadece teknolojiye dayandırmakta yanıřtır, bununla birlikte dış etmenlerde önem arz etmektedir. Bütün detayların iyi bilinmesi ve değeriendirme yaparken teknolojik ve teknolojik olmayan bütün bileşenlerin beraber değeriendirilmesi iş sürekliliği için doğru kararlar alınmasını sağlamaktadır.

İş sürekliliği oluşumunun temel nedeni veriye her zaman her yerden ulaşmaktır. Bu noktada amaç felaket sırasında her yerden veriye kesintisiz ulaşabilmek ve bunu sağlayabilmek için gereken planlama ve çalışmaların en üst seviyede ve yüksek hassasiyette gerçekleştirmektir.

Rekabet ortamlarında işletmeler zamana bağılı hizmet verdikleri için bazen çok kısa sistem kesintileri dahi kabul edilebilir değildir. Özenle yapılan iş sürekliliği planı, yönetimi ve testleri işletmenin oluşan bu felaketlerden en az etkiyle veya hiç etkilenmeden hizmet vermeye devam etmesini sağlar. Bir çok işletme çözüm ortaklarıyla veya başka işletmelerle de entegre olarak çalışmaktadır. Bu yüzden birlikte çalışılan diğer taraflarında iş sürekliliği konusunda aynı özeni göstermeleri önemlidir.

Veri merkezlerinde sürekliliğini sağlayan konular BT ekipmanlarının yedeklenmesi, verinin yeklenmesi ve hatta veri merkezinin fiziksel olarak yedeklenmesi diğer bir ifade ile felaketten kurtarma merkezlerinin kurulması olarak belirlenebilir.

2.7.1. BT ekipmanlarının yedeklenmesi

Enerji altyapısı, iklimlendirme, yangın söndürme, kablolama, güvenlik, izleme gibi bütün altyapı hizmetlerinin sağlanmasındaki esas amaç veriyi korumak olsa da veriyi koruyabilmek için diğer yapılması gereken veriyi barındıran veya veriye erişimi sağlayan BT ekipmanlarını da korumaktır. Fakat her ne kadar korumak için tedbirler

alınırsa bu ekipmanların yedeğinin olması önemlidir. İş sürekliliği konusunda sunucu, ağ aygıtları, depolama üniteleri, güvenlik duvarı gibi cihazların hepsi aktif – aktif başka bir ifade ile eş zamanlı yedekli çalışacak şekilde veya aktif – pasif yani esas cihazda problem olduğunda yedek olarak hazır bekletilen cihazın otomatik olarak devreye girecek şekilde ayarlanabilir. Yedekleme süreçleri BT ekipmanlarından internet erişiminin yedeklenmesine kadar bütün aşamalara uygulanabilir. Veri merkezi süreçlerini, yedeklenmiş sistemler olmadan sağlamak bu sürecin herhangi bir noktasında oluşacak problem, uzun süre sisteme erişilememe veya bazı durumlarda verilerin kalıcı olarak zarar görmesine neden olabilir.

2.7.2. Verinin yedeklenmesi

Veri merkezlerinde verinin yedeklenmesi kesinlikle yapılması gereken tedbirlerden biridir. Yedeklenen veriye ne zaman ihtiyaç olur bilinmez, fakat ihtiyaç olduğunda veri yedeklenmemiş veya yedeklenen veri geri kurtarılamıyorsa işletmelerde geri dönüşü olmayan kayıplar oluşabilir. Dolayısıyla yedekleme tarafında iki konu gündeme gelmektedir. Birincisi başarılı yedeklemedir, ikincisi de yedeklenen verinin ihtiyaç anında istenildiği şekilde geri kurtarılabilesidir. Günümüz teknolojisinin ulaştığı noktada yedekleme birkaç yöntemle farklı kaynaklardan farklı kaynaklara doğru yapılabilmektedir. Yedekleme işlemi; bir yedekleme uygulaması tarafından belirlenen saat ve günlerde otomatik olarak çalışacak görevler aracılığı ile yedekleme ünitelerindeki yedekleme kartuşlarına veya depolama ünitelerine yapılabilir. Belirlenen saat, gün veya yedekleme sıklığı veri miktarı, yoğunluk ve kritiklik seviyesi ile orantılıdır.

2.7.2.1. Yedekleme türleri

Öncelikle yedekleme türünü belirlerken ihtiyaca doğru karar vermek gerekir. Genel olarak tam, farksal ve artan olarak 3 tip yedekleme türü vardır. Son zamanlarda dördüncü olarak tekilleştirme yöntemi de yoğun olarak kullanılmaya başlanmıştır. Çoğunlukla tam yedekleme yöntemi kullanılsa da hepsinin kendisine göre avantaj ve dezavantajları vardır. (Symantec, 2015; Dinçkan, 2008)

Tam yedeklilik;

Tam yedeklilikte seçilen bütün veri olduğu gibi yedeklenir. Bütün verinin yedeklenmesinden dolayı en güvenli yöntemdir ve dolayısıyla en uzun süren yöntemdir. Herhangi bir çalışma yapılacağı veya risk görülen durumlar oluştuğunda özellikle tam yedekleme yöntemi kullanılır.

Farksal yedeklilik;

Bu yöntem, tam yedek yöntemindeki gibi bütün veriyi yedeklemez. En son alınan tam veya artan yedeğe ihtiyaç duyar ve en son yapılan tam veya artan yedeklemelerden sonra sadece değişen verinin yedeğini alır. Sadece değişen verinin yedeklenmesi sayesinde yedekleme işlemi tam yedeklemeye göre daha kısa sürede tamamlanır ve verinin yedekleneceği alanda yer tasarrufu sağlar. Bu özelliği ile faydalı olmakla birlikte veriyi geri yüklerken kendisinden önce alınmış tam veya artan yedeğe ihtiyaç duyması da dezavantajıdır. Veriyi geri yükleme aşamasında kendinden önce tam veya artan olarak yedeklenen veriler zarar görürse veya herhangi bir nedenden dolayı o verilere erişilemezse son aldığı farksal yedeği de geri yükleyemez. Örneğin pazartesi günü veriler tam yedek yöntemi ile yedeklendikten sonra diğer günlerin farksal olarak yedeklendiği durumda, pazartesi günü dışındaki bütün günlerde sadece pazartesiden

sonraki deęiřen veri yedeklenmektedir ve geri ykleme yapılırken pazartesi gnnn tam yedeęindeki verilere de ihtiya duyulur.

Artan yedeklilik;

Artan yedeklilik ynteminde farksal yedeklilik ynteme benzemekle beraber nemli farkları da vardır. Bu yntemde de ama verinin yedeklendięi alanda yer kazanmak ve yedekleme iřleminin daha kısa srmesini saęlamaktır. Fakat artan yedeklilik ynteminde yapılan yedekleme iřleminden sonra, tekrarlanan artan veya farksal yedekleme iřleminde sadece en son yedekleme iřleminden sonra deęiřen veriler yedeklenir. rneęin; pazartesi gn tam yedekleme iřlemi yapıldıktan sonra artan yedekleme yntemi ile yedekleme iřlemine devam edildięi durumda, her gn bir nceki gnden sonra deęiřen veriler yedeklenecektir. Dolayısıyla artan yedekten geri ykleme iřlemi yapılacaęında tam yedek alınan gne kadar olan btn verilerin yedeęine ihtiya duyulacaktır.

Tekilleřtirilmiř (Deduplication) yedek;

Geliřmiř algoritmaya sahip tekilleřtirme iřleminde yedeklenecek veri paralara ayrılır eęer daha nce bu paralar yedeklenmemiřse paralar olduęu gibi yedeklenir. Fakat daha nce blmlere ayrılmıř veri yedeklenmiřse sadece yedeklenen blmn tutulduęu adres referans olarak kaydedilir yani yedeklenmiř paralar tekrar yedeklenmez ve ihtiya halinde veri bu adresten geri yklenir. Bu iřlem zaman ve maliyet aısından ileri derece fayda saęlar. Yedeklemenin dıřında iřletim sistemleri ve depolama nitelerinin alıřma yntemide bu řekilde tasarlanmaya bařlandı. (EMC Corporation, 2016)

2.7.3. Felaketten kurtarma merkezleri

Felaketten kurtarma merkezleri iş sürekliliğini destekleyen konuların en geniş kapsamlısı ve geline son noktadır. Diğer iş sürekliliği için yapılan çalışmaların yetersiz kaldığı, teknoloji, insan veya doğal afetlerden dolayı veri merkezin tamamen erişilmez durumda olduğunda devreye giren yedek veri merkezleridir. Ülkelerin hatta şehirlerin bulundukları coğrafi konumlara göre farklı doğal afetler ve iş sürekliliğini etkileyecek diğer problemler, oluş şekilleri ve sıklıklarına göre değişiklik göstermektedir. Bu felaketlerle karşılaşan firmaların hizmetlerini sürdürebilmeleri ve marka değerlerini koruyabilmeleri gerekmektedir. Bu yüzden alınması gereken birtakım tedbirler vardır.

“Türkiye’de TÜBİTAK UEKAE tarafından 2005 yılında yapılan bir araştırmanın sonucuna göre kurumların sadece %11’i iş sürekliliği planı uygulamaktadır.”
(Dinçkan, 2008)

En büyük felaket, felaketlere karşı hazırlıksız olmaktır. Felaket planı olmayan ve felaketten yaşandıktan sonra önemli veri kaybına uğrayan işletmeler de yapılan araştırmalara göre; *“işletmelerin %43’ünün faaliyetlerinin tamamen durduğu, %51’inin iki yıl içinde kapandığı ve sadece %6’sının varlıklarını sürdürebildiği”* görülmektedir. (Haag & Cummings, 2012)

Kurum ve kuruluşlar faaliyetlerini sürdürebilmeleri için her zaman beklenmedik olaylara karşı tedbirli olmak zorundadırlar. Veri merkezi yöneticileri tarafından iyi yönetilmiş, planlanmış, analiz edilmiş, testleri yapılmış ve dersler çıkartılmış felaket kurtarma merkezleri sayesinde; işletmelerin hatta ülkelerin ekonomileri güven altına alınabilir.

Bu amaçla faaliyet gösteren felaketten kurtarma merkezleri; felaket oluştuktan birkaç saat sonra devreye girebilecek tam donanımlı, felaketten birkaç gün sonra devreye girebilecek yarı donanımlı, felaketten sonra birkaç hafta içinde devreye girebilecek az donanımlı ve asıl veri merkeziyle aynı özelliklere sahip felaketten çok kısa süre sonra devreye girebilecek eş zamanlı felaket kurtarma merkezleri olarak gruplanabilir. (Dinçkan, 2008)

Felaket kurtarma merkezlerinin ihtiyacını ortaya çıkaran felaketleri; doğal afetler, insandan kaynaklı felaketler ve hibrit olarak üç ana başlık altında toplamak mümkündür. (Hiles, 2007; Snedaker, 2007; Doğdu, 2009)

Doğal afetler;

- Sel,
- Çığ,
- Deprem,
- Tsunami,
- Volkan patlaması,
- Heyelan,
- Hortum,
- Kasırga.

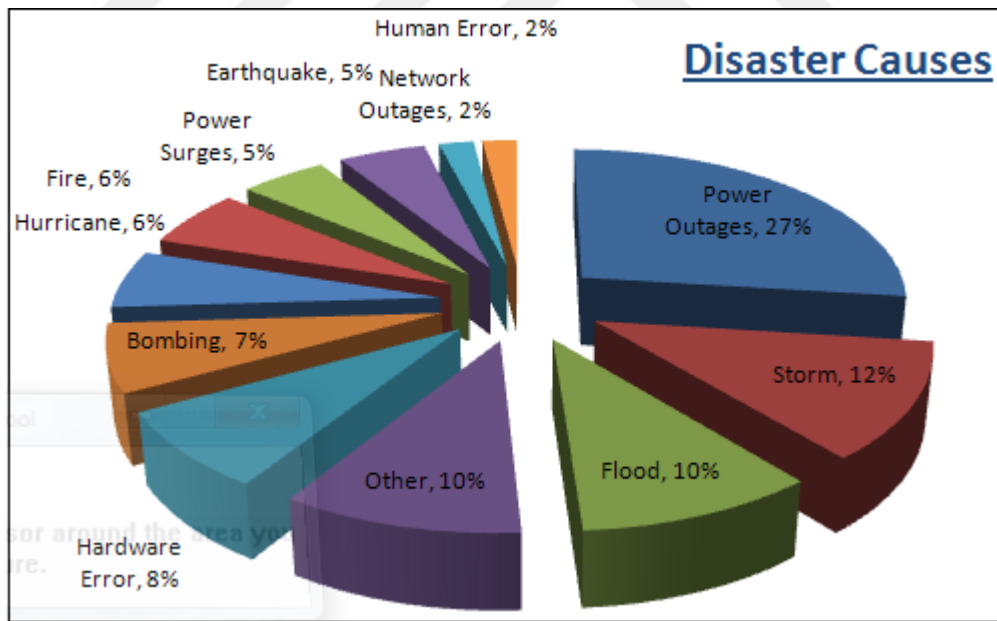
İnsandan kaynaklı felaketler;

- Terörizm,
- Grev,
- Patlama,
- Yangın,
- Siber atak,

- Politik protestolar,
- Doğrudan işletmeye yönelik protestolar,
- Radyoaktif serpinti,
- Hırsızlık,
- Gasp ve adam kaçırma.

Hibrit (Doğal afetler ve insandan kaynaklı);

- Ulaşım kazaları,
- Enerji kesintisi,
- İletişim kesintisi,
- Enformasyon sistemlerinde ortaya çıkan kesintiler,
- Bilgisayar sistemlerinden kaynaklanan hatalar.



Şekil 2.33. Felaket Nedenleri ve Görülme Oranları. (Higgins, 2011)

2.7.3.1. Önemli kavramlar

Felaket kurtarma merkezleri için en önemli kavramlar, asıl veri merkezindeki verilerin felaketten kurtarma merkezine transfer edilme sıklığı yani ne kadarlık veri kaybı

olacağı ve ne kadar sürede felaket kurtarma merkezinin aktif hale getirilebileceğidir. Bu noktada işletmenin kabul edilebilir veri kaybı, kabul edilir kesinti süresi, kabul edilebilir en uzun kesinti süresi ve iş süreçleri süresi gibi kavramlar ortaya çıkmaktadır. (Snedaker, 2007), (Dinçkan, 2008)

Kabul edilebilir veri kaybı (Recovery point objective);

Kabul edilebilir veri kaybı (RPO); verilerin ne sıklıkla felaketten kurtarma merkezine transfer edileceğini gösteren değerdir. Eğer veri transferi eş zamanlı yapılmıyorsa felaketten kurtarma merkezi devreye alındığında veri kaydı olabilir. Bu konuda karar verirken işletmelerin ne kadarlık veri kaybını kabul edebildikleri doğru hesaplanmalıdır. Teknolojinin geldiği noktada maliyetlere bağlı olarak eş zamanlı transfer sayesinde veri kaybı sıfıra indirilebilir.

Kabul edilebilir en uzun kesinti süresi (Maximum tolerable downtime);

Kabul edilebilir en uzun kesinti süresi (MTD); işletmenin fonksiyonlarını yerine getirmesine engel olan, kabul edebileceği en uzun kesinti süresidir. İşletmeler zaman zaman çoklu işlem yapabilirler veya bazı uygulamaları çok yoğun bazıları seyrek olarak kullanılabilir. Bu durumda kabul edilebilir en uzun kesinti süreleri iş süreçlerine bağlı olarak değişebilir. Bu değer hesaplanması için $MTD = RTO + WRT$ olarak formülü kullanılır.

Kabul edilir kesinti süresi (Recovery time objective);

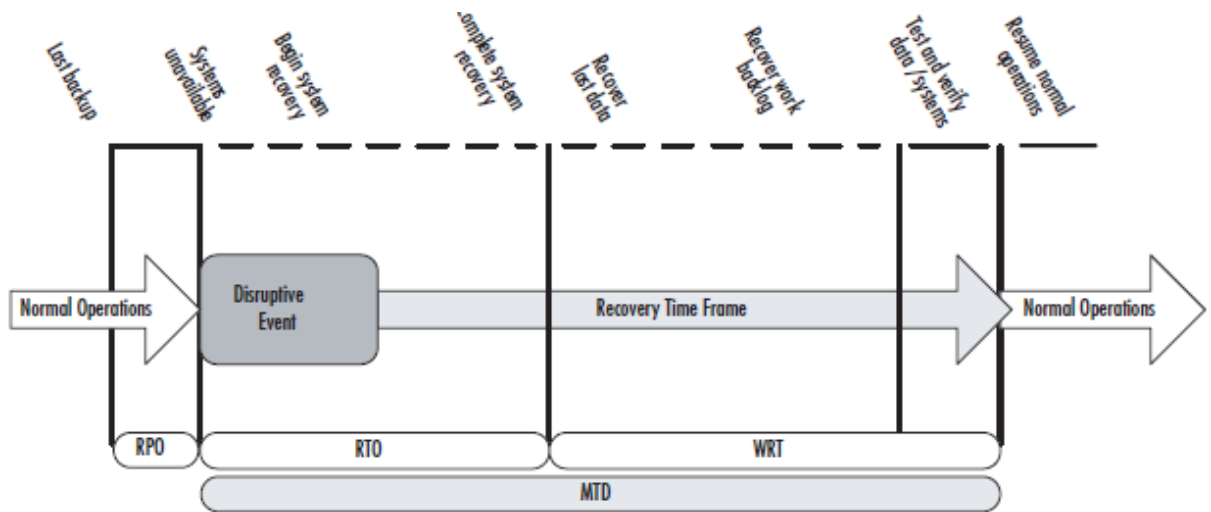
Kabul edilir kesinti süresi (RTO); kabul edilebilir en uzun kesinti süresinin birinci parçasıdır, felaket kurtarma merkezine transfer edilen veriye erişim için gereken sistemin tekrar devreye alınması için harcanan süredir. Yedekleme süreçlerinde olduğu gibi esas amaç transfer edilen veriye çok hızlı şekilde erişmektir. Bu nedenle

felaket anında hizmet verecek bütün ekipmanların hazır olması gerekmektedir. Bu işlem genellikle sistem ve ağ yöneticileri tarafından gerçekleştirilir.

İş süreçleri süresi (Work recovery time);

İş süreçleri süresi (WRT); kabul edilebilir en uzun kesinti süresinin ikinci aşamasını oluşturur. Erişime açılan sistemde transfer edilen son veri tekrar devreye alınır. Bu kesinti süresinde bekleyen ve oluşan kritik veriler manuel olarak sisteme girilir. Erişime hazır olan kritik iş fonksiyonlarının, verinin, uygulama ve diğer hizmetlerin doğruluğu ve bütünlüğünün kontrolü bu aşamada gerçekleştirilir. Verilerde herhangi bir problem tespit edilirse düzeltme yapılır. Bu aşamadan sonra herşey yolunda ise iş süreçlerinin kaldığı yerden devam etmesi için uygunluk verilir. Bu testler genellikle veri tabanı, uygulama ve iş yöneticileri tarafından yapılır.

RTO ve WRT iyi planlanmaz ise en düşük RPO değerleri için yapılan yüksek maliyetler ve çaba boşa gitmiş demektir. Sonuç olarak felaket kurtarma merkezlerine gerçek zamanlı veri transferi yapılmış olsa dahi o veriye zamanında ve doğru şekilde erişebilmek de çok önemlidir.



Şekil 2.34. Felaketten Kurtarma Zaman Çizelgesi. (Snedaker, 2007)

Bazı işletmeler için yaptıkları işe ve verdikleri hizmetlere göre 2 saat kesinti önemli olmazken bazı işletmeler için ise 10 dakika hayati önem taşıyabiliyor. Dolayısıyla işletmeler için felaketten kurtarma zaman çizelgesini belirlerken işletmenin gerekliliklerine göre değerlendirme yapılır.

2.8. Veri Merkezi Bakımı Ve Tatbikatlar

Bakım ve tatbikatların esas konusu ekipmanlardan kaynaklı olası bir problemin önüne geçmektir. Bakım ve tatbikatlar iş sürekliliği kapsamında veri merkezi sertifikalarından ISO 27001’inde kapsamına girdiği için ayrıca önem taşır. ISO 27001 veri merkezi ekipmanlarının bir plan dahilinde bakım ve tatbikatlarının yapılmasını zorunlu olarak belirtmektedir. (ISO, 2013)

2.8.1. Veri merkezi bakımı

Veri merkezi ekipmanları ve destekleyici unsurları sürekli aktif olarak çalışmalarından kaynaklı olarak yıpranma zamanları gelmeden bakımlarının yapıp çalışabilirliklerini artırmak önemlidir. Veri merkezi bakımları, oluşabilecek risk ve problemleri ortadan kaldırmak için düzenli olarak yapılır. Bu periyotlar bakım yapılacak ekipmana göre değişmektedir. Cihazların ne yoğunlukla çalıştıkları, fiziksel ve ekonomik ömürleri bakım sürelerini belirlemede etkili konulardır. Bakım kapsamı BT ekipmanları, yangın koruma, iklimlendirme, enerji altyapısı, kablo altyapısı, güvenlik erişim sistemleri ve veri merkezini ilgilendiren bütün bileşenleri kapsamaktadır. Yapılan bakımlar kayıt altına alınır ve takibi yapılır. Genellikle tavsiye edilen yöntem üretici firmalar ile bakım sözleşmesi imzalayarak üreticinin tavsiye ettiği periyotlarda bakım yapılmasıdır. Üreticinin belirlediği süreler çok önemlidir çünkü her ekipmanın kendine

özel ekonomik, fiziksel ömürleri ve tavsiye edilen bakım periyotları vardır. Periyodik bakım ile beraber hesaplanamayan herhangi bir nedenden dolayı oluşabilecek problemlere karşı SLA destek anlaşmaları da imzalanmaktadır. (Cole, 2010)

Periyodik bakımlar için zaman ve bütçe ayrılmaz ise oluşabilecek büyük problemler için daha uzun zaman ve maliyet ayırmak gerekebilir. *“Emerson Network Power’s servis çözümleri yöneticisi Ben Kissell’e göre donanım hatalarının nedeni %30 - %40 oranlarda düzenli bakımlar sayesinde engellenebilmektedir. Kissell’e göre bu donanım hatalarının işletmelere maliyeti ortalama dakika da 5,600\$’dır.”* Bu sonuç düzenli bakım maliyetlerinden kaçınmanın işletmeye daha büyük maliyetler açtığını göstermektedir. Örnek olarak hiç kimse iklimlendirme sistemlerinde problem olmasını istemez, çünkü bu problem bütün iş süreçlerini etkileyecektir. (Clark, 2012)

Veri merkezlerinde bakım yapmak çok kolay bir iş değildir, profesyonel ekipler tarafından yapılır. Bazı ekipmanlarda bakım yaparken ekipmanları kapatmak gerekebilir. Herhangi bir kesintinin kabul edilemediği durumlarda bakım yapılacak ekipmanı kapatmadan önce yedeğini devreye alarak olası bir kesintiyi engellemek önemlidir. (Woolley, 2013)

Bakımlardan önce yapılması gerekenler ve bakımın faydaları aşağıdaki şekilde özetlenebilir (Clark, 2012; Cole, 2010).

- Bakım amaçları açıkça belirlenir,
- Bakım öncelikleri önceden tespit edilir,
- Bakım yapılacak envanter bilgileri güncel tutulur,
- Çok iyi dökümantasyon yapılır, bu dökümantasyon sayesinde yapılacak işlemlerin geçmişi ve gelecek planı sağlıklı bir şekilde yapılabilir,

- Bakımlar kesinlikle belirli periyotlarda düzenli yapılır,
- Bakımlar tek başına değil ekip olarak yapılır, ihtiyaç halinde çok hızlı destek alabilmek önemlidir,
- Bakım sırasında alınacak sorumluluklar önceden belirlenir, bakım ekibi işlemlerini yaparken veri merkezi sorumlularıda eşlik eder,
- Bakım ekibi dış kaynak ise veri merkezi bakımı sırasında edinecekleri bilgilerden dolayı tarafları koruyacak gizlilik anlaşması imzalatılır,
- Bakım yapılmadan önce bütün güvenlik tedbirleri alınır,
- Veri merkezi bakım ve çalışma şartları belirlenip kontrol edilir,
- Kritik parçalar yedek olarak veri merkezinde tutulur,
- Bakım yapılacak ekipman ile ilgili gerekli bileşenlere sahip olmak önemlidir,
- Yönetime gerekli bilgiler verilerek gelecekte konu ile ilgili bütçeler hesaplanır.

Düzenli yapılan bakımların faydaları aşağıdaki şekilde özetlenebilir;

- Ekipmanların çalışabilir ömürlerini uzatır,
- Ekipmanların durumları hakkında detaylı bilgi edinmeyi sağlar,
- Ekipmanlarda meydana gelecek olası hataları engeller ve sürekliliğini artırır,
- Ekipmanların yüksek performansla çalışmasını sağlar,
- Veri merkezinin sürekliliğini sağlayarak veri ve iş gücü kaybını engeller,
- Veri merkezi genel maliyetlerinin düşmesini sağlar.

2.8.2. Veri merkezi tatbikatı

Yapılan bakımların ne kadar faydalı olduğunu görmenin en iyi yolu tatbikatlardır. Tatbikatların amacı da bakımlarda olduğu gibi kesintisiz iş sürekliliğidir. Tatbikatlar da bakımlar gibi düzenli olarak planlanır ve profesyonel ekipler tarafından yapılır.

Tatbikatlar her ekipman için uygun zamanda ve gerekli sıklıkta bir plan ve öncelik listesi dahilinde yapılır. Tatbikatlar olası herhangi bir felaketi gerçekte yaşamaktan kaçınmak için planlanır. Yapılan planlamalar da iş sürekliliğine etkisi olan bütün veri merkezi ekipmanları tatbikat kapsamına alınır. Yapılan her tatbikattan sonra sonuçlar kayıt altına alınır, böylece tatbikat sırasında bir problem ile karşılaşıldı ise bu problem ile gerçekte karşılaşılması için tedbirler alınır.

2.9. Örnek Veri Merkezleri

Dünyada sayısız hizmete ev sahipliği yapan çok fazla veri merkezleri vardır. Profesyonel olarak tasarlandıkları için hepsi servis verdikleri hizmetin özelliklerine göre planlanmışlardır. Genel olarak veri merkezlerinde profesyonel ekiplerin bulundurulması, 7x24 izleme yapılması ve kayıt alınması, tesislerde fiziksel güvenlik kurallarının uygulanması, müşterilerine ihtiyaç halinde çalışma ortamı sağlanması gibi hizmetler geleneksel bütün veri merkezlerinde sunulmaktadır. Veri merkezleri verdikleri hizmetlere göre veri depolama, güvenlik, iş sürekliliği gibi konuları ön plana çıkartabilir veya bütün gereklilikleri aynı seviyede uygulayabilirler. Bu tür veri merkezlerine Switch SuperNAP, Utah, Google ve Microsoft'un veri merkezleri örnek olarak gösterilebilir.

2.9.1. Switch SuperNAP veri merkezleri

Las Vegas ve Tahoe Reno olmak üzere iki kampüse sahip SuperNAP dünya standartlarında hizmet sunan veri merkezi olma özelliği ile bilinmektedir. Las Vegasta 8 tesisi, 1 inşaat ve 3 adet planlanan tesisi, Tahoe Reno'da ise 1 adet inşaat halinde 6

adette planlanan tesisi vardır. Tesislerin tamamı hizmet vermeye başladığında 975 MVA enerji sağlayabilecek özelliğine sahip olacaktır. (SuperNap, 2015)

Tahoe Reno'nun ilk referans müşterisi eBay Inc. olacaktır (Miller, 2015).

SuperNAP, Uptime Institute tarafından Tier 4 Gold sertifikası verilen ilk veri merkezidir. Tier 4 Gold gerekliliklerine ilave olarak IEEE, ANSI, ASHRAE, ISO 9001, SAS 70/SSAE-16, BICSI ve Green Grid Association standartlarını karşılamakta ve hatta bazı özellikleriyle bu standartların üzerine çıkabilmektedir. (SuperNap, 2015)

SuperNAP aşağıdaki özellikleri ile ön plana çıkmaktadır; (SuperNap, 2015).

- Veri merkezleri yer seçimi konusu dikkate alınarak Nevada bölgesinde kurulmuştur,
- Veri merkezinde kabinet başına 40 kW'ın üzerinde enerji sağlayabiliyor, %100 enerji ve soğutma yapabildiğini ve verimliliğini SLA ile garanti altına almaktadır,
- Las Vegas 1.18 PUE, Tahoe Reno ise 1.20 PUE değeriyle enerji verimliliği sağlamaktadır,
- Las Vegas 43,000 kabinet, Tahoe Reno ise 75,000 kabinete ev sahipliği yapabilecek kapasitedir,
- Las Vegas, McCarran hava alanına 12 dakika, Reno Tahoe ise Reno-Tahoe hava alanına 22 dakika uzaklıkta konumlandırılması özelliğiyle ile ulaşımı kolaylaştırmaktadır,
- Nevada bölgesi düşük vergiler ve düşük enerji maliyetleri ile ön plana çıkarken felaket olaylarının da yaşanmaması bakımından iyi bir bölgedir, (Sandoval, 2015)

- Bin'den fazla müşteriye sahip olan veri merkezi 40'dan fazla bulut bilişim hizmeti sağlayan işletmeye de ev sahipliği yapmaktadır, (Miller, 2015)
- SuperNAP kurucusu Rob Roy'a göre güvenlik, verimlilik ve yedeklilik çok önemli kavramlardır. Dolayısıyla tesisler bu gereklilikler üzerine inşa edilmiştir. (SuperNap, 2015)

SuperNAP veri merkezinden hizmet alan müşterilerden bazıları; Ebay, VMware, Xerox, Fox TV, Logitecs, Cisco, EMC, Intel, PayPal, Harley-Davidson, Citrix, Sony Computer, Eset, McAfee, National University, Deloitte ve Qlogic olarak özetlenebilir (SuperNap, 2015).



Şekil 2.35. SuperNAP Veri Merkezi. (SuperNap, 2015)

2.9.2. Utah veri merkezi

Kod adı; Bumblehive olan Utah veri merkezi, NSA (Ulusal Güvenlik Ajansı) tarafından ABD'nin Utah eyaletinde kurulmuş istihbarat birimine hizmet veren ilk siber güvenlik tesisidir. Veri merkezi istihbarat birimine izleme, destekleme, koruma gibi konularda hizmet etmektedir. Bu özelliği ile bir ilk olan veri merkezi LEED ve Tier III sertifikalarına sahiptir. Utah'ın birçok bölgeye göre daha stabil ve ekonomik

enerji sağlayan bir bölge olması veri merkezi açısından avantaj sağlar. Utah enerji üretimi için gerekli rüzgar, güneş, hidro elektrik kaynakları bakımından da zengin bir bölgedir. (Herbert, 2015)

Utah veri merkezi altmış tam dolu, acil beklemede jeneratör ve tam kapasitede 3 gün yetecek yedek yakıt tesisine sahiptir. Utah bütün iletişim kayıtlarını, telefon görüşmelerini, email trafiğini, internet aramalarını, kişisel bilgileri tutabilecek kapasiteye sahip olmasıyla bilinir. Bu nedenle yüksek kapasiteli saklama alanlarına ve bunların güvenliğinin sağlanmasına ihtiyaç duyar. Depolama kapasitesi yottabyte seviyesinde olan ilk veri merkezidir. Veriler yüksek performanslı Cray XC30 supercomputer olarak isimlendirilen sunucular ile işlenir. Utah depolama ünitesindeki bütün verileri, mail sistemleri ve web tarayıcıları 256 bit AES algoritmasıyla şifreleyerek tutmaktadır. Bu algoritma günümüzde ataklara karşı çok başarılıdır ve günün şartlarında kırılması mümkün değildir. (NSA, 2015)



Şekil 2.36. NSA Veri Merkezi. (NSA, 2015)

2.9.3. Google veri merkezleri

Google'nin benzer ve kendilerine ait özellikleri olan Amerika'da Berkeley Country South Carolina, Council Bluffs Iowa, Douglas County Georgia, Quilicura Chile, Jackson County Alabama, Mayes County Oklahoma, Lenoir North Carolina, The Dalles Oregon, Asya'da Changhua County Taiwan, Singapore ve Avrupa'da Hamina Finland, St Ghislain Belgium, Dublin Ireland, Eemshaven Netherlands olmak üzere üç farklı bölgede 14 adet veri merkezine sahiptir. (Google Inc., 2014)

Google veri merkezleri standart veri merkezlerine göre %50 daha az enerji tüketmektedir. (Google Inc., 2014)

Enerji verimliliği için yıl boyunca bütün veri merkezlerinde TGG'nin PUE standartlarına göre yaptığı ölçüm sonuçlarına göre PUE değerleri 1,12 dir. (Google Inc., 2016)

Çoğu veri merkezi soğutma için chiller veya hava soğutma sistemleri kullanırlar, Google ise kendi özel tasarımı olan su soğutma sistemlerini tercih etmektedir. Veri merkezinde soğutma için kullanılan su ısındığında farklı hatlardan soğutulmak üzere veri merkezi dışındaki soğutma kulelerine transfer edilir, soğutulan su tekrar farklı hatlar aracılığı ile veri merkezine transfer edilir. (Google Inc., 2012)

Google bunun dışında deniz suyundan ve yağmur suyundan faydalanarak veya su geri dönüşümü yaparak ta soğutma sağlayabilmektedir. Pompalar aracılığı ile denizden aldığı soğuk suyu veri merkezine, veri merkezinden aldığı ısınan suyu ise denize ileterek soğutma gerçekleştirebilmektedir. Yağmur suyunu depolamak veya atık sularının geri dönüşümü sayesinde soğutma yapabilmek kullandığı diğer yöntemlerdir. (Google Inc., 2014)

Google ISO 14001, ISO 50001 ve OHSAS 18001 sertifikalarına sahip önemli ilk internet üzerinden hizmet veren işletmedir. (Miller, 2012)

Google'nin özelliklerinden biriside yenilenebilir enerji kullanmasıdır. İhtiyaçları olan enerjinin %35'ini güneş ve rüzgar sistemleri sayesinde yenilenebilir yeşil enerjiden sağlayan Google ihtiyacı olan enerjinin tamamını bu yöntemle sağlamak istemektedir. Bu nedenle veri merkezlerinin çevresindeki rüzgar güllerini barındıran tesislerden enerji satınalmaktadır. TGG üyesi olan Google 2011 yılında EPA'nın (United States Environmental Protection Agency) "Green Power Leadership" ödülünü aldı. (Google Inc., 2014)

Google'nin önem verdiği diğer konularda güvenlik ve iş sürekliliği'dir. Bu kapsamda Google işletme güvenliği politikaları, organizasyonel güvenlik, varlık sınıflandırma ve kontrol, fiziksel ve çevresel güvenlik, operasyonel güvenlik, erişim kontrolü, uygunluk, uygulama güvenliği, sistem geliştirme ve devamlılığı, felaketten kurtarma ve iş sürekliliği konularına önem vermektedir. (Google Inc., 2011)



Şekil 2.37. Google Veri Merkezi. (Google Inc., 2014)

2.9.4. Microsoft veri merkezleri

İlk veri merkezini 1989’da inşa eden Microsoft; Bing, Msn, outlook.com, Office 365, OneDrive, Skype, Xbox ve Azure dahil 200’den fazla bulut bilişim hizmetini Amsterdam, Avusturalya, Çin, Brezilya, İrlanda, Hong Kong, Japonya gibi bölgeler dahil olmak üzere 100’den fazla veri merkezinde 1 milyondan fazla sunucu ile hizmet vermektedir. Bütün veri merkezleri birbirine dark fiber ile bağlıdır. Microsoft veri merkezlerinin enerji verimliliği değerlendirildiğinde PUE değerleri 1989 ile 2005 yılları arasında 2.0 ve üzeri, 2007 yılında 1,4 – 1,6, 2009 yılında 1,2-1,5, 2012 yılında 1,12-1,20 olduğu görülmektedir. Gelecekte ise 1,07 – 1,19 değerlerinde olması planlanmaktadır. Microsoft verimlilik, güvenlik, devamlılık gibi konularını bazı standartlara bağlayarak standartların seviyelerinde hizmet vermektedir. Risk yönetimi ve kontrolü için ISO 27001, tasarım, operasyonel verimlilik, finansal raporlar, güvenlik, gizlilik, bütünlük, iş sürekliliği gibi konular için SSAE 16/ SOC1/ SOC2/ SOC3, bazı özel yasalar gereği ihtiyaç olan özel finansal raporlar için SOX, kart kullanıcıları ve tedarikçileri için PCI-DSS standartlarını uygulamaktadır. (Microsoft Corp, 2015)



Şekil 2.38. Microsoft Veri Merkezi. (Microsoft Corp, 2015)

III. BULGULAR

Veri merkezleri incelendiğinde türleri, sanallaştırılması, standartları, yer seçimi, tasarım ve altyapısı, sürekliliği, bakım ve tatbikatlarının bir bütün olarak değerlendirilmesi gerekir. Bütün konuların kendi içlerinde önemli değerleri vardır. Bu değerler ihtiyacın belirlenmesine göre değişiklik gösterebilir. Hizmet veren veri merkezleri küçük, orta ve büyük ölçekli kurum ve kuruluşların ihtiyaç analizlerini doğru yaparak her seviyedeki işletmeye ihtiyacı olan hizmeti sunabilmesi gerekmektedir. Bu amaçla hizmet veren veri merkezleri hizmet verdikleri işletmenin ölçeklerine göre farklı özelliklere sahip olmaları gerekir.

Bu doğrultuda bu tez çalışmasında küçük, orta ve büyük ölçekli işletmelerin veri merkezi ihtiyaçlarını karşılamak için veri merkezi modelleri oluşturulmuştur. Tablo 3.1’de oluşturulan bu modellerin özeti yer almaktadır.

3.1. Küçük Ölçekli İşletmeler İçin Veri Merkezi Modeli

Küçük ölçekli işletmeler; zamana bağlı işler yapılmadığı ve çok kritik verilere sahip olmadıkları göz önüne alındığında çok yüksek altyapı yatırımı yapılmadan işletme içi veri merkezlerini kullanılabilir. Küçük ölçekli işletmelere hizmet veren veri merkezleri aşağıdaki özelliklere sahiptir;

- Mali yapısı ve verinin kritiklik durumu göz önüne alınarak yüksek altyapı yatırımları yapmadan kendi işletme içi veri merkezlerini kurarlar,

Tablo 3.1. İşletme Ölçeklerine Göre Veri Merkezi Özellikleri.

Veri Merkezi Özellikleri	Küçük Ölçekli İşletmeler	Orta Ölçekli İşletmeler	Büyük Ölçekli İşletmeler
Altyapı Seviyesi	Basit	Orta veya üst seviye	Üst seviye
Yer seçimi	İşletme içi	Genel müdürlük binası, bölge müdürlük binası veya profesyonel veri merkezleri	Uluslararası standartlardaki profesyonel veri merkezleri
Sanallaştırma	Opsiyonel	Kritik ekipmanlar	Özel sistemler hariç bütün veri merkezi
Genel Güvenlik	Standartlar oluşturulup uygulanmalıdır	Kendi standartları veya uluslararası standartlar uygulanmalıdır	Uluslararası standartlar uygulanmalı, ilave olarak standartlar geliştirilebilir
Profesyonel Güvenlik Ekibi	Yok	Tavsiye edilir	Zorunlu
7x24 İzleme	Yok	Var	Var
Veri Merkezi Erişimi	Kilitli ortamlar	Parmak izi veya iris okuma	İris okuma ve ilave güvenlik
Kamera İzleme	Yok	Var	Var
Enerji Altyapısı ve Verimlilik	Jeneratör ve UPS kullanılmalıdır	Yedekli jeneratör, UPS'ler kullanılıp ve verimlilik sağlanmalıdır	En üst düzey yedeklilik ve enerji verimliliği
Kablolama Altyapısı	Karışıklığa izin verilmemelidir	Uluslararası standartlar tavsiye edilir	Uluslararası standartlar zorunludur
İklimlendirme	Oda tipi klima	Oda şartlarını sağlayan gazlı soğutma ile iklimlendirme yapan cihazlar (CRAC) kullanılmalıdır	Oda şartlarını sağlayan gazlı veya sulu soğutma ile iklimlendirme yapan cihazların (CRAC, CRAH) kullanılması zorunludur
Yangın Koruma	Halojen taşınabilir yangın tüpü	Durağan gaz sistemi (FM 200)	Durağan gaz sistemi (FM 200)
Tasarım ve Kurulum	Dikkat edilmeli	Profesyonel destek alınmalı	Profesyonel ekipler tarafından uluslararası standartlara uygun yapılmalı
Gizlilik, Bütünlük, Erişebilirlik	Dikkat edilmeli	Zorunlu	Zorunlu
Veri Yedekleme	Kritik veriler	Kritik veriler	Felaketten kurtarma merkezleri
Yıllık En Fazla Kesinti Süresi	30 Saat	22 Saat	1,2 Saat
Veri Depolama	Sunucu diskleri	Ayrı depolama üniteleri	Ayrı depolama üniteleri
Kullanılabilecek Standartlar	Kendi Standartları	Bilgi güvenliği ve iş sürekliliği: ISO, PCI DSS	Bilgi güvenliği: ISO, PCI DSS
			Süreklilik: ISO, Uptime Institute
			Enerji: LEED, ISO
			İklimlendirme: ASHRAE
			Kablolama: ANSI/TIA-942, CELENEC EN 50173-5
			Tasarım: ANSI/BICSI-002
Müdahale ekibi ve operasyon merkezi	Yok	Tavsiye edilir	Zorulu
Bakım ve Tatbikatlar	Bakım	Bakım ve tatbikat	Bakım ve tatbikat

- Sanallaştırma altyapısının kullanılıp kullanılmaması sahip olunan ekipman sayısına göre tercih sebebi olabilir,
- Güvenliğin sağlanması için kendi standartlarını uygulayabilirler. Veri merkezleri sadece uzman ekiplerin erişebilmesi için kilitli tutulur. Profesyonel güvenlik ekibi, 7x24 izleme ekibi ve kamera kaydına ihtiyaç yoktur,
- Enerji altyapısı için jeneratör ve UPS cihazları kullanılabilir,
- Kablolama altyapısı karışıklığa izin verilmeyecek şekilde düzenlenmelidir,
- İklimlendirme için oda tipi klimalar kullanılabilir,
- Yangın koruma sistemleri için BT ekipmanlarına zarar vermeyen halojen taşıyabilir yangın tüpleri kullanılabilir,
- Altyapı tasarımı yapılırken yıllık 30 saatten fazla kesinti olmayacak şekilde verimlilik, gizlilik, bütünlük, erişebilirlik gibi ilkelere dikkat edilmelidir,
- Kritik verilerin farklı disk veya medyalara yedeklenmesi gerekir,
- Veri depolaması için sunucular üzerindeki mevcut diskler kullanılabilir,
- Veri merkezini ilgilendiren bütün konular için kendi standartlarını kullanabilirler,
- Veri merkezine müdahale edebilmek için operasyon merkezleri ve ekipleri yoktur,
- Veri merkezi ile ilgili bakımlar belirli periyotlar halinde yapılır.

3.2. Orta Ölçekli İşletmeler İçin Veri Merkezi Modeli

Orta ölçekli işletmeler; veri merkezleri açısından düşündüğümüzde bir genel müdürlük ve ona bağlı bir veya birkaç şubesi olan, önemli verileri olan, bazı hizmetleri zamana

bağlı olabilen dolayısıyla veri merkezlerini bu yönde tercih eden işletmelerdir. Orta ölçekli işletmelere hizmet veren veri merkezleri aşağıdaki özelliklere sahiptir;

- Verilen hizmetin kritiklik seviyesine bağlı olarak altyapı seviyesi belirlenir. Bu işi yapmaya uygun olan kendi ofislerinde veri merkezi kurabilir veya profesyonel veri merkezlerinden hizmet alabilirler,
- Orta ölçekli işletmeler veri merkezine karar verirken “2.5. Veri Merkezi Yer Seçimi” başlığında anlatılan konulara dikkat etmeleri gerekir,
- Kritik ekipmanlar için sanallaştırma teknolojisi tercih edilebilir,
- Güvenliğin sağlanması için kendi geliştirdikleri standartlarını veya uluslararası standartları uygulayabilirler. Veri merkezlerine sadece uzman ekiplerin parmak izi veya iris okuma ile erişmesine izin verilir. Profesyonel güvenlik ekibinin bulundurulması tavsiye edilir, 7x24 izleme ekibi ve kamera kayıtlarına ihtiyaç duyulur,
- Enerji altyapısı için yedekli jeneratör ve UPS cihazları verimliliğe dikkat ederek kullanılır,
- Kablolama altyapısında oluşacak problemleri engellemek için uluslararası standartların uygulanması tavsiye edilir,
- İklimlendirme için BT ekipmanlarına gerekli oda şartlarını sağlayan gaz ile soğutma yapan iklimlendirme cihazları (CRAC) kullanılmalıdır,
- Yangın koruma için BT ekipmanlarına zarar vermeyen, ihtiyaç halinde otomatik olarak devreye giren durağan gaz sistemleri kullanılır,
- Altyapı tasarımı yapılırken yıllık 22 saatten fazla kesinti olmayacak şekilde verimlilik, gizlilik, bütünlük, erişebilirlik gibi ilkelere dikkat edilerek profesyonel destek alınmalıdır,

- Kritik verilerin farklı disk veya medyalara otomatik olarak yedeklenmesi gerekir,
- Veri depolaması için ayrı depolama uniteleri kullanılır,
- Veri merkezi bilgi güvenliği ve iş sürekliliği için ISO ve PCS DSS standartları kullanılabildiği gibi diğer veri merkezi konuları için kendi standartlarını kullanabilirler,
- Veri merkezine müdahale edebilmek için operasyon merkezleri ve ekiplerinin olması tavsiye edilir,
- Veri merkezi bakım ve tatbikatları belirli periyotlar halinde uzman ekipler tarafından yapılır.

3.3. Büyük Ölçekli İşletmeler İçin Veri Merkezi Modeli

Büyük ölçekli işletmeler; bu ölçekteki işletmeler ülke içinde veya uluslararası genel müdürlükleri olan, onlara bağlı bölge veya ülke müdürlükleri ve hatta onlara da bağlı şubelerin olduğu büyük organizasyonlardır. Bu büyüklükteki yapılar ülke ekonomilerini etkileyebilirler. Bu nedenle bu ölçekteki işletmeler kendilerine uygun veri merkezlerinden hizmet almak zorundadırlar. Büyük ölçekli işletmelere hizmet veren veri merkezlerinin aşağıdaki özelliklere sahip olması gerekir;

- Verilen hizmetin kritiklik seviyesinden dolayı üst seviye altyapı gerekmektedir. Uluslararası altyapı standartlarına uygun profesyonel veri merkezlerinden hizmet alınır,
- Büyük ölçekli işletmeler veri merkezine karar verirken “2.5. Veri Merkezi Yer Seçimi” başlığında anlatılan konulara dikkat etmek zorundadırlar,

- Özel nedenlerden dolayı fiziksel ekipmanlara ihtiyaç duyulmayan bütün durumlarda sanallaştırma teknolojisi kullanılır,
- Güvenliğin sağlanması için uluslararası standartlar uygulanır, ilave olarak kendilerine özel geliştirdikleri standartları da kullanabilirler. Veri merkezlerine sadece uzman ekiplerin iris okuma veya artırılmış ilave güvenliklerin uygulanması ile erişim sağlanması gerekir. Profesyonel güvenlik ekibinin bulundurulması, 7x24 izleme ve kamera kayıtlarının tutulması zorunludur,
- Enerji altyapısı için yedekli jeneratör ve UPS cihazlarının da tekrar yedekliliği sağlanır. Enerji ekipmanları BT ekipmanlarına birbirinden ayrıştırılmış yedekli kanallardan enerji iletimini sağlamaktadır. Enerji verimliliği en üst seviyede olmalıdır,
- Kablolama altyapısında oluşacak problemleri engellemek için uluslararası standartların uygulanması zorunludur,
- İklimlendirme için BT ekipmanlarına gerekli oda şartlarını sağlayan gazlı veya sulu soğutma ile iklimlendirme yapan sistemlerin (CRAC, CRAH) kullanılması zorunludur,
- Yangın koruma için BT ekipmanlarına zarar vermeyen, ihtiyaç halinde otomatik olarak devreye giren durağan gaz sistemleri kullanılır,
- Altyapı tasarımı yıllık 1,2 saatten fazla kesinti olmayacak şekilde verimlilik, gizlilik, bütünlük, erişebilirlik gibi ilkelere dikkat edilerek profesyonel ekipler tarafından uluslararası standartlara uygun yapılmalıdır,
- Verilerin farklı disk veya medyalarla otomatik olarak yedeklenmesine ilave olarak veri merkezinin kopyası olan felaketten kurtarma merkezleri kurulur,
- Veri depolaması için ayrı depolama uniteleri kullanılır,

- Veri merkezi konuları için aşağıdaki standartlar kullanılır;
 - ✓ Bilgi güvenliği; ISO ve PCS DSS,
 - ✓ İş sürekliliği; ISO ve Uptime Institute standartları,
 - ✓ Enerji yönetimi ve verimliliği; LEED ve ISO standartları,
 - ✓ İklimlendirme; ASHRAE,
 - ✓ Kablolama altyapısı; ANSI/TIA-942, CELENEC EN 50173-5,
 - ✓ Veri merkezi tasarımı; ANSI/BICSI-002
 - ✓ Finansal denetleme; SAS 70/SSAE-16.
- Veri merkezine müdahale edebilmek için operasyon merkezleri ve ekiplerinin olması zorunludur,
- Veri merkezi bakım ve tatbikatları belirli periyotlar halinde uzman ekipler tarafından yapılır.

Veri merkezleri hizmet verirken işletmelerin ölçütlerine göre bir takım servislerini değiştirip bütün seviyelere hizmet edebilmeleri gerekmektedir. Fakat hizmet alan kurum veya kuruluşun ölçütü ne olursa olsun bütün veri merkezlerinde verinin gizliliği, bütünlüğü ve erişilebilirliği önemli olarak değerlendirilmelidir.

IV. TARTIŞMA VE SONUÇ

Geçmişte oda boyutundaki cihazları barındıran ve maliyetlerden dolayı sadece askeri ve devlet işlerinde kullanılabilen veri merkezlerinin günümüzde ulaştığı noktaya bakıldığında teknolojiadaki büyük gelişmeyi görmek mümkündür. Bu gelişim sürecindeki sanallaştırma, bulut bilişim, enerji, kablolama, iklimlendirme, yangın önleme, izleme ve güvenliği ile yedeklilik ve iş sürekliliği adına yapılan bütün geliştirmeler veri merkezleri için yeni dönem niteliğindedir. Veri merkezlerinin gelişimini devam ettirebilmek için teknolojinin yeniliklerini uygulayıp fayda sağlamak gerekir. Veri merkezlerinde inisiyatif kullanılabilecek konular olduğu gibi kesinlikle uygulanması gereken konularda vardır. Profesyonel veri merkezleri test edilmiş ve kabul görmüş standartlara göre tasarlanmalı ve yönetilmelidir.

İş sürekliliği ve bilgi güvenliği konularında özellikle Uptime Institute'nin geliştirdiği Tier seviyeleri ve ISO tarafından geliştirilen ISO 27001 bilgi güvenliği yönetim sistemleri standartları veri merkezlerine artı değerler katmaktadır. ISO 27001 varlık envanterlerinden, risk analizlerine, iş sürekliliği ve bilginin güvenliğine kadar bir çok ana konuyu çerçevesine alarak veri merkezlerini ve kullanan işletmeleri korumaktadır. Uptime Institute ise veri merkezi BT ekipmanları için gereken enerjiyi sağlayan ekipmanların yedekliliğine ve sürekliliğine odaklanarak veri merkezi sürekliliğini artırıp fayda sağlamaktadır.

Enerji altyapısı tasarlanırken yapılacak hata enerjinin verimsiz kullanılıp maliyetlerin artmasından, standartlara uygun enerji yedeklemesi yapılmaz ise sistem kesintilerine kadar problemlere neden olabilir. Enerji yönetimi ve verimliliğinin sağlanması için

TGG ve LEED standartları geliştirilmiştir. TGG en büyük maliyet kalemlerinden olan enerji maliyetlerini düşürmek ve verimliliği artırmak için tesiste tüketilen toplam enerjiyi BT ekipmanlarının tükettiği enerjiye oranını hesaplayarak elde ettiği değer üzerinden verimlilik çalışmaları yapmaktadır. LEED ise kaynak kullanımı ve tasarrufu gibi konulara yoğunlaşarak tesisin su kullanımının ölçülmesi ve su kullanımını düşürmek, tesisin enerji kullanımının ölçeklendirilip en az enerji tüketimini sağlamak, atıkların yönetimi ve planlanması mümkünse geri dönüşümlerinin sağlanması, tesisin hava kalitesinin artırılması gibi konularda çalışmalar yaparak hem tesislere hemde çevreye katma değerler katmaktadır. Bu standartlar çevreci olma özellikleri ile tesislerin örnek tesis olmasına dolayısıyla olumlu bir imaja sahip olmalarını sağlamaktadır.

Veri merkezlerinde soğutma değil, BT ekipmanlarının ihtiyacı olan oda şartlarının sağlanması için iklimlendirme yapılmalıdır. Bu nedenle soğutma klimaları değil iklimlendirme cihazları kullanılmalıdır. Bu altyapı kurulurken ideal yapı sıcak ve soğuk hava koridorlarının birbirinden ayrılmasıdır. Bu yöntem hem daha verimli iklimlendirme yapılmasını hem de enerjinin daha verimli kullanılmasını sağlamaktadır.

Bu amaç ile veri merkezi iklimlendirmesi için ASHRAE üreticiler ile çalışmalar yaparak veri merkezi oda şartları için gereken değerleri belirlemektedir. Bu değerler veri merkezi için gerçek bir iklimlendirme yapıp BT ekipmanlarının yüksek performans ile hizmet vermesini sağlamaktadır.

Kablolama altyapısı için ANSI/TIA-942, CELENEC EN 50173-5 standartları geliştirilmiştir. Bu standartlar enerji ve veri kablolamasının veri merkezinin hangi

bölümünde nasıl yapılması gerektiğini belirterek kablolama hatalarından kaynaklı herhangi bir iş sürekliliğine engel olacak problemin oluşmasını engellemektedir.

Veri merkezlerinde dikkat edilmesi gereken önemli konulardan bir diğeri de yer seçimidir. Yer seçiminde ulaşım, çevresel faktörler, teknoloji problemleri, insandan kaynaklı problemler, enerji sağlama ve doğal afetler gibi birçok konuya dikkat edilmelidir. 2009 yılında Vodafone'nin ikitelli bölgesindeki veri merkezini sel basması sonucu İstanbul Kuzey Batı ve Trakya Bölgesi'ndeki toplam 3.8 milyon abonenin iletişimi kesilmiştir (Milliyet, 2009). Bu felaket tamamen “2.5. Veri Merkezi Yer Seçimi” konusu üzerinde çalışma yapılmaması ve yeteri kadar önemsenmemesinden kaynaklanmıştır.

Yıllarca kullanılan tam, farksal ve artan yedekleme yöntemleri yerini tekilleştirme ve felaket kurtarma merkezlerinin kurulmasına bırakmaya başladı. Tekilleştirme verilerin daha hızlı yedekleme ve kurtarma yapılmasına imkan sağlarken aynı zamanda verinin tuttuğu alandan ve maliyetinden de kazanç sağlamaktadır. Felaket kurtarma merkezleri asıl veri merkezlerinin kopyası olarak tasarlanır. Veri merkezlerinde kesinti olması halinde (doğal afet, yangın, saldırı, terör, vb.) devreye alınarak sürekliliği sağlamaktadır. Felaket kurtarma merkezi olmaması işletmelerin ticari hayatlarının sona ermesine neden olabilir.

Geçmişten bugüne bakıldığında BT ekipmanlarının küçülüp verimlilik ve optimizasyonlarının arttığı görülmektedir. Hala bu alanda geliştirmeler yapılabilir. Daha az ısınan daha ufak ekipmanlar geliştirilip hem veri merkezi konumlandırılmasında daha az yer kaplayıp hemde az ısınmadan dolayı daha az soğutma ihtiyacı sağlanır ise enerji tüketiminden de fayda sağlanmış olur. Bu sonuç

hem hizmet alan işletme hem de hizmet veren veri merkezinin daha düşük maliyetlerle daha verimli hizmet vermesini sağladığı gibi ülke ekonomisine de verimli enerji tüketimi ve çevreci olma özelliği ile fayda sağlayacaktır.



KAYNAKÇA

- U.S. Department of Health & Human Services. (2015). *Department of Health and Human Services*. hhs.gov:
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf> adresinden alındı
- AICPA. (2010). *Reporting on Controls at a Service Organization - SSAE No. 16*. New York City, US: AICPA.
- Akın, G., & Ketenci, S. (2010). *Sistem Odaları İklimlendirme Sistemleri*. İstanbul Teknik Üniversitesi:
http://web.itu.edu.tr/akingok/doktora/iklimlendirme/Sistem_odasi_iklimlendirme_sistemleri.pdf adresinden alındı
- Akpınar, H. (2011). *İş Sürekliliği Yönetimi ve Felaket Planlaması*. 12 06, 2014 tarihinde Prof. Dr. Haldun Akpınar:
http://haldunakpinar.com/felaket_planlamasi.pdf adresinden alındı
- Al-Fares, M., Loukissas, A., & Vahdat, A. (2008). *A Scalable, Commodity Data Center Network Architecture*. 07 09, 2015 tarihinde Kent State University Computer Science: <http://www.cs.kent.edu/~javed/class-CXNET09S/papers-CXNET-2009/FaLV08-DataCenter-interconnect-p63-alfares.pdf> adresinden alındı
- Alkan, P. M., & Coşar, Y. (2014). *TO11-11*. 12 02, 2014 tarihinde Ulusal Mühendislik Ölçmeleri Sempozyumu - 2014:
<http://www.muholc2014.hitit.edu.tr/bildiriler/TO11-11.pdf> adresinden alındı
- ASHRAE. (2011). *2011 Thermal Guidelines for Data Processing Environments—Expanded Data Center Classes and Usage Guidance*. Atlanta, USA.
- ASHRAE. (2016). *About ASHRAE*. 06 26, 2015 tarihinde Shaping Tomorrow's Built Enviroment Today: <https://www.ashrae.org/about-ashrae> adresinden alındı
- ASHRAE Inc. (2012). *Heating, Ventilating and Air-Conditioning Systems And Equipment*. Atlanta, USA: ASHRAE Inc.
- Avelar, V., Azevedo, D., & French, A. (2012). *WP49-A Comprehensive Examination Of The Metric V6*. 01 07, 2015 tarihinde The Green Grid | Carbon, Water and Energy Efficiency Metrics, Measurements and Trends for Data Center Planning: http://www.thegreengrid.org/~media/WhitePapers/WP49-PUE%20A%20Comprehensive%20Examination%20of%20the%20Metric_v6.pdf?lang=en adresinden alındı

- Bacheldor, B. (2012). *Bangalore gets a data center with screaming capacity and tight security*. IT WORLD: <http://www.itworld.com/article/2732389/data-center/bangalore-gets-a-data-center-with-screaming-capacity-and-tight-security.html> adresinden alındı
- Barroso, L. A., Clidaras, J., & Hölzle, U. (2013). *The Datacenter as a Computer*. 07 07, 2015 tarihinde Morgan & Claypool Publishers: <http://www.morganclaypool.com/doi/pdf/10.2200/S00516ED2V01Y201306CAC024> adresinden alındı
- Baweja, P. (2013). *Refining Your Criteria for Data Center Site Selection*. Data Center Knowledge: <http://www.datacenterknowledge.com/archives/2013/07/24/refining-your-criteria-for-data-center-site-selection/> adresinden alındı
- BICSI. (2014). *ANSI/BICSI 002-2014 Data Center Design and Implementation Best Practices*. BICSI: https://www.bicsi.org/pdf/standards/BICSI_002_14_Sample.pdf adresinden alındı
- Bouley, D. (2010). *Impact Of Virtualization On Data Center Physical Infrastructure*. The Green Grid: http://www.thegreengrid.org/~media/WhitePapers/White_Paper_27_Impact_of_Virtualization_Data_On_Center_Physical_Infrastructure_020210.pdf?lang=en adresinden alındı
- Bouley, D., & Brey, T. (2009). *Fundamentals Of Data Center Power And Cooling Efficiency Zones*. 08 01, 2015 tarihinde <http://www.thegreengrid.org/~media/WhitePapers/Fundamentals%20of%20Power%20and%20Cooling%20Zones%20White%20Paper.ashx?lang=en> adresinden alındı
- Bülent Özmen, M. N. (1997). *Coğrafi Bilgi Sistemi ile Deprem Bölgelerinin İncelenmesi*. Ankara: Bayındırlık ve İskan Bakanlığı, Afet İşleri Genel Müdürlüğü.
- BWorks. (2015). *UDP , FTP ve STP Ağ Kablosu Arasındaki Farklar ve Kullanımı*. 07 26, 2015 tarihinde BWorks: <http://www.bworks.tc/destek/faydali-bilgiler/network-faydali-bilgiler/334-udp-ftp-ve-stp-ag-kablosu-arasindaki-farklar-ve-kullanimi.html> adresinden alındı
- Casazza, T. (2015). *Fiber Type vs. Speed and Distance*. 07 15, 2015 tarihinde lanshack.com: <http://www.lanshack.com/Fiber-Type-vs-Speed-and-Distance.aspx> adresinden alındı

- Casey, K. (2014). *The data center of the (near) future*. 05 25, 2015 tarihinde Dell Official Site: <https://powermore.dell.com/technology/the-data-center-of-the-near-future/> adresinden alındı
- Chen, Y., Keys, L., & Katz, R. H. (2009). *Towards Energy Efficient MapReduce*. 07 04, 2015 tarihinde Berkeley University of California: <http://digitalassets.lib.berkeley.edu/techreports/ucb/text/EECS-2009-109.pdf> adresinden alındı
- Cisco System Inc. (2003). *CCNA Self-Study: CCNA Basics*. Indianapolis: Cisco Press.
- Cisco Systems Inc. (1998). *Internetworking Basics*. 07 10, 2015 tarihinde The world's smartest cities: <http://www.cisco.com/cpress/cc/td/cpress/fund/ith/ith01gb.htm#xtocid1668411> adresinden alındı
- Cisco Systems Inc. (1999). *What is a Network Switch vs. a Router?* 07 10, 2015 tarihinde The world's smartest cities: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html?referring_site=smartnavRD adresinden alındı
- Cisco Systems Inc. (2015). *Cisco 800M Series Integrated Services Router Data Sheet*. 07 10, 2015 tarihinde The world's smartest cities: <http://www.cisco.com/c/en/us/products/collateral/routers/800m-integrated-services-router-isr/datasheet-c78-732678.html> adresinden alındı
- Cisco Systems Inc. (2015). *Cisco Catalyst 2900 Series Switches*. 07 10, 2015 tarihinde The world's smartest cities: <http://www.cisco.com/c/en/us/support/switches/catalyst-2900-series-switches/tsd-products-support-eol-series-home.html> adresinden alındı
- Cisco Systems Inc. (2015). *What is a Network Switch vs. a Router?* 07 10, 2015 tarihinde The world's smartest cities: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html?referring_site=smartnavRD adresinden alındı
- Clark, J. (2012). *You Can't Afford to Ignore Data Center Maintenance*. Data Center Journal: <http://www.datacenterjournal.com/you-cant-afford-to-ignore-data-center-maintenance/> adresinden alındı
- Cole, D. (2010). *Developing a Preventive Maintenance Plan for Your Data Center*. Mission Critical:

- http://www.missioncriticalmagazine.com/ext/resources/MC/Home/Files/PDFs/PTS-Developing_Preventive_Maintenance_Plan.pdf adresinden alındı
- Coyle, T. (2014). *Green Building 101: What is LEED ?* 06 24, 2015 tarihinde USGBC: <http://www.usgbc.org/articles/green-building-101-what-leed> adresinden alındı
- Çavdar, D., & Alagöz, F. (2013). *Yeşil Veri Merkezlerinde Enerji Verimliliği*. 07 06, 2015 tarihinde Akademik Bilişim Konferansları: <http://ab.org.tr/ab13/bildiri/276.doc> adresinden alındı
- Diaz, H. (2014). *Explaining the Uptime Institute's Tier Classification System*. 06 20, 2015 tarihinde Uptime Institute: <http://journal.uptimeinstitute.com/explaining-uptime-institutes-tier-classification-system/> adresinden alındı
- DiMinico, C. (2006, 11 08). *Telecommunications Infrastructure Telecommunications Infrastructure Standard for Data Centers Standard for Data Centers*. 07 10, 2015 tarihinde IEEE 802: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf adresinden alındı
- Dinçer, E. (2013). *Felaket Kurtarmada Yeni Yaklaşımlar*. 11 10, 2014 tarihinde Computer World Türkiye - IT Dünyasının Buluş Noktası: <http://www.computerworld.com.tr/genel/felaket-kurtarmada-yeni-yaklasimlar> adresinden alındı
- Dinçkan, A. (2008). *İş Sürekliliği Yönetim Sistemi Kurulumu*. Kocaeli, Türkiye.
- Dinçkan, A. (2008). *Veri Yedekleme Kılavuzu*. Kocaeli, Türkiye.
- Doğdu, E. (2009). *Felaketten Kurtarma ve Depolama*. Ankara: Türkiye Bilişim Derneği.
- Eagle, L. (2013). *Data Center Audit Standards: A Look at SAS 70, SSAE 16, SOC 2, and SOC 3*. <http://www.thewhir.com/web-hosting-news/data-center-audit-standards-a-look-at-sas-70-ssae-16-soc-1-soc-2-and-soc-3> adresinden alındı
- Ebbers, M., Galea, A., Schaefer, M., & Khiem, M. T. (2008). *The Green Data Center: Steps for the Journey*. 12 07, 2014 tarihinde The Green Data Center: Steps for the Journey: <ftp://public.dhe.ibm.com/software/uk/itsolutions/optimiseit/energy-efficiency-solutions/2-new-enterprise-data-centre-the-green-new-enterprise-data-centre-red-books.pdf> adresinden alındı
- EC-Council. (2010). *Certified Ethical Hacker (CEH) V6*. Albuquerque, USA: EC-Council.

- Eko Kablo. (2015). *ekokablo.com*. 07 26, 2015 tarihinde ekokablo.com: http://www.ekokablo.com/kategori/1258/Data_Kablolari.html adresinden alındı
- EMC Corporation. (2016). *Data Deduplication*. 08 11, 2015 tarihinde EMC: <http://www.emc.com/corporate/glossary/data-deduplication.htm> adresinden alındı
- Emerson Electric Co. (2007). *Five Strategies for Cutting Data Center Energy Costs Through Enhanced Cooling Efficiency*. 08 01, 2015 tarihinde Emerson Network Power: http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/data-center-energy-efficiency_151-47.pdf adresinden alındı
- Engelhardt, R. (2016). *Data Centre Cabling: Standards and Structure*. 02 08, 2016 tarihinde R&M Convincing cabling solutions: http://www.rdm.com/asi/Portaldata/1/Resources/APAC/asia1/documents/Data_Centre_Cabling.pdf adresinden alındı
- Ergin, O., Gerede, Ç. E., & Korkmaz, Y. (2012). *Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği Kamu Bilişim Platformu XIV*. Türkiye Bilişim Derneği: http://www.tbd.org.tr/usr_img/kamu_bib/RP1-2012.pdf adresinden alındı
- Ergünay, O. (1996). <http://www.e-kutuphane.imo.org.tr/pdf/3885.pdf>. 12 10, 2014 tarihinde İMO E-Kütüphane: <http://www.e-kutuphane.imo.org.tr/pdf/3885.pdf> adresinden alındı
- Ergünay, O. (2008). *Türkiye'nin Afet Profili*. 12 03, 2014 tarihinde İMO - e-kütüphane: <http://www.e-kutuphane.imo.org.tr/pdf/3885.pdf> adresinden alındı
- Gartner Inc. (2016). *Data Center*. Gartner: <http://www.gartner.com/it-glossary/data-center> adresinden alındı
- Gasiorowski, L. (2012). *ISO publishes new standard for business continuity management*. 06 03, 2012 tarihinde International Organization for Standardization: <http://www.iso.org/iso/news.htm?refid=Ref1587> adresinden alındı
- Gesellschaft, R. (2013). http://www.munichre.com/site/corporate/get/documents/mr/assetpool.shared/Documents/0_Corporate%20Website/6_Media%20Relations/Press%20Releases/2013/natural-catastrophes-2012-wold-map_en.pdf?2. 11 10, 2014 tarihinde Leading Expert on Risk Solution worlwide: http://www.munichre.com/site/corporate/get/documents/mr/assetpool.shared/Documents/0_Corporate%20Website/6_Media%20Relations/Press%20Releases/2013/natural-catastrophes-2012-wold-map_en.pdf?2 adresinden alındı

- Gigerich, L. (2012). *Critical Factors: The Data Center Location Decision*. Area Development: <http://www.areadevelopment.com/siteSelection/April2012/data-center-location-decision-criteria-26255554.shtml> adresinden alındı
- Gilly, L. (2012). *Selecting a Location for an HPC Data Centre*. 08 19, 2015 tarihinde Partnership For Advanced Computing in Europe: <http://www.prace-ri.eu/IMG/pdf/hpc-centre-location-whitepaper-2.pdf> adresinden alındı
- Google Inc. (2011). *Security Whitepaper:Google Apps Messaging and Collaboration Products*. Google: <https://docs.google.com/file/d/0B5Y-fwYJF2hLOTVMmZQ1MjAtMDFmNS00YjFhLWI3MmUtZjI5MDQ5Mzc3NmMz/edit?pli=1> adresinden alındı
- Google Inc. (2012). *Getting the heat out: A look at evaporative cooling*. Google: <http://googlegreenblog.blogspot.de/2012/11/getting-heat-out-look-at-evaporative.html> adresinden alındı
- Google Inc. (2014). *Data center locations*. 08 10, 2015 tarihinde Google: <http://www.google.com/about/datacenters/inside/locations/> adresinden alındı
- Google Inc. (2014). *Efficiency: How we do it*. 08 11, 2015 tarihinde Google: <http://www.google.com/about/datacenters/efficiency/internal/#water-and-cooling> adresinden alındı
- Google Inc. (2014). *Google Data Centers*. 08 11, 2015 tarihinde Google: <http://www.google.com/about/datacenters/> adresinden alındı
- Google Inc. (2014). *Mayes County, Oklahoma*. 08 12, 2015 tarihinde Google: <http://www.google.com/about/datacenters/inside/locations/mayes-county/> adresinden alındı
- Google Inc. (2014). *Renewable energy*. 08 12, 2015 tarihinde Google: <http://www.google.com/green/energy/#power> adresinden alındı
- Google Inc. (2016). *Efficiency: How we do it*. 08 11, 2015 tarihinde Google: <http://www.google.com/about/datacenters/efficiency/internal/> adresinden alındı
- Gökçe, O., Özden , Ş., & Demir, A. (2008). *Türkiye'de Afetlerin Mekansal Ve İstatiksel Dağılımı Afet Bilgileri Envanteri*. T.T. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı: https://www.afad.gov.tr/Dokuman/TR/97-2014061215307-abep_kitap_matbaa_final_04122008_small.pdf adresinden alındı
- Gökmen, H. T., & Küçüksille, E. U. (2013). *Veri Merkezi Tasarımı*. 07 09, 2015 tarihinde Akademik Bilişim Konferansları: <http://ab.org.tr/ab13/bildiri/45.pdf> adresinden alındı

- Green Building Education Services. (2011). *LEED Green Associate Study Guide*. 06 20, 2014 tarihinde http://content.greenexamprep.com/pdf/GBES_LEED_Green_Associate_Study_Guide.pdf adresinden alındı
- Haag, S., & Cummings, M. (2012). *Management Information Systems for the Information Age*. Texas: McGraw-Hill/Irwin.
- Hart, J. R. (2011). *NFPA Standards Specifically Cover IT Equipment, Telecom*. System Sensor Blog: <http://www.systemsensorblog.com/2011/05/nfpa-standards-specifically-cover-it-equipment-telecom/> adresinden alındı
- Health Information Technology. (2015). *Privacy and Security of Electronic Health Information*. <http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf> adresinden alındı
- Herbert, G. R. (2015). *2012 Energy Summit*. Official Blog: <http://blog.governor.utah.gov/2012/02/2012-energy-summit/> adresinden alındı
- Higgins, B. (2011). *Disaster Recovery - Sound Technology Services*. 11 15, 2014 tarihinde Sound Technology Services: <http://www.sounditservices.com/services/offsite-disaster-recovery/> adresinden alındı
- Hiles, A. (2007). *The Definitive Handbook of Business Continuity Management*. Holland Tunnel/Jersey City: John&Wiley&Sons Inc.
- HP. (2016). *HP 3PAR StoreServ 7400c 4-node Field Integrated Storage Base*. 08 10, 2015 tarihinde HP Official Site: <http://www8.hp.com/tr/tr/products/disk-storage/product-detail.html?oid=6824290> adresinden alındı
- HP. (2016). *HP ProLiant DL580 Gen8 Server*. 08 10, 2015 tarihinde HP Official Site: <http://www8.hp.com/tr/tr/products/proliant-servers/product-detail.html?oid=6636692> adresinden alındı
- HP Inc. (1998). *Choosing the Cable Infrastructure*. 08 06, 2015 tarihinde hp: <ftp://ftp.hp.com/pub/networking/software/c1.pdf> adresinden alındı
- HP Invent. (2006). *10 Gigabit Ethernet Cabling*. http://www.hp.com/rnd/pdfs/10gig_cabling_technical_brief.pdf adresinden alındı
- HP Invent. (2006). *10 Gigabit Ethernet Cabling*. http://www.hp.com/rnd/pdfs/10gig_cabling_technical_brief.pdf adresinden alındı

- Hunn, B., Gowans, D., Eldridge, D., Emerson, K. I., Carlson, S., Tubber, K., . . . Friedrich, M. (2011). *Procedures for Commercial Building Energy Audits*. Atlanta: ASHRAE.
- Hunn, B., Gowans, D., Eldridge, D., Emerson, K. I., Carlson, S., Tubber, K., . . . Friedrich, M. (2011). *Procedures for Commercial Building Energy Audits*. Atlanta: ASHRAE.
- Hurley, M. (2013). *Issue 76 - Risk Considerations for Data Center Fire Protection*. Fire Protection Engineering: <http://magazine.sfpe.org/issue-76-risk-considerations-data-center-fire-protection> adresinden alındı
- IBM. (2015). *IBM TS3100 Tape Library*. 08 10, 2015 tarihinde IBM: <http://www-03.ibm.com/systems/storage/tape/ts3100/index.html> adresinden alındı
- ISO. (2009). ISO Guide 73:2009 Risk management -- Vocabulary. Geneva, CH-1211, Switzerland.
- ISO. (2009). Kalite Yönetim Sistemleri - Şartlar. Cenevre, İsviçre. 06 15, 2015 tarihinde alındı
- ISO. (2011). TS ISO 31000 Risk Yönetimi - Prensipler ve Kilavuzlar. Cenevre, İsviçre.
- ISO. (2011). *Win the energy challenge with ISO 50001*. 06 17, 2015 tarihinde the International Organization for Standardization: http://www.iso.org/iso/iso_50001_energy.pdf adresinden alındı
- ISO. (2013). Bilgi teknolojisi- Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Gereksinimler. Cenevre, İsviçre. 06 10, 2015 tarihinde alındı
- Jew, J. (2012). *Updates to TIA & ISO Data Center Standards to Reflect Industry Changes*. 07 11, 2015 tarihinde BICSI - advancing the information and communications technology community: https://www.bicsi.org/uploadedfiles/bicsi_conferences/fall/2012/presentations/GS_TUES_3.pdf adresinden alındı
- Kavzoğlu, T., & Şahin, E. K. (2012). *Bulut Bilişim Teknolojisi ve Bulut CBS Uygulamaları*. 07 07, 2015 tarihinde Gebze Teknik üniversitesi: www.gyte.edu.tr/Files/UserFiles/80/jeodezi/yayinlar/pdf/bulutGIS.pdf adresinden alındı
- Keith Jeffery, B. N. (2010). *The Future Of Cloud Computing*. 06 11, 2015 tarihinde The Future Of Cloud Computing: <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf> adresinden alındı

- Kennedy, D. (2009). *Understanding Data Center Cooling Energy Usage & Reduction Methods*. Rittal - The System:
http://www.rittal4it.nl/uploads/Rittal_White_Paper_507_Understanding_Data_Center_Cooling_Efficiency.pdf adresinden alındı
- Kepekci, S. (2011). *Data Center Standards Standards Roundup Roundup*. 09 21, 2015 tarihinde BICSI:
https://www.bicsi.org/uploadedfiles/PDFs/Presentations/Region_Events/canadian_Lachine,%20QC_4-27-11/Data%20Center%20Standards%20Roundup%20-%20Steve%20Kepekci.pdf adresinden alındı
- Kreasis. (2014). *Single Mode Fiber optik kablo nedir?* 07 26, 2015 tarihinde Kreatif Sistemler, Kreasis Çözümler: <http://www.kreasis.com/single-Mode-Fiber-optik-kablo-nedir-t22-y1.html> adresinden alındı
- Kuma, M., Roberts, S., & Kawalek, C. (2010). *The Most Complete and Integrated Virtualization: From Desktop to Datacenter*. Oracle | Integrated Cloud Applications and Platform Services:
<http://www.oracle.com/us/technologies/virtualization/virtualization-strategy-wp-183617.pdf> adresinden alındı
- Lammle, T. (2000). *CCNA: Cisco Certified Network Associate* (2 b.). Alameda: SYBEX Inc.
- Lammle, T. (2007). *CCNA: Cisco Certified Network Associate* (6 b.). Indianapolis: Wiley Publishing Inc.
- Lee, J. (2012). *Tulip Data Center Services Builds Largest Facility in Bangalore, India*. <http://www.thewhir.com/web-hosting-news/tulip-data-center-services-builds-largest-facility-in-bangalore-india> adresinden alındı
- LEED. (2014). *LEED v4 for Building Design and Construction Checklist*. USGBC:
<http://www.usgbc.org/resources/leed-v4-building-design-and-construction-checklist> adresinden alındı
- Loucks, D., & McCluer, S. (2012). *Data Center Design Guide: WP51-PowerEquipmentandDataCenterDesign_v1*. 02 05, 2015 tarihinde The Green Grid | Carbon, Water and Energy Efficiency Metrics, Measurements and Trends for Data Center Planning:
http://www.thegreengrid.org/~media/WhitePapers/WP51-PowerEquipmentandDataCenterDesign_v1.pdf?lang=en adresinden alındı
- McAfee. (2014). *McAfee Labs Threats Report*. İşletmeniz ve bireysel kullanımınız için sistemleri, ağları ve mobil cihazları koruyan güvenlik çözüm ve hizmetleri:

<http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2014.pdf>
adresinden alındı

McDowall, R. (2006). *Fundamentals of HVAC Systems*. Atlanta, USA: Elsevier.

Microsoft. (2010). *Hyper-V: Using Hyper-V and Failover Clustering*. Microsoft TechNet: https://technet.microsoft.com/en-us/library/cc732181%28v=ws.10%29.aspx#BKMK_Validate adresinden alındı

Microsoft Corp. (2015). *Microsoft Datacenter Blog*. Microsoft: <http://blogs.technet.com/b/msdatacenters/> adresinden alındı

Microsoft Corp. (2015). *We power the Microsoft Cloud*. Microsoft: <http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx> adresinden alındı

Microsoft Corporation. (2014). *The OSI Model's Seven Layers Defined and Functions Explained*. 07 10, 2015 tarihinde Microsoft: <https://support.microsoft.com/en-us/kb/103884> adresinden alındı

Microsoft Inc. (2015). *Description of Twisted-Pair Category Types*. 07 11, 2015 tarihinde Microsoft: <https://support.microsoft.com/en-us/kb/151713> adresinden alındı

Miller, R. (2008). *Google Planning Offshore Data Barges*. 05 28, 2015 tarihinde Data Center Knowledge: <http://www.datacenterknowledge.com/archives/2008/09/06/google-planning-offshore-data-barges/> adresinden alındı

Miller, R. (2012). *Google: Our Data Centers Are Good Neighbors*. Google: <http://www.datacenterknowledge.com/archives/2012/01/19/google-our-data-centers-are-good-neighbors/> adresinden alındı

Miller, R. (2015, 01 15). *Switch Plans Massive \$1 Billion SUPERNAP Data Center in Reno*. Data Center Knowledge: <http://www.datacenterknowledge.com/archives/2015/01/15/switch-plans-massive-1-billion-supernap-data-center-reno/> adresinden alındı

Miller, R. (2015). *Switch Plans Massive \$1 Billion SUPERNAP Data Center in Reno*. Data Center Knowledge: <http://www.datacenterknowledge.com/archives/2015/01/15/switch-plans-massive-1-billion-supernap-data-center-reno/> adresinden alındı

Milli Eğitim Bakanlığı. (2011). *Bilişim Teknolojileri Ağ Temelleri*. 07 12, 2015 tarihinde T.C. Milli Eğitim Bakanlığı:

http://megep.meb.gov.tr/mte_program_modul/moduller_pdf/A%C4%9F%20Temelleri.pdf adresinden alındı

Milliyet. (2009). *Sel telekomünikasyon devi Vodafone'u böyle vurdu*. Basında Güven: <http://www.milliyet.com.tr/sel-vodafone-u-boyle-vurdu/gundem/gundemdetay/11.09.2009/1138047/default.htm> adresinden alındı

Miratec. (2009). *Combining proven experience with technical innovation*. 08 06, 2015 tarihinde Combining proven experience with technical innovation: <http://www.miratecinc.com/products.html> adresinden alındı

Neudorfer, J. (2012). *Understanding "Uptime" and Data Center Tier Levels*. 06 20, 2015 tarihinde Data Center Knowledge: <http://www.datacenterknowledge.com/archives/2012/03/21/understanding-uptime-and-data-center-tier-levels/> adresinden alındı

NFPA. (2003). *NFPA 75 Standard for the Protection of Information Technology Equipment*. NFPA.

NSA. (2015). *Utah Data Center*. Domestic Surveillance Directorate: <https://nsa.gov1.info/utah-data-center/index.html> adresinden alındı

Nusca, A. (2012). *IBM, Tulip partner on India's largest datacenter*. ZDNet: <http://www.zdnet.com/article/ibm-tulip-partner-on-indias-largest-datacenter/> adresinden alındı

Nutt, A. (2008). *History of the Data Centre*. 05 27, 2015 tarihinde Articlesbase: <http://www.articlesbase.com/technology-articles/history-of-the-data-centre-556616.html> adresinden alındı

Odabaş, Y. D. (2008). *Bilgi Yönetimi Ve Yüksek Öğrenim Kurumlarında Kurumsal Açık Erişim*. 05 31, 2015 tarihinde E-Prints in library & information science: http://eprints.rclis.org/12670/1/Y%C3%BCksek_%C3%96%C4%9Frenimde_Bilgi_Y%C3%B6netimi_ve_A%C3%A7%C4%B1k_Ar%C5%9Fivler.pdf adresinden alındı

Önel, D., & Dinçkan, A. (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu*. Kocaeli, Türkiye.

Özbilgin, D. İ. (2015). *Yeni bir standart: ISO 22301 İş Sürekliliği Yönetimi Sistemi: Gereksinimler*. 06 03, 2015 tarihinde Bilişim Dergisi: <http://www.bilisimdergisi.org/pdfindir/s144/pdf/96-101.pdf> adresinden alındı

Patterson, M. (2010). *ERE_WP_101510*. 12 05, 2014 tarihinde The Green Grid | Carbon, Water and Energy Efficiency Metrics, Measurements and Trends for

Data Center Planning:

http://www.thegreengrid.org/~media/WhitePapers/ERE_WP_101510_v2.ashx?lang=en adresinden alındı

PCI Security Standards Council. (2010). *PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard version 2.0*. PCI Security Standards Council:
<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf> adresinden alındı

PCI Security Standards Council. (2010). *Requirements and Security Assessment Procedures*. PCI Security Standards Council:
https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf adresinden alındı

Peirce, S. J. (2011). *Privacy and Security Issues Affecting Employee Benefit Plans*. 08 29, 2015 tarihinde AICPA:
http://www.aicpa.org/interestareas/employeebenefitplanauditquality/resources/testimonyandcmtrltrs/downloadabledocuments/ebpaqc_sas70_testimony_advisory%20council.pdf adresinden alındı

Peter Mell, T. G. (2011). *The NIST Definition of Cloud Computing*. 06 11, 2015 tarihinde National Institute of Standards and Technology:
<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> adresinden alındı

Preeti Gupta, T. S. (2012). *Tulip Telecom and IBM Build India's Largest Data Center to Address Rapid Growth of Mobile Consumers in Emerging Markets*. IBM:
<https://www-03.ibm.com/press/us/en/pressrelease/36693.wss> adresinden alındı

Rasmussen, N. (2001). *Allocation Data Center Energy Costs and Carbon to IT Users*. 04 25, 2015 tarihinde Schneider Electric is the Global Specialist in Energy Management: <http://www2.schneider-electric.com/documents/support/white-papers/wp-data-centre-161-turkish.pdf> adresinden alındı

Rasmussen, N. (2003). *Air Distribution Architecture Options for Mission Critical Facilities*. Universal Networking Services:
<http://www.apcdistributors.com/white-papers/Cooling/WP-55%20Air%20Distribution%20Architecture%20Options%20for%20Mission%20Critical%20Facilities.pdf> adresinden alındı

Rawson, B. P., & Green, K. C. (2012). *Inert Gas Data Center Fire Protection and Hard Disk Drive Damage*. The Data Center Journal:
<http://www.datacenterjournal.com/inert-gas-data-center-fire-protection-and-hard-disk-drive-damage/> adresinden alındı

- Sandoval, B. (2015). *Switch's dual locations transform Nevada into the world's largest active-active data center ecosystem*. SuperNap: <https://www.supernap.com/nevada-advantage.html> adresinden alındı
- Santana, G. A. (2014). *Data Center Virtualization Fundamentals*. Indianapolis, USA: Cisco Press.
- Shroff, G. (2010). *Enterprise Cloud Computing: Technology, Architectures, Applications*. Cambridge University Press.
- Simon, W. L., & Mitnick, K. D. (2003). *The Art of Deception*. Indianapolis: Wiley Publishing Inc.
- Smith, L. (2013). *Major Data Center Designs: Beat the Heat*. Ravica Environment Solutions: <http://www.ravica.com/blog/general/major-data-center-designs-beat-the-heat/> adresinden alındı
- Snedaker, S. (2007). *Business Continuity & Disaster Recovery for IT Professional*. Burlington, Kanada: Syngress Publishing, Inc., Elsevier, Inc.
- Snedaker, S. (2007). *Business Continuity and Disaster Recovery Planning for IT Professionals*. Tucson, AZ, USA: Elsevier Inc.
- SuperNap. (2015). *Clients - Sophisticated Startups To Fortune 100 Powerhouses*. SuperNap A Switch Company: <https://www.supernap.com/clients.html> adresinden alındı
- SuperNap. (2015). *Gallery*. SuperNap A Switch Company: <https://www.supernap.com/gallery/#7> adresinden alındı
- SuperNap. (2015). *SuperNap A Switch Company*. SuperNap A Switch Company: <https://www.supernap.com/locations.html> adresinden alındı
- SuperNap. (2015). *Switch the entire concept of data center design*. Supernap A Switch Company: <https://www.supernap.com/rob-roy-factor.html> adresinden alındı
- SuperNap. (2015). *The most cost-efficient, mission critical, high-availability technology environment on the planet*. SuperNap: <https://www.supernap.com/data-centers.html> adresinden alındı
- Symantec. (2015). *Backup methods in Backup Exec*. Symantec: https://support.symantec.com/en_US/article.HOWTO98909.html adresinden alındı

- Symantec Corporation. (2015). *2015 Internet Security Threat Report*. Symantec:
http://www.symantec.com/security_response/publications/threatreport.jsp
 adresinden alındı
- Telekomünikasyon İletişim Başkanlığı. (2007). *T.C. Bilgi teknolojileri ve iletişim kurumu yer sağlayıcılığı bildirim arayüzü*. T.C. Bilgi teknolojileri ve iletişim kurumu yer sağlayıcılığı bildirim arayüzü:
<https://faaliyet.tib.gov.tr/yetbel/yonetmelik1.html> adresinden alındı
- Turner, P., Seader, J. H., & Renaud, V. (2008). *Tier Classifications Define Site Infrastructure Performance*. 06 27, 2015 tarihinde CSI POWER & ENVIRONMENTAL:
http://www.csipower.com/images/PDF/Tier_Classifications_Define_Site_Infrastructure_performance.pdf adresinden alındı
- Turner, S. (2013, 05 08). *In-house, colocation, dedicated & managed hosting – comparison and examples*. 06 11, 2015 tarihinde IWEB HOSTING:
<http://blog.iweb.com/en/2013/05/in-house-colocation-dedicated-managed-hosting-comparison-and-examples/12020.html> adresinden alındı
- Türk Dil Kurumu. (2006). *Bilim ve Sanat Terimleri Ana Sözlüğü*. Türk Dil Kurumu:
http://www.tdk.gov.tr/index.php?option=com_bilimsanat&view=bilimsanat
 adresinden alındı
- Uptime Institute. (2016). *Tier Certification of Design Documents*. 06 21, 2015 tarihinde Uptime Institute: <https://uptimeinstitute.com/TierCertification/design-document-certifications.php> adresinden alındı
- Uzuner, H. (2010). *Cloud Computing Bulut Bilişim*. 06 04, 2015 tarihinde Çözümпарк:
http://www.cozumpark.com/blogs/cloud_computing/archive/2010/12/26/cloud-computing-bulut-bilisim.aspx adresinden alındı
- Üçler Yangın. (2011). *Sulu Yangın Söndürme Sistemleri*. 08 10, 2015 tarihinde Üçler :
<http://www.ucleryangin.com.tr/detay.asp?Model=17> adresinden alındı
- Verdun, G. (2008). *White Paper 14 - (DCiE) Detailed Analysis*. 03 10, 2015 tarihinde The Green Grid | Carbon, Water and Energy Efficiency Metrics, Measurements and Trends for Data Center Planning:
http://www.thegreengrid.org/~media/WhitePapers/White_Paper_14_-_DCiE_Detailed_Analysis_072208.pdf?lang=en adresinden alındı
- VMware Inc. (2006). *Virtualization Overview*. vmware:
<https://www.vmware.com/pdf/virtualization.pdf> adresinden alındı

- WMware. (2016). *High Availability*. 08 10, 2015 tarihinde WMWare Virtualization: <https://www.vmware.com/tr/products/vsphere/features/high-availability> adresinden alındı
- Woolley, B. (2013). *Assessing Your Data Center Maintenance Program*. Schneider Electric Website: <http://blog.schneider-electric.com/datacenter/2013/01/11/assessing-your-data-center-maintenance-program/> adresinden alındı
- Ye, K., Huang, D., Jiang, X., Chen, H., & Wu, S. (2010). *Virtual Machine Based Energy-Efficient Data Center Architecture for Cloud Computing: A Performance Perspective*. 07 06, 2015 tarihinde CMU Contributed Webserver: <http://www.contrib.andrew.cmu.edu/~kejiangy/greencom2010.pdf> adresinden alındı
- Yüzgeç, U., & Günel, A. (2014). *Üniversitelere Yönelik Bir Veri Merkezinin İklimlendirme Planlaması*. 07 08, 2015 tarihinde Bilecik Şeyh Edebali Üniversitesi Dergileri: <http://edergi.bilecik.edu.tr/index.php/fbd/article/view/35/26> adresinden alındı
- Zenium Technology. (2015). *Veri Merkezi Sektörü Doğal Felaketlerle Sarsılmaya Devam Ediyor*. Data center Design: <https://zeniumdatacenters.com/tr/veri-merkezi-sektoru-dogal-felaketlerle-sarsilmaya-devam-ediyor/> adresinden alındı

ÖZGEÇMİŞ

Kişisel Bilgiler

Ad Soyad : Onur Moral

Doğum Yeri ve Tarihi : Kadıköy – 03.01.1984

Eğitim Durumu

Ön Lisans : Süleyman Demirel Üniversitesi Keçiörlü Meslek
Yüksek Okulu Bilgisayar Teknolojileri ve Programlama
(2004)

Lisans : Anadolu Üniversitesi İşletme Fakültesi İşletme Bölümü
(2013)

Yüksek Lisans : Okan Üniversitesi Fen Bilimleri Enstitüsü Bilişim
Sistemleri

İş Deneyimi

Multinet Kurumsal Hiz. AŞ. Sistem ve Network
Sorumlusu (2008-2009)

CEVA Lojistik Ltd. Şti. Uluslararası BT Sistem Altyapı
Müdürü (2009 - Devam Ediyor)

İletişim

Adres : Güzensu Mahallesi Medeniyet Sokak No: 36/2
Maltepe / İstanbul

E-Posta : onur@onurmoral.com

Başlıca Projeler ve Tecrübeler

Veri Merkezi Tasarım ve Kurulumu,

Felaketten Kurtarma Merkezi Tasarım, Kurulumu ve İş
Sürekliliği Planlaması,

Veri Merkezi Taşıma,

Ağ Altyapısı Yedeklilik ve Sürekliliği,

Yedekleme ve Kurtarma Sistemleri Tasarım ve
Kurulumu,

Log Yönetim Projesi,

Kablosuz İnternet Güvenliği,

ISO 27001 Bilgi Güvenliği Yönetim Sistemi,

Veri Ve İnternet Güvenliği Projesi,

Sanallaştırma Projesi,

Değişiklik, Olay ve Problem Yönetimi,

Veri Tabanı Yönetim Sistemleri.

YENİ NESİL VERİ MERKEZİ TASARIMI VE KURULUMU AŞAMASINDAKİ

GEREKSİNİMLERİ

YÜKSEK LİSANS TEZİ

ONUR MORAL

tarafından

OKAN ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Bilişim Sistemleri Anabilim Dalına

YÜKSEK LİSANS

derecesi şartını sağlamak için sunulmuştur.

Onaylayan Jüri:



Prof. Dr. Ahmet Faik KAŞLI
Danışman



Prof. Dr. Ahmet Mesut RAZBONYALI
Üye



Yrd. Doç. Dr. Nurşen TOPÇUBAŞI
Üye

Haziran 2016

Program: Bilişim Sistemleri