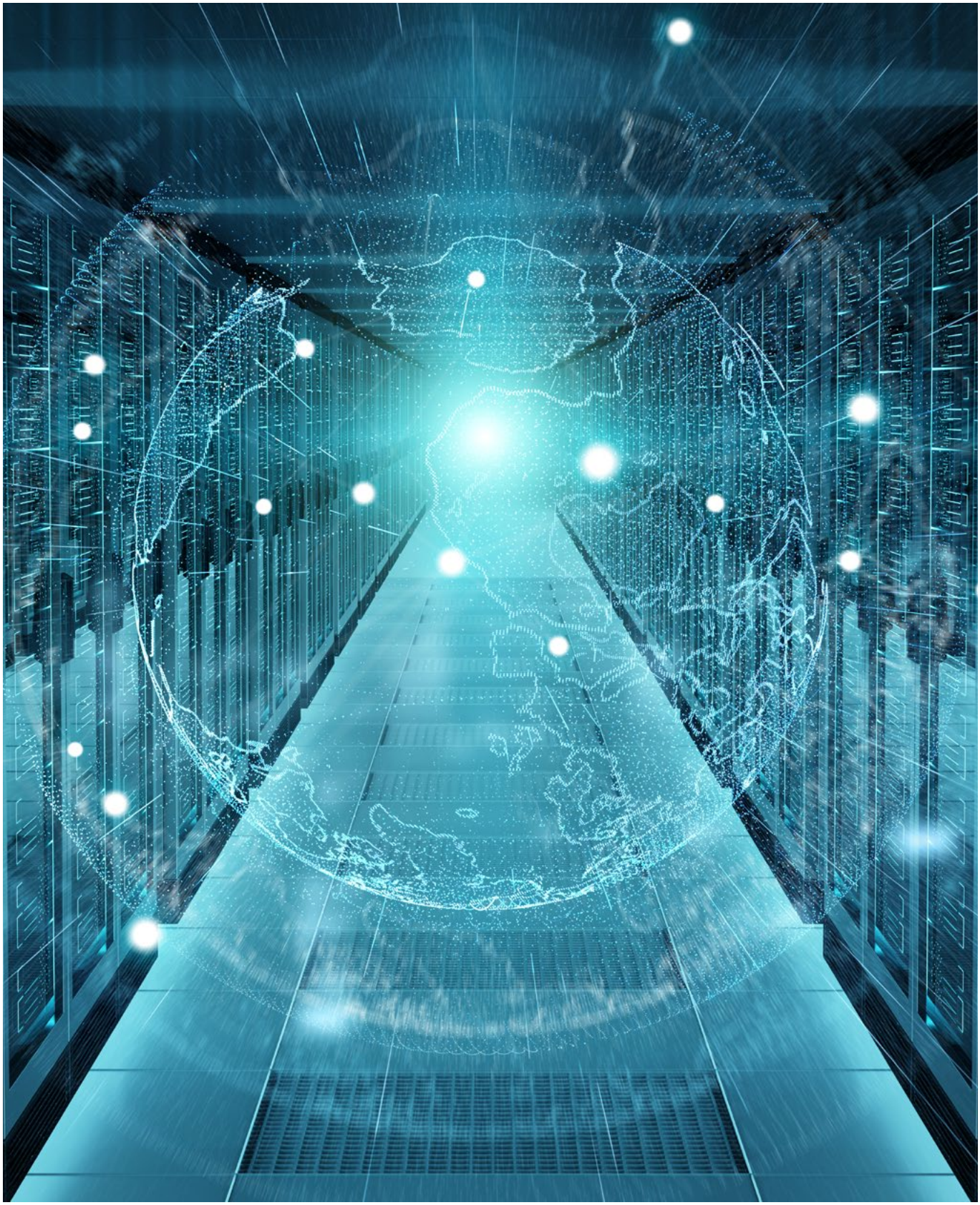
VERİ MERKEZLERİNİN SİBER GÜVENLİĞİ

TREND ANALİZİ HAZİRAN 2021

thinktech
STM Teknolojik Düşünce Merkezi



STM ThinkTech

1. GİRİŞ

Dünya giderek daha dijital bir hâl alırken Dördüncü Sanayi Devrimi'nin de etkisiyle artan veri trafiğinin yönetimi önemli bir konu hâline gelmiştir. Neredeyse her elektronik cihazın çalışmak için ihtiyaç duyduğu kişisel bilgilerin hatta dijital paraların saklandığı verilerin depolanması ise veri merkezleriyle mümkün kılınmıştır.

Ancak bilişim teknolojileri, hayatı kolaylaştırma yönünde sağladıkları imkânların yanında, güvenlik boyutunda da yeni kaygıların gelişmesine sebep olmuştur. Günümüz dünyasında, fiziksel temasa gerek duymadan hırsızlık, dolandırıcılık gibi suç fiilleri mümkün hâle gelmiştir. Bunun yanında bilişim teknolojileri suç gruplarının veya terör örgütlerinin iletişim becerilerini artırmış, propaganda imkânlarını güçlendirmiş ve yeni faaliyet sahalarının ortaya çıkmasını sağlamıştır.

Günümüzde siber güvenliğin savaşın beşinci boyutu olarak kabul edilmesinin ötesinde tüm ülkeler için ulusal güvenliğin ayrılmaz ve en önemli bileşeni olarak değerlendirilmesi, siber güvenliğe verilen önemi de artırmıştır. Veri merkezlerinin siber güvenliği ise günümüz dijital dünyasının en önemli konularının başında gelmektedir. Bu nedenle bu çalışmada veri merkezlerinin önemine değinilerek, veri merkezlerinde siber güvenliği sağlamak için uygulanan stratejiler üzerinde durulmuştur. Ayrıca konunun hukuksal boyutu da ele alınarak veri merkezleri güvenliği için öne çıkan yeni trendlere yer verilmiştir.

2. VERİ MERKEZİ NEDİR?

Günümüzde bilgi işlem operasyonları için kullanılan bilgisayar, sunucu ve veritabanlarının ihtiyaç duyduğu verilerin saklandığı, kontrol edildiği ve işlendiği yerler veri merkezleri olarak adlandırılmaktadır[1].

En basit tanımıyla, bir veri merkezi, kuruluşların kritik uygulamalarını ve verilerini barındırmak için kullandıkları fiziksel bir tesistir. Bir veri merkezinin tasarımı, paylaşılan uygulamaların ve verilerin teslim edilmesini sağlayan bilgi işlem ve depolama kaynakları ağına dayanmaktadır. Veri merkezi tasarımının temel bileşenleri arasında yönlendiriciler, anahtarlar, güvenlik duvarları, depolama sistemleri, sunucular ve uygulama denetleyicileri bulunmaktadır[2].

Veri merkezleri genel hizmet yapısına göre özel veri merkezleri ve internet veri merkezleri olarak iki gruba ayrılmaktadır. Özel veri merkezleri tek bir kuruluşun kendi ihtiyaçları doğrultusunda hizmet verirken, internet veri merkezleri ise genel olarak üçüncü şahıslara hizmet sunmaktadır. İnternet veri merkezleri barındırma (hosting) ve yer paylaşımı (co-location) olarak iki şekilde hizmet vermektedir.

Barındırma, ev sahipliği hizmeti ile internet veri merkezinden hizmet alan kuruluşun kendi işi çerçevesinde kullandığı yazılım, veri ve uygulamalarını internet veri merkezinde bulunan sunucu ve veri depolama birimlerinde çalıştırması ve/veya internet veri merkezi işletmecisi tarafından sağlanan uygulamaların kullanılmasını kapsamaktadır.

Yer paylaşımı hizmeti ise internet veri merkezinden hizmet alan kuruluşun kendi işi çerçevesinde kullandığı (kendisine ait) Bilişim Teknolojileri (BT) sistemlerini internet veri merkezi alanına kurması, internet veri merkezinin temel altyapı olanaklarını ve ağ altyapısını, isteğe bağlı olarak da yönetim hizmetini kullanmasını kapsamaktadır[3].

2.1 Veri Merkezleri Neden Önemlidir?

Günümüz bilişim dünyasında veri merkezleri kuruluşlar ve bireyler için birçok uygulama ve aktivite açısından büyük öneme sahiptir. İletişimde vazgeçilmez bir hâl alan e-posta ve dosya paylaşımı en yaygın veri transferi yöntemleri arasında bulunurken, müşteri ilişkileri yönetimi, işletme kaynak planlaması ve veritabanları, büyük veri, yapay zekâ, makine öğrenmesi, sanal bilgisayarlar ve diğer üretken uygulamalar kullandıkları yoğun veriler nedeniyle veri merkezlerinin temel kullanım alanlarını oluşturmaktadır. Bu alanlarda kullanım için ise farklı veri merkezi çözümleri bulunmaktadır[4].

Çin gibi 800 milyondan fazla internet kullanıcısının olduğu ülkelerde artan ihtiyaçtan dolayı mevcut veri merkezlerinin sayısının 2022 yılına kadar dört katına çıkması beklenmektedir. Pandemi ile birlikte uzaktan çalışma, görüntülü iletişim ve toplantıların da artan veri trafiğine etkisi büyüktür. Dijital iletişimin her geçen gün daha da önem kazanması veri merkezlerinin gelecekte ne kadar önemli bir rol üstleneceğinin de habercisidir[5].

2.2 Veri Merkezi Çeşitleri Nelerdir?

Genel anlamda birçok modelde veri merkezi bulunmaktadır. Ancak kullanım yöntemlerine göre veri merkezleri için bazı sınıflandırmalar yapmak mümkündür. Veri merkezleri çeşitlerine göre dört farklı şekilde sınıflandırılabilir:

2.2.1 Özel Veri Merkezleri

Özel Veri Merkezleri, işletmelerin kendi içlerinde kullandıkları tesislerdir. İşletmeler özel kullanımları için kendi ihtiyaçlarına uygun modelledikleri veri merkezleri tasarlayabilmektedir. Bu veri merkezleri işletmelerin içinde veya özel erişim imkânları ile güvenli lokasyonlarda olabilmektedir.

2.2.2 Genel Kullanım Amaçlı Hizmetler Sunan Veri Merkezleri

Bu merkezler, daha düşük bütçeli ve sınırlı hizmetleri için bireysel olarak veya şirketlerce kullanılabilmektedir. Ortak kullanım yapısında olan bu veri merkezleri en yaygın kullanım imkânı olan modellemedir.

2.2.3 Kolokasyon Veri Merkezleri

Telekomünikasyon, ağ cihazları, bilgisayar, sunucu vb. sistemlerinin bağlantılarının sağlanması maksatlı kullanılan Kolokasyon Veri Merkezleri bir diğer hizmet modelini oluşturmaktadır. Kolokasyon modelinde hizmet talep eden kişi veya kuruluş veri merkezinin bir alanını kendi ihtiyaçları doğrultusunda kiralayabilmektedir. Kolokasyon modelinde hizmeti sunan taraf tesis, ağ genişliği, güvenlik ve sistemlerin soğutulması gibi işleri üstlenirken kiralayan taraf ise sunucuların bakımı, kullanımı, verilerin depolanması ve güvenlik duvarı gibi uygulamaları kendisi oluşturmaktadır.

2.2.4 Bulut Tabanlı Veri Merkezleri

Bulut Tabanlı Veri Merkezleri giderek kullanımı yaygınlaşan bir diğer modellemedir. Bu veri merkezi modelinde veriler Amazon Ağ Hizmetleri (Amazon Web Services -AWS), Microsoft (Azure) veya IBM Bulut gibi kamusal bulut hizmeti sağlayan kuruluşlarca oluşturulan sistemler üzerinden hareket etmektedir[4].

Veri merkezleri işlem yapılarına göre de sınıflandırılabilmektedir. Dört sınıftan oluşan yapıda,

- **Kademe 1 (Tier 1)** çok temel özellikleri olan güvenliği düşük seviyede bir sanal depo gibidir. Güvenlik önlemleri ortalama standartlarda birçok şirketi koruma yetisindendir.
- **Kademe 2 (Tier 2)** sınıflaması Kolokasyon Veri Merkezlerinde tercih edilmektedir. Bu sınıflama ile kullanıcılara Tier 1'de verilen hizmetlerin yanında maliyet yönetimi ve performans bilgileri de sunulmaktadır.
- **Kademe 3 (Tier 3)** veri merkezleri hizmetlerinde belirgin bir aksamaya neden olmadan bakım yapabilme yetisindedir. Tier 3 ayrıca yedekleme kapasitesine de sahiptir.
- **Kademe 4 (Tier 4)** plansız bakım çalışmalarını dahi yaparken veri akışında veya hizmetlerde bir aksamaya neden olmadan çalışma özelliğindedir. Çok daha gelişmiş donanımlar ve yazılımlarla yedekliliğin ve izlemenin üst noktada desteklendiği Tier 4, günlük operasyonlarda aksama olmadan faaliyet gösterebilmektedir[6].

Veri merkezlerinin çeşitliliği arttıkça bu merkezlerin günümüzde hızla artan siber saldırılara karşı da koruması da gerekmektedir. Veri merkezlerinin siber güvenliği günümüz dijital dünyasının en önemli konularından biridir[7].

3. VERİ MERKEZLERİNİN SİBER GÜVENLİĞİ

Veri merkezi güvenliği denildiğinde tesisin genel güvenliğinin yanında daha önemli bir nokta olan siber güvenlik uygulamaları da akla gelmektedir. Günümüzde daha ekonomik ve savunması daha kolay olduğundan Bulut Tabanlı Veri Merkezlerine olan ilgi artarken bu alanlara yapılan saldırıların da artması endişe yaratmaktadır. İşletmelerin ve kişilerin hassas bilgilerini de saklayan ve işleyen veri merkezlerinin güvenliği fiziksel veya yazılımsal olarak sağlanabilmektedir.

Fiziksel güvenlik önlemleri ağırlıklı olarak veri merkezinin dışarıdan gelebilecek saldırı ve sabotajlara karşı korunması amacıyla tasarlanmaktadır. Genellikle penceresi dahi olmayan ve girişi sınırlı tutulan veri merkezleri kamera sistemleriyle sürekli olarak izlenmektedir. Tesis

çalışanları ise biyometrik güvenlik sistemleri olan parmak izi, retina tarama ve yüz tanıma teknolojileriyle içeri giriş yapabilmektedir. Ayrıca yangın söndürme, hareket algılama, sıcaklık kontrolü, sunucuların fiziksel durumlarının izlenmesi ve jeneratörler gibi yedek enerji kaynakları da veri merkezlerinin fiziksel güvenliğini sağlamada önemli bir rol oynamaktadır.

Yazılım güvenliği ise siber saldırılara karşı alınan önlemleri kapsamaktadır. Veri merkezlerine yapılan siber saldırılar genellikle hack'leme, kötücül yazılım ve casus yazılım yöntemleriyle gerçekleşmektedir. Güvenlik Bilgi ve Olay Yönetim Yazılımı (Security Information and Event Management Tool -SIEM) aracılığıyla gerçek zamanlı güvenlik kayıtları kullanılarak korunan veri merkezlerindeki tanımlı veri giriş ve çıkışları dikkatle izlenebilmektedir[8].

Bütün veri merkezleri alınacak önlemler ister fiziksel isterse de yazılımsal olsun sakladıkları ve işledikleri verilerin güvenliğini sağlamayı hedeflemektedir. Verilerin kaybolma olasılığına karşı yedeklenmesi, şifrelenmesi ve bütün sistem süreçlerinin güncel kanunlara uyumlu hâle getirilmesi önemli bir operasyonel süreçtir[10].

Son zamanlarda güvenli veri depolama ve veri paylaşımında blok zinciri (Blockchain) uygulamaları da dikkat çekmeye başlamış ve bu kapsamda faaliyet gösteren start-up'lar önemli yatırımlar almaya başlamışlardır. Bunlardan biri LPS Bilişim Hizmetleri'dir. Şirket geliştirdiği dünyanın ilk blok zinciri teknolojisine sahip veri yönetimi, transferi ve depolama sistemi olan "LpsChain" ile uluslararası alanda önemli bir başarıya imza atarak, Birleşik Krallık Dış Ticaret Bakanlığı tarafından Birleşik Krallık'a yatırım yapmak isteyen ve yüksek büyüme gösteren yenilikçi teknoloji firmalarının dahil edildiği "Global Entrepreneurship Program"ı çerçevesinde destek kapsamına alınmayı başarmıştır[11].

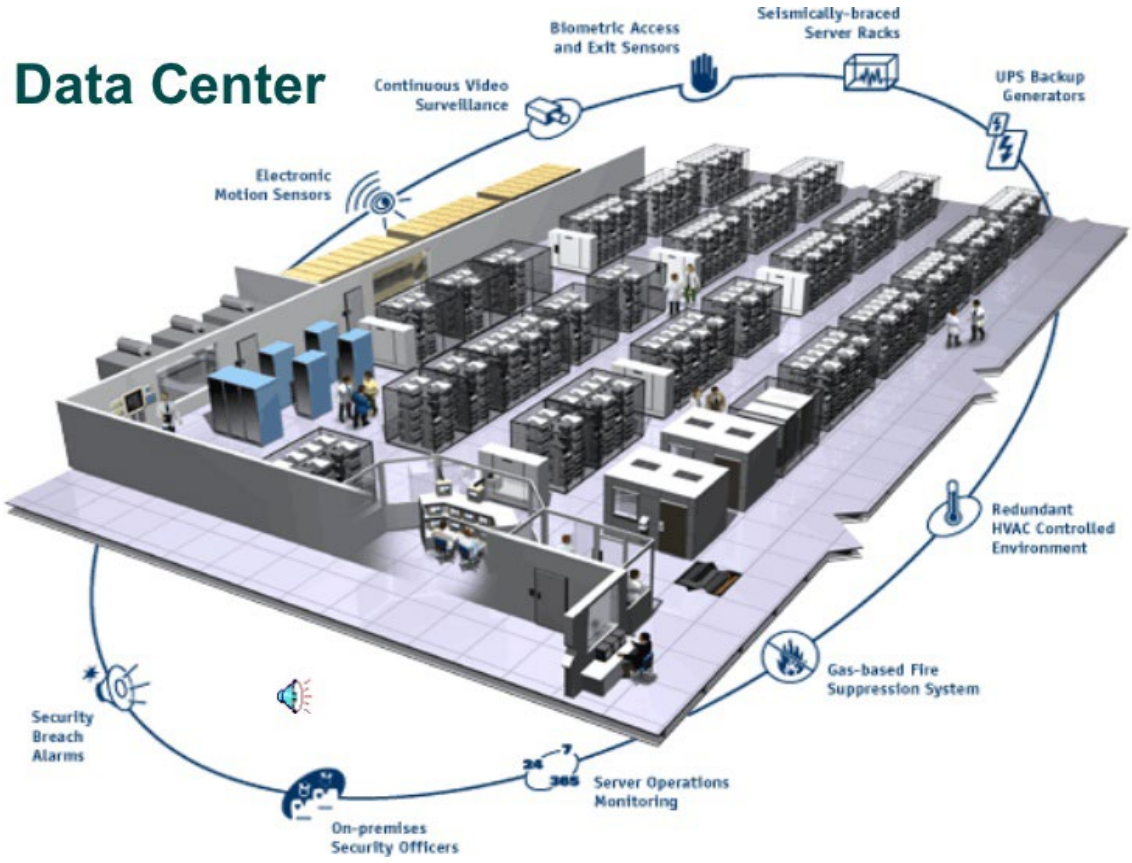
3.1 Veri Merkezlerinde Siber Güvenlik Neden Önemlidir?

Veri merkezlerinin sahip oldukları veriler bütün işletmeler ve iş modelleri için büyük öneme sahiptir. Veri merkezlerinde saklanan ve işlenen veriler işletme veya şahıslar için yıkıcı etkilere sebep olabilecek kritik bilgileri içeriyor olabilir. Finansal kayıtlar, ticari sırlar ve birçok kişisel bilginin de depolandığı veri merkezlerinde güvenliğin sağlanamadığı durumlarda ciddi sorunlar ortaya çıkabilmektedir.

Veri merkezlerinin güvenliği ile ilgili bir sorun yaşandığında ciddi imaj ve müşteri güven kaybı yaşanabilmektedir. Verilen hizmetler özel amaçlı veya genel kullanımlı dahi olsa kullanıcıların güvenliği sağlanamadığı takdirde uzun vadede güveni tekrar kazanmak zor olacaktır.

Ayrıca veri merkezi içerisinde saklanan veriler ve kullanılan sistemler ile veri merkezi güvenliği kapsamında bazı kilit regülasyonlar bulunmaktadır. İçlerinde PCI, DSS, HIPAA, GDPR, SAE 18 ve ISO 27001:2013'ün de bulunduğu bu regülasyonlara uyumsuzluk tespit edildiğinde ciddi cezalarla karşı karşıya kalınabilmektedir.

Son olarak da güvenliğin sağlanamaması işletme veya kişilere ciddi finansal zararlar veya kayıplar



Şekil 1: Veri merkezlerinde uygulanabilecek fiziksel güvenlik önlemleri[9].

verebilmektedir. Bir hizmetin aksaması durumunda iş yapısında yaşanacak aksaklıklar maddi kayıplara neden olabilirken, bilgilerin çalınması gibi riskler tazminat taleplerini ortaya çıkarabilmektedir[12].

5G, Dördüncü Sanayi Devrimi ve IoT gibi teknolojiler yaygınlaştıkça veri merkezi ihtiyacı ve verilerin güvenliğinin önemi artmaktadır. Veri merkezlerinin dijital dönüşümde oynadığı büyük rol düşünüldüğünde kullanıcıların karşılaşacakları riskleri bilmesi ve hazırlıklı olması da önem kazanmaktadır. Dijitalleşen çağda fiziksel saldırılar giderek azalırken siber saldırılar ise hızla artmaktadır[13].

3.2 Verilerin Güvenliğini Sağlamak için Neler Yapılıyor?

Veri merkezleri güvenliği sağlamak için fiziksel ve yazılımsal yöntemler uygulamaktadır. Siber saldırılar yazılımsal önlemlerle engellenebileceğinden artan siber saldırılara karşı yeni geliştirilen yazılım önlemleri önem kazanmaktadır.

Veri merkezlerine fiziksel girişin sınırlandığı kadar sanal girişlerin de sınırlandırılması ve hatta operatör girişi dışında her türlü bağlantının engellenmesi gerekmektedir. Veri merkezlerine zarar veren bağlantılar her zaman kötü niyetli olmayabilir. Yapılan araştırmalar veri merkezi sorunlarının büyük oranda insan hatası kaynaklı olduğunu da göstermiştir. Bu nedenle giriş kontrolleri yedekleme sistemleri ve engelleyici yazılımlar veri merkezleri güvenliğinde önemli bir basamaktır.

Veri merkezi güvenliğinde sunucuların ve verilerin izlenmesi için seçilecek araç, yöntem ve ekipmanlar da önemlidir. Veri merkezi güvenliğinin artırılması için;

- Düzenli denetimlerle varlıkların kontrolü ve güvenlik yönetimi işlemleri ile giriş protokollerinin değerlendirilmesi önemlidir.
- Verilerin transferi sırasında ağ seviyesinde şifreleme ve verilerin iletildiği noktalara ulaştığı veya depolandığı anlarda ise sunucu seviyesinde şifreleme ile önlem alınmalıdır.
- BMS, PMS, SIEM tarzı yazılımlarla izleme ve kontrol aşamalarında otomasyonun entegre edilmesi sayesinde her seviyede sürekli tehdit, durum ve güvenlik etkinliklerinin izlenmesi sağlanmalıdır.

Veri merkezi sunucuları ve sistemlerinin sürekli güncel olması da önemlidir. Düzenli yayınlanan yazılımsal güncellemelerin takibi ve sistemlere entegre edilmesi açık arka kapı veya riskli bağlantı olasılıkların engellenmesinde büyük öneme sahiptir.

Bir siber saldırı sonrası verilerin kaybolması, kullanılmaz hâle gelmesi veya istenmeyen bilgilerle bozulmasının önüne geçilmesi için tesislerde alınacak yedeklemeler kritik bir rol oynayacaktır. Bununla beraber tesis altyapısının da düzenli bakımlarla sağlıklı tutulması gerekmektedir. Aşırı ısınan bir sunucu veya bir enerji kesintisi, sistemde hataya neden olarak siber saldırılar için bir olasılık yaratabilir. Bu sebeple tesislerin düzenli bakımları önem kazanmaktadır.

Ağ segmentasyonu da bir başka veri merkezi güvenliği olarak değerlendirilmektedir. Veri ağının farklı segmentlere bölünerek her birinde ayrı bir güvenlik uygulaması tercih edilmesi hacker'ların işlerini zorlaştırarak saldırılara karşı savunma olasılığını artırmaktadır.

Veri merkezleri olası bir felaket senaryosunda işletmeye ait veya kişisel bilgilerin kurtarılması ve korunması için kritik bir öneme sahiptir. Bu nedenle en yüksek güvenlik uygulamalarıyla korunmaları gerekmektedir. Firmalar kendi özel veri merkezleri için özel güvenlik hazırlıkları yapabilirken ortak veri merkezlerinin sunucu hizmetini sunan sahipleri çok daha geniş ve gelişmiş uygulamaları kullanmak ve takip etmek zorundadır[14].

3.3 Kuruluşlar Siber Güvenliğe Karşı Nasıl Bir Strateji İzliyor?

İşletmelerin verilerini en iyi şekilde saklaması gerekmektedir. Bu veriler ticari sırlar, müşteri bilgileri veya finansal bilgileri içerebilmektedir. Bu sebeple siber güvenlik için oluşturulacak stratejilerin en önemlilerinden biri veri merkezleri güvenliğini kapsamaktadır.

Bazı işletmeler verileri kendi iç sistemlerinde tutarak daha güvenli bir depolama sağladığını düşünmektedir. Bazı işletmeler ise verilerin bulut sistemlerde daha güvenle saklandığını savunmaktadır. Ancak bulut sistemler veya farklı bir kuruluştan hizmet alınması bütün verilerin güvenliğinin üçüncü kişilere devredilmesi anlamına gelebilmektedir. En güvenilir veri merkezi hizmet sunucularının bile çok ağır siber saldırılarla karşılaştığı bilinmektedir. *Forbes*'a göre 2019 yılında kaydedilen veri ihlalleri toplamda 4,9 milyarı geçmiştir. Bu ihlallerin çok azı finansal kazanç amaçlı olarak gerçekleşmektedir. İhlallerde asıl hedeflenen işletmelere para kaybettirmek veya hizmetlerinin engellenmesidir.

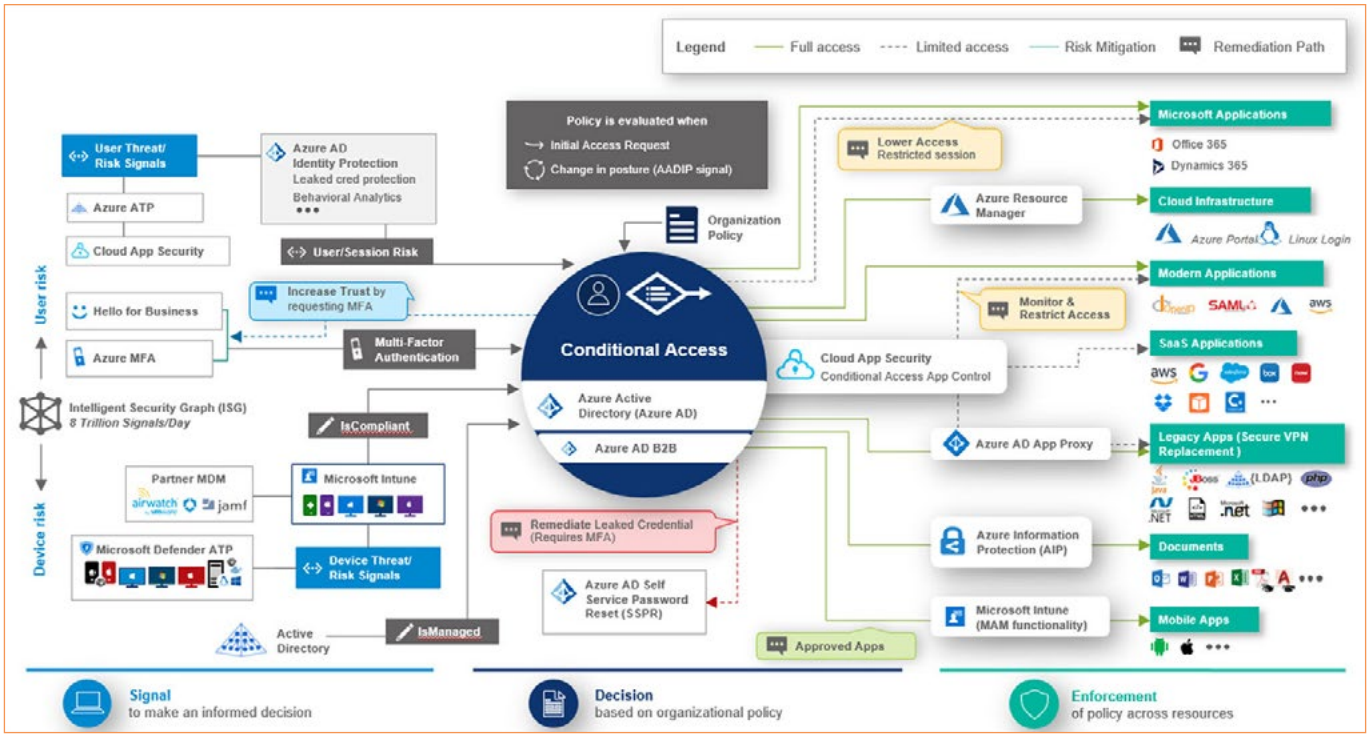
Son zamanlara öne çıkan "Sıfır Güven Mimarisi (Zero Trust Architecture -ZTA)" stratejisi dijital dünyanın siber saldırılarla savaşında önemli bir rol oynamaktadır.

Sıfır Güven Mimarisi, IoT ile birbirine bağlanan cihazların arttığı dünyada veri merkezi ile bağlanan her cihazın güvenliğinin sorgulanmasını kapsamaktadır. Bağlanan cihazlara izin verilse dahi izlemeye devam eden ve en düşük güvenlik seviyelerini uygulayan sistem olası bir saldırıda hızla cevap verme özelliğine sahiptir.

Oluşturulacak güvenlik seviyeleri, olası bir saldırı girişiminde belirli seviyelerde yapay zekâ ve makine öğrenmesi ile geliştirilmiş sisteme otonom olarak cevap verme kabiliyeti sağlarken, alarm seviyesinin yükselmesi durumunda profesyonel müdahale ekiplerince yapılacak savunmalara da imkân vermektedir[15].

Birçok organizasyon siber saldırılarla savaşmak için çeşitli hizmetler ve güvenlik çerçeveleri sunmaktadır. Bu çerçevelerden birinin kabul edilerek uygulanması da veri merkezi güvenliğinde önemli bir adımı oluşturmaktadır.

Bu çerçeveler içerisinde en bilinen ve popüler olanı ABD'nin Ulusal Standartlar ve Teknolojiler Enstitüsü (National Institute of Standarts and Technologies -NIST) tarafından oluşturulan siber güvenlik çerçevesidir. NIST çerçevesi ABD hükümeti ve birçok özel sektör tarafından kabul görmüş ve kullanılmaktadır. NIST siber güvenlik çerçevesi beş ana bölümden oluşmaktadır:



Şekil 2: Sıfır Güven Mimarisi örneği[16].

- **Tanımla:** NIST'nin siber güvenlik çerçevesi ilk olarak kuruluşun bütün siber güvenlik risklerinin tespit edilmesiyle başlamaktadır. Risk tanımlamalarında kuruluşun ihtiyaçları ve mevcut riskleri de gözetilmektedir. Birçok kuruluş daha bu aşamada çok ciddi sorunlar yaşamaktadır. Riskler doğru bir şekilde tanımlanmadan atılacak her güvenlik adımı çökme tehlikesiyle karşı karşıyadır.
- **Koru:** E-posta filtreleme, son kullanıcı kontrolleri ve çalışanlara siber güvenlik eğitimleri verilmesi gibi uygulamalar özellikle kuruluşun içeriden yaratacağı güvenlik açıklarının kapatılması ve savunmada kritik bir konuma sahiptir. Kuruluşun ilk olarak çalışan seviyesinde bir koruma politikası oluşturması ve bu politikayı kademe kademe artırması gerekmektedir. Bütün sistemlerin güncel tutulması da önemlidir. Siber teröristler daha akılcı yöntemler uygularken savunma kademesinde olan çalışan ve hizmet sunucularının da sistemleri korumak için yeni teknoloji ve stratejileri benimsemesi ve uygulaması gerekmektedir. Bu aşamada en büyük sorun birçok kuruluşun pazarda bulunan bütün güvenlik sistemlerini uyguladığı için güvende olacağını düşünmesidir. Bütün güvenlik mekanizmalarına sahip olmak yerine önlem alınması gerekli risklere uygun güvenlik uygulamalarına sahip olmak ve uygulamak en doğru yaklaşım olacaktır.
- **Tespit Et:** İlk iki aşama siber güvenlikte saldırı öncesi aşamaları kapsamaktadır. Bütün çalışmalara rağmen siber saldırılarla karşılaşılma olasılığı her zaman bulunmaktadır. Bu noktada saldırı kaynağı ve nedenlerinin tespiti önemlidir. Sahip olunan izleme yetenekleri çerçevesinde normal dışındaki durumlar tespit edildikten sonra dördüncü aşamaya geçilebilir.
- **Karşılık Ver:** Saldırı tespit edildikten sonra önceden oluşturulmuş müdahale yöntemleriyle saldırıya hızlı bir cevap verilmesi gerekmektedir. Saldırı önemli veri kayıplarına veya sistem kesintilerine neden olmadan engellenmeli veya bu süre en aza indirilmelidir. Bu işlemler sonrasında saldırı engellendiği zaman beşinci aşamaya geçilebilir.
- **Toparlan:** Saldırı sonrası kayıplar, hasarlı sistemler veya verilerde oluşabilecek bozulmalar incelenmeli ve mümkün olduğunca güncel yedeklerle sistem desteklenerek hizmete sunulmalıdır. Bu sırada belirlenen güvenlik açıkları da gelecekte üzerinde çalışılması gereken iyileştirme alanları olarak gündeme alınmalı, döngü olarak işletilecek sürecin birinci aşaması olan Tanımla evresine girdi olarak sunulmalıdır.

Bu aşamaların haricinde sistem sürekli olası saldırılara karşı test edilmelidir. Test sonuçları dikkatle incelendiğinde ortaya çıkan sonuçlar ileride yaşanacak gerçek saldırılarda kılavuz olabilmektedir[17].

Ayrıca veri merkezleri için oluşturulacak giriş kontrol listeleri (Access Control Lists -ACLs), ağ trafiğinde geçişlerin kontrolünü sağlarken, İnternet Protokol (IP) izleme ile güvensiz kullanıcıların engellenmesine destek olabilmektedir. Saldırı Tespit Sistemi (Intrusion Detection System -IDS) gibi araçlar da siber güvenlik aşamalarında saldırıların anlık tespiti ve gelecek saldırıların engellenmesinde önem arz etmektedir.

Siber saldırıların engellenmesinde verilerin güçlü şifreleme yöntemleri önem kazanmaktadır. Web

uygulamalarında 256-bit SSL şifreleme kullanılabilirken, veri transferlerinde 1024-bit RSA şifreleme anahtarları tercih edilmektedir. Veri bankaları ve dosya genel şifrelemesinde ise AES 256-bit şifreleme daha uygun bir yöntemdir.

Veri merkezine giriş yapılması aşamasında ise kullanıcı adı ve şifrelerde yüksek güvenlikli uygulamalar, düzenli değişiklikler ve eski şifrelerin kullanımının engellenmesi de etkili savunma stratejileridir[18].

Veri merkezlerinde depolanan ve işlenen veriler artan bir hızla toplumun ve ekonominin kritik bir parçası hâline gelmektedir. Karşılaşılan siber saldırı her ne olursa olsun veri merkezlerinin korunması işletmelerin ve ekonominin güvenliği için çok önemlidir[13].

3.4 Savunma Sektöründe Veri Merkezleri Güvenliği

Savunma sektörü de artan verilerden ciddi anlamda etkilenmektedir. Komuta kontrol merkezleri, insansız teknolojiler ve kullandıkları sensörler, C4ISR sistemleri sürekli olarak verilere ihtiyaç duymakta ve yeni veriler üretmektedir. Ticari sektörlere göre daha da kritik öneme sahip bu verilerin güvenliğinin askeri seviyede sağlanması önemlidir.

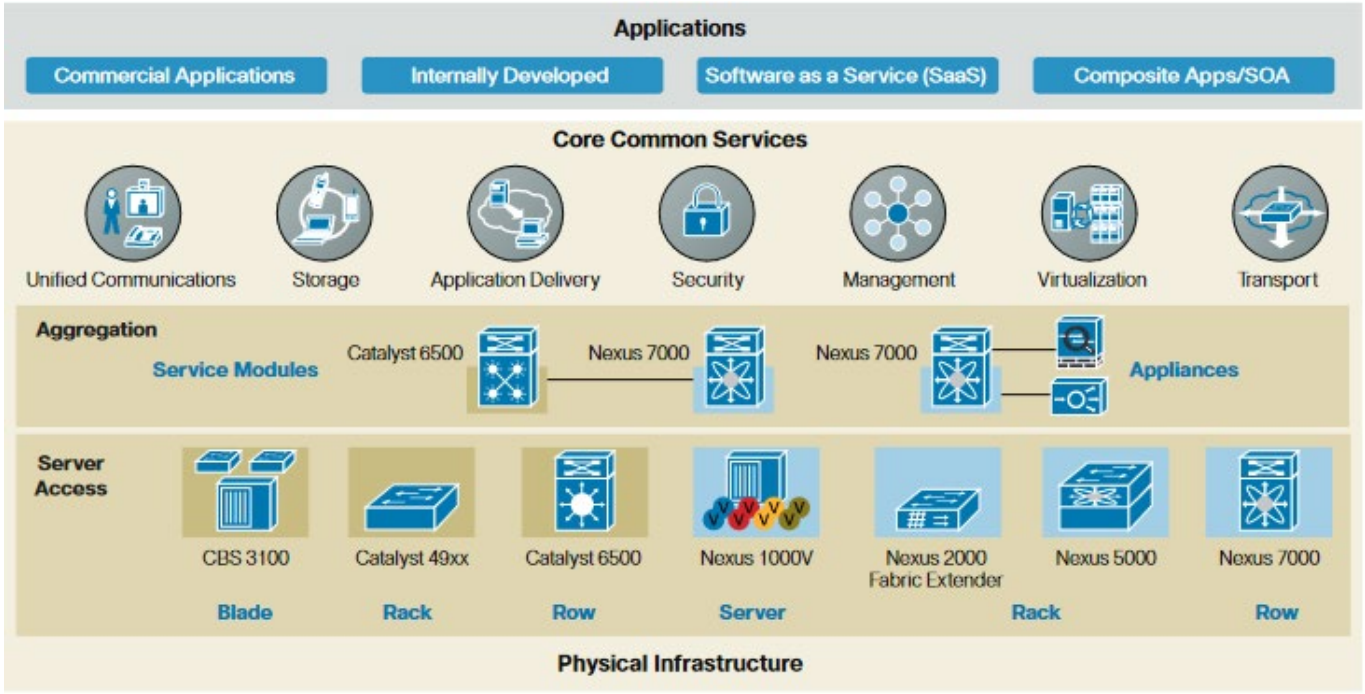
Askeri veri merkezleri öncelikle izole ve gizli tutulmalıdır. Siber saldırı, sabotaj ve terörist aktivitelerde cazip hedefler olan askeri veri merkezleri yoğun fiziki ve sanal güvenlik önlemleriyle korunmaktadır. Sürekli güncel tutulan sistemlerin ağ güvenliği, özel bağlantı çözümleri gibi uygulamaları da desteklemesi beklenmektedir[19].

4. VERİ GÜVENLİĞİNDE HUKUKSAL YAPTIRIMLAR

Veri merkezleri ve veri güvenliği konusundaki tartışmaların çoğu mantıksal kontroller ve yazılımsal süreçleri kapsamaktadır. Veri merkezlerinin güvenliğinin sağlanması ise her geçen gün daha da önem kazanmaktadır. Avrupa Birliği (AB) Genel Veri Koruma Tüzüğü (General Data Protection Regulation -GDPR) AB'de yaşayan herkesin kişisel veri güvenliği ve mahremiyetini katı bir politikayla koruma altına almıştır. GDPR Avrupa ülkeleri için tasarlanmış olmasına rağmen uluslararası birçok firma bu tüzüğe uyum sağlamaya çalışmaktadır. GDPR tüm organizasyonların, birinin kişisel bilgilerinin her bir örneğinin nerede olduğunu tam olarak bilmesini ve bu verilerin korunmasını sağlamak için "uygun teknik ve organizasyonel önlemleri uygulamasını" şart koşmaktadır[20].

GDPR'ye benzer bir yasa ABD'de de 2018 yılında çıkarılmıştır. Ancak yasa 2020'de yürürlüğe girebilmiştir. Kaliforniya Tüketici Gizliliği Yasası (California Consumer Privacy Act -CCPA) Kaliforniya bölgesinde yaşayanların verilerinin gizliliğini güçlendirirken, yapılan çalışmaların şeffaflığını artırmayı hedeflemektedir. Bu yasayla verileri kontrol eden kuruluşların verileri nasıl kullanabileceği, hangi bilgilerin paylaşıma açık olduğu ve yasa ihlalinin nasıl cezalandırılacağı belirlenmiştir.

New York Kalkan Yasası (New York Shield Act), ABD'de geçerli veri güvenliği yasalarından bir diğeridir. Siber saldırılara karşı düşünülmüş bir yasa olan New York Shield, CCPA'dan farklı olarak kişisel verilerin korunması yerine güvenlik regülasyonları üzerine yoğunlaşmaktadır.



Şekil 3: Cisco Veri Merkezi 3.0 çerçevesi (Askeri Güvenlik Seviyesinde Veri Merkezi)[19].

ANSI/TIA-942-A, Telekomünikasyon Endüstrisi Birliğinin veri merkezleri için telekom altyapısını belirleyen standardıdır. TIA/EIA-568 standardı içinde oluşan ANSI/TIA-942-A veri merkezlerinin kablolu bağlantılarının kurulumu, tasarımı ve performansını denetlemektedir. Amerikan Ulusal Standartları içinde yer alan ANSI uluslararası alanda da tercih edilmektedir.

Dünyanın farklı yerlerinde geçerli birçok veri güvenliği regülasyonu bulunmaktadır. Bu regülasyonların en başta gelen ortak yanı kişisel gizliliği korurken siber saldırıların engellenmesi üzerinedir[21].

Türkiye de 2016 yılında kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu uygulamaktadır. Kanun veri merkezlerinden çok verilerin ve kişisel bilgilerin korunmasıyla ilgili hükümleri içermektedir. Türkiye veri merkezlerinde ciddi gelişmeler kaydetmektedir. Yeni veri merkezi yatırımlarında ANSI/TIA-942-A standardı temel alınırken en az Kademe 3 (Tier 3) olması da beklenmektedir[22].

5. VERİ MERKEZLERİNİN SİBER GÜVENLİĞİNDE YENİ TRENDLER

Dünyanın her geçen gün daha dijitalleştiği düşünüldüğünde pandeminin de etkisiyle ortaya çıkan uzaktan çalışma ve artan veri trafiği yeni güvenlik trendlerinin oluşmasına imkân vermiştir.

Genişletilmiş Tespit ve Tepki (Extendend Detection and Response -XDR) uygulaması gelişen siber güvenlik trendlerinden biridir. XDR'nin SIEM, Güvenlik Düzenlemesi, Otomasyonu ve Yanıtı (Security Orchestration, Automation and Response – SOAR), Ağ Trafiği Analizi (Network Traffic Analysis -NTA) ve Son Kullanıcı Tespit ve Cevap (Endpoint Detection and Response -EDR) gibi uygulamalarla birlikte kullanımı veri merkezlerinin güvenliğini en iyi şekilde sağlamaktadır. XDR uygulamasının odak noktası tespit hassasiyetinin artırılması ve tehdit istihbaratının sağladığı bilgilerle karşılaştırılarak en geçerli önlemlerin alınmasının sağlanmasıdır.

Güvenli Erişim Hizmet Sınırı (Secure Access Service Edge -SASE) hassas verileri veya kötücül yazılımları tespit ederek riskler karşısında hızla şifreleme ve sistemi sürekli izleme imkânı sunmaktadır. Geniş alan ağ yapısıyla uyumlu çalışan SASE işyerlerinin veri merkezlerine dinamik güvenli erişim imkânı sunmaktadır.

Pandeminin yarattığı etkiler Sıfır Güven Mimarisi'nin kabullenilmesini de hızlandırmıştır. Her bağlantının sorgulandığı ve takip edildiği Sıfır Güven Mimarisi'nde dört temel prensip hâkimdir.

Bunların ilki kullanıcı kim olursa olsun güvenilmemesidir. İkinci prensip VPN ve Firewall'lar tek başlarına yeterli değildir ve sadece sınır güvenliğinde etkindir. Üçüncü prensip kimlik ve cihaz onaylarının ağ boyunca devam etmesi gerekliliğidir. Son prensip ise mikro segmentasyon ile saldırılara karşı katmanlı güvenlik sisteminin uygulanmasıdır[23].

Güvenlik hizmetinin ayrı bir kuruluştan alınması da yeni bir opsiyon olarak öne çıkmaktadır. Güvenlik Operasyonları Merkezleri (Security Operations Centres -SOC) kuruluşların sistemlerini ve veri merkezi aktivitelerini düzenli bir şekilde izleyerek analiz edip güvenlik durumunu ortaya çıkarabilmektedir. Üçüncü bir gözle bakıldığından kaçırılabilecek güvenlik açıkları daha net bir şekilde ortaya çıkabilmekte ve veri merkezinin güvenliği daha verimli sağlanabilmektedir[24].

Veri merkezlerinin en kritik altyapılarından biri olan güç sistemleri ne yazık ki siber güvenlik denetimlerinin en çok atlandığı alanlardan biridir. Güç sistemlerinin yedek güç sistemleriyle desteklenmesinin yeterli olacağının düşünülmesi en büyük yanılgılardan birini ortaya çıkarmaktadır. Güç sistemleri de artık siber saldırıların hedefi hâline gelmiştir. Güç sistemlerini devre dışı bırakan siber saldırılar yedek sistemleri de etkisizleştirerek veri merkezlerine ve bu merkezleri kullanan kişi ve kuruluşlara ciddi zararlar verebilmektedir. Her ne kadar verilere uzaktan erişim sıkı bir şekilde kontrol edilse de benzer şekilde uzaktan erişim imkânı olan güç sistemleri göz ardı edilmektedir. Veri merkezlerinin siber saldırılara karşı savunulması, risklerin tespiti ve güvenlik önlemleri

bütün altyapı dahil her sistemin ortak bir çatı altında değerlendirilmesiyle mümkündür. İşte bu yüzden veri merkezi güvenliği konseptinin sadece veri ve bilgi sistemleri çerçevesinde değil, veri merkezinin diğer bileşenleri olan otomasyon sistemleri ve fiziksel güvenlik unsurlarının da işin içine katılarak hazırlanması gereklidir[25].

5.1 Veri Merkezlerinin Siber Güvenliğinde Türkiye'deki Çalışmalar

Türkiye, veri merkezlerinin güvenliği için birçok girişimin yapıldığı ülkelerden biridir. Veri merkezi güvenliği alanında hizmet veren çeşitli firmalar veri merkezi kurulumu ve devamında siber güvenlik savunma hizmetleri sunmaktadır.

Türkiye'nin en önemli savunma sanayii şirketlerinden biri olan STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş. (STM) de siber güvenlik alanında dikkat çeken çalışmalara imza atmıştır. Anahtar teslim siber güvenlik kurulumu sunabilen STM ayrıca eğitim, danışmanlık ve Siber Güvenlik Olgunluk Seviyesi Analizi gibi hizmetler de sunmaktadır.

CyDecSys gibi bütünleşik siber güvenlik durum tespit, analiz ve karar destek sistemi yazılımları bilgisayar ağları ve veri merkezlerinin siber güvenlik resmini sunarak alınacak önlemler ve güvenlik açıkları konusunda bilgi sunmaktadır. Otomatik ağ topolojisi özelliği ile veri merkezine bağlı tüm bileşenlerin topolojisini çıkaran ve alt ağ ilişkilerini gösteren sistem açık protokol tabanlı yöntemler kullanmaktadır. Saldırı ağaçları ile çok adımlı saldırının analizlerini gerçekleştirmek, farklı bakış açıları ile sistemin risklerinin tespiti, ağ trafiğini engellemeden tarama yapmak gibi kullanışlı özellikleri olan CyDecSys siber saldırılara karşı avantaj sunmaktadır[26].

STM'nin bir diğer siber güvenlik hizmeti olan Bugshield kırmızı, mavi ve mor takım hizmetlerini sürekli ve kesintisiz olarak sunabilmektedir. Kırmızı takım teknoloji, insan ve fiziki alanda kurumun gerçek risklerini ve zayıflıklarını belirleme amacı güden, birden fazla saldırı metodunu barındıran, kapsama ve metodolojilere bağlı kalmadan bilişim sistemlerinin ve/veya gizli bilgilerinin ele geçirilmesi işlerini üstlenen takımdır. Mavi takım, sahip olunan altyapı ve sistemlere yönelik gerçekleşen gerçek veya simüle saldırılarda erken tespit, olay müdahale, tehdit analizi, adli analiz ve yeniden yapılandırma işlerini üstlenen takımdır. Mor takım ise, kırmızı ve mavi takım yeteneklerini içinde barındıran, iki takım arasındaki iletişimi sürekli kılan ve kurumun en yüksek faydayı sağlaması için tüm verileri birleştirerek uygulanabilir aksiyon adımları çıkaran takımdır[27].

STM'nin önemli siber güvenlik çalışması olan Siber Füzyon Merkezi ise geleneksel siber güvenlik işlevselliklerini, yeni yeteneklerle birleştirerek tek ve entegre bir siber güvenlik yaklaşımı sergilemektedir. Kritik teknoloji ve bilgi varlıklarını koruyan proaktif ve önleyici faaliyetleri içeren STM Siber Füzyon Merkezi (SFM); Siber Tehdit İstihbarat Merkezi, Siber Operasyon Merkezi ve Zararlı Yazılım Analiz Laboratuvarı (Z-Lab) olmak üzere bütünleşik üç ana merkezden oluşmaktadır[28].

6. SONUÇ

İş dünyasının ve günlük yaşamın yarattığı ihtiyaçların önemli oranda dijital ortamlarda karşılık bulduğu düşünüldüğünde veri güvenliğinin önemi her geçen gün daha da artmaktadır.

Bulut, siber güvenlik, nesnelerin interneti, büyük veri, iş çözümleri, sistem entegrasyonu ve yapay zekâ çözümleri de dahil olmak üzere birçok teknolojinin uygulandığı veri merkezleri şirketler ve bireyler için çok hassas verileri barındırdığından bu verilerin mutlaka korunması gerekmektedir. Askeri, ticari veya bireysel her türlü veri siber saldırıların hedefi olabileceği gibi bu verilerin kaybı durumunda maddi ve manevi zararlar doğma potansiyeli oldukça yüksektir. Veri merkezleri henüz inşa aşamasındayken alınan fiziksel güvenlik önlemlerinden siber saldırılara karşı oluşturulacak sanal güvenlik önlemlerine kadar her aşama dikkatle kurgulanmalıdır. Veri merkezlerinin siber güvenliği doğru bir şekilde sağlandığında önemli avantajlar ortaya çıkmaktadır. Güvenlik en üst seviyeye geldiğinde hizmet verilen kişi veya kurumlar tam anlamıyla korunabilmektedir. Doğru veri akışıyla üretim gücü gelişmekte ve kullanıcıların bilgilerini güvenle saklamasına imkân verilmektedir. Savunmadan sağlık ve ticarete kadar hemen her sektörde hassas ve finansal bilgiler içeren verilerin gelişen teknoloji dünyasında hızla artması veri merkezlerinin de yaygınlaşacağı anlamına gelmektedir. Doğru kurgulanan veri merkezleri geleceğin bilgi teknolojilerinin daha da gelişmesine destek olma potansiyelindedir[29].

KAYNAKÇA

[1] *Gartner*, "Data Center", https://www.gartner.com/en/information-technology/glossary/data-center. (Erişim Tarihi:18.06.2021)

[2] *Cisco*, "What Is a Data Center", https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html. (Erişim Tarihi:18.06.2021)

[3] *Wikipedia*, "Veri merkezi", https://tr.wikipedia.org/wiki/Veri_merkezi. (Erişim Tarihi:18.06.2021)

[4] *Cisco*, "Types of data centers", https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html#~types-of-data-centers. (Erişim Tarihi:18.06.2021)

[5] *Schroders*, "What are data centres and why are they so important?", https://www.schroders.com/en/insights/economics/what-are-data-centres-and-why-are-they-so-important/. (Erişim Tarihi:18.06.2021)

[6] Dobran, Bojana; (2018), "Data Center Tier Classification Levels Explained (Tier 1, 2, 3, 4)", *phoenixNAP*, (2 Mayıs 2018), https://phoenixnap.com/blog/data-center-tiers-classification. (Erişim Tarihi:18.06.2021)

[7] Garcia, Eduardo; (2019), "Personal Cybersecurity: What Every Internet User Needs to Know", *What Mobil*, (21 Ağustos 2019), https://www.whatmobile.net/Features/article/personal-cybersecurity-what-every-internet-user-needs-to-know. (Erişim Tarihi:18.06.2021)

[8] *Forcepoint*, "What is Data Center Security?", https://www.forcepoint.com/cyber-edu/data-center-security#:~:text=Data%20center%20security%20refers%20to,store%20large%20amounts%20of%20data.. (Erişim Tarihi:18.06.2021)

[9] Sebastiao, Jorge; (2008), "Integrating Physical And Logical Security", *Slideshare*, (17 Haziran 2008), https://www.slideshare.net/jorges/integrating-physical-and-logical-security. (Erişim Tarihi:18.06.2021)

[10] *Sifytechnologies*, "5 focus areas for Data Center security", https://www.sifytechnologies.com/blog/5-focus-areas-for-data-center-security/. (Erişim Tarihi:18.06.2021)

[11] SonDakika.com, (2021), "LpsChain'e BİRLEŞİK KRALLIK DIŞ TİCARET BAKANLIĞI'NDAN DESTEK", (11 Haziran 2021), https://www.sondakika.com/haber/haber-lpschain-e-birlesik-krallik-dis-ticaret-bakanligi-14194180/. (Erişim Tarihi:18.06.2021)

[12] Crane, Casey; (2020), "What Is Data Center Security? 6 Ways to Ensure Your Interests Are Protected", *Security Boulevard*, (24 Haziran 2020), https://securityboulevard.com/2020/06/what-is-data-center-security-6-ways-to-ensure-your-interests-are-protected/. (Erişim Tarihi:18.06.2021)

[13] Simon, Gerd; (2018), "UNDERSTANDING AND MITIGATING RISKS TO DATA CENTER OPERATION", *dotmagazine*, (Mayıs 2018), https://www.dotmagazine.online/economic-engine-digital-infrastructure/mitigating-risks-to-data-center-operation. (Erişim Tarihi:18.06.2021)

[14] *thesslstore*, (2021), "What Is Data Center Security? 6 Ways to Ensure Your Interests Are Protected", (29 Nisan 2021), https://www.thesslstore.com/blog/what-is-data-center-security-6-ways-to-ensure-your-interests-are-protected/. (Erişim Tarihi:18.06.2021)

[15] *Analyticsinsight*, (2020), "DATA CENTER SECURITY PRACTICES FROM CYBERSECURITY EXPERTS: HOW TO PROTECT YOUR INTERESTS?", (7 Ağustos 2020), https://www.analyticsinsight.net/data-center-security-practices-from-cybersecurity-experts-how-to-protect-your-interests/. (Erişim Tarihi:18.06.2021)

[16] *wipro*, (2020), "Why Zero Trust User Access is vital for secure remote working?", (Eylül 2020), https://www.wipro.com/cybersecurity/why-zero-trust-user-access-is-vital-for-secure-remote-working/. (Erişim Tarihi:18.06.2021)

[17] Korolov, Maria; (2019), "The Must-Haves for Your Data Center Cybersecurity Checklist", (12 Mart 2019), *DataCenter Knowledge*, https://www.datacenterknowledge.com/security/must-haves-your-data-center-cybersecurity-checklist. (Erişim Tarihi:18.06.2021)

[18] *Wikipedia*, "Data center security", https://en.wikipedia.org/wiki/Data_center_security. (Erişim Tarihi:18.06.2021)

[19] *Cisco*, "Data center regulations for the US", https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/solution_overview_c22-504982.pdf. (Erişim Tarihi:18.06.2021)

[20] Wang, Vicky; "Veri Merkezinde Fiziksel Güvenliğin Büyüyen Önemi", *Rahi Systems*, https://tr.rahisystems.com/flexit/the-growing-importance-of-physical-security-in-the-data-center/. (Erişim Tarihi:18.06.2021)

[21] *Site24x7* "Data center regulations for the US", https://www.site24x7.com/learn/compliance/data-center-security-and-privacy-for-usa.html. (Erişim Tarihi:18.06.2021)

[22] *Bilgi Teknolojileri ve İletişim Kurumu*, (2018), "ÜLKEMİZİN VERİ MERKEZİ ÜSSÜ OLMASI İÇİN VAR GÜCÜMÜZLE ÇALIŞIYORUZ", (11 Ocak 2018), https://www.btk.gov.tr/haberler/ulkemizin-veri-merkezi-ussu-olmasi-icin-var-gucumuzle-calisiyoruz. (Erişim Tarihi:18.06.2021)

[23] Novinson, Michael; (2021), "10 Emerging Cybersecurity Trends To Watch In 2021", *CRN*, (17 Mayıs 2021), https://www.crn.com/news/security/10-emerging-cybersecurity-trends-to-watch-in-2021. (Erişim Tarihi:18.06.2021)

[24] Abraham, Priya; (2021), "Top 10 cybersecurity trends in 2021", *Dailyhost*, (17 Mart 2021), https://www.dailyhostnews.com/top-10-cybersecurity-trends-in-2021. (Erişim Tarihi:18.06.2021)

[25] Goud, Naveen; "Power systems in data centers are vulnerable to Cyber Attacks", *Cybersecurity INSIDERS*, https://www.cybersecurity-insiders.com/power-systems-in-data-centers-are-vulnerable-to-cyber-attacks/. (Erişim Tarihi:18.06.2021)

[26] *STM*, "CYDECSYS®" https://www.stm.com.tr/tr/cozumlerimiz/siber-guvenlik-ve-bilisim/cydecsys. (Erişim Tarihi:18.06.2021)

[27] *STM Bugshield*, "BUGSHIELD Nasıl Çalışır?", https://www.stm-bugshield.com/tr/nasil-calisir. (Erişim Tarihi:18.06.2021)

[28] *STM,* "Siber Füzyon Merkezi", https://www.stm.com.tr/tr/cozumlerimiz/siber-guvenlik-ve-bilisim/siber-fuzyon-merkezi. (Erişim Tarihi:18.06.2021)

[29] *RSI Security*, (2020), "TOP DATA CENTER SECURITY THREATS OF 2020", (13 Mayıs 2020), https://blog.rsisecurity.com/top-data-center-security-threats-of-2020/. (Erişim Tarihi:18.06.2021)

thinktech
STM Teknolojik Düşünce Merkezi
http://thinktech.stm.com.tr