T.C.
BEYKENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

BİLGİSAYAR AĞ GÜVENLİĞİNİN ANALİZİ VE ARAŞTIRMASI

Yüksek Lisans Tezi

Tezi Hazırlayan:

Murat ÜSTÜNKAYA

İstanbul, 2022

T.C.
BEYKENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

BİLGİSAYAR AĞ GÜVENLİĞİNİN ANALİZİ VE ARAŞTIRMASI

Yüksek Lisans Tezi

Tezi Hazırlayan:

Murat ÜSTÜNKAYA

Öğrenci No:

2020003038

Orcid : 0000-0002-8381-9390

Danışman:

Dr. Öğr. Üyesi Zeynep ALTAN

İstanbul, 2022

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum “Bilgisayar Ağ Güvenliğinin Analizi Ve Araştırması” başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını, patent ve telif haklarını ihlal edici bir davranışımın olmadığını belirtir ve bunu onurumla doğrularım. 20/10/2022

Murat ÜSTÜNKAYA

T.C.
BEYKENT ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜ
TEZLİ YÜKSEK LİSANS SINAV TUTANAĞI

20/10/2022

Enstitümüz ***Bilgisayar Mühendisliği*** Anabilim Dalı ***Bilgisayar Mühendisliği*** Programı yüksek lisans öğrencilerinden ***2020003038*** numaralı ***Murat ÜSTÜNKAYA***'nın *"Beykent Üniversitesi Lisansüstü Eğitim – Öğretim Yönetmeliği"*nin ilgili maddesine göre hazırlayarak, Enstitümüze teslim ettiği ***"Bilgisayar Ağ Güvenliğinin Analizi Ve Araştırması"*** konulu tezini, Yönetim Kurulumuzun 31/05/2022 tarih ve 2022/22 sayılı toplantısında seçilen ve On-Line toplanan biz jüri üyeleri huzurunda, Beykent Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 29. maddesinin 3. fıkrası gereğince 45 dakika süre ile Zoom programı aracılığıyla on-line olarak aday tarafından savunulmuş ve sonuçta adayın tezi hakkında ***"OYBİRLİĞİ"*** ile ***"KABUL"*** kararı verilmiştir.

İşbu tutanak, 2 nüsha olarak hazırlanmış ve Enstitü Müdürlüğü'ne sunulmak üzere tarafımızdan düzenlenmiştir.

DANIŞMAN
Dr. Öğr. Üyesi Ze*** AL***
(Beykent Üniversitesi)

ÜYE
Dr. Öğr. Üyesi At*** YI***
(Beykent Üniversitesi)

ÜYE
Dr. Öğr. Üyesi Se*** KU***
(Altınbaş Üniversitesi)

Adı ve Soyadı : Murat ÜSTÜNKAYA

Danışmanı : Dr. Öğr. Üyesi Zeynep ALTAN

Türü ve Tarihi : Yüksek Lisans, 2022

Alanı : Bilgisayar Mühendisliği

Anahtar Kelimeler : Ağ Güvenliği, Analiz, Bilgi, Bilgisayar, Makine Öğrenimi, Veri

ÖZ

BİLGİSAYAR AĞ GÜVENLİĞİNİN ANALİZİ VE ARAŞTIRMASI

Araştırmanın amacı, Türkiye'de özel sektörde ağ güvenliği alanında yapılan çalışmalara dair yetkili kesimlerin ve bireylerin konu hakkındaki düşüncelerini, uygulamalarını öğrenebilmek ve katılımcıların şirketlerinde uygulanan sistemlerde hangi yöntemlerin benimsendiği hususunda fikir edinebilmektir. Bu şekilde kurumların, süreçler ile olan etkileşimlerinde uygulamaları kadar karşılaşmış oldukları tehditlerin neler olduğu konusunda tespitlerde bulunmaya çalışmak araştırmanın amaçları arasındadır. Çalışmanın üçüncü bölümünde Türkiye'de özel sektöre hizmet veren ve farklı alanlarda faaliyetleri bulunan şirketlerin Bilgi Teknolojileri departmanlarında görevli, sorumlu ve müdür olan bireyler ile kurumlarındaki ağ güvenliği uygulamaları konusundaki görüşlerinin neler olduğunu belirlemek amacıyla, "Bilgisayar Ağ Güvenliği Analizi" isimli form kullanılarak bir röportaj gerçekleştirilmiştir. Ağ güvenliği, sürdürülebilir bir yapının varlığına atıfta bulunan bir sistemi ifade etmektedir. Temel olarak kurulan bir yapının, uzun süre boyunca devam edebilmesi ve kesin güvenlik sağlaması adına önem arz eden temel husus, sistemin neredeyse her gün güncel olarak takip edilmesidir. Çalışmanın son bölümünde ise, çalışanlardan alınan bilgiler makine öğrenmesi metotlarına dahil edilmiştir ve güvenlik duvarı ürünü için en başarılı tahmini yapan metot belirlenmiştir. Bu işlem yapıldıktan sonra; kullanılan girdi, manuel olarak değiştirilerek ve en başarılı metodun, toplanılan verilerden öğrendiklerinden faydalanması sağlanarak bir güvenlik duvarı önerisi çıktısı alınabilmektedir.

Name and Surname : Murat ÜSTÜNKAYA

Supervisor : Dr. Lecturer Zeynep ALTAN

Degree and Date : Master, 2022

Major : Computer Engineering

Key Words : Analysis, Computer, Data, Information, Machine Learning, Network Security

ABSTRACT

ANALYSIS AND RESEARCH OF COMPUTER NETWORK SECURITY

The aim of the research is to learn the thoughts and practices of the authorized sections and individuals regarding the studies carried out in the field of network security in the private sector in Turkey, and to get an idea about which methods are adopted in the systems applied in the companies of the participants. In this way, it is among the aims of the research to try to determine the threats faced by the institutions as well as their practices in their interactions with the processes. In the third part of the study, a interview was conducted using the form named "Computer Network Security Analysis" in order to determine the opinions of individuals who are responsible, responsible and manager in the Information Technology departments of companies serving the private sector and operating in different fields, and their views on network security practices in their institutions. Network security refers to a system that refers to the existence of a sustainable structure. In order for a basically established structure to continue for a long time and to provide absolute security, the main issue that is important is that the system is followed up-to-date almost every day. In the last part of the study, the information received from the employees was included in the machine learning methods and the method that made the most successful prediction for the firewall product was determined. After this process is done; a firewall recommendation can be output by manually changing the input used and allowing the most successful method to benefit from what it has learned from the collected data.

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

ARP : Address Resolution Protocol (Adres Çözümleme Protokolü)

BT : Bilgi Teknolojileri

DHCP : Dynamic Host Configuration Protocol (Dinamik Ana Bilgisayar Yapılandırma Protokolü)

DLP : Data Loss/Leak Prevention (Veri Kaybı/Sızıntısı Önleme)

DOS : Denial Of Service (Hizmet Reddi)

GB : Gigabyte

KVKK : Kişisel Verileri Koruma Kanunu

LAN : Local Area Network (Yerel Ağ Bağlantısı)

MAC : Media Access Control Address (Medya Erişim Kontrol Adresi)

MEGEP : Mesleki Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projesi

ML : Machine Learning (Makine Öğrenmesi)

MLP : Multi Layer Perfectron (Çok Katmanlı Algılayıcı)

OSI : Open Systems Interconnection (Açık Sistem Arayüzü)

RF : Random Forests (Rastgele Ormanlar)

SIEM : Security Information and Event Management (Güvenlik Bilgileri ve Olay Yönetimi)

SQL : Structured Query Language (Sorgulama Dili)

SSL : Secure Sockets Layer (Güvenli Giriş Katmanı)

SVR : Support Vector Machines (Destek Vektör Makineleri)

VPN : Virtual Private Network (Sanal Paylaşımlı Ağ)

Vd. : Ve diğerleri

WAF : Web Application Firewall (Web Uygulaması Güvenlik Duvarı)

WAN : Wide Area Network (Geniş Alan Ağı)

SÖZLÜK

Ağ: İnternet tabanlı olan iletişim ve veri paylaşımı amacıyla oluşturulan, bilgisayar ve diğer muadil iletişim araçlarının işleyişine tabi olan sistem.

Ağ Güvenliği: Ağ üzerinde gerçekleşen iletişim ve veri paylaşımı süreçlerinde kullanıcıların ve verilerin zarar görmemesi adına alınan önlemler.

Antivirüs: Kötü amaçlı yazılımları algılamak, önlemek, taramak, tespit etmek ve kaldırmak için olarak tasarlanmış yazılım.

Makine Öğrenmesi: Büyük miktarda verinin analizini yapmak ve istatistiğini oluşturmak için, geleceğe yönelik tahminleme yapabilmek için kullanılan yapay zekanın bir alt dalı.

Siber Saldırı: Profesyonel niteliğe sahip bilgisayar korsanlarının, büyük ölçekli kurum ve kuruluşların ağ trafiklerini hedef almak sureti ile web siteleri başta olmak üzere sunuculara, bilgi depolama sistemlerine ve ağın bilgisayarlarına yapmış oldukları saldırılar.

Virüs: Kendini kopyalayabilen ve genellikle sistem bozulması veya veri imhası gibi zararlı sonuçları olan bir kod parçası.

WEB: Bir internet tarayıcısı tarafından erişilebilen sayfalardan oluşan bir alt kümesi olan World Wide Web'in ortak adıdır. Bir çok kişi Web'in internet ile aynı olduğunu varsaymakta ve bu terimleri birbirinin yerine kullanmaktadır.

WIRELESS (Wi-Fi): Bilgisayarları, tabletleri, akıllı telefonları ve diğer cihazları internete bağlamak için kullanılan kablosuz bir teknolojidir. Wi-Fi olarakta bilinmektedir.

GİRİŞ

Bilgisayarların kullanımının dünya genelinde hızlı bir şekilde yaygınlaşması neticesinde bilgisayar kullanımına olan bağımlılık gözle görülür bir şekilde artmıştır. Fakat bilgisayarların kullanımı açısından devrim yaratan unsur bilgisayarlarda yararlanılan ağ üzerinden iletişim şeklidir. Özellikle de internet kullanımının yaygınlaşması ile birlikte ağ üzerinden iletişim çok daha fazla önem kazanırken, kullanıcıların ağ odaklı olarak hareket etme konusundaki eğilimleri ve çabaları da özellikle kurumsal kullanıcılar ekseninde artmaya başlamıştır. Ağ, iletişimin basit düzeyden gelişmiş bir düzeye geçişini sağlarken, ağlar arasındaki iletişim unsurlarının sayısı ve niteliğinde de artış gözlemlenmiştir.

Ağ kullanımının kurumsal kullanıcıların sayısının artışı ile birlikte yoğunlaşması, sunduğu avantajların ötesinde ağ kullanıcıları için tehditler de yaratmaya başlamıştır. Ağlar üzerinde kullanıcıların sahip olduğu veri ve bilgilerin sayısı ve değeri arttıkça bu ağlar üzerinde oluşan tehditlerin derecesi de artmaya başlamıştır. Gerek belirli bir finansal gelir elde etmek, gerekse de bir bireye ya da kuruma zarar vermek adına ortaya çıkan tehditler ve yaşanan ağ temelli saldırılar, ağların sağlıklı bir şekilde kullanımının önünde engel teşkil etmiştir. Özellikle de kurumsal yapıların ağlar üzerinden yaşamış oldukları saldırılar, sistemlerinin büyük ölçüde zarar görmesine sebebiyet verirken mali anlamda da büyük kayıpların yaşanması söz konusu olmuştur. Kurumlar ve bireyler ağ üzerinden kendilerine yönlendirilen saldırılarda ciddi ölçekli ve onarılması zor veri kayıpları da yaşamışlardır. Bu nedenle, ağ temelli saldırılar bireysel ve kurumsal anlamda korunmayı zorunlu hale getirmektedir.

Özellikle iş yaşamında verilerin giderek artan önemi göz önünde bulundurulduğunda, kurumların önemli bütçeler ayırmak suretiyle sahip oldukları ve iletişim için kullandıkları ağların güvenliğini korumak adına, ciddi ölçekli bütçeler ayırmaları artık bir zorunluluk haline gelmiştir. Veriyi sadece kendisi için değil, aynı zamanda paydaşları içinde toplayan, işleyen, depolayan ve paylaşan kurumlar için ağ kullanımının değeri herhangi bir maddi ölçütle hesaplanmamaktadır.

Ağ güvenliği, sadece ciddi ölçekte bir bütçe ayrılmasını değil, bunun yanı sıra nitelikli yazılım desteği ve nitelikli çalışan katılımını önemli ve zorunlu kılmaktadır. Ağ güvenliği açısından kullanılan yazılım ve yararlanılan insan kapasitesi, güvenliğin en üst seviyede olması ve sürdürülebilir bir şekilde kullanılması adına sistemin en önemli hususu olmaktadır. Kamu ya da özel sektör fark etmeksizin tüm yapılar ağ güvenliği konusunda süreci çok boyutlu olarak ele almak ve bunun neticesinde de ortaya çıkan tabloya göre sürdürülebilir bir şekilde kendilerini ağ güvenliği konusundaki gelişmelere uyumlu hale getirmek durumundadırlar. Bu araştırmada ağ güvenliği konusunda, farklı sektörlerde bulunan şirketlerin farklı güvenlik algılamalarına dayalı olarak ağ güvenliği konusunda takip ettikleri yol haritası, uygulamaları, yaklaşımları, beklentileri ve karşılaştıkları sorunlar ele alınmaktadır.

Araştırmanın amacı, Türkiye'de özel sektörde ağ güvenliği alanında yapılan çalışmalara dair yetkili kesimlerin ve bireylerin konu hakkındaki düşüncelerini, uygulamalarını öğrenebilmek ve katılımcıların şirketlerinde uygulanan sistemlerde hangi yöntemlerin benimsendiği hususunda fikir edinebilmektir. Bu şekilde kurumların, süreçler ile olan etkileşimlerinde uygulamaları kadar karşılaşmış oldukları tehditlerin neler olduğu konusunda tespitlerde bulunmaya çalışmak araştırmanın amaçları arasındadır.

Araştırmanın birinci bölümünde ağ güvenliğinin uygulama açısından genel çerçevesine dair hususlara yer verilmektedir. Bu bölümde genel olarak kavramsal olarak ağ güvenliği, ağ güvenliğinin genel ve kurumsal anlamda önemi ve ağ güvenliği prensiplerine odaklanan başlıklar ön plana çıkmaktadır. İkinci bölümde, ağ güvenliği konusunda tehdit oluşturan unsurlar yine genel çerçevesi dahilinde ele alınmaktadır. Bu bölümde ağ güvenliği açısından korunma ve bilinç noktasında ön plana çıkan hususlara da yer verilmektedir. Çalışmanın üçüncü bölümünde Türkiye'de özel sektöre hizmet veren ve farklı alanlarda faaliyetleri bulunan şirketlerin Bilgi Teknolojileri (BT) departmanlarında görevli, sorumlu ve müdür olan bireyler ile kurumlarındaki ağ güvenliği uygulamaları konusundaki görüşlerinin neler olduğunu belirlemek amacıyla, "Bilgisayar Ağ Güvenliği Analizi" isimli form kullanılarak bir röportaj gerçekleştirilmiştir.

Çalışmanın son bölümünde, çalışmada kullanılan 11 adet makine öğrenmesi metodu tanıtılmış, detaylı anlatılmış ve tahminlerinin grafiksel gösterimleri yapılmıştır. Çalışmada, en yüksek doğruluk oranına ulaşmak için toplanılan veriler Python'da Synthetic Data Vault (SDV) kütüphanesi kullanılarak sentetik olarak çoğaltılmıştır. Bu verilerin %20'si test verisi olarak, %80'i öğrenme verisi olarak ayrılarak farklı makine öğrenmesi yöntemleri ile tahminler gerçekleştirilmiştir. Tahminlemeler sonucu elde edilen doğruluk oranları kıyaslanmış ve doğruluk oranlarına göre metotların istatiksel analizi yapılmıştır. Çalışmada kullanılan makine öğrenimi metotlarından hangisinin daha iyi ve verimli olduğu tespit edilmiş ve bu metodun, toplanılan verilerden öğrendiklerinden faydalanması sağlanarak bir güvenlik duvarı önerisi çıktısı vermesi sağlanmıştır.

BİRİNCİ BÖLÜM
AĞ GÜVENLİĞİ

1.1. Ağ Güvenliği Kavramı

Teknolojinin ve uzak iletişim ve etkileşimin giderek yaygınlaştığı mevcut süreçte, bireysel ve kurumsal olarak kullanılan internet vb. temelli ağlar, insan yaşamının kolaylaştırılması adına önemli fırsatlar sunmaktadır. Öyle ki bireyden topluma ve toplumdan kuruma uzanan silsile içerisinde söz konusu ağlar, hemen her faaliyetin içerisinde yer almaktadır. Bu yoğun kullanıcı grubu ve yoğun kullanım, ağ kullanımı ile birlikte ağ güvenliği sorunlarını da beraberinde getirmektedir. Bilgisayarlar başta olmak üzere, farklı ağlar üzerinden iletişim kurmaya yarayan tüm teknolojik araçların karşılaştığı ya da karşılaşması muhtemel tehditlerin hemen hepsi ağ güvenliği kapsamında değerlendirilmektedir. Ağ üzerindeki açıklar ağ güvenliği ana başlığı altında ele alınmaktadır. Web sitesi açıkları, Sıfır gün saldırıları, Denial of Service (DOS) saldırıları, ağ güvenliğini tanımlamak adına önemli güvenlik sorunları olarak görülmektedir (Arık, 2017, 40-42). Ağ güvenliği güvenlik için tehdit oluşturan unsurlar ile birlikte güvenliği temin eden unsurları bir arada içermektedir. Bu nedenle de ağ güvenliği kavramı, önemi ve olumlu-olumsuz yanları ile birlikte değerlendirilen bir kavramdır.

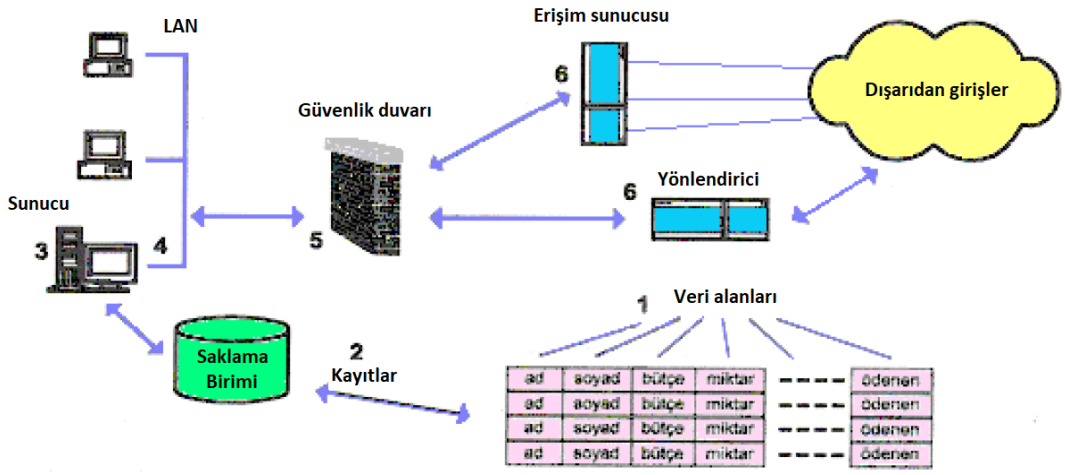
Mevcut süreçte özellikle bilgisayarlar aracılığı ile edinilmek istenen hizmetlerin sayısı ve niteliği hakkındaki beklentiler artış göstermektedir. Bu beklentiler arasında en önemli olanı, bilgisayarlar arasındaki iletişim ve etkileşimin yoğunlaştırılmasıdır. Bu nedenle özellikle kurumsal düzeyde bir ağ yapısı ya da ağlar oluşturulmaya çalışılmaktadır. İnternet aracılığıyla kurulan bu ağlar ağın üye sayısı arttıkça ciddi ölçekli güvenlik sorunlarıyla karşılaşabilmektedir. Bu nedenle ağ güvenliği kurumsal açıdan ele alındığında, sistemin parçası olan ve sistem için veri ürettiği kadar sistem için veri de saklayan tüm unsurların karşılaştığı ya da karşılaşabileceği tehditlerin teknik olarak engellenmesi çabasıdır (MEGEP, 2011, 38). Kurumlar, ağları çok daha yoğun ve etkin bir şekilde kullanmaları nedeni ile çok daha fazla tehdit altında olmaktadırlar. Özellikle de veri odaklı yoğun bir çalışma temposu

ve iş yükü olan kurumlar açısından ağ güvenliği çok daha fazla kritik bir öneme sahiptir.

Ağ güvenliği kavramı ön plana çıkarıldığı süre zarfında, dikkati çeken önemli sorunlardan biri, açık ağ kanalları üzerinde bulunan bilginin gizliliği ve bütünlüğü olmaktadır. Bilgi gizliliği, ağ güvenliğindeki temel unsurlardan biri olarak verilerin yaratıcısı/yaratıcıları ve kullanıcısı/kullanıcıları dışında başka kimse tarafından görülememesi ve kullanılamaması anlamına gelmektedir. Bilgi bütünlüğü ise verinin herhangi bir değişikliğe uğramadan alıcıya iletilmesi anlamını taşımaktadır. Ağ güvenliği bu süreçlerde kritik bir unsur olmakla birlikte bir ispat mekanizması da sağlamaktadır. Buna göre ağ güvenliği veri transferi, paylaşımı, iletimi ve depolanması süreçlerinde, verinin herhangi bir manipülasyon ya da değişime uğraması neticesinde, asıl halinin korunmasını ve herhangi bir soruna sebebiyet vermemesini sağlamaktadır (Al, 2002, 40). Ağ güvenliği açısından ilk akla gelen unsur verilerin çalınmasına yönelik saldırılar olarak görülse de aslında, ağ içerisinde bulunan verilerin içeriklerinin değiştirilmesine yönelik olarak gerçekleştirilen saldırılar da veri hırsızlığı kadar büyük tehlike arz etmektedir.

Ağ güvenliği geçen zaman içerisinde artık tüm kullanıcılar için önem arz eden bir noktaya gelmiştir. Buna göre kullanıcılar, bireysel ya da kurumsal olmalarına bakılmaksızın, mutlak olarak ağ güvenliği unsurunu göz önünde bulundurmak durumunda kalmaktadırlar. Bu noktada, ağ güvenliğinin verilerinin dolaşım hızının artışı ve alanının genişlemesi neticesinde önem kazanan bir husus olduğu görülmektedir. Ağ ile ilintili tüm unsurlardan ya da en az bir unsurdan faydalanan bireyler için güvenlik elzem bir konudur. Çünkü sürecin içerisine dahil olan tüm kullanıcılar sistemi dışarıdan takip eden tüm çevrelerin doğrudan tehdidi altındadır. Bu nedenledir ki ağ güvenliği, kullanıcıların tamamını ilgilendiren teknik ve veri odaklı koruma faaliyetlerinin tamamını kapsamaktadır (Gündüz ve Daş, 2014, 295-296). Ağ içerisindeki tüm içeriden ve dışarıdan katılım gerçekleştiren kullanıcılar, ağın güvenlik sistemi içerisinde korunması gereken unsurlar olmaktadırlar. Onların korunması bir bakıma ağın kendisinin tam anlamıyla korunmasını ifade etmektedir ve bu nedenle de ağ güvenliği iç ve dış tüm unsurlarıyla bir bütün olarak değerlendirilmek durumundadır.

İnternet tabanlı bir ağ etkileşiminden bahsedildiği süre zarfında, internet kullanımının yoğunluğu ile birlikte giderek zorlaşan bir ağ güvenliği uygulamasından bahsetmek mümkündür. Kullanıcı sayısının artışı özellikle kullanıcılara ait veri miktarının da artmasına izin vererek bu şekilde kullanıcıların sahip oldukları verilerin güvenlik risklerini de arttırmaktadır. Bu noktada ağ güvenliğinin artan veri miktarına paralel olarak, bu verilerden illegal bir şekilde getiri elde etmeye çalışan kesimler karşısında verilerin sahiplerinden verileri güvenli yoldan elde etmeye çalışan, buna hakkı olan kesimlere kadar tüm çevreleri korumaya çalışan bir sistem olduğu anlaşılmaktadır. Öte yandan ağ güvenliğinde verinin sahibi ve paylaşımcısı olan tarafların, sadece korunma ve güvenlik gözetimi düşüncesi ile hareket ettiklerini söylemek mümkün değildir; bu çevreler, aynı zamanda, ağ içerisindeki tüm güvenlik karşıtı unsurları takip edebilmektedirler (Deshpande, 2015, 124-127). Geniş ölçekli bir takip ağ güvenliğinin caydırıcılığını arttıracağı gibi, herhangi bir kombine ya da yeni nesil saldırı türüne karşı da güçlü bir koruma şansı sunmaktadır.



Şekil 1. Basit bir ağ güvenliği işleyişi

Kaynak: MEGEP (2011). Elektrik-Elektronik Teknolojisi - Ağ Güvenliği Ve Ağ Protokolleri. Ankara: MEB Yayını.

Şekil 1 üzerinde ele alınan basit bir ağ modelinde, güvenlik duvarı unsurunun önemi ön plana çıkmaktadır. Buna göre güvenlik duvarları, ağın içerisindeki tüm aktör ve birimlerin korunması adına, dışarıdan gelebilecek olan tüm saldırılara karşı güçlü bir engel oluşturmaktadır.

Ağ güvenliği temel olarak siber suçların yaygınlaşması ile birlikte daha fazla anlam kazanmış bir konudur. Bilgi hırsızlığı ve illegal yollarla elde edilen verilerin yine illegal amaçlar için kullanılması nedeni ile siber suçların giderek çekici hale gelmesi ağ güvenliği konusunda her geçen gün daha fazla yenilikçi uygulamanın kabul görmesini sağlamaktadır. Sürekli olarak belirli bir noktadan diğerine illegal yollarla veri transfer etmek isteyen tarafların sayısının artışı ağ güvenliği konusunda, özellikle kurumsal anlamda bir kez daha düşünülmesine sebebiyet vermiştir. Bu şekilde, kurumlar gerek dışarıdan destek sağlamak gerekse de kendileri güvenlik sistemleri geliştirmek sureti ile çeşitli adımlar atmaktadırlar (Pande, 2017, 16-18). Güvenlik sistemi oluşturmak açısından kurumların dışarıdan destek almaları sık olarak rastlanan bir durum olsa da kurumların bütçeleri ve güvenlik konusundaki algılamalarına göre kurum içerisinde bir ağ güvenliği sisteminin ve bu sistemi yöneten bir yapının kurulması mümkündür.

Öte yandan ağ güvenliği, sürdürülebilir bir yapının varlığına atıfta bulunan bir sistemi ifade etmektedir. Temel olarak kurulan bir yapının, uzun süre boyunca devam edebilmesi ve kesin güvenlik sağlaması adına önem arz eden temel husus sistemin, neredeyse her gün güncel olarak takip edilmesidir. Ağ güvenliği kurumsal açıdan işletmelerin düzenli bir veri toplama, depolama ve paylaşma çabaları adına koruyucu bir mekanizma olmaktadır. Bu mekanizma sistemsel olarak sıklıkla yaşanan güvenlik tehditlerinin tespitini ve gündelik olarak raporlanmasını da içermektedir. Kurumsal kapasite büyüdükçe ağ güvenliği konusunda karşılaşılan tehditlerin boyutu da aynı oranda artmaktadır (Ahonen, 2011, 9-10). Çünkü kurumların büyümesi ellerinde bulunan ya da biriken verinin de büyümesi anlamını taşımaktadır. Bu şekilde kurumlar, ellerindeki verinin kapasitesi ve değeri arttıkça giderek çok daha fazla ağ güvenliği yatırımı gerçekleştirmek hususunda kendilerini sürece adapte etmek durumunda kalmaktadırlar.

Ağ güvenliği özellikle internetin kullanım alanının genişlemesi sonucunda, verinin son derece kritik olduğu alanlarda ve departmanlarda kullanılmasıyla birlikte hayati bir anlam taşımaya başlamıştır. Bu noktada ağ güvenliği, sadece belirli tehditlere hazırlıklı olmayı değil, aynı zamanda muhtemel tehditlere hazırlıklı olmayı ve tehditleri tahmin etmeyi zorunlu hale getirmektedir. Bu nedenle ağ güvenliği

uzmanları artık var olan tehditler ile ilgili olarak kendileri de farklı boyutları ön plana çıkararak düşünmektedirler. Bu sayede kendileri için uygun olan güvenlik sistemini geliştirmeye çalışmaktadırlar. Bu sayede ağ güvenliği, çok boyutlu olarak düşünülmesini ve buna uygun olarak hareket edilmesini öngören bir sistem olmaktadır (Funmilola ve Oluwafemi, 2015, 40-41). Genellikle ağın içerisindeki bazı aktörlerin ağın güvenliğini değerlendirmek adına yeterli olduğu düşünülebilecekse de aslında, ortaya çıkan görüntü ağın içerisinde olmayan, hatta ağ için tehdit oluşturması mümkün olmayan unsurların da potansiyel bir tehdit oluşturma konusundaki durumlarının göz önünde bulundurulmasını zorunlu hale getirmektedir.

Son yıllarda ağ güvenliğinin kapsamı genişlemiştir ve konu, tahmin edilenden çok daha büyük boyutlara erişmiştir. Buna göre ağ güvenliği kapsamında ele alınan konulardan bir başkası sosyal ağ güvenliğidir. Dünya genelinde milyarlarca insanın dahil olduğu sosyal ağlar, artık insanların yaşamlarının önemli bir parçası olarak görev görmekte ve bu şekilde de aktif olarak gün içerisinde sosyal ağlarda önemli bir veri trafiği gerçekleşmektedir. Bu trafik aynı zamanda güvenlik sorunlarının da artışına sebebiyet vermektedir. Söz konusu ağların güvenliği, bireylere ait bilgilerin kolaylıkla elde edilebilmesi açısından büyük önem arz etmektedir. Bu nedenledir ki son yıllarda kişisel ağ güvenliği açısından sosyal ağların yarattığı riskler çok daha büyük bir önem arz etmektedir (Yıldırım ve Varol, 2013, 1-2). Sosyal ağların, kurumsal anlamda kullanılan ağlardan çok daha aktif olması ve içerisinde bulunan kişilerin ya da kurumların hangi amaçla sosyal ağları kullandıklarının bilinmesinin zor olması, sosyal ağlardaki güvenlik risklerinin çok daha büyük ölçekli olmasına sebebiyet vermektedir. Bu durum temel olarak sosyal ağların bireysel kullanıcılardan başlamak üzere, çok geniş bir kesim üzerinde olumsuz etki yarattığını göstermektedir.

1.2. Ağ Güvenliğinin Önemi

Ağ güvenliği konusunda, bireysel ve kurumsal anlamda atılan önemli adımlar söz konusu olsa da bu adımların güncelliği, bir sonraki aşamaya hazırlıklı olması ve kullanım açısından uygunluğu büyük bir önem arz etmektedir. Bu nedenle, ağ güvenliği konusunda çok boyutlu ve uzun soluklu bir şekilde düşünmenin önemi büyüktür. Temel olarak ağ güvenliğinin kullanıcılar açısından taşıdığı önemi aşağıdaki hususlar dahilinde ele almak mümkündür (Şahinaslan, Şahinaslan ve Kantürk, 2011, 3-4):

- Tehditlerden korunma: Sahip olunan verinin niteliği zaman içerisinde söz konusu veriden faydalanmaya çalışan tarafların ilgisini arttırmaktadır. Bu şekilde zaman içerisinde farklı tehditler ortaya çıkabilmektedir.

- Açıklık ve zafiyetleri giderme: Ağlar, her ne kadar güvenli bir şekilde oluşturulmuş gibi görünseler de aslında kendi içlerinde çeşitli açıklık ve zafiyetlere sahiptirler. Bu açıklık ve zafiyetlerin önceden tespit edilmesi ve giderilmesi elzemdir.

- Risklerin tespiti: Ağ tasarımcıları yalnızca tehditler ile karşılaşıldığında değil, aynı zamanda risklerin neler olduğunu çevrelerinde gözlemledikleri ya da doğru şekilde tahmin ettiklerinde ağ güvenliği sağlayabilmektedirler.

- Önlem: Ağ güvenliği açısından önemli olan husus, önlemler konusunda ihtiyaçlara yönelik hususları göz önünde bulundurmakla birlikte bir sonraki aşamaya yönelik önlemleri de göz önünde bulundurmaktır.

Sıralanan ve ağ güvenliği ile ilgili önem arz eden hususlar göz önünde bulundurulduğunda ön plana çıkan husus, önceden tespit ve güçlü bir şekilde tehditlere karşı tahminleme eğilimidir.

Bu şekilde ağ güvenliği konusunda ihtiyaç duyulan hususlar ile ilgili olarak özellikle yoğun ağ kullanımının söz konusu olduğu durumlar için verilerin daha güçlü bir şekilde korunması mümkün olmaktadır. Genel olarak sürecin anlık tehditler ekseninde değerlendirilmesi bir sonraki süre zarfında karşılaşılması muhtemel tehditlerin görülmesini engellerken, öte yandan ağ güvenliği ile ilgili olarak atılan adımların eski kalmasına sebebiyet verebilecektir.

Öte yandan, sıradan kullanıcılardan başlamak sureti ile kurumsal yönetimlere kadar etki edecek türden sorunlar ekseninde ağ güvenliğine dair unsurları, aşağıdaki şekilde değerlendirmek mümkündür (Fırlar, 2003, 10-11):

- Kişisel bilgilerin arz ettiği önemin bireysel ve kurumsal anlamda her geçen gün artması.
- Verilerin bütünlüğünün korunmasının, verilerin oluşturulması ve depolanması kadar önem arz etmesi.
- Verilerin ve bilgilerin üretiminin maliyetinin giderek artmasına paralel olarak korunmalarının öneminin de artması.
- Sadece kişisel değil, başkaları adına saklanan veri ve bilgilerin, kaybının ve zarar görmesinin bireysel ve kurumsal anlamda prestij sorunları yaratması.
- Kimlik bilgilerinin kullanılması sureti ile bireylerin ve kurumların haberleri olmadan onlar adına işlem yapılması.
- Güvenlik açıklarını kullanan tarafların, ağ içerisindeki bilgisayarlar arasında kolaylıkla işlem yapabilmesi.
- Bir güvenlik ihlalinin başarılı olmasının, beraberinde diğer güvenlik ihlallerini de getirmesi.
- Kontrol dışı ağ trafiğinin sağlanması ve bu sayede ağ trafiğinin sağlıklı bir şekilde ilerlemesinin önüne geçilmesi.

Sıralanan unsurlar incelendiğinde, ağ güvenliğinin bireysel ve kurumsal olarak kontrolden çıkmasıyla birlikte, sürecin ciddi ölçekli olarak zarara uğramasının kuvvetle muhtemel olduğu görülmektedir. Bu noktada özellikle, sürecin kontrolden çıkmasıyla birlikte güvenlik önlemlerinin yetersiz kalmasının söz konusu olacağı öngörülmektedir. Bu nedenledir ki ağ güvenliği, bir temel kurulması ile birlikte uygulamada fayda sağlayabilecek ve uzun vadede bireysel ve kurumsal olarak korunma sağlanmasını mümkün hale getirebilecektir.

Bir başka açıdan değerlendirildiğinde, ağ güvenliğinin önemini ön plana çıkarmak adına "Sıfır Güven" prensibi ön plana çıkarılmaktadır. Bu prensibin temel yaklaşımları aşağıdaki gibidir (Assunção, 2019, 67-68):

- Hiçbir veri, hiçbir zaman güvenle korunamaz; bu nedenle sürekli olarak doğrulanması gerekmektedir.

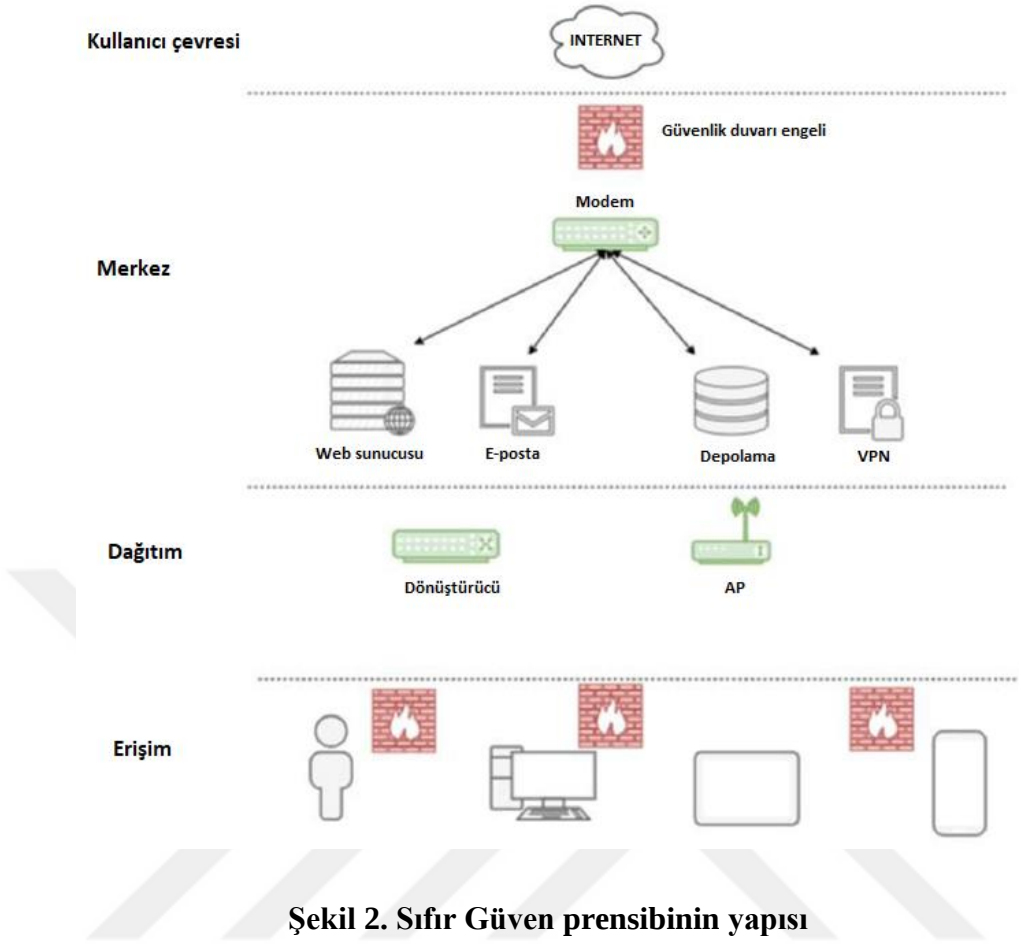
- Veriler ile legal olarak muhatap ise söz konusu tarafların verilere erişim haklarının sürekli olarak sorgulanması gerekmektedir.

- Verilere erişim konusunda ağ güvenliğinin sürdürülebilir olarak kontrol edilmesi ve sağlıklı bir şekilde erişimin olduğunun teyit edilmesi önem arz etmektedir.

- Tüm veri trafiği unsurları ve süreçlerinin sisteme, güvenli ve sorgulanacak şekilde erişmesi elzemdir.

- Verileri üreten ve depolayan tarafların veri erişim ilkelerini sürekli olarak güncellemesi gerekmektedir.

Sıralanan unsurlara bakıldığında Sıfır Güven sistemi, verilerin sahiplerinin dahi sorgulanmasını zorunlu hale getirmektedir. Bunun temel getirisi, ağ güvenliğini sağlamak adına sisteme legal olarak erişim hakkı olan tarafların, süreç ile olan ilişkilerinin sürdürülebilir şekilde kontrol edilmesi ve erişim hakkı olmayanların, her seferinde sistemin dışına atılmasıdır. Bu sayede sadece veriler korunmamakta, aynı zamanda verilerin dolaştığı ağın güvenliği de güçlü ve etkili bir şekilde korunmuş olmaktadır.



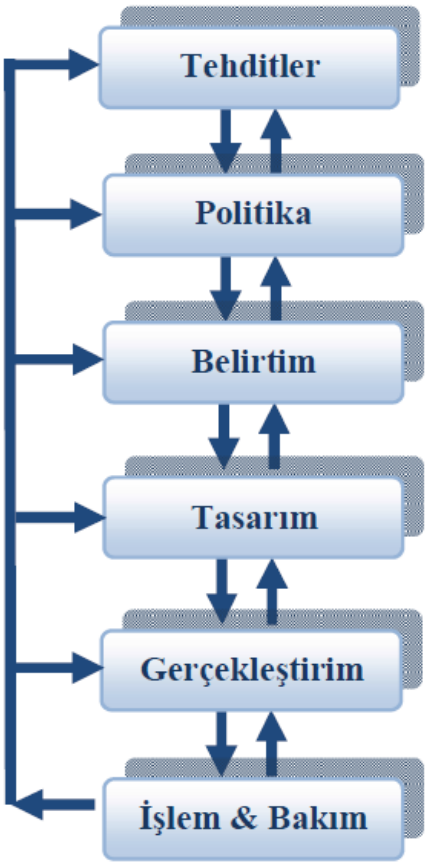
Şekil 2. Sıfır Güven prensibinin yapısı

Kaynak: Assunção, P. (2019).A Zero Trust Approach to Network Security. Erişim adresi https://privacyandsecurityconference.pt/proceedings/2019/DPSC2019-paper14.pdf

Şekil 2 üzerinde gösterilen şemada, sıfır güven prensibinin yapısında aşamalı olarak kullanılan, farklı unsurlardan oluşan ancak sürekli olarak güvenlik duvarlarına bağlı bir şekilde gerçekleşen bir güvenlik anlayışının bulunduğu görülmektedir. Bu anlayış, ağ içerisinde ve ağ dışında herhangi bir aktörün herhangi bir şekilde güvenli olmayacağına dair söz konusu olan inancın da bir sonucu olarak değerlendirilebilir. Ağ güvenliğinin giderek artan önemi düşünüldüğünde sıfır güven prensibi, açıkların minimize edilmesi adına mükemmeliyetçi bir yapı olarak değerlendirilebilir.

Öte yandan ağ güvenliği açısından önem arz eden konulardan biri de sistemin güvenliğini sağlayan taraflar arasındaki iletişim ve etkileşimdir. Ağ güvenliği kritik bir gereklilik olmasına rağmen kolaylıkla uygulanabilecek güvenlik yöntemlerinde

önemli bir eksiklik vardır. Güvenlik teknolojisi geliştiricileri ile ağ geliştiricileri arasındaki iletişim boşluğu sorunu bunun temelini oluşturmaktadır. Ağ tasarımı Open Systems Interconnection (OSI) modeline dayanan sağlam geliştirilmiş bir süreçtir. Modüler geliştirmeye izin veren yığınlar oluşturmak için farklı katmanların protokolleri kolayca birleştirilebilir. Bireysel katmanların uygulanması daha sonra başka ayarlamalar yapılmadan değiştirilebilir; bu da geliştirmede esneklik sağlar. Ağ tasarımının aksine, güvenli ağ tasarımı iyi geliştirilmiş bir süreç değildir. Güvenlik gereksinimlerinin karmaşıklığını yönetmek için herhangi bir metodoloji olmaması önemli bir sorundur. Aynı zamanda güvenli ağ tasarımı, ağ tasarımı ile aynı avantajları içermemektedir. Ağ güvenliği her zaman her iki uç bilgisayarı da güvence altına almak anlamına gelmemektedir. Süreç içerisinde önemli olan, veri iletirken iletişim kanalının saldırılara açık olmamasıdır. Muhtemel bir bilgisayar korsanı iletişim kanalını hedef alabilir, şifrelenmiş verileri elde edebilir ve şifresini çözerek yeniden yanlış bir mesaj ekleyebilir. Orta ağın güvenliğini sağlamak, bilgisayarların güvenliğini sağlamak ve mesajı şifrelemek kadar önemlidir (Sanghavi, Mehta ve Soni, 2013, 1). Bu nedenle ağ güvenliğinde ağın güvenliğinden sorumlu tüm taraf, birim, araç ve sistemlerin birbirleri ile sürekli olarak iletişim halinde kalmaları gerekmektedir.



Şekil 3. Ağ güvenliği yaşam döngüsü

Kaynak:(Can ve Akbaş, 2014, 20)

Şekil 3'te değinildiği üzere, ağ güvenliğinin oluşumunun temelinde, mutlak olarak tehditler yer almaktadırlar. Bu tehditler sistemin güvenlik açısından inşası için önem arz etmektedir ve her son aşama olan işlem ve bakım neticesince, oluşan ya da oluşması muhtemel olan tehditlere göre yeni bir sistem tasarımı gerçekleştirilmektedir.

1.3. Ağ Güvenliği Prensipleri ve Ağ Güvenliği Önlemleri

Ağ güvenliği, her ne kadar ağı kuran, kullanan ve ağdan faydalanan tüm kesimlerin beklentilerine, ihtiyaçlarına ve güvenlik endişelerine göre şekillendiriliyor olsa da bazı temel prensipler bu yapı açısından son derece önemlidir. Genel olarak kabul gören ağ güvenlik prensipleri aşağıdaki şekilde sıralanabilecektir (Can ve Akbaş, 2014, 17-18):

- Gizlilik (Confidentiality): Bilgiye ya da kaynağa sadece yetkili kişiler tarafından erişilmesi, yetkisiz kişilerin bilgiye ya da kaynağa erişiminin engellenmesidir.

- Bütünlük (Integrity): Verinin yetkilendirilmemiş bir şekilde değişiminin engellenmesidir. Verinin bozulması, değiştirilmesi ya da silinmesi gibi durumların önlenmesi amaçlanmaktadır.

- Erişilebilirlik (Availability): Bilginin sürekli ulaşılabilir ve kullanılabilir olması amaçlanmaktadır. Verilere erişim yetkisi olan kullanıcıların ağlara, sunuculara ve veri tabanı gibi uygulamalara güvenilir bir şekilde ulaşıp işlemlerini gerçekleştirmeleri sağlanmalıdır.

- Kimlik Denetimi (Authentication): Bilgiye, sisteme veya ağa erişmek isteyen kişinin gerçekten iddia ettiği kişi olduğundan emin olunması gerekmektedir. Kullanıcıların kişisel bilgisayarlarında kullandıkları şifreler, bir sisteme erişilmek istendiğinde kullanılan kullanıcı adı ve şifre, günümüzde kullanımı giderek yaygınlaşan biyometrik sistemler de birer kimlik denetim mekanizmasıdır.

- İnkâr Edememe (Non-Repudiation): Veri iletişiminde mesajı gönderenin veya mesajı alanın, gönderdiği veya aldığı mesajı inkâr edememesi durumudur. Bu durumda mesajın gönderilmiş olduğu ve alınmış olduğu garanti edilmektedir.

- İzlenebilirlik (Accountability): Ağ üzerinde veya herhangi bir sistem üzerinde gerçekleşen her türlü olayın, sonrasında incelenmek üzere kayıt altına alınmasıdır. Herhangi bir web sayfasına bağlanılması, sunucuya erişim, e-posta gönderimi gibi durumlar birer izlenebilirlik örneğidir.

Sıralanan bu prensiplerin hemen hepsi, ağ güvenliği konusunda, özellikle, kurumsal anlamda kritik bir öneme sahiptir. Bu şekilde ağın birçok farklı şekillerde korunması ve kontrol altına alınması mümkün hale gelmektedir.

Öte yandan ağ güvenliği konusunda alınacak önlemler de tıpkı prensiplerde olduğu gibi ağı kuran, kullanan ve ağdan faydalanan tüm kesimlerin beklentilerine, ihtiyaçlarına ve güvenlik endişelerine göre şekillendiriliyor olsa da bazı temel önlemleri içerisinde barındırmaktadır. Genel olarak söz konusu ağ güvenlik önlemleri, aşağıdaki şekilde sıralanabilecektir (MEGEP, 2013, 14-16):

- Tanımlama ve Kimlik Doğrulama İlkeleri: Bilgisayar ağlarında tanımlama, belirli bir kimlik sahibinin gönderilen mesaja bu bilgiyi eklemesi ile ifade edilir. Kimlik doğrulama, sunucu bilgisayar tarafından belirli kullanıcıları tanımlamak ve kendi verilerine erişim izinlerini doğrulamak için kullanılan işlemdir.

- Parola İlkeleri: Bilgisayar ağlarında güvenlik önlemlerinden biri de ağa erişim için parola korumasıdır. İnternet erişimi için veya dosya sunucusuna erişim için güvenlik uzmanları parolalı koruma yöntemini geliştirmiştir.

- Kabul Edilebilir Kullanım İlkeleri: Güvenlik tehditlerinin çoğu tanınmış web sitelerinden gelebilir. Web sitelerine erişimlerini yönetmeyen organizasyonlar risk altındadır. Ağ güvenlik filtreleme çözüm olarak kabul edilebilir.

- Uzaktan Erişim İlkeleri: Uzaktan erişerek kullanılacak sistem başka bir binada veya kilometrelerce uzakta olabilir. Uzaktan erişim yapılacak bilgisayarı bir uzaktan erişim sunucusu gibi çalışmak üzere yapılandırarak, uzak veya hareketli çalışanların kuruluşunuzun ağlarına bağlanması sağlanabilir.

- VPN Bağlantıları: Ağ güvenlik önlemlerinden biri de Virtual Private Network (VPN) kullanılmasıdır. VPN çalışma mantığı, aslında olmayan ama farklı hatlar üzerindeki İnternet sistemleri, uydu bağlantıları, kablo net yapıları farklı noktada olan iki ağı aynı ağda çalıştırmaktır.

- Ağ Bakım Yordamları: Ağ cihazı işletim sistemlerini ve son kullanıcı uygulamalarını güncelleme yordamlarını belirler.

- Olay İşleme Yordamları: Güvenlik olaylarının nasıl işleneceğini açıklar.

Sıralanan söz konusu eylemlerin her biri birçok farklı şekilde ağa ve verilere erişim sürecinde tarafların çok sayıda sınamadan geçmesini sağlamaktadır. Böylelikle ağa, izin verilen tarafın/tarafların dışında kimsenin/kimselerin girmemesi sağlanmaktadır.

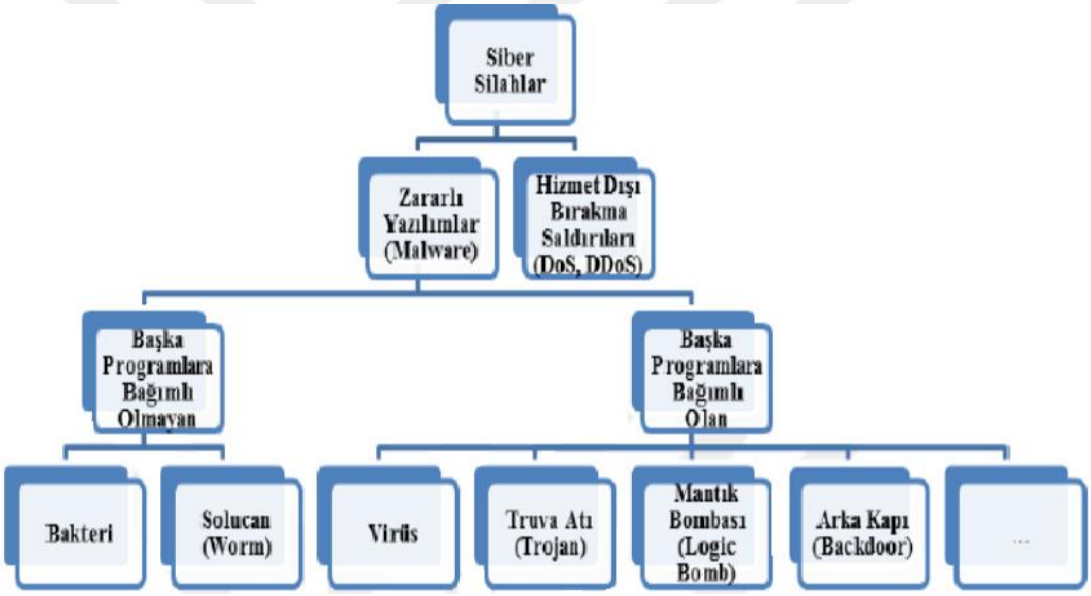
Genel olarak bakıldığında, verimlilik ve otomasyon elde etmek için adımları detaylı bir şekilde ele almak ve aşamaların şartlarını iyileştirmek, iş akışı geliştirmede temel gereksinimdir. Uçtan uca kullanıcı provizyonu ve provizyonunun kaldırılması için tutarlı ve güvenli süreçler oluşturmak güvenli, sorunsuz ve tutarlı kullanıcı deneyimi ile sonuçlanacaktır. Kullanıcılara kaynak sağlamak için rol tabanlı erişimi kullanmak, yalnızca görevleri tamamlamak için gerekli yetkileri sağlayarak en düşük ayrıcalık erişimini sağlamanın bir yoludur. Erişim yönetimi sistemini kullanarak çoklu oturum açma, ayrıntılı yetkilendirme ve temsilci yönetimi dağıtma, kuruluşun erişim kontrolünü merkezileştirmesini sağlar (Schuett ve Rahman, 2011, 18). Bu tür bir merkezileştirme sisteminin en önemli avantajı, ağa dahil olacak olan tüm aktörlerin merkezi sistemde var olan kimlik kayıtlarında kendisine hali hazırda yer bulmuş olmasıdır. Bu da sistemin, çok sık müdahale olmadan kendi kendisine bir güvenlik yapısı oluşturmasına imkân sağlamaktadır.

1.4. Ağ Güvenliği ile Birlikte Ortaya Çıkan Bir Sorun Olarak Siber Güvenlik

Ağ güvenliği sorunu genel olarak bireysel ve kurumsal kullanıcıları yakından ilgilendiren bir konu olsa da konunun boyutları gelişerek bir başka önemli sorun olan ve kurumsal anlamda tehditleri beraberinde getiren siber güvenlik hususunu ön plana çıkarmıştır.

Siber saldırılar, profesyonel niteliğe sahip bilgisayar korsanlarının büyük ölçekli kurum ve kuruluşların ağ trafiklerini hedef almak sureti ile web siteleri başta

olmak üzere sunuculara, bilgi depolama sistemlerine ve ağın bilgisayarlarına yapmış oldukları saldırıları kapsamaktadır. Siber saldırılar çok farklı boyutlarda gerçekleştiriliyor olmaları nedeni ile tespit, kontrol, engelleme ve karşı saldırı açısından zorlu faaliyetlerdir. Siber saldırıların temel hedefi, bir ağ üzerindeki bilgiyi illegal bir şekilde ele geçirmek, manipüle etmek, programlama sistemini bozmak ve kimi zamanda bir kurumu ya da spesifik olarak bir kişiyi küçük ve zor duruma düşürmek adına gerçekleştirilen eylemleri kapsamaktadır (Yıldırım, 2018, 2-3). Son yıllarda giderek yaygınlaşan siber saldırılar, bireysel bir kullanıcıdan, büyük ölçekli, kurumsal bir kullanıcıya kadar uzanan silsilede gerçekleşebilmektedir. Özellikle de devlet yönetimlerinin sürekli olarak muzdarip oldukları bu saldırılar, modern teknoloji çağındaki en kritik sorunlardan biri olarak değerlendirilmektedir.



Şekil 4. Siber saldırılarda kullanılan ve "silah" olarak nitelendirilen bazı temel araçlar

Kaynak: Çifçi, H. (Ed.) (2013). Her Yönüyle Siber Savaş. İstanbul: TUBİTAK Popüler Bilim Kitapları.

Şekil 4'te gösterilen kırılım aslında siber saldırıların ne denli çok boyutlu ve çok tehlikeli bir nitelikte olduğunu da göstermektedir. Saldırganların hedef olarak belirledikleri sistemlere en uygun siber saldırı yöntemini belirlemelerine izin veren, kırılım üzerindeki siber saldırı türleri, konunun ağ yönetimi açısından ne denli zorlu bir hale getirildiğini göstermektedir.

Siber saldırıların genel niteliğine bakıldığında aşağıdaki hususlar dikkati çekmektedir (Önal, 2021, 118):

- Tespit edilmesi ve bir güvenlik mekanizması oluşturulabilmesi adına, saldırının kime yönelik olduğunun, doğru şekilde tespit edilmesi gerekmektedir.
- Farklı amaçlarla yapılmış olabileceği gibi geniş kitlelere mesaj verecek nitelikte olma ihtimali vardır; bu da siber saldırıları uluslararası hale getirmektedir.
- Siber saldırılarda sadece kurumsal olarak da, birey kullanıcılar bazında da büyük hasarların oluşturulmasına çalışılmaktadır.
- Saldırlar içerisinde, doğrudan virüs menşeili saldırılar söz konusu olabildiği gibi reklam içerikleri üzerinden de saldırılar gerçekleştirilebilmektedir.
- Saldırılarda doğrudan bilgiyi ve veriyi elde etmek kadar dolaylı yollardan bilgi ve verinin farklı yerlere aktarılmak sureti ile elde edilmeye çalışılması da söz konusudur.

Yukarıda yer alan unsurlar göstermektedir ki siber saldırılar, çeşitli şekillerde ortaya çıkmak sureti ile hem geniş kitlelere zarar vermeyi hem de geniş ölçekli olarak bilgi edinmeyi hedeflemektedir. Bu şekilde siber saldırılar veri hırsızlığı adına ağlarda, çok farklı kesimlere aynı anda zarar vermeyi amaçlayan suç davranışları olarak nitelendirilebilir.

Siber saldırıların ortaya çıkışı ve yayılımı ile birlikte siber güvenlik kavramının, çok daha yaygın ve etkin bir şekilde kullanılmaya başlandığı görülmüştür. Kavramsal olarak siber güvenlik, bilgi ve verilerin alt yapılarının dayandırıldığı bilgisayar ve bilişim sistemlerindeki güvenliğin daha fazla kullanıcı, daha kurumsal ve daha uluslararası boyutta ele alınması ile ortaya çıkmıştır (Güngör, 2015, 19). Özellikle artan kullanıcı sayısı ve genişleyen, küreselleşen ağ alanlarının artışından dolayı siber saldırılar, suç işleme eğiliminde olan kesimler için çekici birer unsur

haline dönüşmüştür. Kolay bir şekilde farklı ağlardan, çok sayıda kişi ve kurumun verilerine erişebilmek ve bunun üzerinden çeşitli çıkarlar sağlayabilmek, siber saldırı gerçekleştirerek ağlara zarar veren kesimlerin öncelikli hedefidir.

Siber güvenlik içerisinde, bilgi gizliliği ve erişilebilirliğinin kontrolü, bilginin güvenceye alınması, siber saldırı ihtimallerinin tahminlenmesi, siber saldırı olması muhtemel olan faaliyetlerin analizi ve otomatik kontrol mekanizmalarının ön plana çıkarılması söz konusu olmaktadır (Güleç ve Kişman, 2021, 132). Bu açıdan siber güvenliğin detaycı ve geniş çaplı bir operasyonel yapı olduğunu düşünmek mümkündür. Siber güvenliğe dair en önemli unsur, tahminleme mekanizmasıdır. Siber güvenlik tasarımcıları, muhtemel her türlü tehdit üzerinde düşünerek ağ üzerindeki iletişim mekanizmalarını tasarlamak ve kullanmak durumundadırlar.

Kurumsal olarak özellikle kamu kuruluşlarının ve dünya genelinde aynı anda milyonlarca, hatta milyarlarca aktif kullanıcısı bulunan kurumlar açısından siber güvenlik konusunda önemsenmesi gereken hususları aşağıdaki şekilde sıralamak mümkündür (İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku Enstitüsü, 2012, 4):

- Kurum yapısına ve faaliyetlerine özgü siber güvenlik stratejisinin belirlenmesi ve oluşturulması.
- Kamu bünyesinde her kademedeki kamu faaliyetlerine uygun siber güvenlik yapıların oluşturulması.
- Farklı kurum ve birimlerin uyum içerisinde çalışabileceği akıllı bir altyapının kurulması.
- Özellikle ulusal bazda olmak üzere kurumların kendi içlerinde siber güvenlik alanında bir hukuk yapısını oluşturmaları.
- Konunun hassasiyetine aşina nitelikte çalışan ihtiyacını karşılayacak istihdam ve eğitim programlarının verilmesi.

- Uluslararası alanda, kurumsal olarak gelişmeleri takip ederek bu alanda AR-GE merkezlerinin kurulması.

Kurumlar açısından ciddi bir hassasiyet gerektiren siber güvenlik konusunda dikkat çeken önemli husus, konu ile ilintili olan çalışanların tespiti, istihdamı ve bu konuya dair sürdürülebilir olarak eğitilmeleridir. Bu durum, nitelikli çalışanlarla daha güçlü bir şekilde ve geniş bir ağ üzerinde güvenlik kalkanı oluşturulmasına imkân sunacaktır.

Öte yandan, bireysel ve kurumsal anlamda temel olarak kullanılan ağ güvenliği uygulamalarının sık bilinenlerini aşağıdaki şekilde sıralamak mümkündür:

- Antivirüs Programı: Bilgisayarın zararlı programlardan korumak için hazırlanan güvenlik yazılımlarına antivirüs denir. Antivirüs programları genel olarak zararlı programları bulup yok etmekle görevli olsa da bilgisayar kullanıcılarının tercihlerine göre görevleri vardır. Çoğu antivirüs programının otomatik görevleri olsa da bunun yanında virüs ve zararlı kodlar bulunduğunda kullanıcıya bu kodu içeren program için ne yapılması gerektiğini de sorar (Çakır ve Kesler, 2012, 469-470).

- Güvenlik Duvarı (Firewall): Güvenlik duvarı, özel Local Area Network (LAN) ve güvenli olmayan genel internet gibi iki ağ arasında bir erişim denetimi politikası uygulayan bir sistemdir. Güvenlik duvarı, hangi iç hizmetlere dışarıdan erişilebileceğini ve bunun tersini belirler. Bunun gerçekleştirildiği gerçek araçlar çok çeşitlidir, ancak prensipte güvenlik duvarı bir çift mekanizma olarak düşünülebilir: biri trafiği engellemek, diğeri trafiğe izin vermek (3COM, 2000, 2).

- Web Application Firewall (WAF): Bu sistem, web güvenlik duvarı algılama ve kontrol sürecinde güvenlik niteliklerini geliştirmek için yeni bir yaklaşım oluşturan ve onu bağımsız web güvenlik duvarı hizmetlerinden farklı kılan tüm web güvenlik duvarı teknolojisine uygulanabilen bir sistemdir (Manaseer ve Al Hwaitat, 166).

- Güvenlik Bilgileri ve Olay Yönetimi (SIEM): Sistem, tehditleri veya olayları tespit etmek için güvenlikle ilgili verileri merkezi bir şekilde toplamaktan sorumludur. Böylece çoklu günlük olaylarını ilişkilendirerek gerçek zamanlı veya geçmiş olaylar üzerinde güvenlik analitiği yetenekleri sağlamaktadır. Diğer işlevleri, bağlam verileriyle zenginleştirme, heterojen veri kaynaklarının normalleştirilmesi, raporlama, uyarı ve otomatik olay yanıt yetenekleridir (Vielberth, 2021, 1).

- Veri Kaybı/Sızıntısı Önleme (DLP): Veri sızıntısı, bir kuruluş ile harici bir hedef veya alıcı arasında yetkisiz veri alışverişidir. Veri sızıntısı, bir programcı saldırısı, kuruluşun çalışanları tarafından kasıtlı olarak sızdırılması veya kasıtlı olmayan veri kaybı veya açığa çıkması nedeniyle olabilir. Sistem, çeşitli varyasyonlar ile bu sızıntıları tespit edip olası tehditlere karşı korumaktadır (Jadhav ve Chawan, 2019, 1).

Bunların dışında, bir önlem olarak özellikle kurumlar tarafından gerçekleştirilen penetrasyon testleri bulunmaktadır. "Sızma testi" olarak da bilinen bu güvenlik yöntemleri, donanım, yazılım ve insanlardan oluşan eksiksiz, entegre, operasyonel ve güvenilir bilgi işlem tabanını test etmek için kapsamlı bir yöntemdir. Süreç, zayıf veya uygun olmayan sistem yapılandırması, donanım ve yazılım kusurları ve süreçteki operasyonel zayıflıklar veya teknik önlemler dahil olmak üzere olası güvenlik açıkları için sistemin aktif bir analizini içerir. Penetrasyon testi, güvenlik fonksiyonel testinden farklıdır. Sistemin güvenlik kontrollerinin doğru davranışını gösterirken, sızma testi birinin bilgi ve bilgi sistemlerine yetkisiz erişime karşı bir kuruluşun güvenlik kontrollerine girmesinin zorluğunu belirlemektedir. Otomatik araçlar veya manuel yöntem veya her ikisinin bir kombinasyonu kullanılarak sisteme saldıran yetkisiz bir kullanıcının simüle edilmesiyle yapılmaktadır (Bacudio vd., 2011, 19).

Sosyal mühendislik; etkileme, zorlama, aldatıcı ilişkiler geliştirme, sorumluluğu, etik değerleri, dürüstlüğü ya da bağlılığı azaltma amacını güden yöntemler kullanarak kişileri gizli bilgi vermeleri veya erişim sağlamaları için aldatma

sürecidir. Sosyal mühendislik saldırılarına karşı açıkları tam olarak kapatabilecek garanti edilmiş bir yöntem bulunmamakla birlikte, riskleri hafifletebilecek ve zararları minimize edebilecek yöntemler bulmak mümkündür. Siber saldırılara karşı bilgisayar ve ağ altyapısına yönelik tedbirler alınırken sosyal mühendislik saldırılarına karşı daha farklı savunma yöntemlerinin geliştirilmesi gerekmektedir. Bununla birlikte kurumsal yapı içerisindeki çalışanlara, söz konusu saldırılar ve olası etkileri ile ilgili eğitimler verilmesi önem arz etmektedir (Bağcı, 2009, 43-46).

1.5. Yeni Ağ Teknolojisi Olarak Bulut Ağlar ve Güvenlik

Bulut bilişim, satıcılar, ağ operatörleri ve hizmet sağlayıcılar dahil olmak üzere bilgi işlem ve iletişim endüstrilerindeki taraflardan son yıllarda çok fazla ilgi toplamıştır. Aslında bulut bilişimin dayandığı hizmet programı iş modeli yeni değildir. Yine de internet ve web teknolojilerinin varlığı ve altyapı sanallaştırmasının tanıtılması, bu vizyonun mevcut süreçte gerçekleştirilmesini sağlamıştır. Hizmet sağlayıcının altyapı sağlayıcısından ayrılması, çevrimiçi olarak yeni hizmetler üretmeyi ve bu hizmetleri talep doğrultusunda ölçeklendirmeyi kolaylaştırmaktadır. Hizmet sağlayıcı için bu, kapasiteyi değiştirmek için çok az veya hiç teslim süresi olmadan kaynaklara erişim için gerektiği gibi, ödeme yapmalarından dolayı sermaye ve operasyonel harcamaları ve finansal riski azaltmaktadır. Altyapı sağlayıcısı için ise bu, ölçek ekonomilerinden yararlanan büyük altyapılar inşa etme ve birden fazla müşterinin iş yükü boyunca maliyetleri amorti etme fırsatı vermektedir (Schoo vd., 2010, 3). Avantajlı bir uygulama olarak görülebilecek olan bulut ağlar, bireysel ya da kurumsal olmasına bakılmaksızın, tüm kullanıcılar açısından büyük kolaylıklar sağlamaktadır. Hem ticari hem de gündelik kullanım açısından bakıldığında bulut ağlar, gelecek adına da önemli bir alternatif olarak görülebilecektir.

Bulut tabanlı ağ, bir kuruluşun ağını dünya çapında dağıtmasına olanak tanır. Bulut, bir kurumsal ağ sisteminin geliştirilmesini önemli ölçüde basitleştirir. Bulutta temel alınan ağ bir bulut sağlayıcısı tarafından oluşturulur. Bir kuruluşun tüm yapması gereken şirket içi ağını, küresel bir kurumsal sınıf ağ sistemi oluşturmak için bulutta yerleşik ağa bağlamaktır. Bu tür bir küresel ağ sisteminde ilk sermaye yatırımı yoktur. İnternetin aksine, bulut tabanlı ağ, ağ görünürlüğü üzerinde merkezi kontrol sağlar. Bulut tabanlı ağ aracılığıyla kuruluş, birden çok kiracıya hizmet veren bir yazılım

uygulaması olan çok kullanıcılı bir uygulama sağlayabilir. Her kullanıcı uygulamanın bir parçasına abone olur. Her kullanıcının verileri yalıtılır ve diğer kullanıcılar tarafından görülmez. Öte yandan uygulamanın bakımı ve güncellenmesi büyük ölçüde basitleştirilebilir. Bulut tabanlı ağ, kuruluşun BT altyapılarını dakikalar içinde uzak konumlara dağıtmasını sağlar (Chao, 2016, 4). Hız ve etkililik açısından değerlendirildiğinde bulut tabanlı ağlar, uzaktan erişim konusundaki avantajı ile dikkat çekmektedir. Bu avantaj, bulut ağların geniş bir kitle tarafından kabul görmesi kullanılması açısından teşvik edicidir. Lokasyon sınırlaması olmadan verileri ve sistemlere erişilebilme imkanının bulunması, bulut ağ teknolojisini özellikle kurumsal açıdan daha çekici hale getirmektedir.

Bulut ağlarda ağ mimarisini oluşturan unsurları aşağıdaki şekilde sıralamak mümkündür (Moura ve Hutchison, 2016, 122-127):

- Güvenilir İletişim: Verilerin bir bulut altyapısı içinde hedeflenen alıcıya/alıcılara doğru ve zamanında ulaştırılması için tam iletişim güvenilirliği desteklenmelidir. Halihazırda standardizasyon kuruluşları, mevcut ve gelecek ağ altyapıları aracılığıyla iletişimi geliştirmek için çeşitli çözümler üzerinde çalışmaktadır.

- Verimli İletişim: Hız etkisinin yanı sıra kolay ve sorunsuz erişilebilirlik bulut ağlardaki verimliliğin temel unsuru olmakta, özellikle de işletmeler bu yöntemi daha fazla tercih etmektedirler.

- Sanal Ağ: Bir bulut veri merkezinin tipik bir fiziksel ana bilgisayarı, çeşitli sanal makinelerin aynı ana bilgisayar donanımı üzerinde çalışmasını sağlayan bir hiper yöneticiye sahiptir. Sistem ve ağ öğeleri arasında daha güçlü bir birlikte çalışma ve birlikte çalışabilirlik sunmak için, bir bulut altyapısı içinde ağ kaynaklarının sanallaştırılması çok önemli bir gereklilik haline gelmektedir.

- Esneklik ve Birlikte Çalışabilirlik: Çalışma ortamının sınırsızlığı ile birlikte tipik yerleşik ağlar gibi bulut ağlar da birlikte çalışmak adına yeterli derecede uygun bir yapıya sahiptir.

Yukarıdaki unsurlar göz önünde bulundurulduğu süre zarfında, bulut ağ sistemlerinin, mümkün olduğunca etkili ve nitelikli bir şekilde kullanımı adına, güvenlik ve esneklik unsurlarının bir arada ele alınmasının önemine dair atıflar ön plana çıkmaktadır. Sistem, bulut yapısına sahip olmasına ve kullanıcılar açısından bir esneklik sağlamasına karşın ilerleyen süre zarfında, bu esnekliğin yaratabileceği güvenlik açıklarının da göz önünde bulundurulması gerekmektedir.

Fakat bulut bilişime ek olarak kullanılan sanal ağ, farklı sanal bileşenler arasında iletişimi mümkün kılarak yeni güvenlik sorunları ortaya çıkarmaktadır. Bir sanal ağ kullanıcısının bakış açısından ağ özel olabilirken, gerçekte iletişimin kendisi bir kamu altyapısı aracılığıyla gerçekleşir. Bu nedenle bu iletişimi güvence altına alacak mekanizmalar (örneğin, şifreleme yoluyla) oluşturulmalıdır. Bir seçenek, bunu her sanal bileşende yapmaktır; bu, sanal ağ müşterisinin iletişimi güvence altına almakla ilgilenmesi gerektiği anlamına gelir. Diğer bir seçenek, sanal ağ sağlayıcısı tarafından bir hizmet olarak güvenli iletişim sağlamaktır; bu, iletişimin varsayılan olarak güvenli ve müşteri için şeffaf olduğu anlamına gelir. Bulut ağ iletişimi yönetimi için fiziksel altyapıya ve ağ özelliklerine erişim gereklidir. Bu erişim, kullanıcının isteğe bağlı olarak birkaç parametre belirleyebileceği tek bir arabirim olarak uygulanmalıdır. Geçen zamanla birlikte fiziksel sanallaştırma altyapısına ve ağ altyapısına birleşik erişimle yeni saldırılar ortaya çıkmaktadır. Bu süreçte zorluklardan biri, yönetim arayüzüne erişim kurallarını ve bu kuralların nasıl uygulanacağını tanımlamaktır. Ayrıca sanal altyapıların ağlar üzerinde taşınmasına yönelik politikaların da dağıtılması gerekmektedir (Schoo vd., 2010, 11-12). Bulut ağların merkezi yapılarının güçlü olmaması ve uzaktan erişim niteliklerinin yüksek olması beraberinde ciddi ağ güvenliği tehditlerini de getirmektedir. Bu nedenle bulut ağlar, kolaylıklarıyla ciddi ölçekli bir avantaj sağlasalar da güvenlik endişeleri ile bu endişeleri gidermeye yönelik yoğun çabaları ekseninde değerlendirilmektedir.

Bulut ağlarda, Xen ve VMWare gibi iyi bilinen hipervizörlerin canlı geçişinin mevcut uygulamasında açıklanan birkaç güvenlik açığı vardır. En büyük sorun, aktarılan verilerin geçiş işlemi sırasında şifrelenmemesidir. Çekirdek belleği, uygulama durumu, parolalar ve anahtarlar gibi hassas veriler ve diğer geçiş verileri, hiçbir gizlilik olmadan net bir şekilde aktarılır. Diğer güvenlik açıkları ise şu şekilde

sıralanabilir; sanal makinelerin güvenilir bir hedef platforma taşındığının garantisinin olmaması, kimlik doğrulamasının olmaması, işlem yetkilendirmesinin olmaması, sanal makine verilerinin bütünlük garantisinin olmaması ve hipervizör ve geçiş modülü kodunda güvenlik açıklarına neden olan hataların varlığı (Mattos, Ferraz ve Duarte, 2015, 12). Söz konusu güvenlik açıkları mutlak olarak ağ güvenliği sistemleri içerisinde değerlendirilerek çözüme kavuşturulabilecektir. Fakat bulut ağların sayılarının giderek artması ve bu şekilde kullanıcı sayılarının çok hızlı bir şekilde artmasının neticesinde, bulut ağların güvenliğine yönelik nitelikli çözümlerin bulunması da zorlaşmaktadır.

Genel olarak değerlendirildiğinde ise bulut ağ güvenliği için ön plana çıkarılan unsurlar aşağıdaki gibidir (Mattos, Ferraz ve Duarte, 2015, 12-13):

- Kullanılabilirlik ve İzolasyon: Herhangi bir sanal makinenin diğer sanal makinelere ne erişmesi ne de müdahale etmesi gerektiği gerçeğini ifade eder. Birkaç sanal makine aynı altyapıyı paylaşsa da bir sanal makine diğer sanal makine verilerine erişemez veya bilgi işlem sonuçlarını değiştiremez.

- Bütünlük: Sanal bir ortamın bütünlüğü doğrulamak ve kanıtlamak için araçlar sağlaması gerektiğini ve bu nedenle işleme bellek ve depolamasının değiştirilip değiştirilmediğinin tespit edilmesinin mümkün olmasını amaçlar.

- Sanal Makine Atomikliği: Aynı anda yalnızca bir sanal makine örneğinin çalışmasını sağlar. Bu nedenle sanal makine geçişi ne yeni sanal makineler eklemeli ne de kimseyi ortadan kaldırmamalıdır. Böylece başarılı bir geçişten sonra sistem, kaynak ana bilgisayardaki sanal makine örneğini kaldırır ve taşıma hatası durumunda sistem, hedef ana bilgisayardaki sanal makine örneğini kaldırır.

- Gizlilik: Bir saldırganın bir sanal makinenin geçişi sırasında veri aktarımının içeriğine müdahale edememesini, erişememesini veya değiştirememesini sağlar. Bu nedenle sistem, eş ana bilgisayarlar

arasında veri aktarmak için güvenli iletişim kanalı kullanabilir. Ayrıca güvenli iletişim kanalının eşleri, benzersiz şifreleme anahtarları üzerinde anlaşabilmeli ve bunların yalnızca eşler tarafından bilinmesini sağlamalıdır.

- Kimlik Doğrulama: Ağdaki bir varlığın gerçek kimliğini sağlar, dolayısıyla diğer güvenlik gereksinimleri başarılı kimlik doğrulamaya bağlıdır. Kimlik doğrulama önemli bir özelliktir çünkü diğer güvenlik gereksinimleri kimlik doğrulamaya dayalı olarak meşru ve yetkili katılımcıları gayri meşru katılımcılardan ayırt etmek için yetkilendirme gibi kimlik doğrulamaya bağlıdır.

- Yeniden Oynatma Direnci: Bir saldırganın tespit edilmeden geçiş prosedürünü yeniden oluşturamamasına yöneliktir. Bu nedenle tüm geçiş paketleri benzersizdir ve geçişten sonra geçerliliğini kaybeder.

Yukarıda sıralanan ve bulut ağlar açısından önemli olarak nitelendirilebilecek olan güvenlik hususları, bulut ağlarda çok kademeli ve geniş bir iletişim, etkileşim ve hizmet alanının, güvenli bir şekilde gerçekleştirilmesini sağlayacaktır.

İKİNCİ BÖLÜM
AĞ GÜVENLİĞİNDE RİSKLER

2.1. Ağ Güvenliğinde Temel Risk Unsurları: Saldırılar

Ağ güvenliğinde en önemli sorunların başında, gerçekleştirilen saldırıların tasarımı ve yarattığı etkiler gelmektedir. Ortaya çıkan saldırılar önlenebilse bile durdurulamamakta ve saldırıyı gerçekleştiren taraflar zaman içerisinde yeni saldırılar tasarlayarak süreci devam ettirmektedirler.

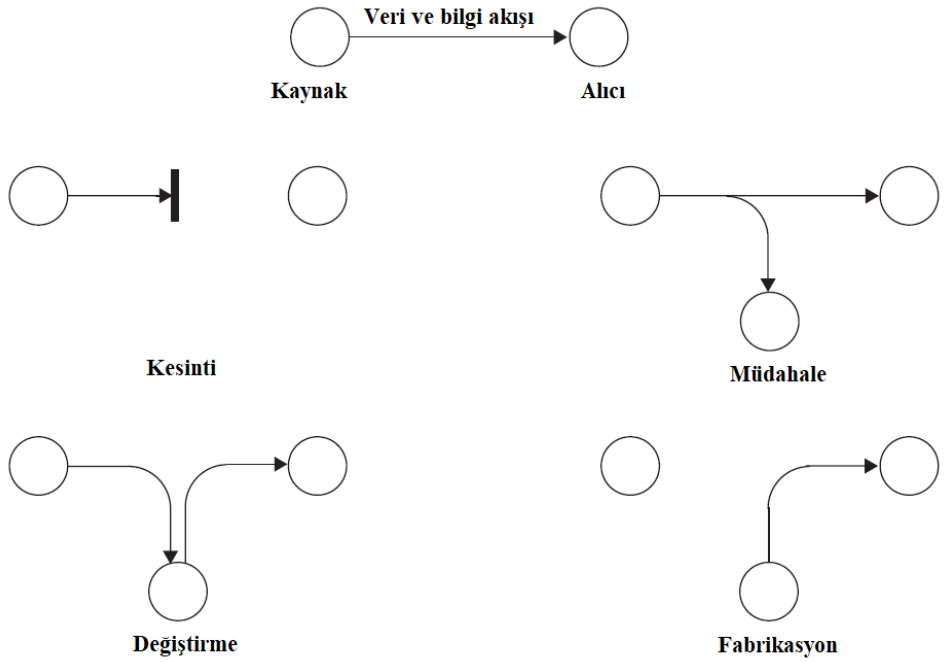
Oluşturulan bir ağı hedef alan çeşitli saldırı kategorilerini aşağıdaki şekilde sıralamak mümkündür (Kruegel, 2022)

- Kesinti: Sistemin işleyen mekanizması yok edilir veya kullanılamaz hale getirilir. Bu saldırı, kaynağı veya iletişim kanalını hedef alır ve bilginin amaçlanan hedefe ulaşmasını engeller (örneğin, kabloyu kesmek, bağlantıyı aşırı yüklemek, böylece tıkanıklık nedeniyle veri akışının kesilmesi). Bu kategorideki saldırılar, bir tür hizmet reddi (DOS) gerçekleştirmeye çalışır.

- Müdahale: Yetkisiz bir taraf iletişim kanalına gizlice girerek (örneğin, telefon dinleme) bilgilere erişim şansı kazanır.

- Değiştirme: Bilgiler yalnızca ele geçirilmez, kaynaktan hedefe geçiş sırasında yetkisiz bir tarafça değiştirilir. Bilgiler üzerinde oynanarak, aktif olarak değiştirilir (örneğin, mesaj içeriğinin değiştirilmesi).

- Fabrikasyon: Saldırgan, göndericiye hiçbir şey yaptırmadan sisteme sahte nesneler ekler. Daha önce ele geçirilen bir nesne eklendiğinde bu işleme "Yeniden Oynatma" denir. Saldırgan meşru kaynak gibi davrandığında ve istediği bilgileri girdiğinde, saldırıya "Maskeleme" denir (örneğin, bir kimlik doğrulama mesajını tekrar oynatma, bir dosyaya kayıt ekleme).



Şekil 5. Ağ güvenliği karşısında söz konusu olan saldırı riskleri

Kaynak: Kruegel, Christopher ,2022, https://sites.cs.ucsb.edu/~chris/research/doc/iit04_security.pdf.

Şekil 5 ile de açıklanmaya çalışıldığı gibi ağ güvenliğine yönelik gerçekleştirilen saldırılarda doğrudan engelleme davranışından, sürecin içerisine dahil olarak verileri ve bilgileri manipüle etmeye dek uzanan geniş bir yelpazede risklerin bulunduğu görülmektedir. Bu saldırılar, temel olarak verilerin akışını engellemeyi, uzun vadede ise değiştirilen bilgiler ile ağın içerisindeki taraflardan bilgi toplamayı amaçlamaktadır.

2.2. Yeni Nesil Saldırı Türleri

Gelişen teknoloji ile birlikte artan riskler, ağ güvenliği için yeni tehditlerin ortaya çıkmasına da sebebiyet vermiştir. Kimi zaman keyfiyete dayalı kimi zaman da belirli bir amaç ya da hedefe yönelik olarak gerçekleştirilen saldırılar, ağ güvenliği açısından önemli bir risk teşkil ederken, aynı zamanda ağlara gerçekleştirilen saldırıların türlerinde de değişikliğe sebebiyet vermektedir.

Bu tehditler arasında aşağıda sıralanan ve kişisel ya da kurumsal olarak geliştirilen unsurlar yer almaktadır (Nieles, Dempsey ve Pillitteri, 2017, 21-24):

- Dolandırıcılık ve Hırsızlık Sistemleri: Geleneksel dolandırıcılık yöntemlerini "otomatikleştirerek" veya yeni yöntemler kullanarak, dolandırıcılık ve hırsızlık için kullanılabilir. Sistem sahtekarlığı ve hırsızlığı, içerdekiler (yani yetkili kullanıcılar) ve dışarıdakiler tarafından gerçekleştirilebilir. Yetkili sistem yöneticileri ve sisteme erişimi olan ve sisteme aşina olan kullanıcılar (örneğin, kontrol ettiği kaynaklar, kusurlar) genellikle dolandırıcılıktan sorumludur.

- İçeriden Bilgi Tehdidi: Çalışanlar, işverenin sistemlerine ve uygulamalarına aşinalıklarının yanı sıra hangi eylemlerin en fazla zarara veya düzensizliğe neden olabileceği göz önüne alındığında, bir kuruluşa yönelik içeriden bir tehdidi temsil edebilir.

- Kötü Amaçlı Hacker: Kötü niyetli bilgisayar korsanı, ağlara ve sistemlere yasa dışı olarak erişmek, hasara neden olmak veya bilgi çalmak için bir anlayış kullanan kişi veya grubu tanımlamak için kullanılan bir terimdir. Kötü niyetli bir bilgisayar korsanını harekete geçiren motivasyonu anlamak, bir kuruluşun sistem ihlali olasılığını önlemek için uygun güvenlik kontrollerini uygulamasına yardımcı olabilir.

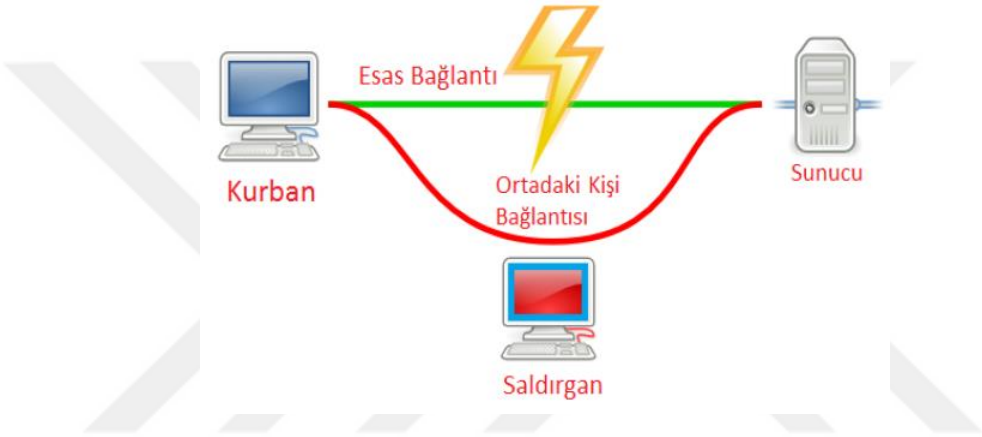
- Kötü Amaçlı Kod: Bir platforma saldırmak amacıyla oluşturulmuş virüsleri, Truva atlarını, solucanları, mantık bombalarını ve diğer tüm yazılımları ifade eder.

Sıralanan unsurlar, ağ güvenliği için tehditlerin ağın kendi içerisinden gelebileceği gibi dışarıdan gelebileceğini de göstermektedir. Bu durum, ağ güvenliği konusunda gelişen ağ teknolojisinin karşısında, teknik olarak tehdit şeklinde algılanabilecek tüm unsurların da sürecin içerisinde değerlendirilmesi gerektiğini göstermektedir. Özellikle de ağın kendi yapısı içerisinde bulunan unsurlar, güvenlik açısından son derece büyük bir önem arz etmektedir.

Başka bir açıdan bakıldığında, ağlara yönelik saldırıların popüler bir nitelik kazanmasıyla birlikte birçok kullanıcının kendi geliştirdikleri saldırı yöntemlerini

sıklıkla uygulamak sureti ile sistemlere, verilere ve bilgilere zarar verdikleri görülmektedir. Söz konusu yeni nesil sayılabilecek olan saldırıları aşağıdaki şekilde açıklamak mümkündür (Erol, 2019, 32-36):

- Ortadaki Kişi (Man In The Middle) Saldırısı: Şekil 6'da gösterildiği üzere, temelde Adress Resolution Protocol (ARP) aldatma saldırısının kullanıldığı bu yöntemde saldırgan, bulunduğu ağdaki hedef cihaz ile hedefin iletişimde bulunduğu başka bir cihaz arasındaki trafiği kendi üzerinden geçirir.



Şekil 6. Basit ölçekli ortadaki kişi saldırısı örneği (Erol, 2019, 32)

- Kaba Kuvvet (Brute Force) Saldırısı: Brute Force Attack olarak da bilinir ve Türkçe'ye Kaba Kuvvet Saldırıları olarak çevrilir. Kaba Kuvvet Saldırısı, kimlik doğrulamada kullanılan kullanıcı adı ve parola değerleri için alt ve üst sınırları belirli olacak şekilde karakter, uzunluk ve çeşitlerinin oluşturulup denenmesi ile yapılmaktadır.

- Sözlük (Dictionary) Saldırısı: Bu tür saldırılar önceden oluşturulmuş belirli bir listedeki tüm sözcüklerin denenmesi ile yapılır. Bu listeler genellikle GB'lar boyutunda olup daha önceden çalınmış veri tabanlarından çıkartılmış en çok kullanılan kullanıcı adı ve parola bilgilerini içerir.

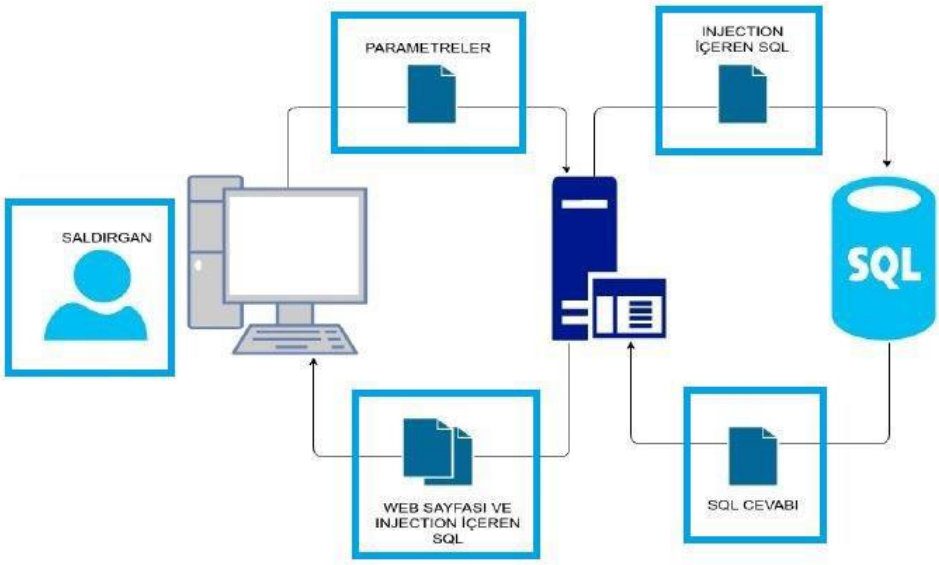
- Oltalama (Phishing) Saldırısı: Phishing yönteminde gönderilen e-posta içeriklerine görünürde gerçek bir kurumun ismi yazılmasına karşın

aslında verilen link gerçek sitenin birebir kopyası olan sahte tuzak sitedir.

- Kablosuz Ağ Saldırıları: Kullanıcıların Wi-Fi, kızılötesi, radyo frekansları gibi kablosuz erişim noktalarını kullanarak bir ağa bağlanması pratiklik ve kolaylık açısından tercih edilmektedir.

- DHCP Saldırısı: Saldırganın kaynak MAC adresini değiştirerek DHCP sunucusunun otomatik ataması için tanımlanmış bütün IP'leri kendisine alması ile gerçekleştirilen saldırıdır.

- SQL Injection Saldırısı: Şekil 7'de bir örneği gösterildiği üzere, kullanıcıdan (istemciden – client) alınan verilerin herhangi bir kontrolden geçmeden izinsiz olarak arka tarafta SQL sorgusuna manipüle edilip, belirli bir amaca yönelik uygulama da kullanılarak sonuçlar vermesini sağlayan bir zafiyet tipidir.



Şekil 7. SQL injection senaryosu

Kaynak: Erol, B. (2019). Ağ Trafik Özelliklerinin Analizini Yaparak Anormalliklerin Tespit Edilmesi (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Aydın Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

- Secure Sockets Layer (SSL Saldırıları): SSL, ağ üzerinden iletişim kuran client ve server arasındaki trafiği şifreleyerek güvenli bilgi alışverişini sağlayan ve default'ta 443 portunu kullanan bir güvenlik protokolüdür. Saldırılar, bu protokolün bozularak alternatif ve saldırganın istediği türden bir protokolün oluşturulmasına yöneliktir.

Sıralanan saldırılar, ağın içerisinde her gün gelişen teknolojilerin açıklarını bulmaya ve buna göre bir saldırı sistemi geliştirmeye yöneliktir. Özellikle de saldırıları gerçekleştiren tarafların kendi istedikleri şekilde ağın içerisine sızmak sureti ile geliştirdikleri yöntemler, ağ güvenliğinin sürekli olarak kontrolünü ve korunmasını zorunlu hale getirmektedir. Saldırıların geneline bakıldığında da saldırıları gerçekleştiren tarafların, süreci kendi isteklerine göre şekillendirmeye çalıştıkları ve ağ akışını saldırı fark edilene kadar kendileri için uygun hale getirmeye çalıştıkları görülmektedir. Bu durum beraberinde sistemin kontrolünün giderek zorlaşması sorununu getirmektedir. Bir kez ağın içerisinde kendisine hareket alanı ve veri ile bilgi toplama imkânı bulan saldırgan taraf, sistemin açıklarını kolaylıkla öğrenmekte ve sürdürülebilir ağ atakları gerçekleştirmektedir.

2.3. Ağ Güvenliğini Tehdit Eden Saldırılarda Kullanıcı Faktörü

Ağ güvenliğini tehdit eden saldırılarda, ağın tasarlanma şekli kadar ağın kullanılma şekli de büyük bir öneme sahiptir. Özellikle de ağın kullanımı süre zarfında kullanıcıların, güvenlik açığına sebebiyet verebilecek unsurları bilgisayarlarında kullanmaları ve birbirlerine transfer etmeleri; bunun da ötesinde, ağın güvenlik kontrolünün 24 saat boyunca sağlanmaması, sistemin işleyişine önemli ölçüde zarar vermektedir.

Genel olarak ele alındığında ağ güvenliğini tehdit eden saldırılarda kullanıcı faktörüne dair unsurlar şu şekilde ele alınmaktadır (Stallings, 2011, 13-14):

- Gizlilik, kimlik doğrulama, reddedilme ve bütünlük konuları karmaşık olmakla birlikte ağı aktif olarak kullananların konuya dair yeterli bilgi ve fikrinin olmaması sürecin geleceğini tehdit etmektedir.

- Ağ tasarımcıları, belirli bir güvenlik mekanizması veya algoritması geliştirirken, bu güvenlik özelliklerine yönelik olası saldırılar her zaman göz önünde bulundurulmalıdır. Çoğu durumda başarılı saldırılar soruna tamamen farklı bir şekilde bakılarak tasarlanır ve bu nedenle mekanizmadaki beklenmedik bir zayıflıktan yararlanılır.

- Belirli hizmetleri sağlamak için kullanılan prosedürler çoğu zaman mantığa aykırıdır. Tipik olarak bir güvenlik mekanizması karmaşıktır. Ayrıntılı güvenlik mekanizmaları ancak tehdidin çeşitli yönleri düşünüldüğünde anlam kazanır.

- Tasarımcılar çeşitli güvenlik mekanizmaları tasarladıktan sonra, bunların nerede kullanılacağına karar vermek zorundadırlar. Bu hem fiziksel yerleştirme açısından hem de mantıksal bir anlamda gereklilik arz eden bir durumdur.

- Güvenlik mekanizmaları tipik olarak belirli bir algoritma veya protokolden fazlasını içerir. Ayrıca katılımcıların bazı gizli bilgilere (örneğin, bir şifreleme anahtarı) sahip olmalarını da gerektirir. Fakat bu konuda kullanıcıların dikkat eksikliği ve doğru şekilde odaklanmamaları, gizli bilgilerin oluşturulması, dağıtılması ve korunması hakkında sorunları gündeme getirmektedir.

- Bilgisayar ve ağ güvenliği, esasen, boşlukları bulmaya çalışan bir fail ile bunları kapatmaya çalışan tasarımcı veya yönetici arasındaki bir fikir savaşıdır. Saldırganın sahip olduğu en büyük avantaj, tasarımcının mükemmel güvenliği elde etmek için tüm zayıflıkları bulup ortadan kaldırması gerekirken, kullanıcıların hataları ile yalnızca tek bir zayıflığı bulması gerektiğidir.

- Kullanıcıların ve sistem yöneticilerinin, bir güvenlik arızası meydana gelene kadar güvenlik yatırımından çok az fayda sağlamalarına yönelik doğal bir eğilim vardır ki bu güvenlik algısının sürdürülebilir olmasına engeldir.

- Güvenlik, düzenli hatta sürekli izleme gerektirmektedir fakat maliyetler nedeni ile kurumların bundan uzak durmaları süreci daha tehlikeli hale getirmektedir.

- Güvenlik, tasarım sürecinin ayrılmaz bir parçası olmaktan ziyade, tasarım tamamlandıktan sonra canlı tutulması gerektiği halde, bireysel ihmaller sürecin başa dönmesine ve daha maliyetli güvenlik uygulamalarının ortaya çıkmasına neden olmaktadır.

- Birçok kullanıcı ve hatta güvenlik yöneticisi, güçlü güvenliği bir bilgi sisteminin verimli ve kullanıcı dostu çalışmasına veya bilgi kullanımına bir engel olarak görmektedir.

Sıralanan kullanıcı hatalarına dayalı unsurlar sistemin kusursuz şekilde inşa edilmesine karşın, herhangi bir saldırı için uygun zemin yaratılmasını sağladığı gibi aynı zamanda, ağın kontrolü konusunda da bariz sorunlar yaratmaktadır.

Bu şekilde ağ inşa eden ve kullanan taraflar arasında, ağın sağlıklı bir biçimde kullanılması konusunda bir ortak noktanın sağlanması gerektiği konusunda eylem birliğine ihtiyaç duyulduğu görülmektedir. Özellikle de basit kullanıcıların ağı kullanımları süre zarfında, herhangi bir saldırıya sebebiyet verecek şekilde e-posta, USB, yan uygulama vb. unsurları kullanmaları ağın yeniden tasarlanmasına sebebiyet verecektir ki bu süre zarfında yaşanan saldırılar, ağın sahibi olan tarafa teknik, mali yönetimsel anlamda zarar verebilecektir.

ÜÇÜNCÜ BÖLÜM
ARAŞTIRMA VE BULGULAR

3.1. Araştırma

3.1.1. Araştırma Modeli

Araştırmada, Türkiye'deki özel sektör şirketlerinin, ağ güvenliği alanında yapılan çalışmalara dair yetkili bireylerin konu hakkındaki düşüncelerini, uygulamalarını öğrenebilmek ve katılımcıların şirketlerinde uygulanan sistemlerde hangi yöntemlerin benimsendiği hususunda fikir edinebilmek amacı ile tarama araştırma modeli tercih edilmiştir.

Tarama modelinde katılımcıların yetenekleri, tercihleri, davranışları veya fiziksel ortamların özellikleri tanımlanır. Tarama araştırmalarının üç temel özelliği bulunmaktadır (Büyüköztürk, Çakmak ve Akgün 2010).

- Araştırılan konuya ilişkin katılımcıların görüşlerinin ya da özelliklerinin (bilgi, beceri, kaygı, ilgi, vb.) betimlenmesi için, topluluğu temsil edebilecek insanlardan oluşan bir parça seçilir (Evrenden örneklemin seçilmesi).

- Araştırma için ihtiyaç duyulan verileri toplama süreci, veri kaynakları olan kişilere yöneltilen sorulara verilen cevaplara dayalıdır.

- Veriler, özelliği betimlenecek topluluğun her bireyinden değil, bu topluluğu temsil eden bir parçasından yani örneklemden toplanır.

Tarama modeli nesnelerin, toplumların, kurumların, olayların doğasını ve özelliklerini tanımlamayı, geçmişte veya halen var olan durumlarını var olduğu şekilde betimlemeyi hedeflemektedir. Tarama modelleri araştırma konusuna ilişkin verilerin toplanması, sınıflandırılıp düzenlenmesi ve çözümlenmesi süreçlerinden oluşur. Bu modelde, araştırmaya katılan bireylerin görüşleri herhangi bir değiştirme çabası içinde bulunulmadan kendi ortamlarında tanımlanmaya çalışılır (Karasar 2012).

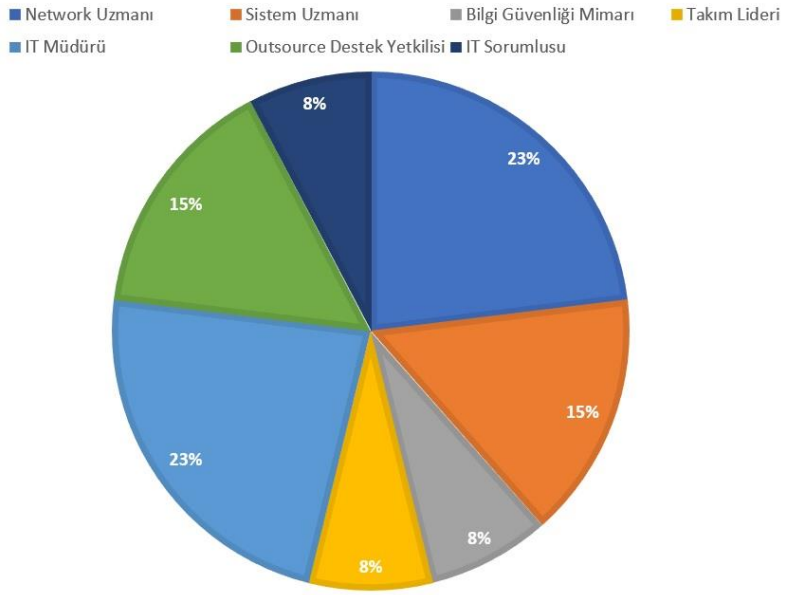
3.1.2. Araştırma- Çalışma Grubu

Araştırma için Türkiye'de, özel sektöre hizmet veren ve farklı alanlarda faaliyetleri bulunan şirketlerin BT departmanlarında görevli, sorumlu ve müdür olan bireyler araştırma grubunun birer parçası olarak belirlenmiştir. Araştırma grubuna mensup bireylerin bağlı bulundukları kurumların sektörel dağılımı ve katılımcıların kurumlarındaki görevlerinin dağılımı aşağıda, Tablo 1'de verilmiştir.

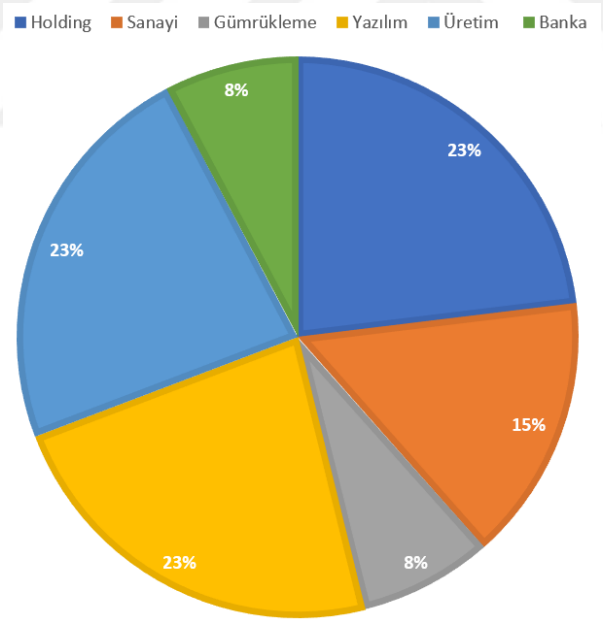
Tablo 1. Katılımcıların sektörel bazda ve kurumlarındaki görevlerinin durumuna göre dağılımı

Sektör	Pozisyon	Kurumlarında geçirdikleri süre (Yıl)	Alanlarında geçirdikleri süre (Yıl)
Banka	Network Uzmanı	2	17
Gümrük / Taşımacılık	Sistem Uzmanı	1	12
Holding 1	Network Uzmanı	7	15
Holding 2	Kıdemli Bilgi Güvenliği Mimarı	10	20
Holding 3	Güvenlik Operasyonları Takım Lideri	2	6
Sanayi 1	Sistem Uzmanı	3	7
Sanayi 2	IT Müdürü	6	9
Üretim 1	IT Müdürü	3	8
Üretim 2	IT Sorumlusu	6	9
Üretim 3	Outsource destek veren firma yetkilisi	4	9
Yazılım 1	IT Müdürü	6	14
Yazılım 2	Outsource destek veren firma yetkilisi	4	12
Yazılım 3	Network Uzmanı	3	8

Tablo 1'de yer alan dağılıma bakıldığında, katılımcıların, alanlarında uzman ve üst düzey yetkililer olduğu görülmektedir. Özellikle de katılımcıların, çok uzun yıllardır bu alanda hizmet veriyor olmaları ve kurumlarında uzun yıllardır yer almaları, araştırmaya olan katkıları açısından da son derece önemlidir. Şekil 8 ve 9'da katılımcıların sektörel bazda ve kurumlarındaki görevlerinin durumuna göre ve sektörel duruma yüzdelik dağılımı yer almaktadır.



Şekil 8. Katılımcıların kurumlarındaki görevlerinin yüzdesel dağılımı



Şekil 9. Katılımcıların kurumlarının sektörel olarak yüzdesel dağılımı

3.1.3. Veri Toplama Aracı

Ağ güvenliği konusunda yetkili olan çalışanın görüşlerinin neler olduğunu belirlemek amacıyla "Bilgisayar Ağ Güvenliği Analizi" isimli form hazırlanmıştır. Görüşleri belirlemek amacıyla kullanılan formda aşağıdaki sorular yer almıştır;

1. Çalışanı olduğunuz şirkette Firewall kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?

2. Çalışanı olduğunuz şirkette WAF kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?

3. Çalışanı olduğunuz şirkette SIEM kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?

4. Çalışanı olduğunuz şirkette DLP kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?

5. Çalışanı olduğunuz şirkette Antivirüs kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?

6. Çalışanı olduğunuz şirkette ağ ve veri güvenliği için yapılan ekstra çalışmalar var mıdır? Var ise bunlar ne tür çalışmalardır?

7. Çalışanı olduğunuz şirkette ne kadar sıklıkta Penetraston Testi yapılmaktadır/yaptırılmaktadır?

8. Çalışanı olduğunuz şirkette ne kadar sıklıkta LAN ve WAN atak testleri yapılmaktadır/yaptırılmaktadır?

9. Çalışanı olduğunuz şirkette ağ ve veri güvenliği ile alakalı herhangi bir zaafiyetle karşılaşıldı mı? Karşılaşıldı ise bu zaafiyetler nelerdir?

10. Çalışanı olduğunuz şirkette dosya yedekleri ne kadar sıklıkta alınmaktadır?

11. Çalışanı olduğunuz şirkette kullanıcı hatalarına karşı şirket içi eğitim verilmekte midir?

12. Çalışanı olduğunuz şirkette ne kadar sıklıkta sosyal mühendislik (şirket içi çalışan farkındalığı) testleri yapılmaktadır?

13. Çalışanı olduğunuz şirketin BT departmanlarında çalışanların güvenlik eğitimi alınması sağlanmakta mıdır?

14. Çalışanı olduğunuz şirketin BT güvenliği için yıllık ayırdığı bütçe hangi aralıktadır?

15. Çalışanı olduğunuz şirketin ayrı bir güvenlik departmanı bulunmakta mıdır? Bulunmuyor ise güvenlik ile ilgili çalışan kişiler da BT departmanı dahilinde mi çalışmaktadır?

3.1.4. Verilerin Analizi

Nitel yöntemle yapılan araştırmalarda kullanılan bilgi toplama teknikleri sonucunda elde edilen bilgiler veriye dönüştürüldükten sonra verilerin çözümlenmesi için iki genel yöntem kullanılabilir. Birinci yöntem; derinlemesine analiz gerektirmeyen ve verilerin incelenmesinde kullanılan betimsel analizdir. İkinci yöntem ise elde edilen verileri daha yakından incelemeyi ve bu verileri açıklayan kavram ve temalara ulaşmayı gerektiren içerik analizidir (Altındağ, 2005).

Röportaj yoluyla elde edilen verileri analiz edebilmek için aşağıdaki adımlar takip edilmiştir:

1. Görüşler konu ile ilgili soruları içeren çevrimiçi röportaj ile toplanmıştır.

2. Röportajdaki sorulara verilen cevaplar benzerliklerine göre kategorize edilmiştir.

3. Her bir soru için belirlenen kategoriler gözden geçirilip tekrarlar giderilerek, birbirine yakın ve benzer kategoriler birleştirilmiştir.

4. Her bir soru için oluşturulan kategoriler, içerikleri dikkate alınarak belli ana başlıklar altında toplanmıştır.

5. Katılımcıların kategorilere ilişkin görüşleri frekans ve yüzde olarak görselleştirilmiştir.

Kurumlarında ağ güvenliği konusunda sorumlu yetkililerin "Bilgisayar Ağ Güvenliği Analizi"ne dair görüşlerini belirlemek amacıyla yapılan röportaj vasıtasıyla elde edilen verileri betimlemek için içerik analizi yöntemi kullanılmıştır.

3.2. Bulgular

3.2.1. Firewall Kullanımı

Görüşmelerin ilk sorusunda, katılımcılara, şirketlerinde firewall kullanımları ile ilgili durumları sorulmuştur.

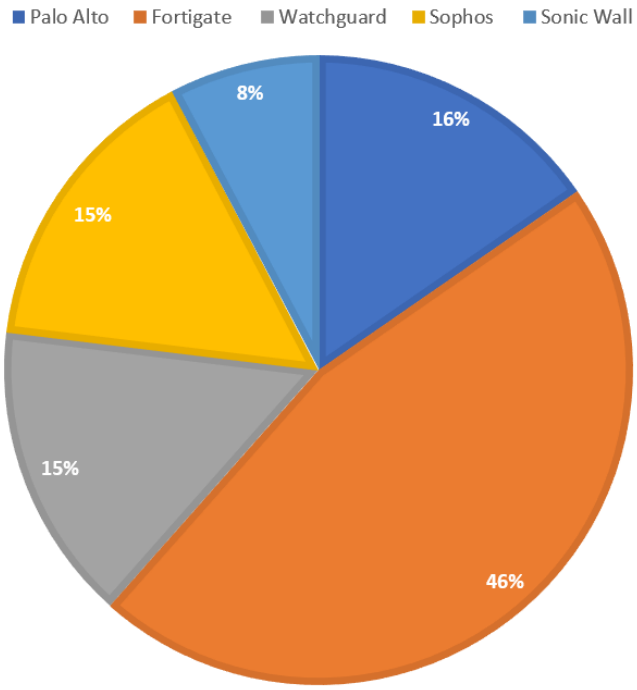
Tablo 2. Katılımcıların şirketlerinde kullanılan firewall markaları

FIREWALL						
Şirket Sayısı	**Sektör**	Fortigate	Palo Alto	Watchguard	Sonicwall	Sophos
3	Holding	1	2			
3	Üretim/İmalat			1	1	1
1	Banka	1				
3	Yazılım	2		1		
2	Sanayi	1				1
1	Taşımacılık	1				

Tablo 2'de gösterildiği üzere firewall kullanımı, katılımcıların hepsinin bağlı bulunduğu şirket için vazgeçilmez konumda olan bir unsurdur. Katılımcılar, şirketlerinde kullanılan firewall ile ilgili bilgi verirken konuya verdikleri önemi çok

boyutlu olarak açıklamaya çalışmışlardır. Şirketler genel olarak Palo Alto, Fortigate, Watchguard, Sonicwall ve Sophos markalarını tercih etmektedirler.

Sadece bir katılımcı, aynı anda, farklı firewall programlarından faydalandıklarını dile getirmiştir. Nihai noktada, tüm katılımcıların şirketleri, en az bir firewall kullanımı konusunda gereken uygulamaları gerçekleştirmekle birlikte gereken bütçeleri de ayırmışlardır. Şekil 10'da, katılımcıların şirketlerinde kullanılan firewall markalarının yüzdelik dağılımı yer almaktadır.



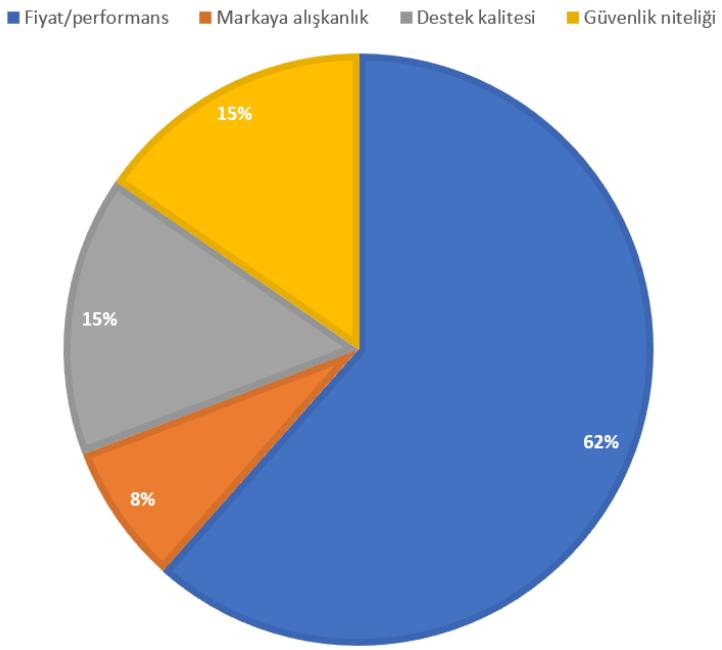
Şekil 10. Katılımcıların şirketlerinde kullanılan firewall markalarının yüzdelik dağılımı

Tablo 3. Şirketlerin sektör bazlı olarak firewall tercih sebepleri

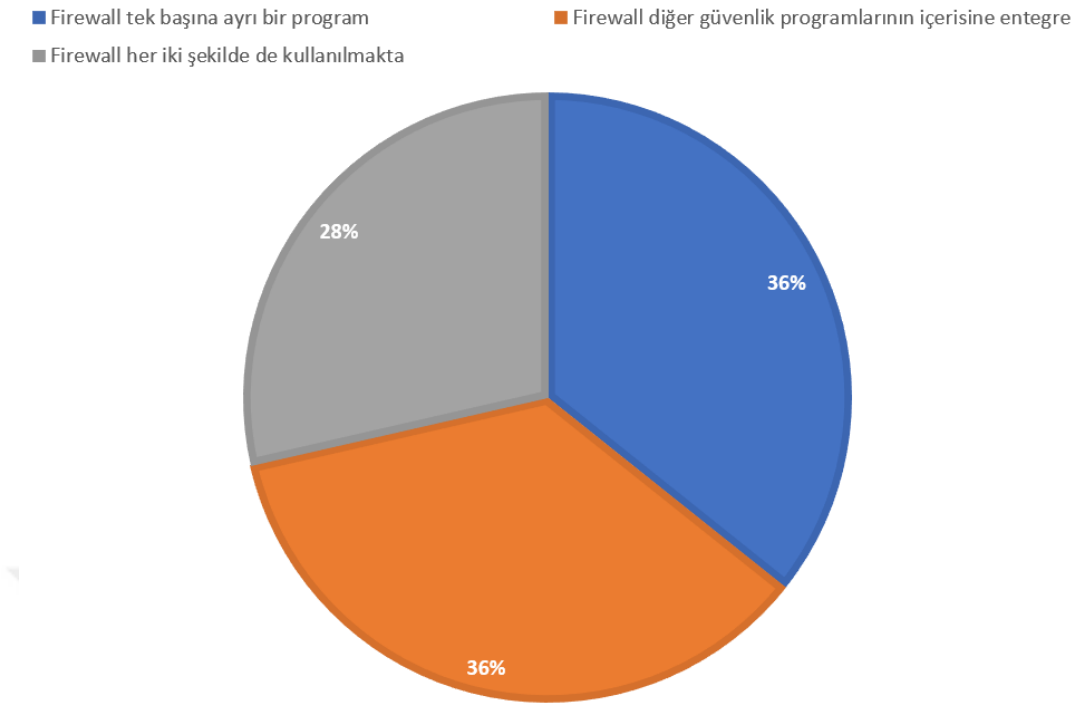
FIREWALL Tercih Sebepleri					
Şirket Sayısı	**Sektör**	Fiyat/Performans	Destek Kalitesi	Güvenlik Niteliği	Markaya Alışkanlık
3	Holding	1		2	
3	Üretim/İmalat	1	1		1
1	Banka	1			
3	Yazılım	3			
2	Sanayi	1	1		
1	Taşımacılık	1			

Tablo 3'te gösterilen dağılımda, firewall tercih nedenleri açısından ele alındığında ise fiyat performans etkisi başta olmak üzere güvenlik niteliği destek kalitesi ve markaya alışkanlık için yeterlilik unsurları ön plana çıkmaktadır. Bunun yanı sıra alışkanlık ve fiyatının uygun olması konuları da ön plana çıkmaktadır.

Aynı zamanda katılımcılar, mevcut kullandıkları firewall programlarını daha önceki süreçte de kullanmış olmaları nedeni ile firewall programlarını çok fazla değiştirmeye ihtiyaç duymamaktadırlar. Mevcut, alışık oldukları görünüm ve güvenlik tatmini sürecin devamlılığı açısından bir kriter olmaktadır. Şekil 11'de şirketlerin sektör bazlı olarak firewall tercih sebeplerinin yüzdelik dağılımı yer almaktadır.



Şekil 11. Şirketlerin sektör bazlı olarak firewall tercih sebeplerinin yüzdelik dağılımı



Şekil 12. Katılımcıların şirketlerinde firewall programının kullanılış şeklinin yüzdelik dağılımı

Şekil 12 üzerinde gösterilen yüzdelik dağılımlarda katılımcıların firewall programlarını kullanım tercihleri yer almaktadır. Bazı şirketler için firewall için ayrı bir uygulama tercih edilirken, bazı şirketler için firewall programlarının diğer güvenlik programlarının içerisine entegre olduğu görülmektedir. Diğer şirketler ise farklı biçimlerde firewall programlarının kullanımına odaklanmaktadırlar ki burada maliyet ve güvenlik konusundaki beklentiler, firewall kullanımı açısından belirleyici olarak değerlendirilebilecektir.

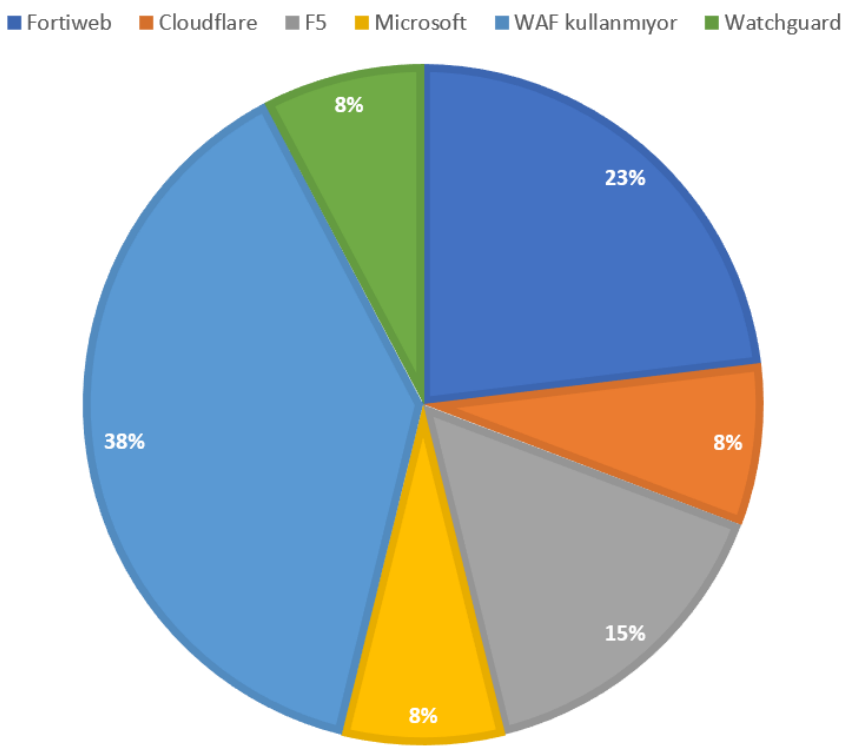
3.2.2. WAF Kullanımı

Görüşmelerin ikinci sorusunda katılımcılara şirketlerinde WAF kullanımları ile ilgili durumları sorulmuştur.

Tablo 4. Şirketlerin sektör bazlı olarak kullandıkları WAF markaları

WAF						
Şirket Sayısı	**Sektör**	Fortiweb	Microsoft	F5	Watchguard	Cloudflare
3	Holding		1	1		
3	Üretim/İmalat			1	1	
1	Banka	1				
3	Yazılım	1				
2	Sanayi	1				
1	Taşımacılık					1

Tablo 4'te yer alan ve kullanıcılardan elde edilen bilgilere göre WAF kullanımı konusunda büyük bir ilgi ve eğilimin olmadığı, çoğunlukla firewall ve diğer güvenlik sistemleri ile birlikte gelen yan uygulamalar aracılığıyla WAF kullanımı gerçekleştirildiği görülmektedir. Beş katılımcının şirketinde WAF kullanılmadığı tespit edilmiştir. WAF tercih eden şirketlerde, Fortiweb, F5, Watchguard, Cloudflare ve Microsoft uygulamalarının ön plana çıktığı görülmektedir. Şekil 13'te şirketlerin sektör bazlı olarak kullandıkları WAF markalarının yüzdelik dağılımı yer almaktadır.



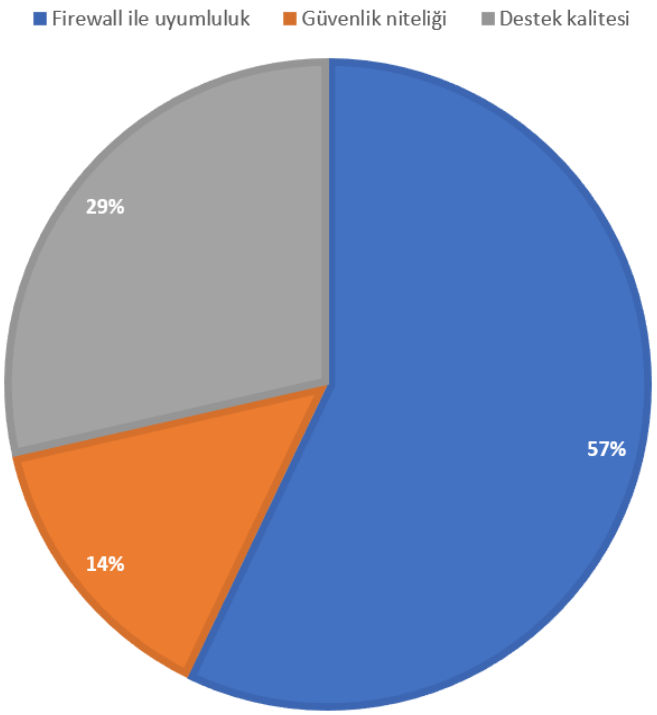
Şekil 13. Şirketlerin sektör bazlı olarak kullandıkları WAF markalarının yüzdelik dağılımı

Tablo 5. Şirketlerin sektör bazlı olarak WAF tercih sebepleri

WAF Tercih Sebepleri				
Şirket Sayısı	**Sektör**	Firewall ile Uyumluluk	Destek Kalitesi	Güvenlik Niteliği
3	Holding			2
3	Üretim/İmalat	1	1	
1	Banka	1		
3	Yazılım	1		
2	Sanayi	1		
1	Taşımacılık		1	

Öte yandan Tablo 5'te yer aldığı üzere, WAF kullanan şirketlerde program sahibi olan şirketin desteği ve güncelleme konusunun sürdürülebilir olması ve güvenlik seviyesinin yüksekliğine duyulan güven hissiyatı önemli tercih nedenlerinden olmaktadır.

WAF kullanan şirketler sistematik olarak ihtiyaç duyduklarını düşündüklerinden dolayı bu ürüne yönelirken, buna sektörel ve operasyonel olarak ihtiyaç duymadığını düşünen şirketler üründen faydalanma eğiliminde olmamaktadırlar. Şekil 14'te şirketlerin sektör bazlı olarak WAF tercih sebeplerinin yüzdelik dağılımı yer almaktadır.



Şekil 14. Şirketlerin sektör bazlı olarak WAF tercih sebeplerinin yüzdelik dağılımı

3.2.3. SIEM Kullanımı

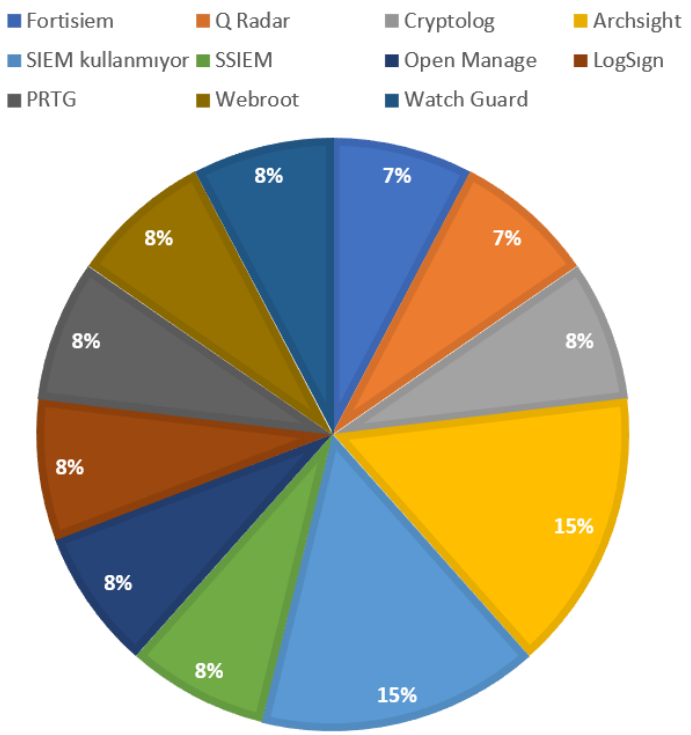
Görüşmelerin üçüncü sorusunda, katılımcılara, şirketlerinde, SIEM kullanımları ile ilgili durumları sorulmuştur.

Tablo 6. Katılımcıların şirketlerinde kullanılan SIEM markaları

SIEM											
Şirket Sayısı	**Sektör**	Fortisiem	Qradar	Archsight	SSIEM	Watchguard	Open Manage	Log Sıgn	PRTG	Cryptolog	Webroot
3	Holding		1	1	1						
3	Üretim/İmalat					1	1				1
1	Banka			1							
3	Yazılım							1	1		
2	Sanayi	1									
1	Taşımacılık									1	

Tablo 6'da yer alan ve kullanıcılardan elde edilen bilgilere göre SIEM kullanımı konusunda, birbirinden farklı çok sayıda markanın tercih edildiği

görülmektedir. Katılımcılar şirketlerinde kendilerinin bildiği ve alışık oldukları markaları daha fazla tercih etmektedirler. Şekil 15'te katılımcıların şirketlerinde kullanılan SIEM markalarının yüzdelik dağılımı yer almaktadır.



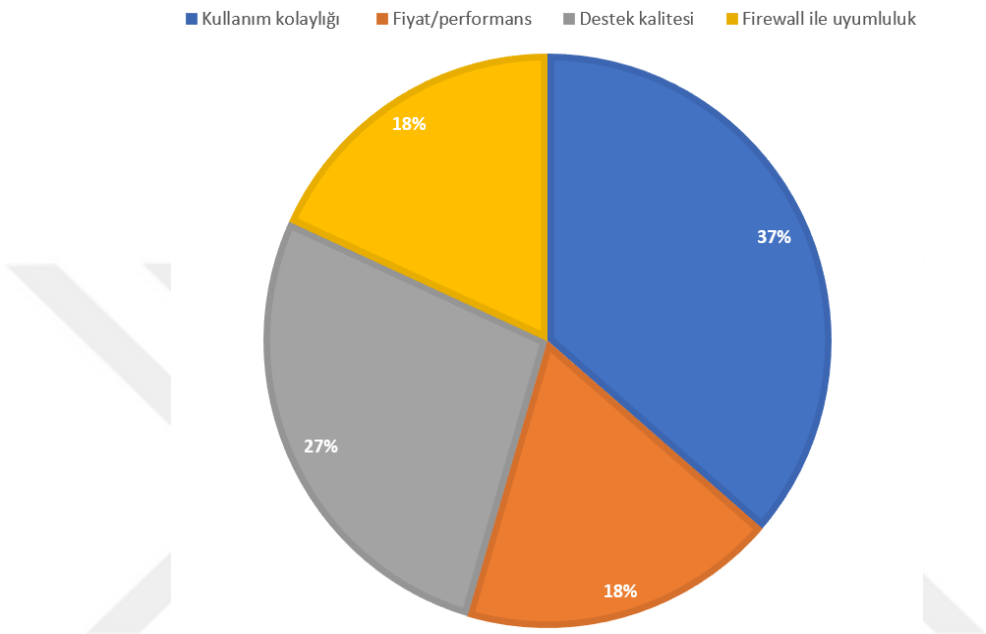
Şekil 15. Katılımcıların şirketlerinde kullanılan SIEM markalarının yüzdelik dağılımı

Tablo 7. Şirketlerin sektör bazlı olarak SIEM tercih sebepleri

SIEM Tercih Sebepleri					
Şirket Sayısı	**Sektör**	Fiyat/Performans	Firewall ile Uyumluluk	Destek Kalitesi	Kullanım Kolaylığı
3	Holding			2	1
3	Üretim/İmalat	1	1		1
1	Banka			1	
3	Yazılım	1			1
2	Sanayi		1		
1	Taşımacılık				1

Öte yandan, Tablo 7'de gösterildiği şekli ile SIEM kullanan şirketlerde, fiyat performans, destek kalitesi ve güncelleme konusunun sürdürülebilir olması, kolaylığı

ve firewall ile uyumluluk önemli tercih nedenlerinden olmaktadır. SIEM kullanan şirketler, sistematik olarak ihtiyaç duyduklarını düşündüklerinden dolayı bu ürüne yönelirken, buna sektörel ve operasyonel olarak ihtiyaç duymadığını düşünen şirketler, üründen faydalanma eğiliminde olmamaktadırlar. Şekil 16'da şirketlerin sektör bazlı olarak SIEM tercih sebeplerinin yüzdelik dağılımı yer almaktadır.



Şekil 16. Şirketlerin sektör bazlı olarak SIEM tercih sebeplerinin yüzdelik dağılımı

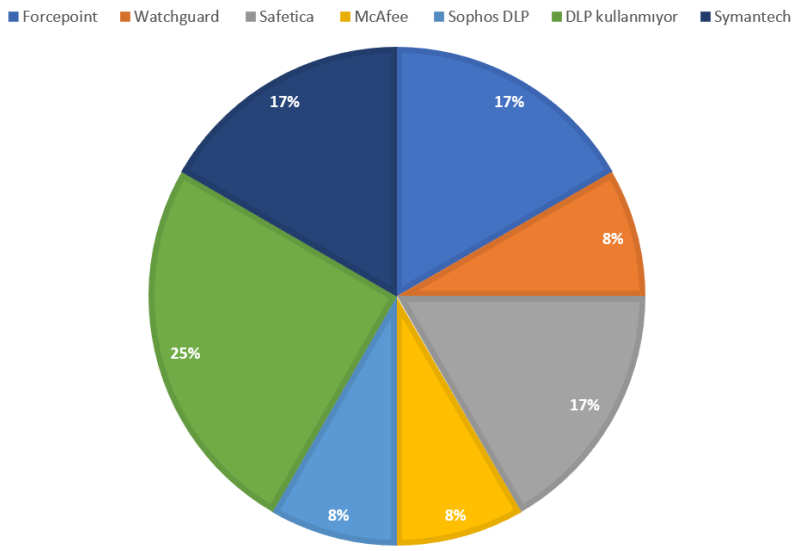
3.2.4. DLP Kullanımı

Görüşmelerin dördüncü sorusunda, katılımcılara, şirketlerinde, DLP kullanımları ile ilgili durumları sorulmuştur.

Tablo 8. Katılımcıların şirketlerinde kullanılan DLP markaları

DLP								
Şirket Sayısı	**Sektör**	Forcepoint	Symantech	Watchguard	Safetica	McAfee	Sophos DLP	Webroot
3	Holding	1	1					
3	Üretim/İmalat			1				1
1	Banka	1						
3	Yazılım				1		1	
2	Sanayi		1			1		
1	Taşımacılık				1			

Tablo 8'deki dağılım ekseninde, kullanıcıların belirttikleri hususlara göre DLP kullanımını önemsedikleri ve sistemi gerek kendileri tasarlamak gerekse de dışarıdan destek almak sureti ile yönlendirmeye ve kontrol etmeye çalıştıkları görülmektedir. Bu şekilde katılımcılar, birbirilerinden farklı markaları uzun süredir alışık oldukları sistemler dahilinde kullanmaktadırlar. Şekil 17'de katılımcıların şirketlerinde kullanılan DLP markalarının yüzdelik dağılımı yer almaktadır.



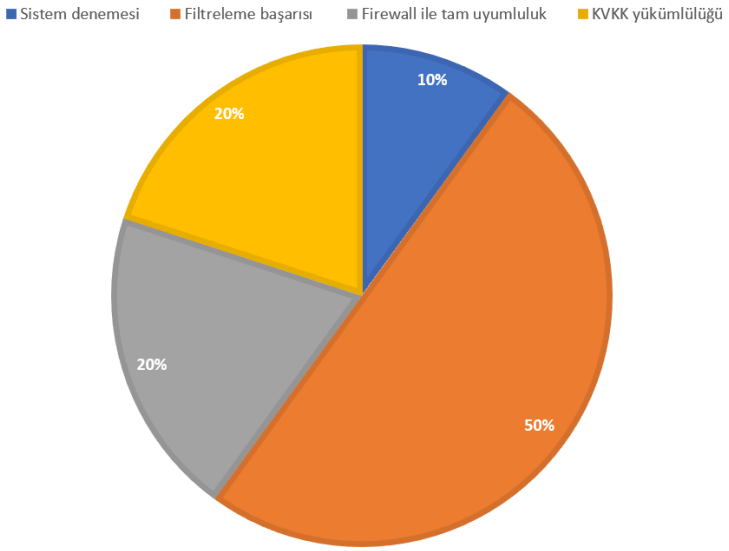
Şekil 17. Katılımcıların şirketlerinde kullanılan DLP markalarının yüzdelik dağılımı

Tablo 9. Şirketlerin sektör bazlı olarak DLP tercih sebepleri

DLP Tercih Sebepleri					
Şirket Sayısı	**Sektör**	Sistem denemesi	Firewall ile Tam Uyumluluk	KVKK Yükümlülüğü	Filtreleme Başarısı
3	Holding			2	
3	Üretim/İmalat		1		1
1	Banka		1		
3	Yazılım	1			1
2	Sanayi				2
1	Taşımacılık				1

Tablo 9'da yer alan, şirketlerin kullanım tercihlerini etkileyen unsurlar arasında, DLP konusundaki tercihlerinde sistemin denenmesi, firewall ile uyumluluk, Kişisel Verilerin Korunumu Kanunu (KVKK) yükümlülüğü ile oluşan zorunluluklar ve filtreleme konusundaki başarısı ön plana çıkmaktadır.

Bunun dışında katılımcıların şirketleri, DLP konusunda kendilerine destek sağlayacak olan tarafların yaklaşımlarının, ilgilerinin ve bu alandaki tecrübelerinin önemli olduğunu düşünmektedirler. Bu nedenle de tercihlerini bu doğrultuda gerçekleştirmektedirler. Şekil 18'de şirketlerin sektör bazlı olarak DLP tercih sebeplerinin yüzdelik dağılımı yer almaktadır.



Şekil 18. Şirketlerin sektör bazlı olarak DLP tercih sebeplerinin yüzdelik dağılımı

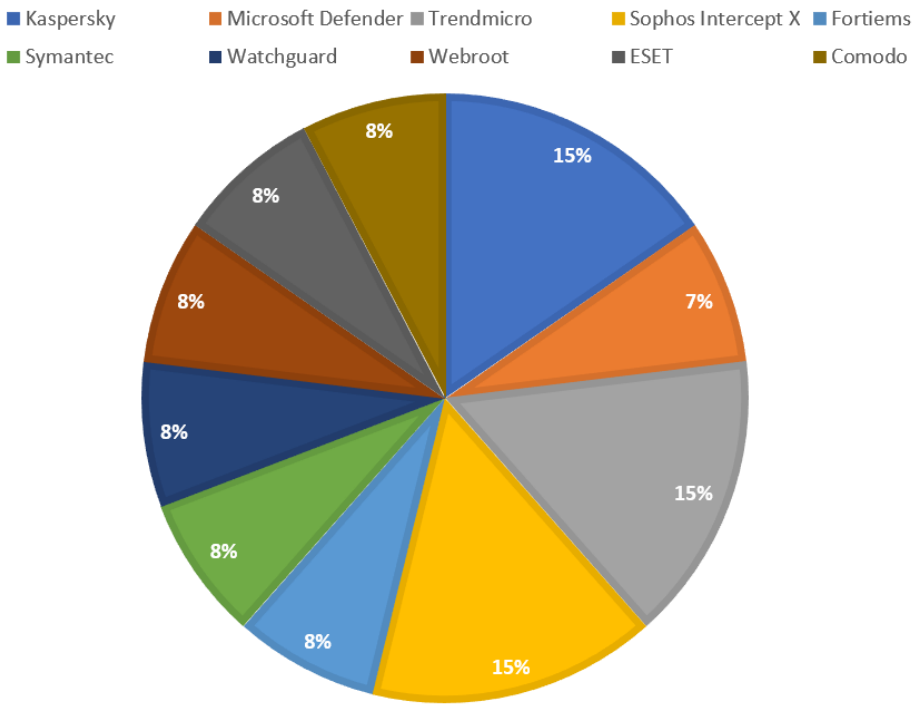
3.2.5. Antivirüs Programı Kullanımı

Görüşmelerin beşinci sorusunda, katılımcılara şirketlerinde antivirüs programı kullanımları ile ilgili durumları sorulmuştur.

Tablo 10. Katılımcıların kullandıkları antivirüs programı markaları

Antivirüs Programları											
Şirket Sayısı	**Sektör**	Fortiems	Microsoft Defender	Symantech	Kaspersky	Watchguard	Trendmicro	Comodo	ESET	Sophos Intercept	Webroot
3	Holding		1	1	1						
3	Üretim/İmalat				1	1					1
1	Banka						1				
3	Yazılım							1	1	1	
2	Sanayi	1								1	
1	Taşımacılık						1				

Tablo 10'da yer alan görüntüde, antivirüs sistemlerinin kullanımı konusunda katılımcılar, şirketlerinin bilindik markalar, iş ortakları ve alışkanlıkları ekseninde karar vererek sistemlerine entegre ettiklerini belirtmektedirler. Şirketler, birbirinden farklı markaları özellikle kullanım alışkanlıkları doğrultusunda seçmektedirler. Şekil 19'da katılımcıların kullandıkları antivirüs programı markalarının yüzdelik dağılımı yer almaktadır.



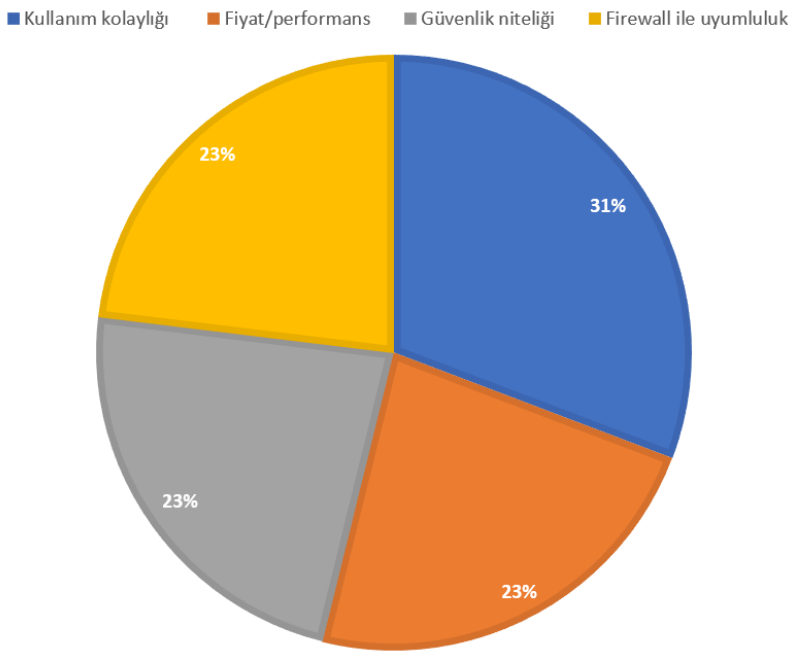
Şekil 19. Katılımcıların kullandıkları antivirüs programı markalarının yüzdelik dağılımı

Tablo 11. Şirketlerin sektör bazlı olarak antivirüs tercih sebepleri

Antivirüs Tercih Sebepleri					
Şirket Sayısı	**Sektör**	Fiyat/Performans	Firewall ile Tam Uyumluluk	Güvenlik Niteliği	Kullanım Kolaylığı
3	Holding	1		1	1
3	Üretim/İmalat		1	1	1
1	Banka				1
3	Yazılım	2		1	
2	Sanayi		2		
1	Taşımacılık				1

Tablo 11'de gösterildiği üzere, güncelleme niteliği, güvenlik düzeyinin yüksekliği, kullanım kolaylığı, fiyat/performans ve firewall ile tam uyumluluk, katılımcıların şirketlerinin antivirüs sistemi seçerken en fazla dikkat ettikleri unsurlardandır. Katılımcıların şirketleri açısından, ortak olarak antivirüs markalarının maliyetleri önemli bir husus olmaktadır.

Lisanslama konusu nedeni ile artan fiyatlar, katılımcıların bağlı bulundukları şirketlerin finansal anlamda süreci çok boyutlu olarak değerlendirmelerini zorunlu kılmaktadır. Fakat buna karşın üç şirket fiyat ekseninde performansı; iki şirket güvenlik kalitesini; iki şirket ise kullanım kolaylığını ön plana çıkarmaktadırlar. Şekil 20'de şirketlerin sektör bazlı olarak antivirüs tercih sebeplerinin yüzdelik dağılımı yer almaktadır.



Şekil 20. Şirketlerin sektör bazlı olarak antivirüs tercih sebeplerinin yüzdelik dağılımı

3.2.6. Ağ ve Veri Güvenliği İçin Yapılan Ekstra Çalışmalar

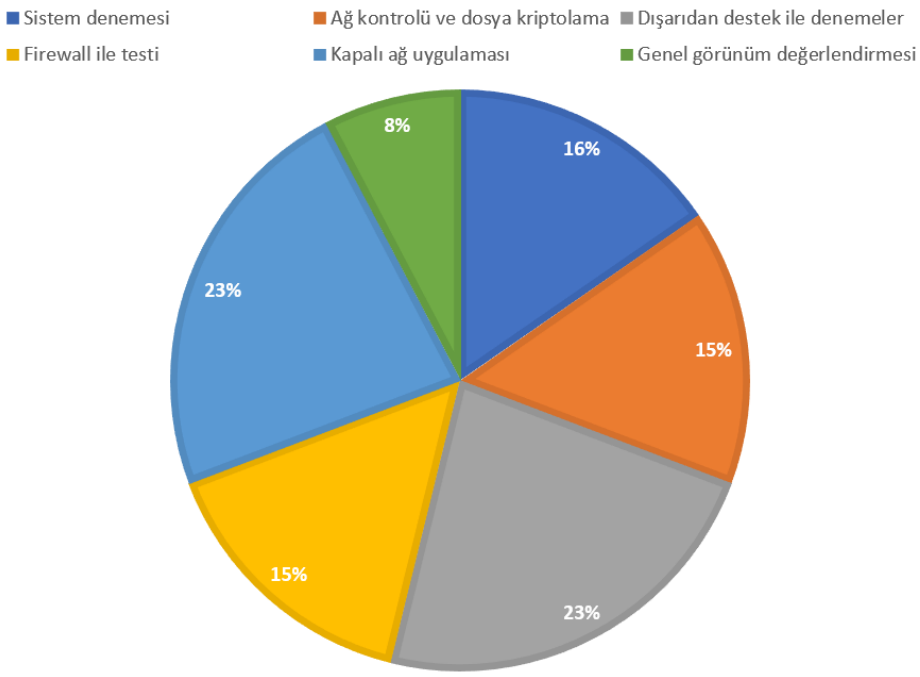
Görüşmelerin altıncı sorusunda, katılımcılara şirketlerinde ağ ve veri güvenliği için yapılan ekstra çalışmalar ile ilgili durumları sorulmuştur.

Tablo 12. Şirketlere göre ağ ve veri güvenliği için yapılan ekstra çalışmalar

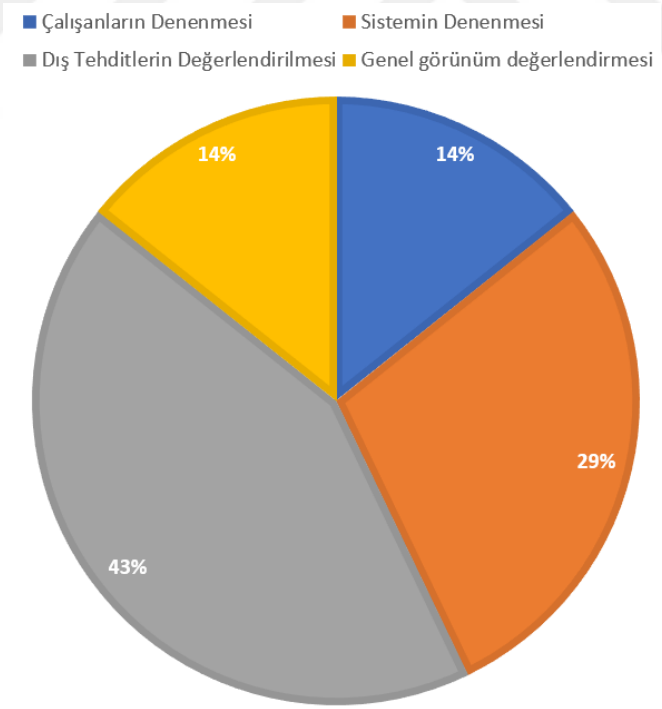
		Faaliyetler					
Şirket Sayısı	**Sektör**	Sistem denemesi	Ağ kontrolü ve dosya kriptolama	Dışarıdan destek ile denemeler	Firewall ile test	Kapalı ağ uygulaması	Genel görünüm değerlendirmesi
3	Holding			2		1	
3	Üretim/İmalat	1	1				1
1	Banka		1				
3	Yazılım	1		1	1		
2	Sanayi					2	
1	Taşımacılık				1		

Tablo 12'deki dağılıma göre katılımcılar, şirketlerinin ihtiyaçlarına göre faaliyetler yürütmeye çalışmaktadırlar. Şirketler açısından ön plana çıkan hususlar, düzenli olarak ağ kontrolü ve dosya kriptolama gerçekleştirilmesi; dışarıdan destek almak sureti ile şirketin sisteminin ihtiyaçlarına göre denemeler gerçekleştirilmesi; firewall denemesi ile birlikte saldırı yönlendirme ve mobil uygulama ve mobil cihaz denetimi çalışmaları; kapalı ağ uygulaması, genel görünüm değerlendirmesi yapılmasıdır.

Şirketler, değişen sıklıklarda gerçekleştirmiş oldukları ağ güvenliğine dair faaliyetlerde, ortak olarak sistem hatalarını bulabilmek adına, yoğun bir biçimde sistemi zorlamaktadırlar. Bu şekilde sistemin açıklarının daha rahat bir şekilde görülmesi sağlanmaktadır. Şekil 21'de Şirketlere göre ağ ve veri güvenliği için yapılan ekstra çalışmaların yüzdelik dağılımı yer almaktadır.



Şekil 21. Şirketlere göre ağ ve veri güvenliği için yapılan ekstra çalışmaların yüzdelik dağılımı



Şekil 22. Katılımcıların şirketlerinde, ağ ve veri güvenliği için yapılan ekstra çalışmaların hedeflerinin yüzdelik dağılımı

Şekil 22'de, katılımcıların şirketlerinde, ağ ve veri güvenliği için yapılan ekstra çalışmaların hedefleri yer almaktadır. Şirketlerin hedeflerinde çoğunlukla, dış tehditlerin değerlendirilmesi unsuru ön plana çıkmaktadır. Ardından bu uygulamayı, çalışanların ve sistemin denenmesi ile genel hedefler takip etmektedir.

3.2.7. Penetrasyon Testi Sıklığı

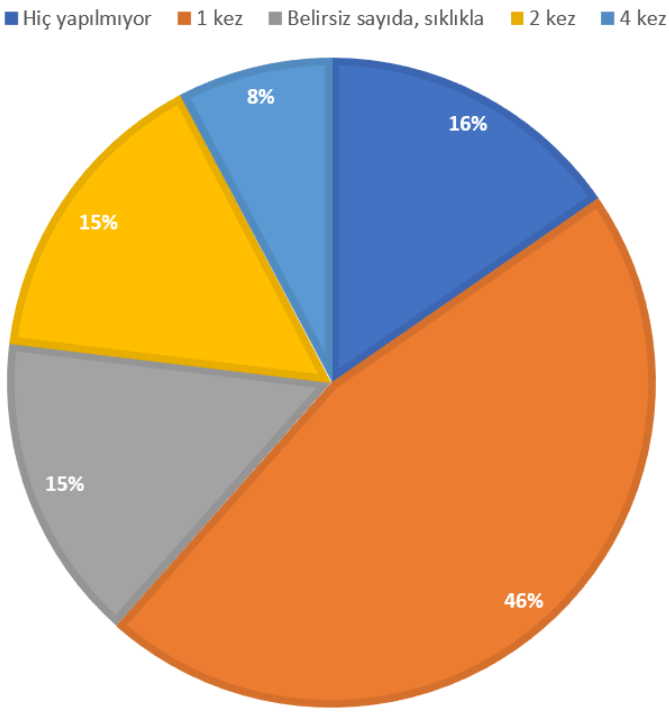
Görüşmelerin yedinci sorusunda katılımcılara, şirketlerinde Penetrasyon testi sıklığı ile ilgili durumları sorulmuştur.

Tablo 13. Şirketlere göre ağ ve veri güvenliği için yapılan Penetrasyon testi sıklığı

Penetrasyon Testi	
Firma Sayısı	**Yılda Kaç Kez**
2	0
6	1
2	2
1	4
2	Sayısı belirsiz, sık sık yapılıyor

Tablo 13'de gösterildiği şekli ile şirketlerin Penetrasyon testine verdikleri önem, bu testin gerçekleştirilme sıklığına da etki etmektedir. Katılımcıların büyük bir bölümü Penetrasyon testleri konusunda bir yıllık bir süre zarfına yayılan bir süreçten bahsetmek sureti ile birkaç seferde gerçekleştirilen testlerden bahsetmektedir.

Diğer yandan ise katılımcılarından birinin şirketi, denetim odaklı olarak ihtiyaç duyulan zamanlarda bu testlerin gerçekleştirilmesini sağlarken, diğer bir katılımcı şirket, özel bir ekip oluşturmak sureti ile sık bir biçimde ağ ve veri güvenliği için testler ve çeşitli çalışmalar gerçekleştirmektedir. Bu durum, katılımcıların söylemlerine göre şirketlerin iç yapısının büyüklüğüne ve küçüklüğüne göre farklılık göstermek sureti ile zaman aralıkları ve söz konusu test ve çalışmalardan yana olan beklentiler de değişmektedir. Şekil 23'te şirketlere göre ağ ve veri güvenliği için yapılan Penetrasyon testi sıklığının yüzdelik dağılımı yer almaktadır.



Şekil 23. Şirketlere göre ağ ve veri güvenliği için yapılan penetrasyon testi sıklığının yüzdelik dağılımı

3.2.8. LAN ve WAN Testi Sıklığı

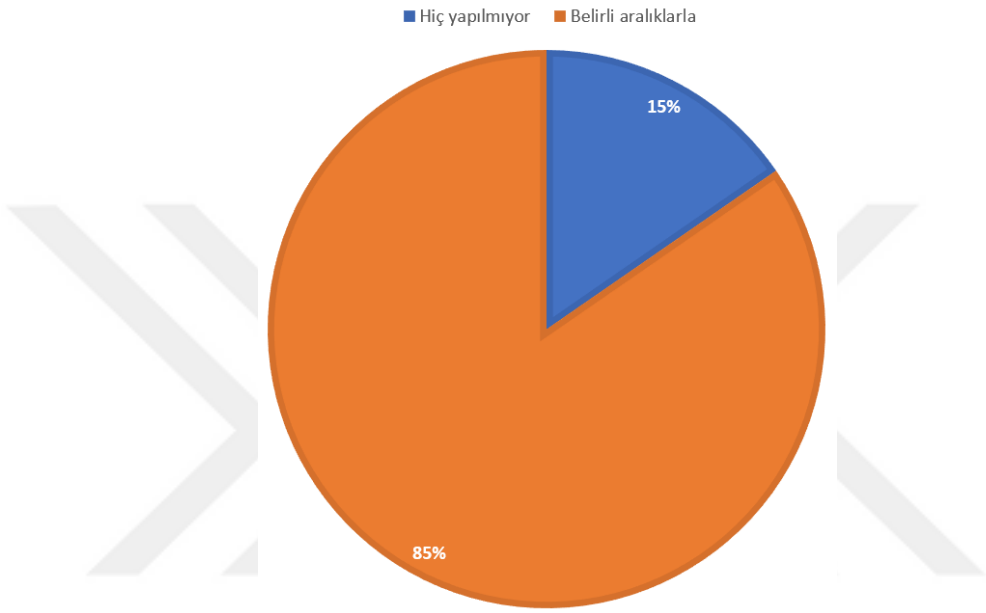
Görüşmelerin sekizinci sorusunda katılımcılara, şirketlerinde LAN ve WAN testi sıklığı ile ilgili durumları sorulmuştur.

Tablo 14. Katılımcıların şirketlerinde LAN ve WAN testi sıklığı

Sosyal Mühendislik Faaliyetlerinin Sıklığı			
Şirket Sayısı	**Sektör**	Belirli aralıklarla	Hiç yapılmıyor
3	Holding	2	1
3	Üretim/İmalat	3	
1	Banka	1	
3	Yazılım	2	1
2	Sanayi	2	
1	Taşımacılık	1	

Tablo 14'te yer aldığı şekilde katılımcılar, şirketlerin WAN ve LAN testlerinin genel olarak gerçekleştirdikleri ağ denetim testleri ile birlikte gerçekleştirildiğini dile

getirmişlerdir. Bu yaklaşımlarına göre şirketler, WAN ve LAN testleri için özel bir zaman ayırmamakta ve ağ denetimleri süre zarfında WAN ve LAN üzerindeki sorunları tespit etmek adına çaba sarf etmektedirler. Bir başka deyişle, katılımcıların şirketlerinin bu testler konusunda özel bir zaman ayırmadan, ellerine geçen raporlara istinaden süreç ile ilgili bir karar verdikleri görülmektedir. Şekil 24'te katılımcıların şirketlerinde LAN ve WAN testi sıklığının yüzdelik dağılımı yer almaktadır.



Şekil 24. Katılımcıların şirketlerinde LAN ve WAN testi sıklığının yüzdelik dağılımı

3.2.9. Ağ Zafiyetleri

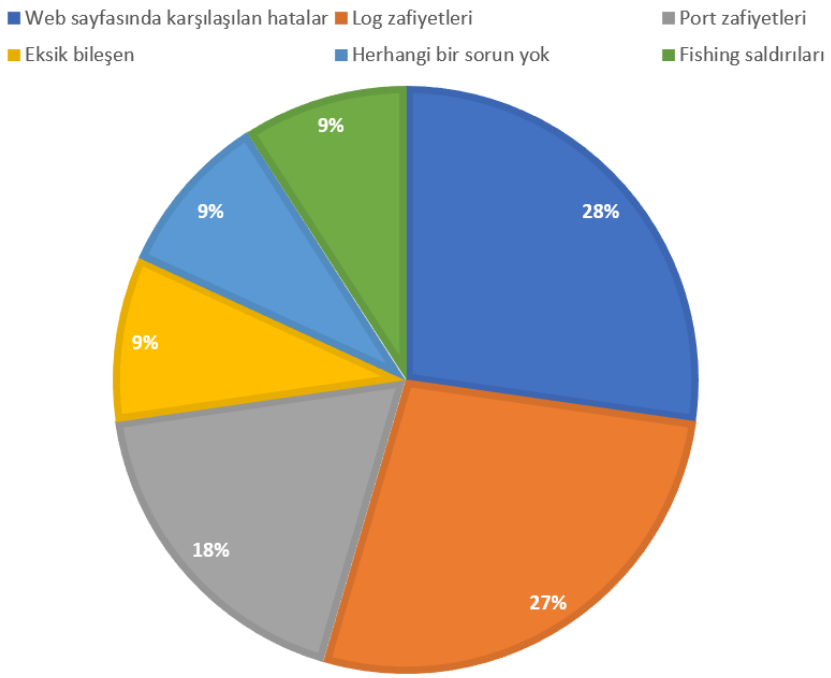
Görüşmelerin dokuzuncu sorusunda katılımcılara, şirketlerinde yaşanan ağ zafiyetleri ile ilgili durumları sorulmuştur.

Tablo 15. Katılımcıların şirketlerinde yaşanan ağ zafiyetleri

		Zafiyetler					
Şirket Sayısı	**Sektör**	Web sayfasında karşılaşılan hatalar	Log zafiyetleri	Port zafiyetleri	Eksik bileşen	Phishing saldırıları	Herhangi bir sorun yok
3	Holding	2	1				
3	Üretim/İmalat			1		1	1
1	Banka		1				
3	Yazılım	1			1		1
2	Sanayi		1				1
1	Taşımacılık			1			

Tablo 15'te gösterildiği üzere, katılımcıların her biri, ağ denetimi süre zarfında gerçekleştirdikleri çalışmalarında, birbirinden farklı sorunlar ile karşılaştıklarını dile getirmişlerdir. Katılımcıların belirttikleri sorunlar arasında, web sayfasında karşılaşılan hatalar, log zafiyetleri, phishing saldırıları ve buna bağlı port sorunlu zafiyetler, web servislerindeki bileşenlerin eski olmasından kaynaklanan sorunlar ve kullanıcı ve sistem kaynaklı çeşitli sorunlar ile karşılaşmışlardır.

Katılımcılardan üçünün herhangi bir sorun ile karşılaşmadığı süreçte, yine katılımcılar açısından ortak olarak kabul edilebilecek olan husus, sistemlerinin düzenli olarak saldırıya uğramasıdır. Fakat katılımcıların şirketlerinin farklı sektörlerde ve farklı hedeflere yönelik olarak çalıştıkları düşünüldüğünde, tehditlerin ve zafiyetlerin boyutu şirketlerin web adresleri ve ağlarının kapasitesi ile doğrudan ilintili olmaktadır. Bu nedenle şirketlerin, sürece dair güvenlik algılamaları arasında büyük ve doğal farklılıklar da görülmektedir. Şekil 25'te katılımcıların şirketlerinde yaşanan ağ zafiyetlerinin yüzdelik dağılımı yer almaktadır.



Şekil 25. Katılımcıların şirketlerinde yaşanan ağ zafiyetlerinin yüzdelik dağılımı

3.2.10. Dosya Yedekleme Sıklığı

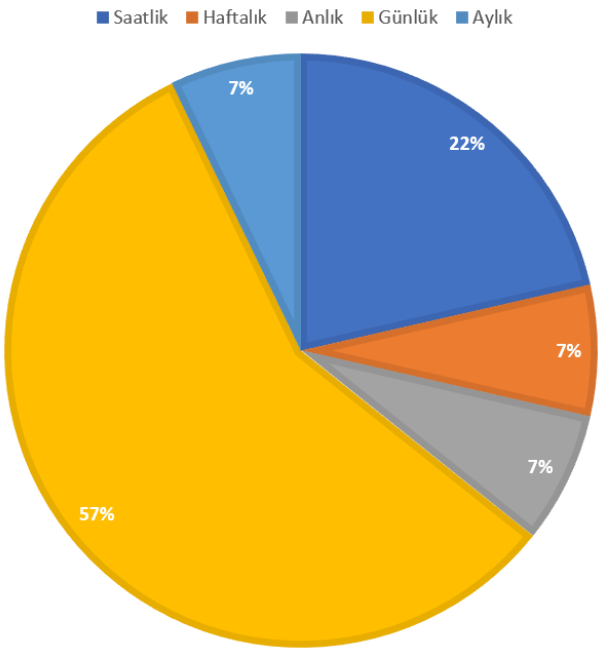
Görüşmelerin 10. sorusunda katılımcılara, şirketlerinde dosya yedekleme sıklığı ile ilgili durumları sorulmuştur.

Tablo 16. Katılımcıların şirketlerindeki dosya yedekleme sıklığı

Dosya Yedekleme Sıklığı						
Şirket Sayısı	**Sektör**	Anlık	Saatlik	Günlük	Haftalık	Aylık
3	Holding			3		
3	Üretim/İmalat		1	1		1
1	Banka			1		
3	Yazılım	1		1	1	
2	Sanayi		1	1		
1	Taşımacılık			1		

Tablo 16'da gösterildiği üzere yedekleme, katılımcıların şirketleri açısından son derece önemli olarak görülmektedir. Bu nedenle de şirketlerin büyük bir bölümünün ortak olarak günlük yedekleme gerçekleştirdikleri görülmektedir. Günlük yedekleme sabit ve rutin bir işlem olmakla birlikte şirketlerin aylık, haftalık ve saatlik olarak yedeklemeler de gerçekleştirdikleri görülmektedir. Sadece bir katılımcının şirketinin belirsiz olan aralıklar dahilinde yedekleme gerçekleştirdiği görülmektedir.

Yine bu soruya verilen cevaplarda, katılımcıların bağlı bulundukları şirketlerin kapasitelerinin ve ellerinde bulunan verinin büyüklüğü ile niteliğinin, yedekleme aralıklarının sıklığının belirlenmesi adına önemli birer faktör olduğu anlaşılmaktadır. Bazı şirketlerin kimi zaman anlık yedekleme gerçekleştirdikleri ve bu sayede de şirketin hassas verilerini korumaya çalıştıkları görülmektedir. Şekil 26'da katılımcıların şirketlerindeki dosya yedekleme sıklığının yüzdelik dağılımı yer almaktadır.



Şekil 26. Katılımcıların şirketlerindeki dosya yedekleme sıklığının yüzdelik dağılımı

3.2.11. Kullanıcı Hatalarına Karşı Şirket içi Eğitimler

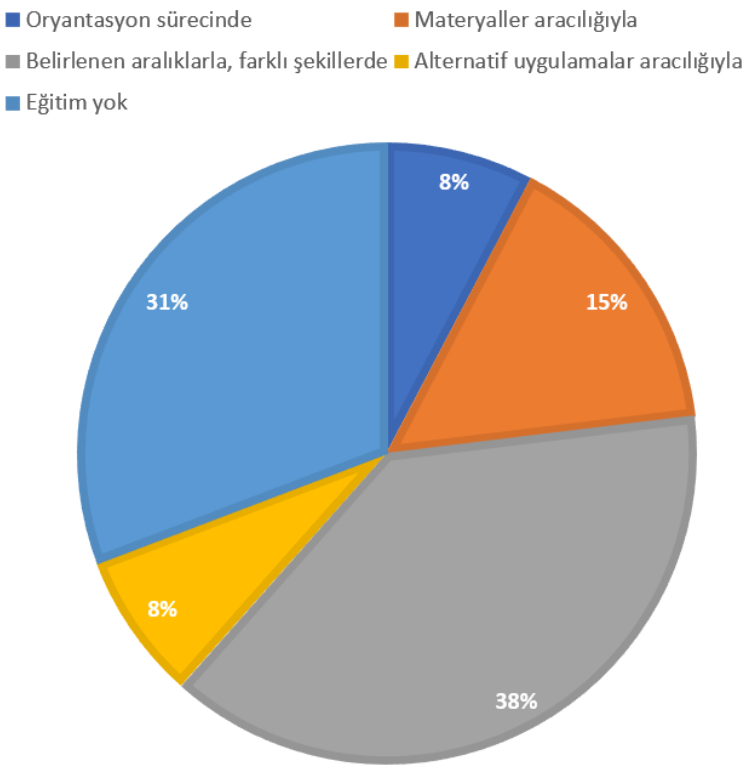
Görüşmelerin 11. sorusunda katılımcılara, şirketlerinde kullanıcı hatalarına karşı şirket içi eğitimler ile ilgili durumları sorulmuştur.

Tablo 17. Katılımcıların şirketlerinde kullanıcı hatalarına karşı şirket içi eğitimler

Şirket İçi Eğitimler						
Şirket Sayısı	**Sektör**	Oryantasyon sürecinde	Materyaller aracılığıyla	Belirlenen aralıklarla, farklı şekillerde	Alternatif uygulamalar aracılığıyla	Eğitim yok
3	Holding			2	1	
3	Üretim/İmalat	1	1	1		
1	Banka		1			
3	Yazılım			1		2
2	Sanayi					2
1	Taşımacılık			1		

Tablo 17'de yer alan dağılıma göre katılımcıların hepsi farklı şekillerde ve farklı sıklıklarda olacak şekilde çalışanlara, kullanıcı hatalarına dair eğitim verildiğini belirtmişlerdir. Bu konuda katılımcıların hepsinin şirketlerinin, konuya yaklaşma şekillerinin farklı olduğu ancak konu ile ilgili hassasiyet düzeylerinin yüksek olmadığı belirlenmiştir.

Katılımcılar şirketlerinde, kullanıcıların eğitimi açısından sistem kullanımına dair sürdürülebilir hatalar bulunmasından dolayı büyük bir özen göstermedikleri ve daha çok, sistemin kontrolünü bilgi işlem ya da muadil departmanlara bıraktıkları anlaşılmaktadır. Bu durum sistemin işleyişi açısından çalışanların dikkati nezdinde belirli eksikliklerin bulunduğunu göstermektedir. Şekil 27'de katılımcıların şirketlerinde kullanıcı hatalarına karşı şirket içi eğitimlerin şeklinin yüzdelik dağılımı yer almaktadır.



Şekil 27. Katılımcıların şirketlerinde kullanıcı hatalarına karşı şirket içi eğitimlerin şeklinin yüzdelik dağılımı

3.2.12. Sosyal Mühendislik Testleri Sıklığı

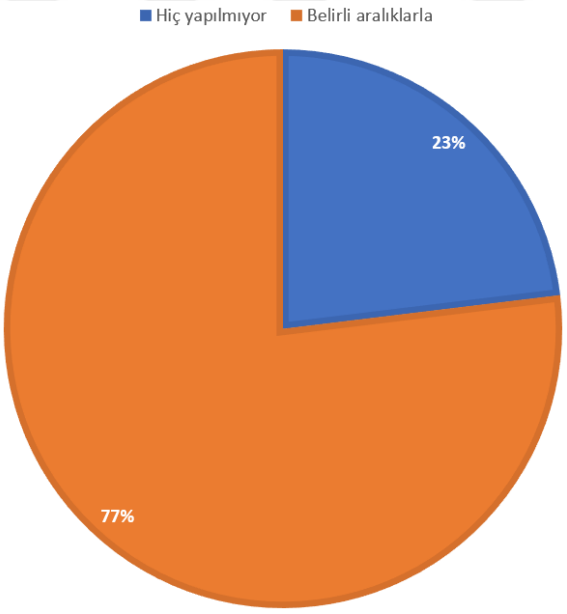
Görüşmelerin 12. sorusunda, katılımcılara, şirketlerinde, sosyal mühendislik testleri sıklığı ile ilgili durumları sorulmuştur.

Tablo 18. Katılımcıların şirketlerinde gerçekleştirilen sosyal mühendislik faaliyetlerinin sıklığı

Sosyal Mühendislik Faaliyetlerinin Sıklığı			
Şirket Sayısı	**Sektör**	Belirlenen aralıklarla	Hiç yapılmıyor
3	Holding	3	
3	Üretim/İmalat	2	1
1	Banka	1	
3	Yazılım	2	1
2	Sanayi	2	
1	Taşımacılık		1

Tablo 18'de gösterildiği şekli ile sosyal mühendislik uygulamaları açısından katılımcıların büyük bir bölümünün şirketleri sık olmamakla birlikte rastgele zamanlarda çeşitli faaliyetler ve denemeler gerçekleştirmektedirler. Yalnızca bir şirketin, son derece sık bir biçimde sosyal mühendislik konusunda faaliyetler yürüttüğü görülmüştür. Bununla birlikte üç şirket herhangi bir şekilde sosyal mühendislik çalışması yapmamaktadırlar.

Katılımcıların büyük bir bölümün şirketleri sosyal mühendislik konusunda kendi iç mekanizmalarında bilgi işlem departmanlarının desteği ile çeşitli uygulamalarda bulunmaktadırlar. Ağ üzerinden çeşitli şekillerde gerçekleştirilen bu uygulamalarla hem sistemin hem de sistem kullanıcıların eksikliklerinin tespit edilerek çözülmeye çalışıldığı görülmektedir. Katılımcıların şirketlerinden sadece bir tanesi, sosyal mühendisliğin kalıcı etkiler yaratacağına inanması sureti ile dışarıdan, profesyonel bir destek almaktadır. Şekil 28'de katılımcıların şirketlerinde gerçekleştirilen sosyal mühendislik faaliyetlerinin sıklığının yüzdelik dağılımı yer almaktadır.



Şekil 28. Katılımcıların şirketlerinde gerçekleştirilen sosyal mühendislik faaliyetlerinin sıklığının yüzdelik dağılımı

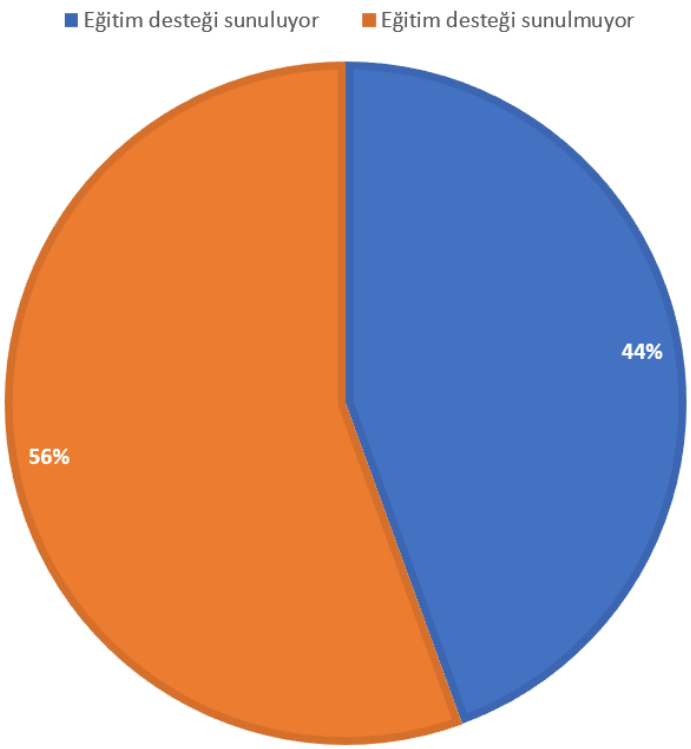
3.2.13. BT Departmanı Çalışanlarının Güvenlik Eğitimi Alma Durumu

Görüşmelerin 13. sorusunda katılımcılara, şirketlerinde BT departmanı çalışanlarının güvenlik eğitimi alma durumu ile ilgili durumları sorulmuştur.

Tablo 19. Katılımcıların şirketlerinde BT departmanı çalışanlarının güvenlik eğitimi alma durumu

Güvenlik Eğitimi			
Şirket Sayısı	**Sektör**	Eğitim desteği sunuluyor	Eğitim desteği sunulmuyor
3	Holding	3	
3	Üretim/İmalat	2	1
1	Banka		1
3	Yazılım		3
2	Sanayi	2	
1	Taşımacılık	1	

Tablo 19'de gösterilen dağılımda, şirketlerin çoğunluğunun bir eğitim desteği sunmak sureti ile çalışanlarının güvenlik konusundaki bilgi düzeylerini arttırmaya çalıştıkları gözlemlenmektedir. Fakat şirketler arasında güvenlik konusunda en yoğun ve en etkili güvenlik bilgisine sahip olması beklenen banka ve yazılım şirketlerinin güvenlik eğitimi konusunda herhangi bir tasarruflarının bulunmaması dikkat çekicidir. Şekil 29'da katılımcıların şirketlerinde BT departmanı çalışanlarının güvenlik eğitimi alma durumunun yüzdelik dağılımı yer almaktadır.



Şekil 29. Katılımcıların şirketlerinde BT departmanı çalışanlarının güvenlik eğitimi alma durumunun yüzdelik dağılımı

Tablo 20. Katılımcıların şirketlerinde BT departmanı çalışanlarının güvenlik eğitimi için bütçe ayrılması

Eğitim Bütçesi Olan	Eğitim Bütçesi Olmayan
7	6

Tablo 20'de yer alan dağılım, katılımcıların şirketlerinin, BT departmanı çalışanlarının güvenlik eğitimi için bütçe ayırma konusundaki durumlarını göstermektedir. Bütçesi olan yedi şirket, doğrudan doğruya, bu eğitim faaliyetleri için birer bütçe ayırmışlardır. Bütçesi olmayan altı şirketten beşi, bu eğitim faaliyetlerini gerçekleştirmemeleri neticesinde bütçe ayırmazken, bütçe ayırmayan şirketlerden biri, eğitim desteği sağlamasına karşın bu eğitimin maliyetini, genel bütçesinden karşılamaktadır.

3.2.14. IT Departmanı İçin Ayrılan Bütçe

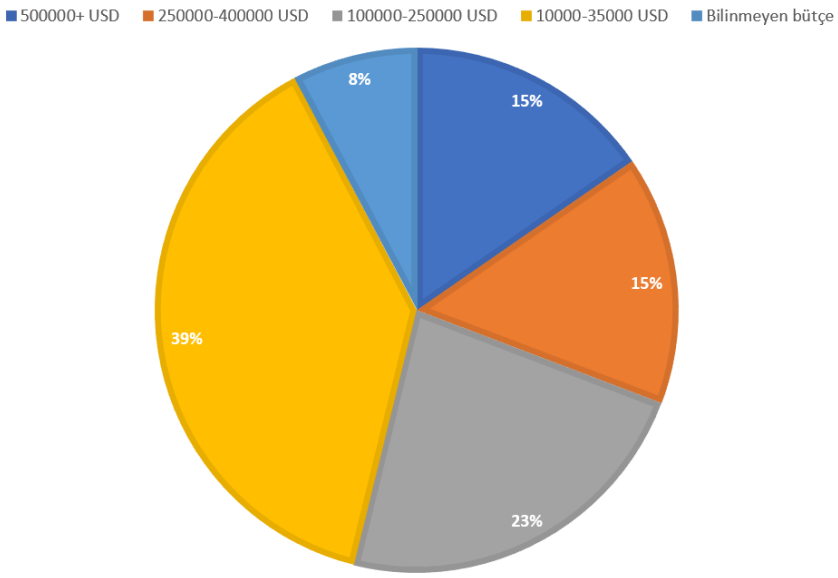
Görüşmelerin 14. sorusunda, katılımcılara, şirketlerinde, IT için ayrılan bütçe ile ilgili durumları sorulmuştur.

Tablo 21. Katılımcıların şirketlerinde IT departmanı için ayrılan bütçe

Bütçe	Sektör	Çalışan Sayısı
500000+ USD	Holding 1	12572
500000+ USD	Holding 2	7300
250000-400000 USD	Holding 3	95920
250000-400000 USD	Banka	873
100000-250000 USD	Sanayi 1	150
100000-250000 USD	Yazılım 1	370
100000-250000 USD	Üretim 1	500
10000-35000 USD	Sanayi 2	30
10000-35000 USD	Yazılım 2	50
10000-35000 USD	Yazılım 3	2000
10000-35000 USD	Üretim 2	65
10000-35000 USD	Üretim 3	1000
Bütçesi bilinmiyor	Gümrük-Taşımacılık	800

Tablo 21'de gösterildiği üzere, katılımcıların bağlı bulundukları şirketlerin sistem ve ağ güvenliği için ayırmış oldukları bütçeler arasında, çalışan kapasitesi temelinde, iş ve sektördeki büyüklük açısından farklılıkların bulunduğu düşünülebilir. Sadece bir şirketin genel sistem ve ağ bütçesinin rakamlarının öğrenilemediği çalışmada, katılımcıların, spesifik olarak 15.000 dolar ile bir milyon dolar arasında değişen bir bütçe skalasından bahsettikleri görülmektedir.

Şirketlerin iş potansiyeli, ellerindeki verinin büyüklüğü, ağdaki kullanıcı sayısı ve ağda akışı gerçekleşen verinin niteliği, sistemin korunması adına harcanacak olan bütçenin büyüklüğünü de belirlemektedir. Şekil 30'da katılımcıların şirketlerinde IT departmanı için ayrılan bütçe değerlerinin yüzdelik dağılımı yer almaktadır.



Şekil 30. Katılımcıların şirketlerinde IT departmanı için ayrılan bütçe değerlerinin yüzdelik dağılımı

3.2.15. Ağ Güvenliği Departmanının Durumu

Görüşmelerin 15. sorusunda katılımcılara, şirketlerinde ağ güvenliği departmanının ayrı birim olup olmadığı ile ilgili durumları sorulmuştur.

Tablo 22. Katılımcıların şirketlerinde ağ güvenliği departmanının durumu

Güvenlik Departmanı Ayrı	Bilgi İşlem Departmanı Dahilinde
4	9

Tablo 22'de yer aldığı üzere, katılımcıların söylemleri değerlendirildiğinde, şirketlerinin içerisinde ağ güvenliği için özel bir birim ayıran şirket sayısı sadece dörttür. Diğer şirketlerde söz konusu güvenlik faaliyetleri, bilgi işlem bünyesinde gerçekleştirilmektedir. Bu durum, katılımcıların tamamı tarafından eldeki bütçenin yaratmış olduğu bir durum olarak görülmektedir. Bu nedenle de bilgi işlem departmanı içerisinde, çalışanların iki yönlü olarak hareket etmeleri beklenmektedir. Günümüzde BT ile alakalı iş ilanları göz önüne alındığında "Sistem & Network", "Network & Güvenlik" gibi ilanlar fazlasıyla görülebilecektir. Artık BT sektöründe insanların birden fazla iş kolunu aynı anda idare edebilmeleri beklenmektedir.

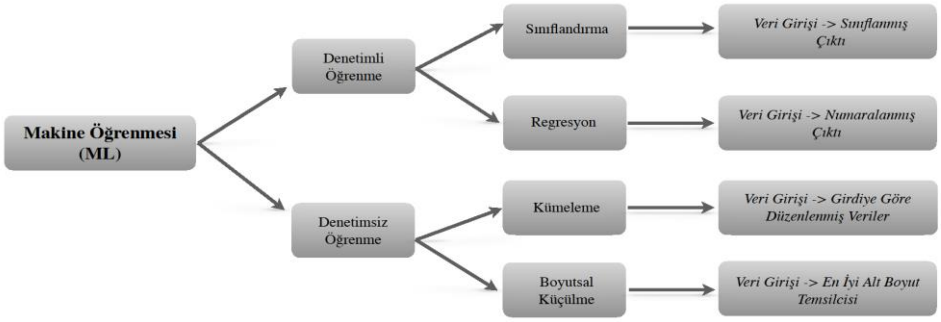
DÖRDÜNCÜ BÖLÜM
YÖNTEMLER ve METOTLAR

4.1. Makine Öğrenmesi

Makine öğrenmesi (Machine Learning, ML), bilgisayarların örneklerden ve deneyimlerden otomatik olarak öğrenmesini ve karar vermede insanları taklit etmesini sağlayan, belirli bir problemi, problem ortamından elde edilen verilere göre modelleyen bilgisayar algoritmalarının genel adı ve bir yapay zekanın alt dalıdır. Günümüz teknolojisinde çok önemli yeri olan veri biliminin en önemli alt bileşenlerinden birisidir. Çok büyük miktarda verinin analizini yapmak ve istatistiğini oluşturmak manuel bir şekilde mümkün olamayacağı için bu analizleri gerçekleştirmek ve istatistiğini oluşturmak için ML kullanılmaktadır.

ML'deki en önemli ve temel amaç, geçmiş verileri kullanıp, analizini yaparak gelecekteki verilerin modellenmesi, analizleri ve istatistikleri için tahminlerde bulunmasıdır. ML, büyük verileri en ideal biçimde sınıflara ayırarak ve tahminleyerek, manuel şekilde yapılacak olan tüm işlemleri, hızlı ve kolay bir biçimde algoritma mantığı ile modellemektedir. ML'nin, maliyetleri ve riskleri azaltmak, genel yaşam kalitesini iyileştirmek, ürün/hizmet önerileri, siber güvenlik ihlallerinin tespiti ve benzeri insan yaşamını etkileyen her türlü alanda kullanımı mevcuttur.

Her geçen gün teknolojinin ilerlemesi ve yapay zekanın insan yaşamına dahil olması ile birlikte yapay zekanın alt dalı olan ML de daha yaygın hale gelmekte ve her türlü alana entegre olabilmektedir.



Şekil 31. ML Algoritmalarının Hiyerarşik Yapısı

Şekil 31'de de görülebileceği gibi ML'nin temel bileşenleri ve algoritmalara göre hiyerarşik bir yapısı mevcuttur.

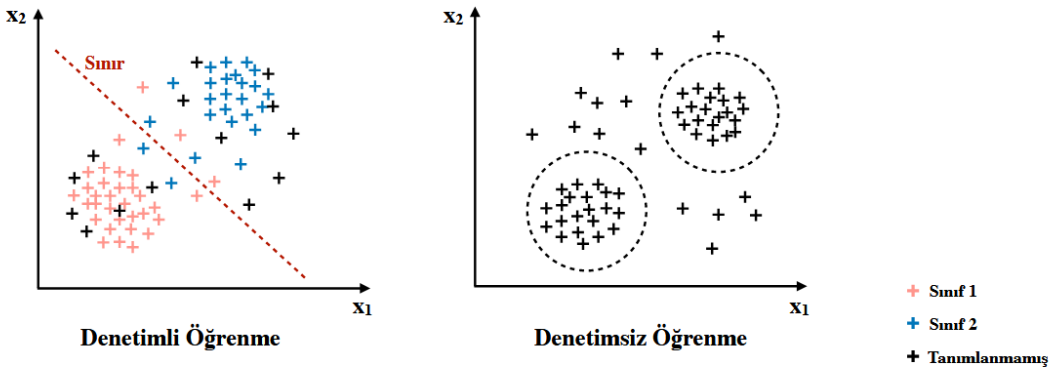
Verinin şekline, büyüklüğüne, oranına göre kullanılabilecek farklı ML algoritmaları mevcuttur. Algoritma çerçevesine göre ML, denetimli ve denetimsiz olmak üzere iki yönteme sahiptir.

Denetimli Öğrenme: ML, yaşam döngüsünün eğitim aşamasında etiketlenmiş giriş ve çıkış verilerini gerektirir. Eğitim verileri, modeli eğitmek ve test etmek için kullanılmadan önce genelde hazırlık aşamasında veri bilimcisi tarafından etiketlenir. Bu şekilde oluşturulan model, girdi ve çıktı verileri arasındaki ilişkiyi öğrendikten sonra yeni ve görünmeyen veri kümelerini sınıflandırmak ve sonuçları tahmin etmek için kullanılabilir.

Denetimli öğrenme, görünmeyen verileri belirlenmiş kategorilerde sınıflandırmak ve tahmine dayalı bir model olarak gelecekleri eğilimleri ve değişiklikleri tahmin etmek için kullanılır. Bu yaklaşım ile geliştirilen bir model, nesneleri ve onları sınıflandıran özellikleri tanımayı öğrenecektir. Tahmine dayalı modeller de genellikle denetimli öğrenme ile eğitilir. Girdi ve çıktı verileri arasındaki kalıpları öğrenerek, yeni ve görünmeyen verilerden sonuçları tahmin edebilir.

Denetimsiz Öğrenme: Modellerin ham ve eğitilmemiş verileri üzerinde eğitilmesidir. Genellikle ham veri kümelerindeki kalıpları ve eğilimleri tespit etmek veya birbirine benzeyen verileri belirli sayıda grup halinde ayırmak için kullanılır. Veri kümelerini daha iyi anlamak için genelde keşif aşamasında kullanılan bir yaklaşımdır.

Adından da belli olduğu üzere, denetimsiz öğrenme, denetimli öğrenmeden daha çok uygulamalı bir yaklaşımdır. Bir insan, küme noktalarının sayısı gibi model hiperparametrelerini ayarlar, ancak model büyük veri dizilerini faydalı bir şekilde ve insan gözetimi olmadan işler. Bu nedenle denetimsiz öğrenme verilerin kendi içindeki görünmeyen kalıplar ve ilişkiler hakkındaki soruları yanıtlamak için uygundur, ancak insan gözetimi az olduğu için açıklanabilirliğine özen gösterilmesi gerekmektedir.



Şekil 32. Denetimli ve Denetimsiz Öğrenme

ML'de çalışma yapılabilecek birçok algoritma mevcuttur. Algoritmalar arasından en uygun olanı seçmek önemlidir ve bu seçimi de uygulamayı yazan programcı yapmaktadır. Modeli oluşturmak için kullanılacak algoritmaları gruplandırmak, doğru olanı seçmek açısından programcıya, model üzerinde çalışacak olan kişi/kişilere yardımı olacaktır.

Bu tez çalışmasında ise hangi algoritmaların ve hangi ML metotlarının kullanıldığına dair detaylı bilgilendirmeler 4.2. bölümünde yer almaktadır.

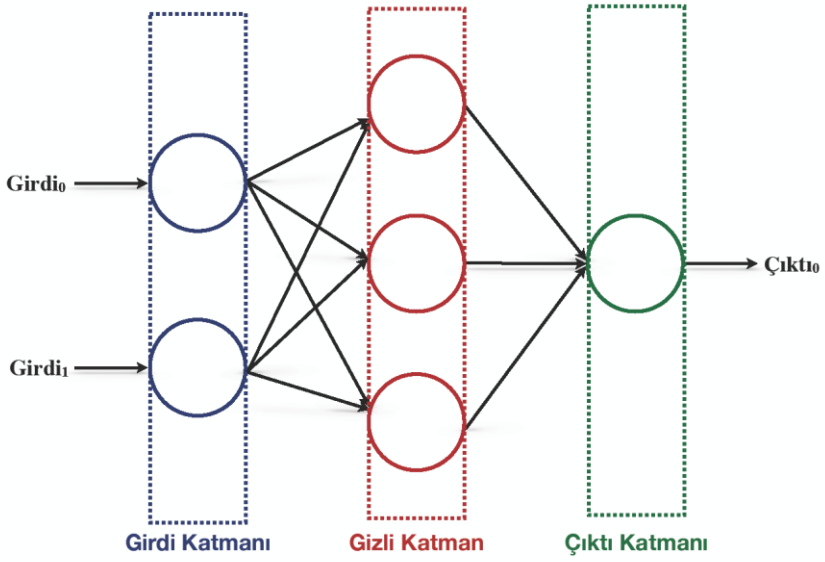
4.2. ML Metotları

Bu tez çalışmasında, elde edilen veriler kullanılarak oluşturulan istatistiklerin bir sonraki adımlarının tahmin edilebilmesi için Pyhton programlama dili ile ML metotları kullanılmıştır.

4.2.1. Çok Katmanlı Algılayıcı Metodu

Çok Katmanlı Algılayıcı (Multi Layer Perceptron Regressor, MLP Regressor), girdi katmanına girilen verilerin gizli katman(lar) yoluyla çıktı katmanına bir yönde yayılım yaptığı bir ileri-geri yapay sinir ağıdır. Gizli ve çıktı katmanları, perceptronlar olarak adlandırılan tek birimlerden oluşur. MLP'deki her algılayıcı, önce ağırlıklandırılan ve daha sonra birlikte eklenen bir girdi seti alır. Elde edilen değer kombine girdileri uygun çıktı tepkisine eşleyecek bir aktivasyon işlevini tetiklemek için kullanılır. Eğitim verileri ve simülasyon verileri için tren ve sim işlevi kullanılır (Alkalidi, 2017, 41).

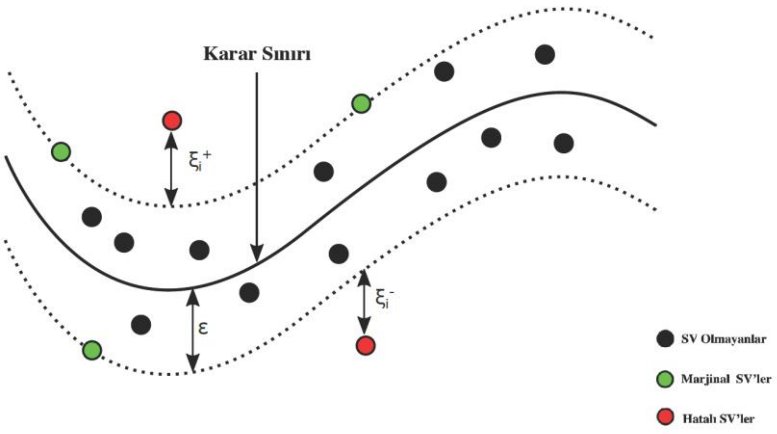
MLP'nin çalışma biçimi Şekil 33'de gösterilmektedir.



Şekil 33. MLP'nin Çalışma Biçimi

4.2.2. Destek Vektör Metodu

Destek Vektör Metodu (Support Vector Regression, SVR) maksimal marjin algoritmasındaki tüm temel özellikleri muhafaza ederek regresyon problemine uygulanabilir: doğrusal olmayan bir fonksiyon kernele bağlı özellik uzayında lineer öğrenme makineleri ile öğrenilir. Sistemin kapasitesi uzayın boyutlarına bağlı olmayan bir parametre ile kontrol edilir. Sınıflandırma probleminde olduğu gibi öğrenme algoritması konveks fonksiyonu minimize eder ve çözümü seyrektir. Kullanılan yaklaşım "genelleme sınırlarını optimize edeni bulmak" olarak özetlenebilir ve hedef değerine belli mesafe uzaklık içerisinde olan hatayı yoksayan kayıp fonksiyonu (loss function) tanımlamaya dayanır. Bu tip fonksiyona **"ε -duyarsız kayıp fonksiyonu (ε -insensitive loss function)"** denir. ε - duyarsız kayıp fonksiyonu kullanmak global minimumun varolması ve güvenilir genelleme sınırının optimizasyonu avantajlarını sağlar. Çözümün eğitim verilerinin alt kümesi ile elde edilmesi hesaplamada büyük avantaj sağlamaktadır (Yürekli, 2017, 14).



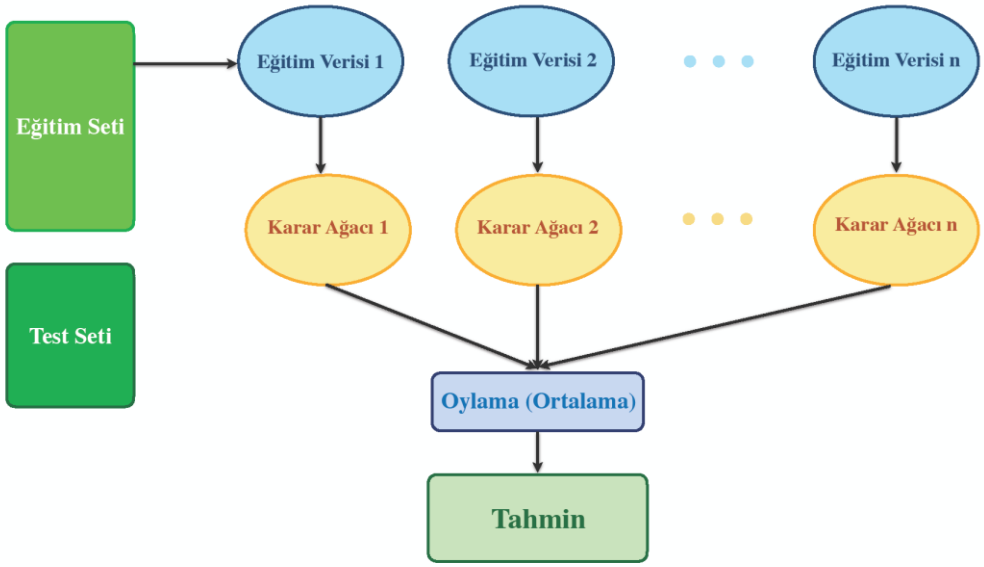
Şekil 34. SVR Yapısı

4.2.3. Rastgele Orman Metodu

Karar ağaçları, iyi bilinen makine öğrenimi ve veri madenciliği teknikleridir. Herhangi bir nesneyi veya veri noktasını sınıflandırmak için karar ağaçlarını kullanabiliriz. Karar ağacı kullanarak bir sınıflandırma probleminin çözümünde en önemli konu doğru ağacı oluşturmaktır. Brieman ve diğerleri karar ağacı yönteminden farklı olarak Rastgele Orman (Random Forests, RF) adı verilen yeni bir yöntem açıklamışlardır (Breiman, 2001, 5-32). RF, makine öğreniminde kategorik veri kümeleri için çok yararlı olan bir topluluk yöntemidir. RF, ormanın yapısını oluşturan bir dizi karar ağacına sahiptir. Ormandaki her karar ağacının maksimum derinliği ve bölünmüş özellikleri içeren düğümleri vardır.

RF eğitim bölümünde, her bölüm işlevi, rastgele bir işlev alt kümesinden seçilir. En ayrımcı eşikleri kullanmak yerine, rastgele bir özellik alt kümesi kullanılır. Bu rastgelelik nedeniyle ormanın yanlılığı artar. RF, büyük miktarda veri eksik olduğunda doğruluğu korumak için önemli bir yönteme sahiptir ve torba dışı hata tahminini kullandığından RF'nin çapraz doğrulanmasına gerek yoktur. Torba dışı hata tahmin yönteminde, üç eğitim veri setinden biri, oluşturulan tahminleri veya ağaçları test etmek için ayrılmıştır. Ağaçlar oluşturulduktan sonra her ağaç, ağaçta olmayan örneklerle test edilir ve her ağaç için hata oranı tahmin edilir. Torba dışı hata tahminin tarafsız olduğu kanıtlanmıştır. RF'de her ağaç mümkün olduğu kadar büyüyebilir çünkü RF bunu engellemez.

RF'nin çalışma biçimi Şekil 35'de gösterilmektedir.



Şekil 35. RF Metodunun Çalışma Biçimi

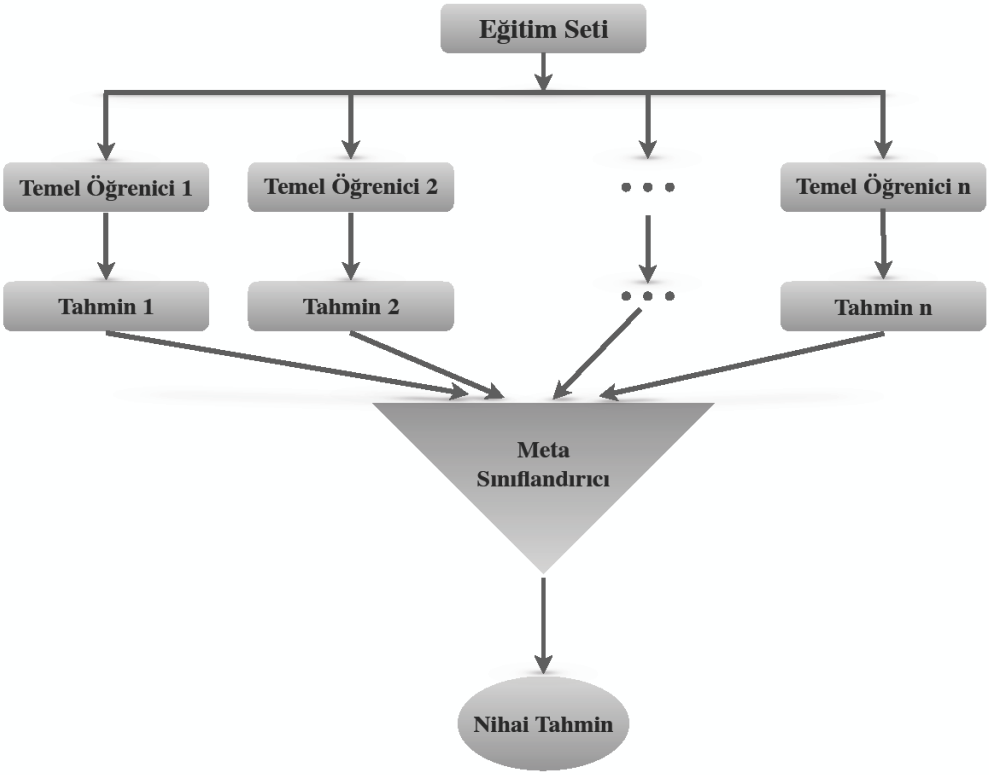
4.2.4 Ekstra Ağaçlar Metodu

Ekstra Ağaçlar (Extra Trees Regression) topluluğu yöntemi, denetimli öğrenme yöntemi ile karar ağaçlarına dayalı bir topluluk öğrenme yöntemidir. Ormandan toplanan birbiriyle ilgisiz birkaç karar ağacından gelen tahminleri birleştirerek nihai bir tahmin elde eden topluluk öğrenme yöntemidir. Ekstra Ağaçlar, fazla öğrenmeyi indirgemek için bazı kararları ve veri alt kümelerini rastgele seçimi bakımından RF'ye benzer. RF yönteminden daha basit bir algoritma kullanılır ancak daha iyi performans elde edilebilir.

4.2.5 Yığınlama Metodu

Yığınlama Metodu (Stacking Regressor) birden fazla metodun çıktılarını biraraya getirerek ve bunları meta öğrenici adı verilen başka bir ML modeli ile çalıştırarak model tahminlerini iyileştirmenin bir yöntemidir.

Temel olarak, yığılmış bir model, birden fazla modelin çıktısını bir meta öğrenici ile çalıştırır. Meta öğrenici, tüm modelllerin güçsüz yönlerini en aza indirmeye, güçlü yönlerini ise en üst seviyeye çıkarmayı hedefler. Genellikle iyi sonuçlar alınan başarılı bir modeldir.



Şekil 36. Stacking Regressor Çalışma Mimarisi

4.2.6 Ada Boost Regressor Metodu

AdaBoost algoritmasında; sınıflandırma sonucunda değerlendirme yapılır. Değerlendirme sonucunda yanlış sınıflandırılan örneklere odaklanılarak algoritma

geliştirilmiştir. Her yinelemede doğru sınıflandırılan örneklerin ağırlık katsayıları azaltılırken, yanlış sınıflandırılan örneklerin ağırlıkları artırılır. İkinci eğitim, ilk eğitimin yanlış verilerini; üçüncü eğitim ise ikinci eğitimin hatalı verilerini hedef alarak sınıflandırılır. Böylece hatalı numunelerin ele alınması ve hata miktarının en aza indirilerek daha doğru bir sınıflandırma yapılması amaçlanmıştır. Algoritmaları Bagging yönteminde olduğu gibi aynı anda çalıştırmak ve nihai kararı vermek yerine, önceki algoritmanın hatasını en aza indiren özyinelemeli çalışmalar sırasıyla elde edilir (Dilek, 2022, 44).

4.2.7 Bagging Regressor Metodu

Bagging yönteminde; veri setindeki eğitim ve test setlerine ayrılan bölümlerden eğitim seti bölümünden rastgele örnekler alınır. Bu numuneler alınırken; örneklenen kısım eğitim bölümüne geri gönderilir. Daha önce seçilen numuneler eğitim setinde değiştirilir ve eklenen sette seçim yapılarak yeni numuneler oluşturulur. Bagging yönteminde kullanılan sınıflandırma yöntemi sabit kalsa da eğitim örnekleri değişmektedir. Aynı sınıflandırma algoritması ile çalışan farklı örnek eğitim setleri aynı anda ve birbirine paralel olarak devam eder. Çalışmalar birbirini etkilemez ve birbirinden bağımsız çalışır (Dilek, 2022, 43).

4.2.8 Karar Ağacı Metodu

Karar Ağacı Metodu (Decision Tree Regressor), denetimli bir öğrenme algoritmasıdır. Regresyon ve sınıflandırma ile ilgili problemleri çözmek için kullanılmaktadır. Karar ağaçları hem kategorik hem de nümerik verileri işleyebilmektedir (Akcan, 2021, 27).

Basit bir karar ağacı algoritmasının çalışma mekanizması şu şekildedir:

1. Ağaca, tüm veri kümesini içeren kök düğüm ile başlanılır.
2. Öznitelik Seçimi Ölçüsü kullanılarak veri kümesindeki en iyi öznitelik seçilir.
3. Seçilen en iyi öznitelik, bir karar düğümü yapılır ve veri kümesi daha küçük alt kümelere bölünür.

4. Düğümler, daha fazla sınıflandırılamayana ve son düğüm, yaprak düğümü olarak adlandırılabilene kadar; bu işlem her çocuk için tekrarlanılarak ağaç oluşturulmaya devam edilir (Akcan, 2021, 27).

4.2.9. Gradient Boost Regressor Metodu

Gradient Boost, topluluk ML tekniklerinden biridir. Sağlam bir model oluşturmak için birçok zayıf öğreneni sırayla birleştirerek kullanır. Hem regresyon hem de sınıflandırma problemlerinde kullanılabilecek esnek ve güçlü bir yöntemdir. Çok küçük ayarlarla bile iyi sonuçlar alınması mümkündür. Ayrıca, uyum sağlamaya diğer ML yöntemlerinden daha yatkındır ve büyük verilerde öğrenmesi yavaş olabilir.

4.2.10. Hist Gradient Boost Regressor Metodu

Gradyan artırmanın yakınsama hızını iyileştirmek amacıyla Hist Gradient Boost Regressor ortaya çıkmıştır. Bu yaklaşım, fonksiyonlarda sayısal optimizasyon perspektifinden analiz edilir ve geleneksel yöntemlerle takdir edilen önceki adımlardaki gradyanları dikkate alır. Tarihsel gradyan bilgisinin yol gösterici etkisinden daha iyi yararlanmak için hem önceki birikmiş gradyanlar hem de mevcut gradyan fonksiyonlarda iniş yönünün hesaplanmasına dahil edilir. Algoritma tarafından verilen iniş yönüne uyum sağlayarak, zayıf öğrenen en dik iniş yönünün açgözlülüğünü azaltan tarihsel eğimlerin avantajlarından faydalanılabilir. Deneysel sonuçlar, yaklaşımın doğrulukta önemli bir azalma olmaksızın gradyan artırmanın yakınsama hızının geliştiğini gösterecektir.

4.2.11. Voting Regressor Metodu

Voting Regressor modeli, bir tahmin ediciler grubunun tahminlerinin topluluğu anlamına gelir. Bu nedenle birden fazla tahmin ediciden oluşur. Bu tahminlerin her biri model tarafından nihai bir tahminde toplanır. Hangi sınıflandırma yönteminin kullanılacağı konusunda kararsız kalındığında sıklıkla uygulanılabilir. Bu nedenle birden fazla gelen tahminleri kullanarak en sık görülene dayalı tahminler yapar.

4.3. Modeldeki Girdilerin Numerik Olarak Etiketlenmesi

Çalışmanın bu bölümünde modelin girdilerinin ML'de temsil edilebilmesi için veri etiketleme yöntemine başvurulmuştur. Tablo 23'de görüldüğü gibi veriler; Palo Alto 1, Fortigate 2, Watchguard 3, Sonicwall 4, Sophos 5 ile temsil edilmiştir. Bu sayede numerik olarak firewall markaları modellenmiştir. Aynı şekilde Tablo 24, Tablo 25, Tablo 26, Tablo 27, Tablo 28, Tablo 29, Tablo 30, Tablo 31, Tablo 32, Tablo 33 ve Tablo 34'de görülebileceği gibi diğer etiketleme işlemleri listelenmiştir.

Tablo 23. Firewall Markalarına Karşılık Gelen Rakamlar

Marka	Rakam
Palo Alto	1
Fortigate	2
Watchguard	3
Sonicwall	4
Sophos	5

Tablo 24. WAF Markalarına Karşılık Gelen Rakamlar

Marka	Rakam
Fortiweb	1
Microsoft	2
F5	3
WatchGuard	4
Cloudflare	5
Kullanmayan	6

Tablo 25. SIEM Markalarına Karşılık Gelen Rakamlar

Marka	Rakam
Fortisiem	1
Qradar	2
Archsight	3
SSIEM	4
Watchguard	5
OpenManage	6
LogSign	7
PRTG	8
Cryptolog	9
Webroot	10
Kullanmayan	11

Tablo 26. DLP Markalarına Karşılık Gelen Rakamlar

Marka	Rakam
Forcepoint	1
Symantech	2
Watchguard	3
Safetica	4
McAfee	5
SophosDLP	6
Webroot	7
Kullanmayan	8

Tablo 27. ANTIVIRUS Markalarına Karşılık Gelen Rakamlar

Marka	Rakam
Fortiems	1
MicrosoftDefender	2
Symantech	3
Kaspersky	4
Watchguard	5
Trendmicro	6
Comodo	7
ESET	8
SophosInterceptX	9
Webroot	10

Tablo 28. Yedekleme Sıklığı Sorusuna Verilen Cevapların Rakam Karşılıkları

Yedekleme Sıklığı	Rakam
Anlık	1
Saatlik	2
Günlük	3
Haftalık	4
Aylık	5

Tablo 29. Penetrasyon Testi Sorusuna Verilen Cevapların Rakam Karşılıkları

Penetrasyon Testi	Rakam
Yılda 1 Kez	1
Yılda 2 Kez	2
Yılda 4 Kez	3
Sık Sık	4
Hiç Yapmayan	5

Tablo 30. Eğitim Desteği Sorusuna Verilen Cevapların Rakam Karşılıkları

Ekstra Eğitim Desteği	Rakam
Sağlanması	1
Sağlanmaması	2

Tablo 31. IT Güvenlik Departmanı Sorusuna Verilen Cevapların Rakam Karşılıkları

IT Güvenlik Departmanı	Rakam
Ayrı Olanlar	1
Ayrı Olmayanlar	2

Tablo 32. Sosyal Mühendislik Testi Sorusuna Verilen Cevapların Rakam Karşılıkları

Sosyal Mühendislik Testi	Rakam
Yapanlar	1
Yapmayanlar	2

Tablo 33. IT Departmanı Bütçe Sorusuna Verilen Cevapların Rakam Karşılıkları

Bütçe	Rakam
500000 USD+	1
250000-400000 USD	2
100000-250000 USD	3
10000-35000 USD	4
Bilinmeyen	5

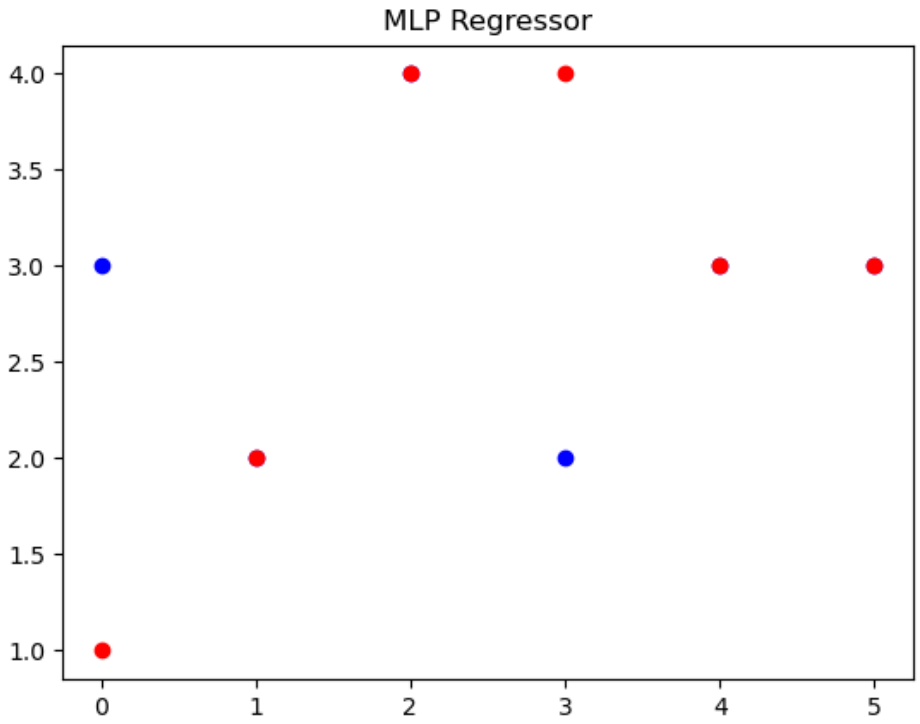
Tablo 34. Lan-Wan Atak Testi Sorusuna Verilen Cevapların Rakam Karşılıkları

Lan-Wan Atak Testi	Rakam
Yaptıranlar	1
Yaptırmayanlar	2

4.4 Makine Öğrenmesi Metotlarının Grafiksel Gösterimi

4.4.1 MLP Regressor Metodunun Başarı Oranı

Şekil 37'de görüldüğü üzere firewall kullanımı için MLP Regressor yöntemi kullanılmıştır. Her firewall markası için bir rakam atanmıştır. Tablo 23'de her markaya karşılık gelen rakamlar gösterilmiştir.



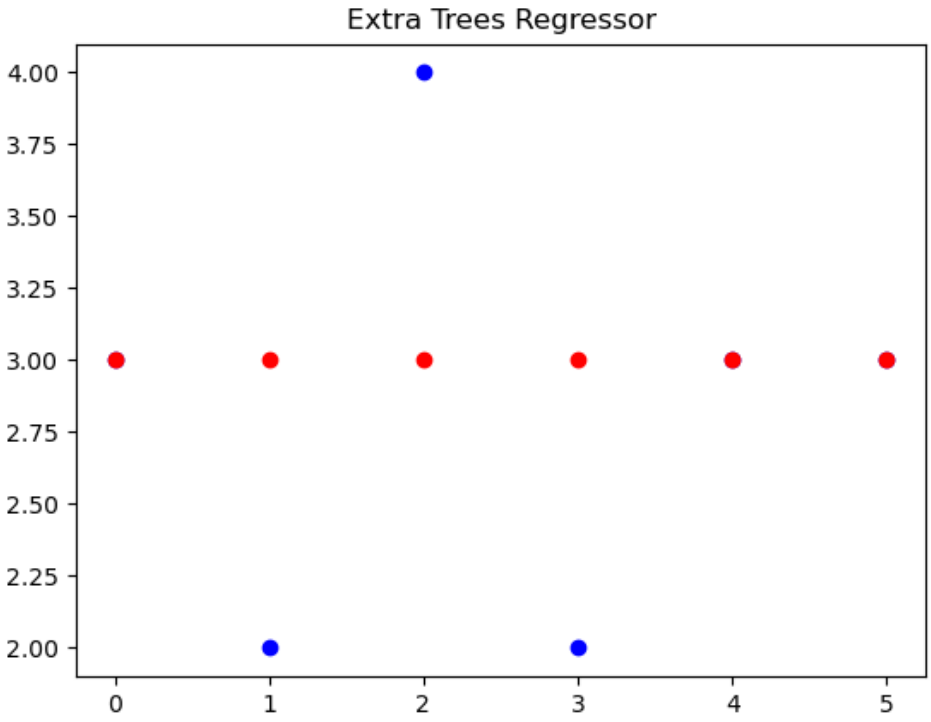
Şekil 37. MLP Regressor Başarı Oranı Gösterimi

Şekil 37'de gösterilen mavi noktalar gerçek firewall markasını gösterirken, kırmızı noktalar modelin tahminini göstermektedir. Aynı sütun da hem mavi hem kırmızı nokta bulunması yanlış tahminleri, sadece kırmızı nokta bulunması ise modelin yaptığı doğru tahminleri göstermektedir.

Birinci adımda gerçek kullanılan firewall markası Watchguard iken, model önceki verilerden yararlanarak yaptığı tahminde bunu Palo Alto olarak yanlış tahmin etmiştir. İkinci adımda ise gerçek değer Fortigate ve model bu adımda doğru tahminlemede bulunarak Fortigate sonucunu bulmuştur. Bu yöntem için model %66 başarıya ulaşmıştır. Bu oran kullanılan yöntemler arasında en yüksek başarı ölçütüdür.

4.4.2. Extra Trees Regressor Metodunun Başarı Oranı

Şekil 38'de firewall kullanımı için Extra Trees Regressor yönteminin başarı oranı görülmektedir.

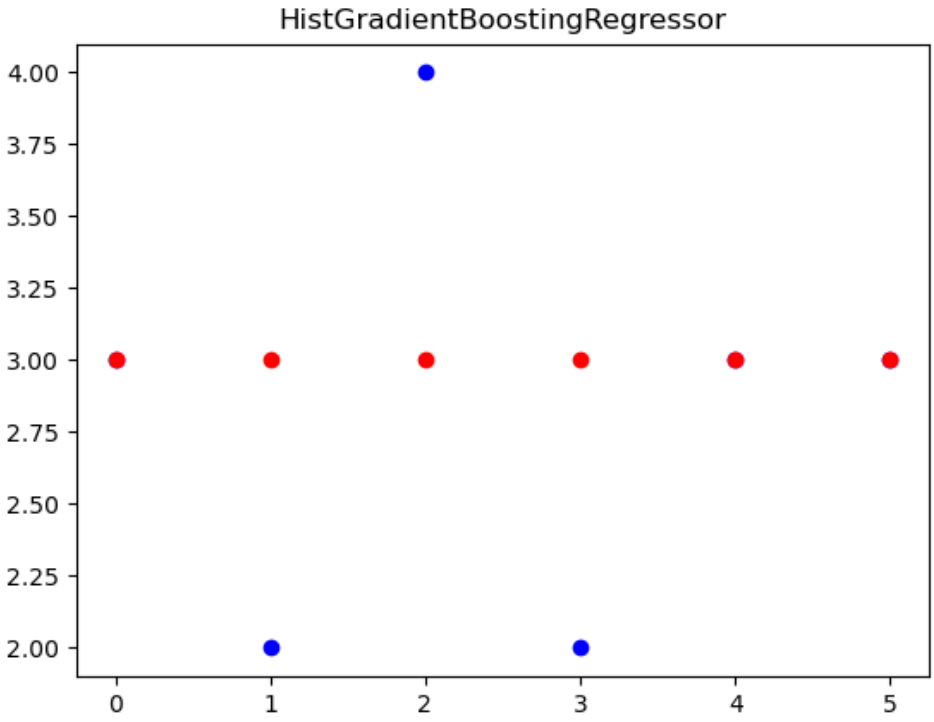


Şekil 38. Extra Trees Regressor Başarı Oranı Gösterimi

Tablo 23'deki bilgilere istinaten; birinci adımda gerçek değer Watchguard ve model de Watchguard olarak tahmin ederek bu adımda doğru tahminde bulunmaktadır. İkinci adımda ise gerçek değer Fortigate iken model Watchguard tahmini yaparak yanlış bir tahminlemede bulunmaktadır. Bu yöntemde başarı oranı %50 olarak tespit edilmiştir.

4.4.3. Hist Gradient Regressor Metodunun Başarı Oranı

Şekil 39'da firewall kullanımı için Hist Gradient Regressor yönteminin başarı oranı görülmektedir.

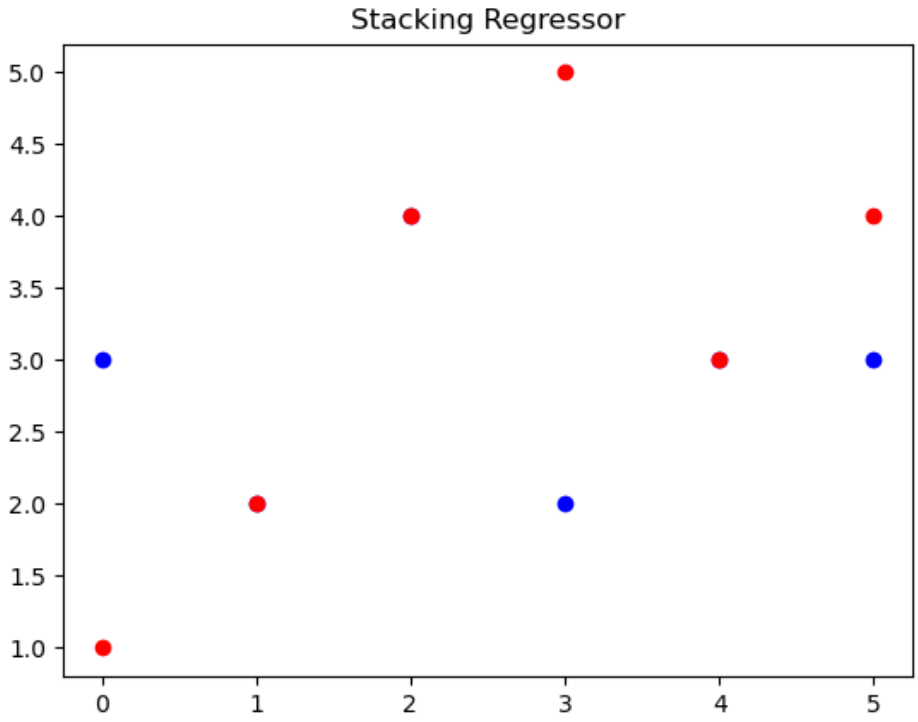


Şekil 39. Hist Gradient Regressor Başarı Oranı Gösterimi

Tablo 23'deki bilgilere istinaten; birinci adımda gerçek değer Watchguard ve model de Watchguard olarak tahmin ederek bu adımda doğru tahminde bulunmaktadır. İkinci adımda ise gerçek değer Fortigate iken model Watchguard tahmini yaparak yanlış bir tahminlemede bulunmaktadır. Bu yöntemde başarı oranı %50 olarak tespit edilmiştir.

4.4.4. Stacking Regressor Metodunun Başarı Oranı

Şekil 40'da firewall kullanımı için Stacking Regressor yönteminin başarı oranı görülmektedir.

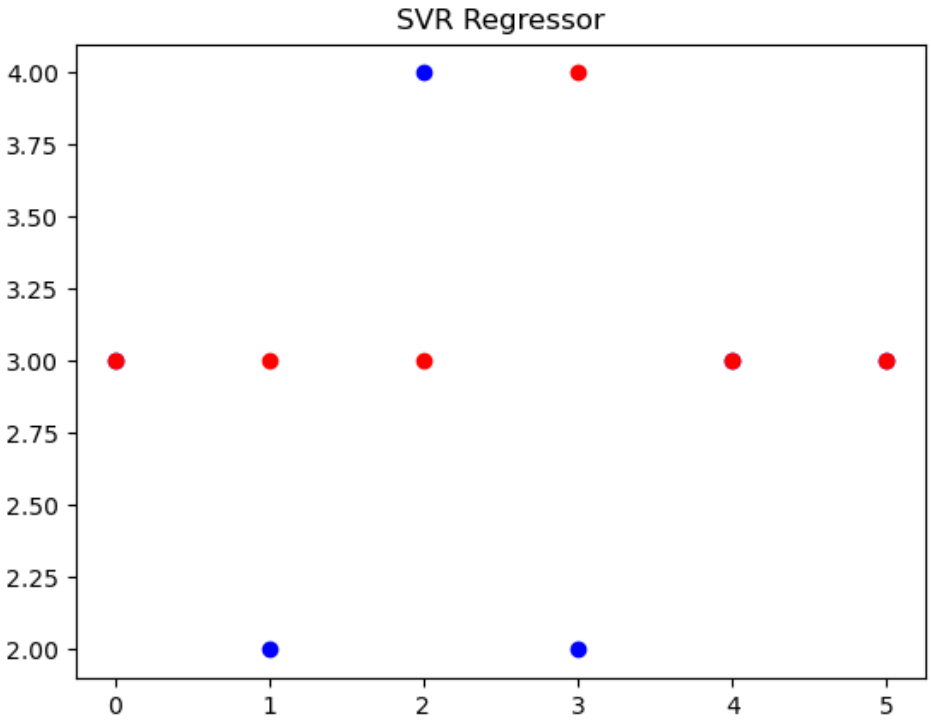


Şekil 40. Stacking Regressor Başarı Oranı Gösterimi

Tablo 23'deki bilgilere istinaden; birinci adımda gerçek değer Watchguard olmasına karşın, model Palo Alto olarak tahmin ederek bu adımda yanlış tahminde bulunuyor. İkinci adımda ise gerçek değer Fortigate ve model de Fortigate bularak bu adımda doğru tahminlemede bulunmaktadır. Modelin bu yöntemdeki başarı oranı %50 olarak tespit edilmiştir.

4.4.5. SVR Regressor Metodunun Başarı Oranı

Şekil 41'de firewall kullanımı için SVR Regressor yönteminin başarı oranı görülmektedir.

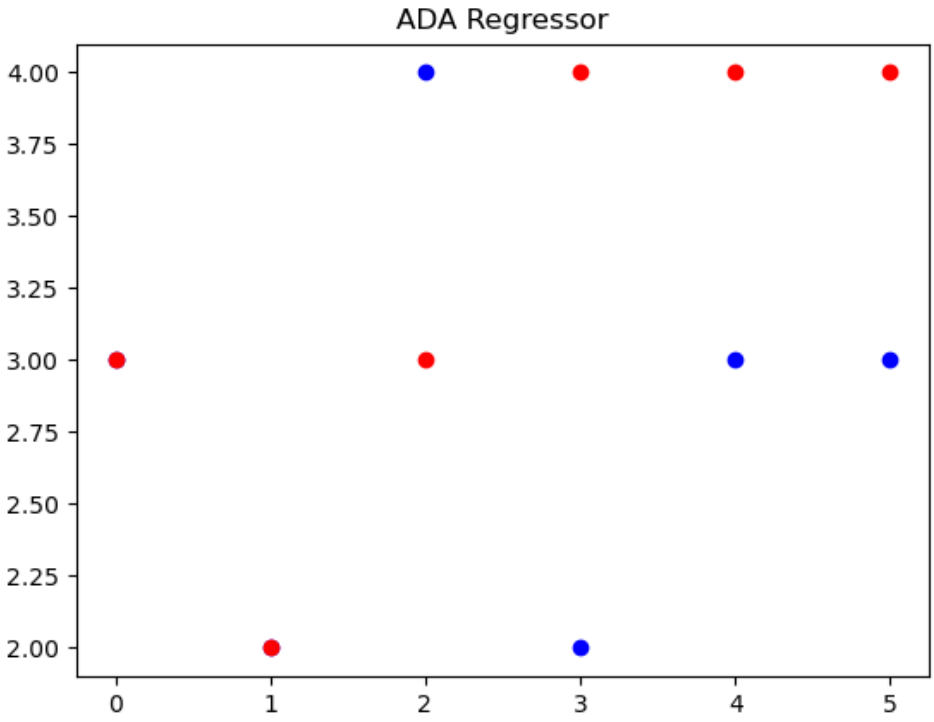


Şekil 41. SVR Regressor Başarı Oranı Gösterimi

Tablo 23'deki bilgilere istinaden; birinci adımda gerçek değer Watchguard ve model de Watchguard olarak tahmin ederek bu adımda doğru tahminde bulunmaktadır. İkinci adımda ise gerçek değer Fortigate iken model Watchguard tahmini yaparak yanlış bir tahminlemede bulunmaktadır. Bu yöntemde başarı oranı %50 olarak tespit edilmiştir.

4.4.6. Ada Boost Regressor Metodunun Başarı Oranı

Şekil 42'de firewall kullanımı için Ada Boost Regressor yönteminin başarı oranı görülmektedir.

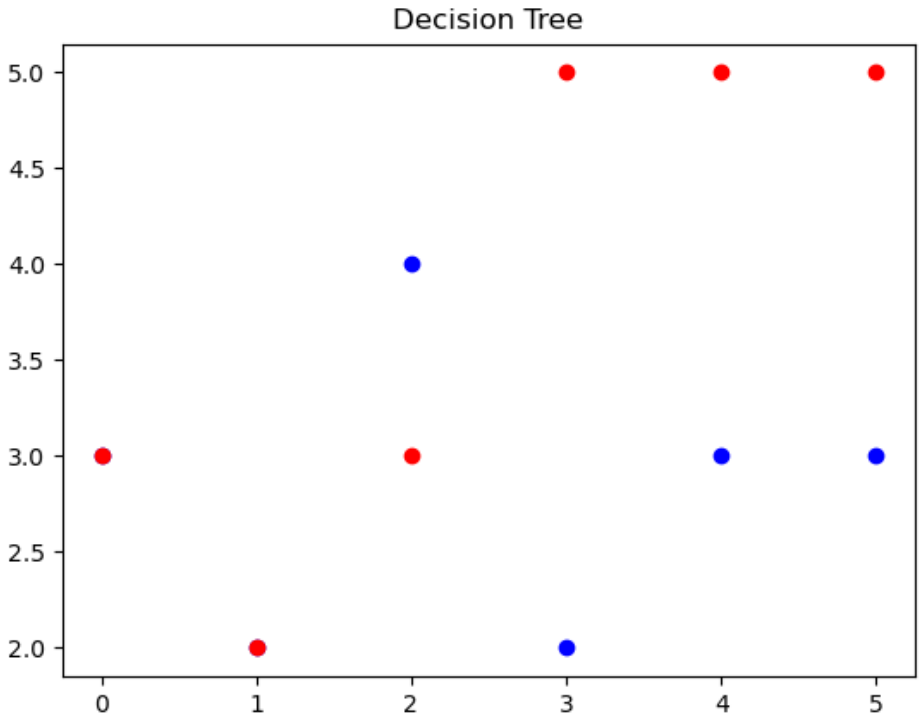


Şekil 42. Ada Boost Regressor Başarı Oranı Gösterimi

Tablo 23'deki bilgilere istinaden; birinci adımda gerçek değer Watchguard ve model de Watchguard olarak tahmin ederek bu adımda doğru tahminde bulunuyor. İkinci adımda gerçek değer Fortigate ve model de Fortigate bularak bu adımda da doğru tahminde bulunuyor; ancak daha sonraki dört denemede yaptığı tahminler yanlış olduğundan bu yöntem için başarı oranı %33 olarak tespit edilmiştir.

4.4.7. Karar Ağacı Metodunun Başarı Oranı

Şekil 43‘de firewall kullanımı için Decision Tree Regressor yönteminin başarı oranı görülmektedir.

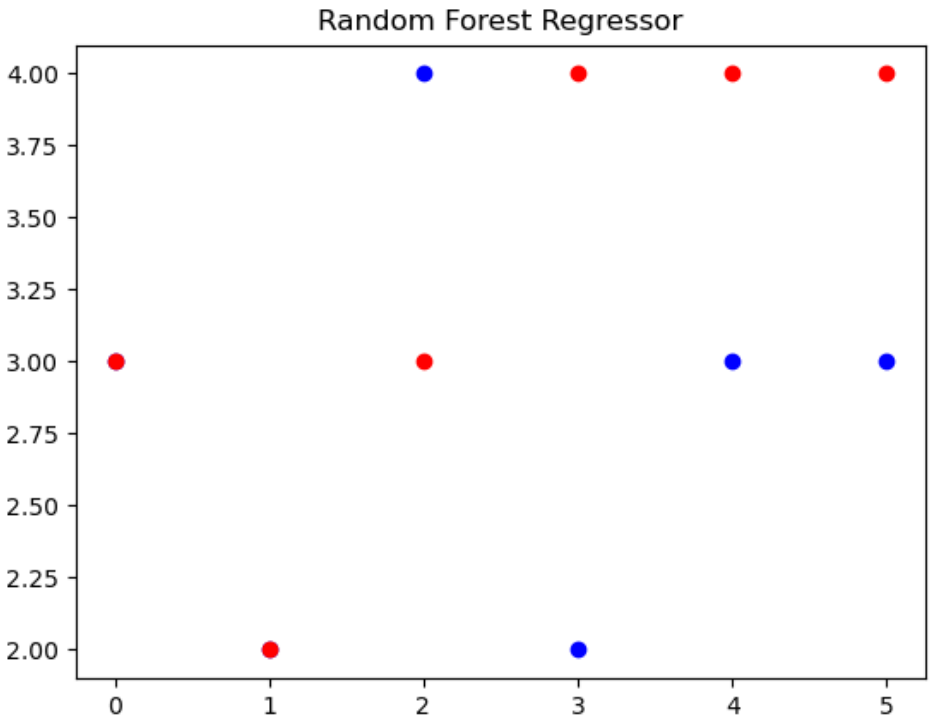


Şekil 43. Decision Tree Regressor Başarı Oranı Gösterimi

Tablo 23‘deki bilgilere istinaden; birinci adımda gerçek değer Watchguard ve model de Watchguard olarak tahmin ederek bu adımda doğru tahminde bulunuyor. İkinci adımda gerçek değer Fortigate ve model de Fortigate bularak bu adımda da doğru tahminde bulunuyor; ancak daha sonraki dört denemede yaptığı tahminler yanlış olduğundan bu yöntem için başarı oranı %33 olarak tespit edilmiştir.

4.4.8. RF Metodunun Başarı Oranı

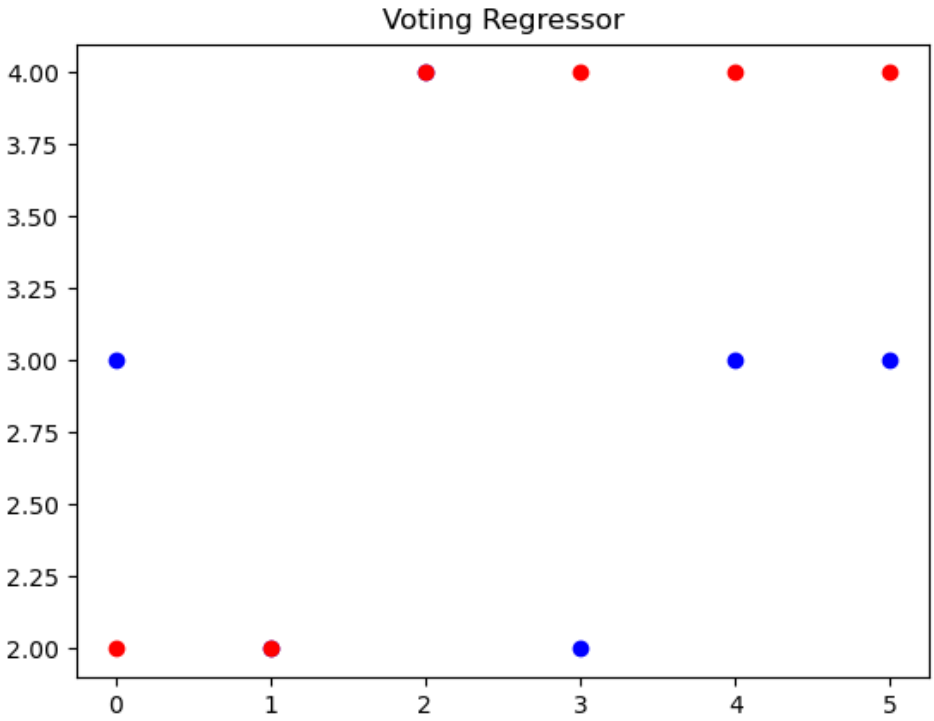
Şekil 44‘de firewall kullanımı için RF yönteminin başarı oranı görülmektedir.



Şekil 44. Random Forests Başarı Oranı Gösterimi

Tablo 23‘deki bilgilere istinaden; birinci adımda gerçek değer Watchguard ve model de Watchguard olarak tahmin ederek bu adımda doğru tahminde bulunuyor. İkinci adımda gerçek değer Fortigate ve model de Fortigate bularak bu adımda da doğru tahminde bulunuyor; ancak daha sonraki dört denemede yaptığı tahminler yanlış olduğundan bu yöntemin başarı oranı %33 olarak tespit edilmiştir.

4.4.9. Voting Regressor Metodunun Başarı Oranı

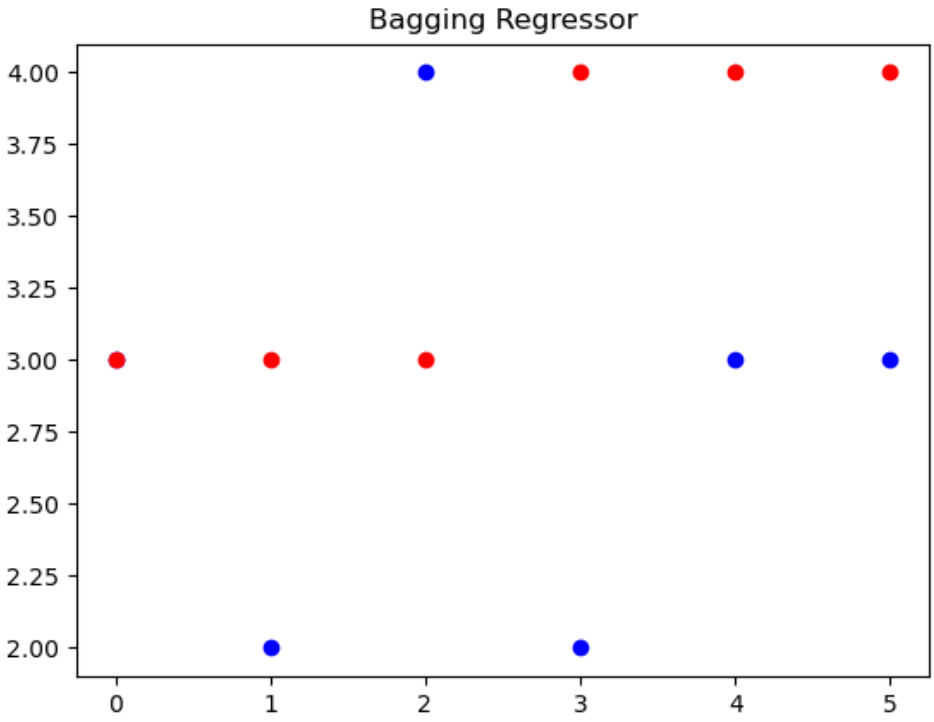


Şekil 45. Voting Regressor Başarı Oranı Gösterimi

Şekil 45'de firewall kullanımı için Voting Regressor yönteminin başarı oranı görülmektedir. Birinci adımda gerçek kullanılan firewall markası Watchguard iken, model önceki verilerden yararlanarak yaptığı tahminde bunu Fortigate olarak yanlış tahmin etmiştir. İkinci adımda ise gerçek değer Fortigate ve model de bu adımda doğru tahmin ederek Fortigate sonucunu bulmuştur. Üçüncü adımda gerçek değer Sonicwall, model bu adımı da doğru tahmin etmiştir ancak sonraki adımlarda yanlış tahminler yaptığından bu modelin başarı oranı %33 olarak tespit edilmiştir.

4.4.10. Bagging Regressor Metodunun Başarı Oranı

Şekil 46'da firewall kullanımı için Bagging Regressor yönteminin başarı oranı görülmektedir.

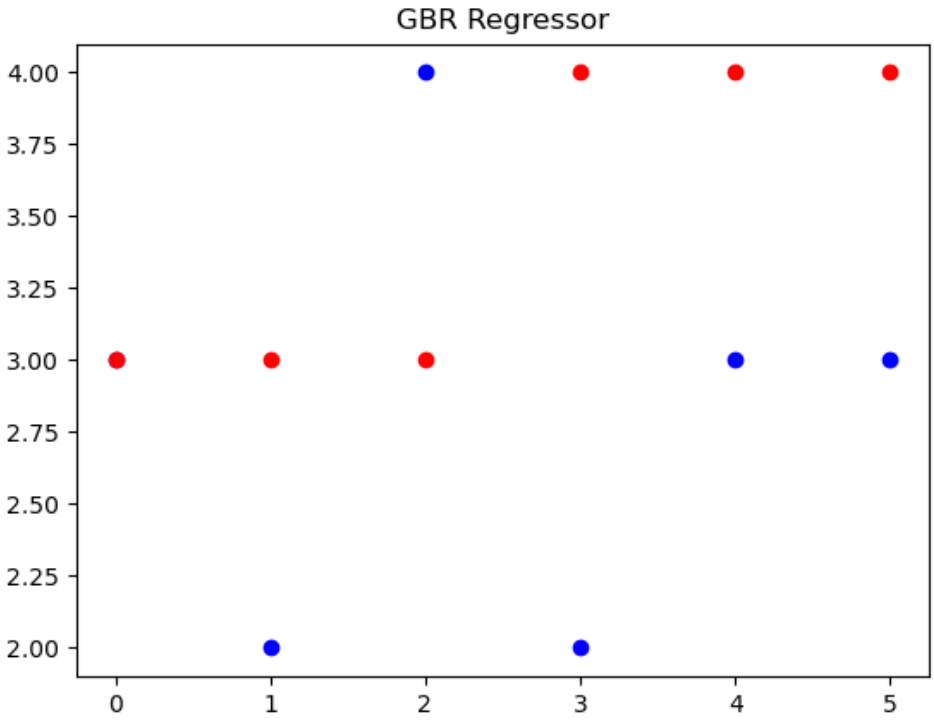


Şekil 46. Bagging Regressor Başarı Oranı Gösterimi

Tablo 23'deki bilgilere istinaten; birinci adımda gerçek değer Watchguard ve model de Watchguard olarak tahmin ederek bu adımda doğru tahminde bulunmaktadır. İkinci adımda ise gerçek değer Fortigate iken model Watchguard tahmini yaparak yanlış bir tahminlemede bulunmaktadır. Sadece bir kez doğru tahminde bulunduğundan bu yöntemde başarı oranı %16 olarak tespit edilmiştir.

4.4.11. Gradient Boost Regressor Metodunun Başarı Oranı

Şekil 47'de firewall kullanımı için Gradient Boost Regressor yönteminin başarı oranı görülmektedir.



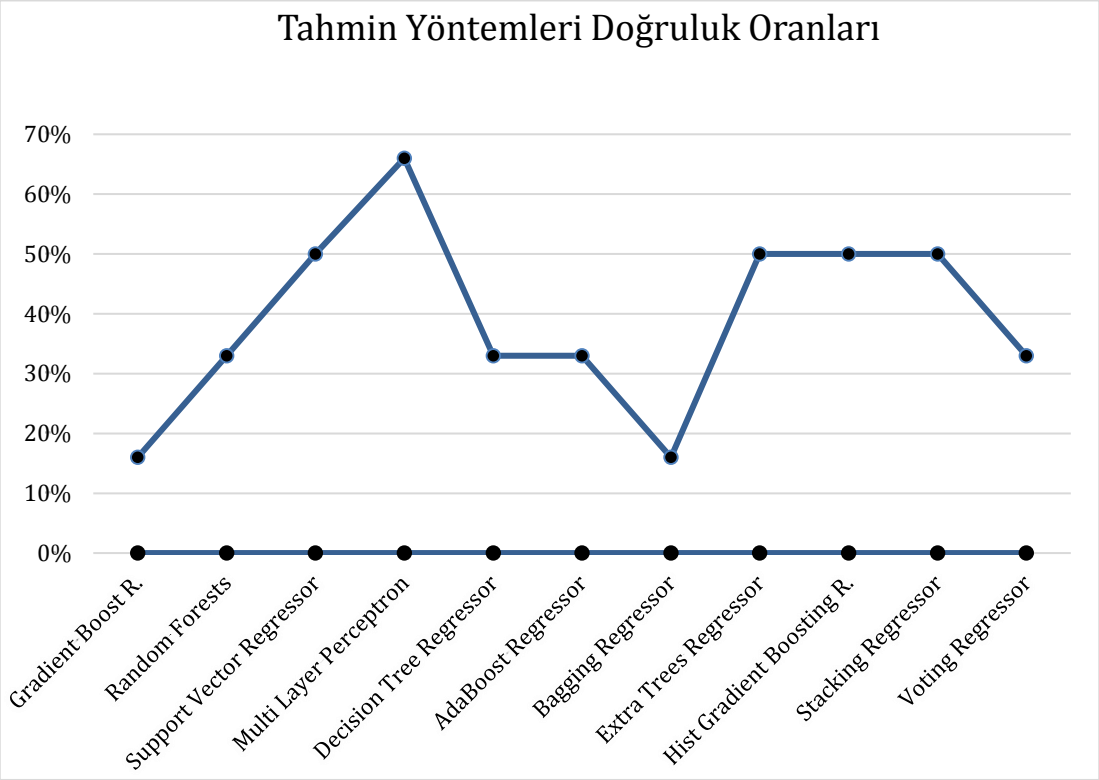
Şekil 47. Gradient Boost Başarı Oranı Gösterimi

Tablo 23'deki bilgilere istinaden; birinci adımda gerçek değer Watchguard ve model de Watchguard olarak tahmin ederek bu adımda doğru tahminde bulunmaktadır. İkinci adımda ise gerçek değer Fortigate iken model Watchguard tahmini yaparak yanlış bir tahminlemede bulunmaktadır. Sadece bir kez doğru tahminde bulunduğundan bu yöntemde başarı oranı %16 olarak tespit edilmiştir.

4.5. ML Yöntemlerinin Optimizasyonu ve Tahmini

Çalışmada 11 adet ML metodu kullanılmıştır ve bunlar sırasıyla, AdaBoost Regressor, Bagging Regressor, Decision Tree Regressor, Extra Trees Regressor, Gradient Boost Regressor, Hist Gradient Boosting Regressor, Multi Layer Perceptron, Random Forests, Stacking Regressor, Support Vector Regressor ve Voting Regressor metotlarıdır.

Doğruluk oranlarına göre kullanılan tüm yöntemlerin grafiği aşağıdaki gibidir;



Şekil 48. ML Yöntemlerinin Doğruluk Oranları

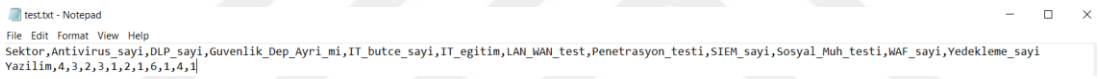
Çalışmada kullanılan metotlar doğruluk oranlarına göre küçükten büyüğe doğru; %16 doğruluk oranı ile Bagging Regressor, %16 doğruluk oranı ile Gradient Boosting Regressor, %33 doğruluk oranı ile AdaBoost Regressor, %33 doğruluk oranı ile Decision Tree Regressor, %33 doğruluk oranı ile RF, %33 doğruluk oranı ile Voting Regressor, %50 doğruluk oranı ile Extra Trees Regressor, %50 doğruluk oranı ile Hist Gradient Boosting Regressor, %50 doğruluk oranı ile Stacking Regressor, %50 doğruluk oranı ile SVR ve %66 doğruluk oranı ile MLP Regressor şeklinde tespit

edilmiştir. Yapılan çalışma sonucu ve elde edilen veriler dahilinde, modelleme değerlendirildiğinde en yüksek başarıyı sağlayan metodun, %66 doğruluk oranı ile MLP Regressor olduğu tespit edilmitşir.

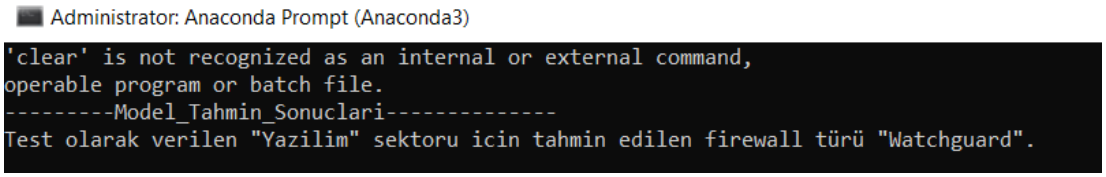
Python programlama dili ile yapılan çalışmada kullanılan girdi, manuel olarak değiştirilerek ve metodun toplanılan verilerden öğrendiklerinden faydalanması sağlanarak bir firewall önerisi çıktısına erişilebilmektedir.

Katılımcılara sorulan sorular manuel olarak .txt dosyası üzerinden cevaplanmıştır ve cevapların bulunduğu .txt dosyası ile çalıştırılan metot bir firewall önerisi çıktısı vermiştir.

Metin belgesi çıktısı ve firewall önerisi ise Şekil 49 ve Şekil 50‘de görülmektedir.



Şekil 49. Makine Öğrenmesi Girdilerinin Metin Belgesindeki Görünümü



Şekil 50. Metin Belgesindeki Girişlere Göre Yapılan Tahminin Gösterimi

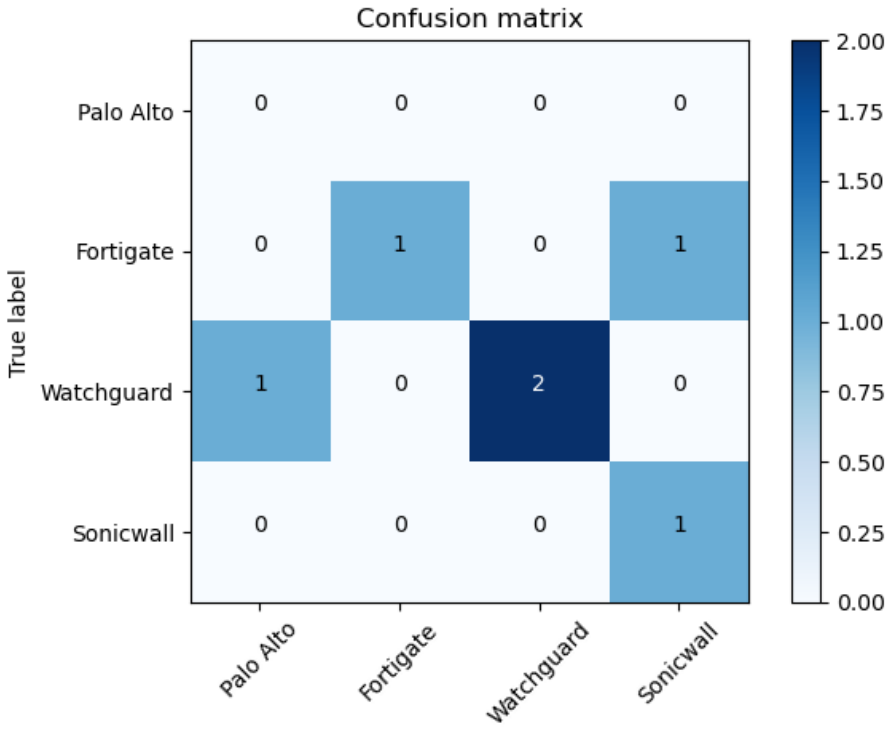
4.6. Karmaşıklık Matrisi

Karmaşıklık Matrisi (Multiclass Confusion Matrix), tahmine yönelik oluşturulan modelin çıktılarını ve performansını tablo haline getiren bir görselleştirme yöntemidir. Karmaşıklık matrisi bir modelin ya da sınıflandırmanın değerlendirilmesinde önemli rol oynar.

Karmaşıklık matrisinde; sütunlar gerçek veri sayısını, satırlar ise tahmin edilen veri sayısını göstermektedir. Bu sayede gerçek veriler ve tahmin edilen veriler arasında bir karşılaştırma sağlanır. Karmaşıklık matrisi, n x n matrisidir. "n" bu matrisde, sınıf veya çıktıyı ifade feder. Dolayısıyla çalışmada kaç adet sınıf var ise matris bu sınıflardan oluşarak, modelin performansını tablo haline getirir.

Bu çalışmada, Palo Alto, Fortigate, Watchguard ve Sonicwall olmak üzere dört sınıf bulunmaktadır. Bu nedenle oluşturulan karmaşıklık matrisi, dört satır ve dört sütundan oluşmakta ve 4 x 4'lük bir Karmaşıklık matrisi ortaya çıkartmaktadır.

Oluşturulan modelin Karmaşıklık Matrisi şekil 51'de gösterilmiştir.



Şekil 51. Karmaşıklık Matrisi

SONUÇ

Ağ güvenliği, özellikle internetin kullanım alanının genişlemesi sonucunda verinin son derece kritik olduğu alanlarda ve departmanlarda kullanılmasıyla birlikte hayati bir anlam taşımaya başlamıştır. Bu noktada, ağ güvenliği sadece belirli tehditlere hazırlıklı olmayı değil, aynı zamanda muhtemel tehditlere hazırlıklı olmayı ve tehditleri tahmin etmeyi zorunlu hale getirmektedir. Bu nedenle, ağ güvenliği uzmanları artık var olan tehditler ile ilgili olarak kendileri de farklı boyutları ön plana çıkararak düşünmektedirler ve bu sayede, kendileri için uygun olan güvenlik sistemini geliştirmeye çalışmaktadırlar.

Ağ güvenliği, temel olarak siber suçların yaygınlaşması ile birlikte daha fazla anlam kazanmış bir konudur. Bilgi hırsızlığı ve illegal yollar elde edilen verilerin yine illegal amaçlar için kullanılması nedeni ile siber suçların giderek çekici hale gelmesi, ağ güvenliği konusunda, her geçen gün, daha fazla yenilikçi uygulamanın kabul görmesini sağlamaktadır. Sürekli olarak belirli bir noktadan diğerine illegal yollarla veri transfer etmek isteyen tarafların sayısının artışı, ağ güvenliği konusunda özellikle kurumsal anlamda bir kez daha düşünülmesine sebebiyet vermiştir.

Bu noktada özellikle, sürecin kontrolden çıkmasıyla birlikte güvenlik önlemlerinin yetersiz kalmasının söz konusu olacağı öngörülmektedir. Bu nedenledir ki ağ güvenliği, bir temel kurulması ile birlikte uygulamada fayda sağlayabilecek ve uzun vadede bireysel ve kurumsal olarak korunma sağlanmasını mümkün hale getirebilecektir.

Araştırmada, katılımcı yetkililer ile gerçekleştirilen röportaj neticesinde ağ güvenliği hususunda kurumsal anlamdaki görüşleri ve değerlendirmeleri farklı açılardan ele alınmıştır. Araştırmanın ortaya koymuş olduğu sonuçlara bakıldığında, ağ güvenliği konusunda katılımcıların bağlı bulundukları şirketlerin hepsinin konuya ciddi olarak önem verdikleri fark edilmektedir. Bu bilinç ve farkındalık katılımcıların şirketlerinin ağ güvenliği konusunda yaşanan ve yaşanabilecek riskler hakkında ciddi ölçekli bir bilinç sahibi olduklarını göstermektedir. Genel olarak ise gerçekleştirilen röportajların sonuçları dahilinde ön plana çıkarılabilecek dört adet olumlu bulgu söz konusudur.

Araştırmaya dair elde edilen bulgulardan ilki, katılımcıların şirketlerinin ağ güvenliği elemanlarını, unsurlarını ve araçlarını tercih ederken yerleşik bir bilinç ve yerleşik bir tecrübe ile kararlarını veriyor olmalarıdır. Bir güvenlik programını ya da uygulamasını seçerken uygulamanın neleri beraberinde getirip ne noktalarda eksikliklerinin olduğunu görebilmek adına hem katılımcılar hem de katılımcıların şirketleri yetkinliğe sahiptirler. Bu yetkinlik, sistemin sağlığı için nelere ihtiyaç duyulduğu konusunda, daha önceki süre zarfında gerçekleştirilmiş olan eylemlerin ortaya çıkardığı sonuçlarla mümkün olmuştur. Katılımcıların neredeyse tamamı, ağ güvenliği konusunda kullandıkları tüm unsurları geçmişte test etmiş ve detaylı bir biçimde inceledikten sonra mevcut süreçte ağ güvenliği için birincil tercihleri haline getirmişlerdir.

Araştırma bulgularına dair ikinci bir tespit katılımcıların hem kendilerinin hem de şirketlerinin ağ güvenliği konusunda eğitim ve gelişim açısından yeterli derecede iyi algılamalarının olduğu ve bu konuya yeterli düzeyde ilgi gösterdikleri ve bütçe ayırdıklarıdır. Hem kuruma ilk katıldıkları andan itibaren hem de ilerleyen süre zarfı içerisinde BT bünyesinde görev alanların ve genel olarak da kurum çalışanlarının ağ ve veri güvenliği konusunda yeterli bir bilgi düzeyine gelişmesi açısından, katılımcı yetkililerin şirketleri gereken yönetimsel sorumlulukları almaktadırlar. Bazı katılımcıların belirttiği üzere, şirketler dışarıdan almış oldukları ağ güvenliği desteğine paralel olarak kendileri de bu konudaki gelişmeleri yakından takip etmektedirler. Bu bakış açısı, söz konusu kurumlar için ağ güvenliği konusunun değişim odaklı olarak yakından takip edildiğini göstermektedir.

Bulgularla ilgili üçüncü bir husus, katılımcıların şirketlerinin ağ güvenliği konusundaki eksikliklerini anlamak ve kendi sistemlerinin zayıf noktalarını tespit edebilmek adına, düzenli olarak almış oldukları ağ güvenliği desteğinin dışında da denemeler, çalışmalar ve araştırmalar yapıyor olmalıdır. Böyle bir durum şirketlerin ağ güvenliği gibi kritik bir konuda kontrolü tamamı ile dışarıdan almış oldukları yazılımsal ve teknik desteğe bırakmadıklarının; bir başka deyişle, süreci içerisindeki teknik tüm detaylara hâkim olup kendilerini, ağlarını ve ağlarındaki verileri en güçlü şekilde korumaya çalıştıklarını göstermektedir. Katılımcıların belirttiği üzere, şirketleri geçmiş zamanda ağ güvenliği konusunda yaşanan açıklar, eksiklikler, yanlış

tasarımlar ve denetim yoksunlukları nedeniyle farklı saldırılara maruz kalmışlardır. Halen de katılımcıların şirketleri çeşitli şekillerde ağ temelli saldırılarla karşılaşmaktadırlar. Bu nedenle, sistemin içerisinde kendilerinin de entegre olmaları kritik bir öneme sahiptir.

Nihai bir bulgu olarak ise dosya yedekleme konusunda şirketlerin sahip oldukları düzen ve disiplindir. Bu düzen ve disiplin içerisinde, ağ üzerinde akışı sağlanan ve aktif olarak şirketlerin işleyişi açısından hassasiyet içeren verilerin ve bilgilerin sık, düzenli ve korunaklı bir biçimde ağ üzerinde ve farklı alanlarda saklanmaları adına yedeklenmeleri, katılımcıların şirketlerinin ağ güvenliği konusunda kendi önlem mekanizmalarını aktif ve güçlü bir şekilde yönettiklerini ve yürüttüklerini göstermektedir.

Araştırma bulguları açısından olumsuz olarak değerlendirilebilecek üç farklı noktadan bahsetmek gerekmektedir. Bunlardan ilki, katılımcıların şirketlerinin ağ güvenliği için seçilen uygulamalar konusunda fiyat hususuna çok fazla odaklanmaları ve bu nedenle de ağ güvenliği konusunda ayırdıkları bütçenin göreceli olarak düşük kalmasıdır. Her ne kadar şirket yönetimleri kullanımından, güvenilirliğinden ve sağladığı faydalardan memnun olsalar da şirketlerin verilerinin şirketler açısından söz konusu olan önemi arttıkça ağ temelli olarak işleyen sistemlerin korunması adına harcanması gereken bütçenin de aynı oranda artması gerekmektedir. Katılımcılardan yalnız birinin ağ güvenliği odaklı olarak BT departmanı bünyesindeki faaliyetleri harcamış olduğu bütçe çok yüksektir; diğer şirketlerin bütçeleri göreceli olarak düşüktür. Bu durum, söz konusu şirketin büyüklüğü ile alakalı olsa da hedef verilerin korunması ise şirket ölçekleri belirli bir noktadan itibaren pek bir anlam ifade etmemektedir.

Araştırmaya dair olumsuz olarak nitelendirilebilecek bir diğer nokta ise ağ üzerinde aktif olarak çalışan şirket çalışanlarının güvenlik algılaması konusunda bireysel anlamda ki ciddi eksiklikleri ve zaaflarıdır. Şirketler halen bu konuda yeterli derecede bir ilerleme kaydedememişlerdir. Bu durumun temel nedeni, ağ güvenliği konusunda şirketlerin üst yönetimi ile BT birimlerinin tek başlarına konuya daha fazla ehemmiyet göstermesidir. Her ne kadar çalışanlara bu konuda yeterli düzeyde eğitimler verilse de halen ağ güvenliğini ve ağdaki verilerin değerini zarara uğratacak

şekilde hatalar yapılmaya devam edilmektedir ve katılımcılar bundan son derece şikayetçidir. Bu noktada ağ güvenliği açısından, şirketlerde toplu olarak bir bilincin yerleşik olmasının ne denli önemli olduğu daha iyi anlaşılmaktadır.

Araştırmaya dair olumsuz yönde değerlendirilebilecek son bulgu ise şirketlerin bu denli ağ güvenliği konusuna önem veriyorlarken WAF ürünü kullanımı ve LAN ve WAN testlerinin uygulanması konusunda çok istekli ve çok gönüllü olmamalarıdır. Katılımcıların çok büyük bir bölümü bu ağ ile ilgili kritik değere sahip olabilecek ürün ve hizmetleri kullanmak hususunda farklı alternatifler ile süreci işletmeyi tercih etmişlerdir. Bu durum, mevcut süreçte herhangi bir sorun içermiyor gibi gözükse de ilerleyen süre zarfında yaşanması muhtemel olan ağ temelli sorunlar için şirketlerin kendi elleriyle yaratacakları bir riski ifade etmektedir.

Ayrıca bu tez çalışmasında, röportaj ve analiz sonuçlarının kıyaslamasını istatiksel anlamda değerlendirmek ve sonuçların analizlerini algoritma mantığı çerçevesinde modelleyerek değerlendirmek adına yapay zekanın bir alt dalı olan ML ve ML altındaki metotlar kullanılmıştır. Kullanılan metotların kıyaslaması yapılmış ve çıkan sonuçlar dahilinde, doğruluk oranlarına göre en iyi ML metodunun hangisi olduğuna karar verilmiştir. Çalışmada kullanılan metotlar doğruluk oranlarına göre küçükten büyüğe doğru; Bagging Regressor (%16 doğruluk oranı), Gradient Boosting Regressor (%16 doğruluk oranı), AdaBoost Regressor (%33 doğruluk oranı), Decision Tree Regressor (%33 doğruluk oranı), Random Forest (%33 doğruluk oranı), Voting Regressor (%33 doğruluk oranı), Extra Trees Regressor (%50 doğruluk oranı), Hist Gradient Boosting Regressor (%50 doğruluk oranı), Stacking Regressor (%50 doğruluk oranı), Support Vector Regressor (%50 doğruluk oranı) ve MLP Regressor (%66 doğruluk oranı) şeklinde tespit edilmiştir. Yapılan çalışma sonucu ve elde edilen veriler dahilinde modelleme değerlendirildiğinde, en yüksek başarıyı sağlayan metodun %66 doğruluk oranı ile MLP Regressor olduğu tespit edilmiştir. Bu orana istinaden yapılan son firewall tahmin işleminde başarı ve doğruluk oranından dolayı MLP Regressor metodu detaylı bir şekilde tanıtılmış ve kullanılmıştır. Doğruluk oranları kıyaslaması yapıldığında diğer dört metodun da %50 olması çalışmanın tahminlemesine destekleyici unsurlar sağlamıştır. %50 altında bulunan metotların

sonuçları değerlendirilmiş fakat analiz çalışmasında %50 ve üzerinde doğruluk oranı veren metotlar mukayese edilmiştir.

Çalışmaya katılan şirket sayısı ve diğer unsurlar bu metotların doğruluk oranlarında etki etmiştir. Katılım sağlayan şirket sayısı, çalışmadaki soruların sayısı ve alınan cevapların istatiksel oranları sayesinde elde edilen veriler, kullanılan 11 metot sayesinde incelenmiş, kıyaslanmış ve algoritma çerçevesine oturtulmuştur.

Elde edilen sonuçlar ve karşılaştırmalar sayesinde, %66 doğruluk oranıyla en iyi ML metodunun MLP Regressor olduğuna karar verilmiş ve benzer bir çalışmaya/çalışmalara motivasyon kaynağı olabileceği belirlenmiştir. En yüksek doğruluk oranına sahip MLP Regressor metodu kullanılarak yeni bir model oluşturulmuş ve bu modelde, katılımcılara sorulan soruların cevapları .txt dosyası üzerinden manuel olarak değiştirilmiştir. Oluşturulan yeni modelde verilen bu cevaplara göre daha önce öğrenilen veriler kullanılarak en uygun firewall tahmininin yapılması sağlanmıştır.

Röportaj sonuçlarından elde edilen verilere ek olarak, kullanılan veri sayısının arttırılması ve katılımın daha yüksek oranlarda sağlanabildiği çalışmalarda, metotların tahmin başarısının daha yüksek çıkabileceği öngörüsünde bulunulabilmektedir. Dolayısıyla gerçek veri sayısının arttırılması, tahmin başarısının yüksek çıkması açısından ve doğruluk oranlarının mukayese edilebilmesi açısından faydalı olacaktır.

KAYNAKÇA

Kitaplar:

Ahonen, P. (2011). *Constructing Network Security Monitoring Systems*. Espoo: VTT Technical Research Centre of Finland.

Chao, L. (2016). *Cloud Computing Networking - Theory, Practice, and Development*. Florida: CRC Press.

Çakır, S. ve Kesler, M. (2012). *Bilgisayar Güvenliğini Tehdit Eden Virüsler ve Antivirüs Yazılımları*. Akademik Bilişim'12 - XIV. Akademik Bilişim Konferansı Bildirileri 1 - 3 Şubat 2012 Uşak Üniversitesi, 469-476.

Çifçi, H. (Ed.) (2013). *Her Yönüyle Siber Savaş*. İstanbul: TUBİTAK Popüler Bilim Kitapları.

Gündüz, M. Z. ve Daş, R. (2014). *Kablosuz Yerel Alan Ağlarına Sızma Uygulaması ve Temel Güvenlik Önerileri*. 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 17-18 Ekim 2014, İstanbul, 295-300.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, (2012). *Siber Güvenlik Raporu*. İstanbul: İstanbul Bilgi Üniversitesi Bilişim Ve Teknoloji Hukuku Enstitüsü.

MEGEP (2011). *Elektrik-Elektronik Teknolojisi - Ağ Güvenliği Ve Ağ Protokolleri*. Ankara: MEB Yayını.

MEGEP (2013). *Bilişim Teknolojileri - Ağ Güvenliği*. Ankara: MEB Yayını.

Mattos, D. M. F., Ferraz, L. H. G. & Duarte, O. C. M. B. (2015). *Cloud Services, Networking and Management*. New Jersey: Wiley.

Nieles, M., Dempsey, K. & Pillitteri, V. Y. (2017). *An Introduction to Information Security*. Washington: National Institute of Standards and Technology.

Pande, J. (2017). *Introduction to Cyber Security*. Haldwani: Uttarakhand Open University.

Schoo, P. et al. (2010). *Challenges for Cloud Networking Security*. Mobile Networks and Management - Second International ICST Conference, MONAMI 2010, Santander, Spain, September 22-24, 2010, 1-14.

Stallings, W. (2011). *Cryptography And Network Security Principles And Practice* (5th Edition). New York: Prentice Hall.

Şahinaslan, Ö., Şahinaslan, E. ve Kantürk, A. (2011). *Kablosuz Ağlarda Bilgi Güvenliği ve Farkındalık*. IV. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, 25-26 Kasım 2011, Ankara, 1-6.

Vielberth, M. (2021). *Security Information and Event Management (SIEM)*. In S. Jajodia et al. (Eds.), "Encyclopedia of Cryptography, Security and Privacy". Berlin: Springer, 1-3.

Yıldırım, E. Y. (2018). *Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması*. 2. Uluslararası Mesleki Bilimler Sempozyumu, IVSS 2018, 1-10.

Süreli Yayınlar:

Al, U. (2002). İnternet'te Veri Güvenliği. *Oluşum*, (38), 37-50.

Bacudio, A. G. et al. (2011). An Overview Of Penetration Testing. International *Journal of Network Security & Its Applications (IJNSA), 3*(6), 19-38.

Bağcı, H. (2009). Sosyal Mühendislik ve Denetim. Denetişim, (Kış 2009), 42-51.

Deshpande, A. V. (2015). Introduction to Network Security. *International Journal of Computer Sciences and Engineering, 3*(9), 124-134.

Fırlar, T. (2003). Ağ Güvenliği. *SAU Fen Bilimleri Enstitüsü Dergisi, 7*(1), 9-16.

Funmilola, A. & Oluwafemi, A. (2015). Review of Computer Network Security System. *Network and Complex Systems, 5*(5), 40-46.

Güleç, Ö. ve Kişman, Z. A. (2021). Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri. *Akademik Açı, 1*(1), 127-154.

Jadhav, P. & Chawan, P. M. (2019). Data Leak Prevention System: A Survey. *International Research Journal of Engineering and Technology (IRJET),* 6(9), 1-4.

Manaseer, S. & Al Hwaitat, A. K. (2018). Centralized Web Application Firewall Security System. *Modern Applied Science, 12*(10), 164-170.

Moura, J. & Hutchison, D. (2016). Review and Analysis of Networking Challenges in Cloud Computing, *Journal of Network and Computer Applications, 60*, 113-129.

Önal, M. A. (2021). Siber Uzay ve Güvenlik İlişkisi Bağlamında Siber Güvenliğin Boyutları. *Hitit Ekonomi ve Politika Dergisi, 1*(2), 114-123.

Sanghavi, P., Mehta, K. & Soni, S. (2013). Network Security. *International Journal of Scientific and Research Publications, 3*(8), 1-5.

Schuett, M. & Rahman, S. S. M. (2011). Information Security Synthesis in Online Universities. *International Journal of Network Security & Its Applications (IJNSA), 3*(5), 1-20.

Yıldırım, N. ve Varol, A. (2013). Sosyal Ağlarda Güvenlik: Bitlis Eren ve Fırat Üniversitelerinde Gerçekleştirilen Bir Alan Çalışması. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 6*(1), 1-11.

Tezler

Akcan, F. (2021). *Kollektif Makine Öğrenmesi Metodları ve Göğüs Kanseri Teşhisi* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Üniversitesi Cerrahpaşa Lisansüstü Eğitim Enstitüsü, İstanbul.

Alkalidi, O,T,A. (2017). *GRNN ve MLP Metotları Kullanılarak Geri Dönen Meme Kanser Tesbiti* (Yayımlanmamış Yüksek Lisans Tezi). Türk Hava Kurumu Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Arık, İ. (2017). *İdeal Kampüs Ağ Yapısının Tasarımı ve Güvenlik Performansının Değerlendirilmes*i (Yayımlanmamış Yüksek Lisans Tezi). Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyonkarahisar.

Dilek, A, İ. (2022). *Modeling Educational Data With Machine Learning Methods* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Kültür Üniversitesi Matematik ve Bilgisayar Bilimleri Enstitüsü, İstanbul.

Erol, B. (2019). *Ağ Trafik Özelliklerinin Analizini Yaparak Anormalliklerin Tespit Edilmesi* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Aydın Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Güngör, M. (2015). *Ulusal Bilgi Güvenliği Strateji ve Kurumsal Yapılanma* (Uzmanlık Tezi). Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı, Ankara.

Yürekli, Ş. (2017). *Geniş Çalışma Bölgeli Bir Mikrodalga Transistörünün Destek Vektör Regresyon Makinesi İle Modellenmesi* (Yayımlanmamış Yüksek Lisans Tezi). Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

İnternet Kaynakları

3COM (2000). Network Security: A Simple Guide to Firewalls. Erişim adresi http://www.uky.edu/~dsianita/390/firewall1.pdf (29.05.2022).

Assunção, P. (2019). A Zero Trust Approach to Network Security. Erişim adresi https://privacyandsecurityconference.pt/proceedings/2019/DPSC2019-paper14.pdf (21.04.2022).

Kruegel, Christopher 2022,https://sites.cs.ucsb.edu/~chris/research/doc/iit04_security.pdf, Erişim tarihi 03.05.2022)

Makaleler

Breiman, L. (2001). Random Forests. Erişim adresi

https://link.springer.com/content/pdf/10.1023/A:1010933404324.pdf

EKLER

Ek-1: Araştırmada Kullanılan Röportaj Formu

Türkiye'de Özel Sektörde Hizmet Veren ve Farklı Alanlarda Faaliyetleri Bulunan Şirketlerin, Bilgisayar Ağ Güvenliğine Karşı Aldaıkları Aksiyonları İnceleyen Bir Araştırma: Bilgisayar Ağ Güvenliğinin Analizi ve Araştırması.

İzin ve Açıklama

Ben Murat Üstünkaya, Beykent Üniversitesi Bilgisayar Mühendisliği Bölümü Tezli Yüksek Lisans öğrencisiyim. Üzerinde çalıştığım tez için, Türkiye'deki özel sektör şirketlerinin, ağ güvenliği alanında yapılan çalışmalara dair yetkili bireylerin konu hakkındaki düşüncelerini ve uygulamalarını öğrenebilmek, katılımcıların şirketlerinde uygulanan sistemlerde hangi yöntemlerin benimsendiği hususunda fikir edinebilmek amacı ile araştırma yapmaktayım.

Araştırma konusuna bağlı olarak yapılan görüşmeye ilişkin bilgiler ve kimliğiniz yüksek lisans tezim dışında hiçbir yerde kullanılmayacak ve hiçbir kurum/kuruluş ve kişiler ile paylaşılmayacaktır. Araştırmanın herhangi bir aşamasında araştırmadan çekilebilirsiniz.

Araştırma konusuna karşı gösterdiğiniz ilgi ve çalışma hayatınıza ait deneyim ve tecrübelerinizi benimle paylaşarak araştırma konuma sağladığınız katkılarınızdan ötürü teşekkür ederim.

Katılımcılara Yöneltilen Sorular

- Çalışanı olduğunuz şirkette Firewall kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?
- Çalışanı olduğunuz şirkette WAF kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?
- Çalışanı olduğunuz şirkette SIEM kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?
- Çalışanı olduğunuz şirkette DLP kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?

- Çalışanı olduğunuz şirkette Antivirüs kullanılmakta mıdır? Kullanılmakta ise hangi marka kullanılmaktadır? Bu markanın tercih edilme sebebi nedir?
- Çalışanı olduğunuz şirkette ağ ve veri güvenliği için yapılan ekstra çalışmalar var mıdır? Var ise bunlar ne tür çalışmalardır?
- Çalışanı olduğunuz şirkette ne kadar sıklıkta Penetraston Testi yapılmaktadır/yaptırılmaktadır?
- Çalışanı olduğunuz şirkette ne kadar sıklıkta LAN ve WAN atak testleri yapılmaktadır/yaptırılmaktadır?
- Çalışanı olduğunuz şirkette ağ ve veri güvenliği ile alakalı herhangi bir zaafiyetle karşılaşıldı mı? Karşılaşıldı ise bu zaafiyetler nelerdir?
- Çalışanı olduğunuz şirkette dosya yedekleri ne kadar sıklıkta alınmaktadır?
- Çalışanı olduğunuz şirkette kullanıcı hatalarına karşı şirket içi eğitim verilmekte midir?
- Çalışanı olduğunuz şirkette ne kadar sıklıkta sosyal mühendislik (şirket içi çalışan farkındalığı) testleri yapılmaktadır?
- Çalışanı olduğunuz şirketin BT departmanlarında çalışanların güvenlik eğitimi alınması sağlanmakta mıdır?
- Çalışanı olduğunuz şirketin BT güvenliği için yıllık ayırdığı bütçe hangi aralıktadır?
- Çalışanı olduğunuz şirketin ayrı bir güvenlik departmanı bulunmakta mıdır? Bulunmuyor ise güvenlik ile ilgili çalışan kişiler da BT departmanı dahilinde mi çalışmaktadır?