ULUSLARARASI SOSYOLOJİ VE EKONOMİ DERGİSİ
INTERNATIONAL JOURNAL OF SOCIOLOGY AND ECONOMICS
www.isoec.net
e-ISSN: 2651-527X

DOI: http://doi.org/10.5281/zenodo.14295734 **Accepted:** 01.12.2024

Kurumsal Siber Güvenliğe Yönelik Tehditler

Threats to Corporate Cyber Security

Sakin KARAÇIRAK
Yalova İl Sağlık Müdürlüğü
skaracirak@gmail.com, ORCID: https://orcid.org/0009-0002-1372-8677

Özet

Kurumsal siber güvenlik, dijital dünyada kurumların karşılaştığı en büyük tehditlerden biridir. Bu çalışma, kurumsal siber güvenlik tehditlerinin türlerini, bu tehditlerin organizasyonlar üzerindeki etkilerini ve alınması gereken savunma önlemlerini incelemektedir. Çalışmanın bulguları, ransomware (fidye yazılımı), sosyal mühendislik saldırıları, biyometrik güvenlik zayıflıkları gibi çeşitli tehditlerin kurumlar için önemli riskler oluşturduğunu göstermektedir. Ransomware saldırıları, finansal zararlar ve veri kayıplarına yol açarken, sosyal mühendislik ve biyometrik güvenlik açıkları da insan hataları ve güvenlik ihlalleri ile sonuçlanmaktadır. Bu tehditlere karşı alınan önlemler arasında şifreleme, yedekleme, antivirüs yazılımları ve çalışan eğitimi gibi stratejiler yer almaktadır. Çalışma, kurumsal siber güvenlik stratejilerinin sadece teknolojik önlemlerle değil, aynı zamanda insan faktörüyle de desteklenmesi gerektiğini vurgulamaktadır.

Anahtar Kelimeler: Kurumsal Siber Güvenlik, Ransomware**,** Sosyal Mühendislik**,** Biyometrik Güvenlik**,** Şifreleme**,** Veri Kaybı

Abstract

Corporate cybersecurity is one of the biggest threats that organizations face in the digital world. This study examines the types of corporate cybersecurity threats, the effects of these threats on organizations, and the defensive measures that should be taken. The findings of the study show that various threats such as ransomware, social engineering attacks, and biometric security weaknesses pose significant risks to organizations. While ransomware attacks lead to financial losses and data loss, social engineering and biometric security vulnerabilities also result in human errors and security breaches. The measures taken against these threats include strategies such as encryption, backup, antivirus software, and employee training. The study emphasizes that corporate cybersecurity strategies should be supported not only by technological measures but also by the human factor.

Keywords: Corporate Cybersecurity, Ransomware, Social Engineering, Biometric Security, Encryption, Data Loss

ULUSLARARASI SOSYOLOJİ VE EKONOMİ DERGİSİ
INTERNATIONAL JOURNAL OF SOCIOLOGY AND ECONOMICS
www.isoec.net
e-ISSN: 2651-527X

GİRİŞ

Kurumsal siber güvenlik, bir organizasyonun dijital varlıklarını, bilgi sistemlerini ve verilerini potansiyel tehditlerden koruma amacı güder. Son yıllarda, siber saldırılar giderek daha karmaşık hale gelmiş ve organizasyonlar için büyük riskler oluşturmuştur. Siber güvenlik tehditleri, yalnızca dış saldırılarla sınırlı kalmayıp, iç tehditler, sosyal mühendislik saldırıları, zararlı yazılımlar ve sistem zafiyetlerinden kaynaklanan riskler gibi çeşitli boyutlarda ortaya çıkmaktadır. Bugün, siber saldırılar giderek daha sofistike ve hedefli hale gelmektedir. Phishing, spear-phishing, ransomware (fidye yazılımı), cryptojacking gibi saldırılar, kurumsal ağlar ve veri güvenliği açısından önemli tehditler arasında yer almaktadır (Blyth & Kovacich, 2015; Gupta & Kaur, 2016). Özellikle kurumsal sistemlerde zafiyetleri hedef alan false data injection attacks ve man-in-the-middle attacks gibi saldırılar, bilgi güvenliğini ciddi şekilde tehdit etmektedir (Gönen et al., 2020; Taştan et al., 2023). Bir başka önemli tehdit kategorisi ise iç tehditlerdir. İçeriden gelen tehditler, genellikle çalışanlar veya iş ortakları tarafından gerçekleştirilen, organizasyonun bilgi sistemlerine zarar verme amacını taşıyan eylemleri ifade eder. Bu tür tehditler, genellikle kötü niyetli çalışanlar veya güvenlik önlemleri zayıf kişiler tarafından gerçekleştirilir (Bishop, 2018; CERT Insider Threat Center, 2018). İç tehditler, organizasyonun gizli bilgilerine, finansal verilerine ve diğer kritik bilgilere doğrudan zarar verebileceği için büyük bir risk oluşturur. Biyometrik verilerin güvenliği de önemli bir tehdit alanıdır. Biyometrik kimlik doğrulama sistemleri, güvenliği sağlamak amacıyla yaygın olarak kullanılmaktadır, ancak bu sistemler de çeşitli güvenlik açıklarına sahiptir. Biyometrik sahtekarlık ve biometric spoofing gibi saldırılar, biyometrik verilerin çalınmasını veya manipüle edilmesini hedefler (Sudar et al., 2019; Jain et al., 2006). Bu tür güvenlik açıkları, özellikle kurumların fiziksel ve dijital güvenlik önlemlerini birleştirdiği durumlarda büyük tehlikeler yaratabilir.

Ayrıca, ransomware saldırıları, organizasyonları hedef alarak verilerini şifreler ve fidye ödemeleri talep eder. Bu tür saldırılar, sadece finansal kayıplara neden olmakla kalmaz, aynı zamanda organizasyonun itibarı üzerinde de kalıcı hasarlar bırakabilir (Bajpai & Srivastava, 2016; Ferreira et al., 2019). Cryptojacking gibi yeni nesil tehditler, saldırganların kurumsal sistemleri kullanarak kripto para madenciliği yapmalarını sağlar, bu da organizasyonun kaynaklarını tükenmesine yol açar (Casey, 2018; Oberoi et al., 2018). Kurumsal siber güvenlik stratejilerinin geliştirilmesi, bu tehditlere karşı etkili savunmalar inşa etmek için büyük bir önem taşır. Etkin bir siber güvenlik altyapısı, zafiyetleri tespit etmek ve tehditlere karşı proaktif önlemler almak için gerekli olan güvenlik araçlarını ve politikalarını içerir. Ayrıca, kurum içi eğitimler, çalışanların sosyal mühendislik saldırılarına karşı bilinçlendirilmesi ve güvenlik prosedürlerinin sürekli olarak gözden geçirilmesi gibi adımlar da büyük önem arz eder (Hadnagy, 2011; Mitnick & Simon, 2003).

Siber tehditler giderek daha çeşitli ve karmaşık hale gelmektedir. Bu bağlamda, organizasyonların güvenlik stratejilerini sürekli olarak güncellemeleri ve yenilikçi savunma yöntemlerini benimsemeleri gerekmektedir. Aksi takdirde, bu tehditler sadece finansal kayıplara yol açmakla kalmayacak, aynı zamanda kurumların operasyonel süreçlerini de kesintiye uğratacaktır.

1. Sosyal Mühendislik Saldırıları

Sosyal mühendislik saldırıları, insanların güvenlik açıklarından yararlanarak sistemlere izinsiz erişim sağlamayı hedefleyen bir tekniktir. Bu tür saldırılar, hedef kişinin psikolojik zayıflıklarını kullanarak, onları kandırmak ve manipüle etmek için tasarlanır. **Phishing** (oltalama) saldırıları, sosyal mühendislik tekniklerinin en yaygın örneklerinden biridir ve genellikle e-posta veya mesaj aracılığıyla gerçekleştirilir. Phishing saldırısının temel amacı, kurbanı sahte bir web sitesine yönlendirmek veya onları zararlı bir dosya açmaya ikna etmektir (Basharat et al., 2017). **Spear-phishing**, daha hedeflenmiş ve kişiselleştirilmiş bir phishing saldırısıdır. Bu saldırıda, saldırgan yalnızca belirli bir kişiyi veya kurum hedef alır ve genellikle o kişiye ait hassas bilgileri (e-posta adresi, başlık, iş yerindeki ilişkiler gibi) kullanarak kurbanı tuzağa düşürür (Blyth & Kovacich, 2015).

Sosyal mühendislik saldırıları, teknik güvenlik önlemleri (örneğin, güçlü şifreler veya antivirüs yazılımları) olsa bile etkili olabilir, çünkü bu saldırılar insan hatalarına dayanır. Bu nedenle, kurumsal siber güvenlik stratejileri, sadece teknolojik çözümlerle sınırlı kalmamalı, aynı zamanda çalışanları sosyal mühendislik saldırılarına karşı bilinçlendirmeyi de içermelidir (Hadnagy, 2011). Çalışanların eğitimleri, şüpheli e-postaların tanınması, kişisel bilgilerin paylaşılmaması gibi önlemler, kurumların bu tür tehditlere karşı daha güçlü bir savunma oluşturmasına yardımcı olur.

2. Ransomware (Fidye Yazılımı)

Ransomware, özellikle son yıllarda kurumsal siber güvenlik açısından büyük bir tehdit haline gelmiştir. Ransomware, kullanıcıların veya kurumların verilerini şifreleyerek erişimlerini engelleyen ve verilerin serbest bırakılması için fidye talep eden zararlı yazılımlar olarak tanımlanır (Bajpai & Srivastava, 2016). Bu tür yazılımlar genellikle e-posta ekleri, kötü amaçlı web siteleri veya güvenlik açığı bulunan yazılımlar aracılığıyla sisteme bulaşır. Bir ransomware saldırısı sonrası saldırganlar, şifrelenmiş verilere yeniden erişim sağlanabilmesi için yüksek meblağlarda fidye talep ederler. Fidye ödenmediği takdirde, veriler ya tamamen silinir ya da daha da kötüleşen bir duruma getirilir (Gupta & Kaur, 2016).

Ransomware saldırıları, sadece bireyleri değil, büyük kurumsal ağları da hedef alabilir. Kurumsal sistemlere yönelik ransomware saldırıları, hem finansal kayıplara hem de operasyonel sürekliliği tehdit edebilir. Bu tür saldırılar, büyük veri kayıplarına, itibar kaybına ve hatta hukuki sorunlara yol açabilir (Ferreira et al., 2019). Bu nedenle, kurumların ransomware saldırılarına karşı koruma önlemleri geliştirmeleri önemlidir. İyi bir yedekleme stratejisi, verilerin şifrelenmesini engellemek için gelişmiş antivirüs yazılımları ve güvenlik duvarları kullanmak, etkili bir siber güvenlik altyapısı oluşturmak için kritik öneme sahiptir (Choo et al., 2017).

Son yıllarda ransomware türleri giderek daha sofistike hale gelmiştir. Cryptojacking, ransomware saldırılarının bir alt türüdür ve saldırganlar, kurbanın bilgisayarını veya ağını kullanarak kripto para madenciliği yaparlar. Bu saldırılar, organizasyonların kaynaklarını tüketerek finansal kayıplara yol açar, ancak fidye talep edilmez. Cryptojacking, kurumlar için genellikle fark edilmeyen bir tehdit

olmakla birlikte, yine de ciddi bir güvenlik riski oluşturur (Casey, 2018; Oberoi et al., 2018). Bu tür tehditlere karşı etkili bir savunma stratejisi geliştirmek, kurumların finansal ve operasyonel sürekliliği sağlamak için kritik bir gerekliliktir.

3. Biyometrik Kimlik Doğrulama Güvenliği

Biyometrik kimlik doğrulama, güvenlik sistemlerinde giderek daha fazla tercih edilen bir yöntemdir. Biyometrik veriler, bir kişinin fiziksel veya davranışsal özelliklerinden (parmak izi, yüz tanıma, iris taraması vb.) elde edilen verilerdir ve bu veriler kişisel güvenliği artırmak amacıyla kimlik doğrulama için kullanılır (Jain et al., 2006). Biyometrik sistemler, özellikle fiziksel erişim kontrolü ve dijital kimlik doğrulama için yaygın olarak kullanılır, çünkü biyometrik özellikler her birey için benzersizdir ve bu da güvenliği önemli ölçüde artırır.

Ancak, biyometrik kimlik doğrulama sistemleri de siber güvenlik tehditlerine açıktır. Biyometrik spoofing veya sahtekarlık, sahte biyometrik veriler kullanılarak bu sistemlerin manipüle edilmesidir (Sudar et al., 2019). Bu tür saldırılarda, saldırganlar parmak izi veya yüz tanıma gibi biyometrik verileri taklit ederler. Biyometrik verilerin güvenliği, şifreleme, biyometrik verilerin depolanma şekli ve kullanıcı verilerinin korunmasına yönelik katı güvenlik protokollerine dayanır (Jain et al., 2006). Kurumsal siber güvenlik açısından biyometrik güvenliğin sağlanması, verilerin korunması, izinsiz erişimlerin engellenmesi için son derece önemlidir. Biyometrik sistemlerin zayıflıkları, kötü amaçlı kişilerin biyometrik verileri çalmasına veya manipüle etmesine yol açabilir, bu da kurumsal veri güvenliği için büyük bir tehdit oluşturur. Ayrıca, biyometrik verilerin korunması, kişisel gizliliği ihlal etmemek için de önemlidir (Natgunanathan et al., 2016). Bu nedenle, biyometrik sistemlerin tasarımında yüksek güvenlik önlemleri ve veri gizliliği politikaları izlenmelidir. Kurumsal siber güvenlik stratejileri, biyometrik sistemlerin zayıf noktalarını analiz etmeli ve çok faktörlü doğrulama yöntemleri kullanarak bu tür tehditlere karşı güvenliği artırmalıdır. Ayrıca, biyometrik verilerin depolanması ve işlenmesi konusunda uluslararası standartlara uyulması, güvenliği sağlamak için kritik bir adımdır.

METODOLOJİ

Amaç

Bu araştırmanın amacı, kurumsal siber güvenliğe yönelik tehditlerin kapsamlı bir şekilde analiz edilmesidir. Araştırma, sosyal mühendislik saldırıları, ransomware saldırıları ve biyometrik güvenlik sistemlerinin zayıflıkları gibi ana tehdit başlıkları üzerinden giderek, bu tehditlerin organizasyonların bilgi güvenliği üzerindeki etkilerini incelemeyi hedeflemektedir. Ayrıca, bu tehditlere karşı etkin savunma stratejilerinin belirlenmesi ve kurumsal siber güvenliğin güçlendirilmesine yönelik öneriler sunulması amaçlanmaktadır.

Araştırma Yöntemi

Araştırma, nitel bir araştırma yöntemiyle gerçekleştirilecektir. Literatür taraması, vaka analizleri

ve tematik analiz gibi yöntemlerle veriler toplanacak ve analiz edilecektir. Literatür taraması, siber güvenlik tehditlerinin genel yapılarını ve önceki çalışmaların bulgularını ortaya koyacaktır. Vaka analizi ise gerçek dünyadaki siber saldırılar ve bunlara karşı uygulanan savunma stratejileri üzerine odaklanacaktır. Bu iki yöntem, araştırmanın temel veri toplama aşamalarını oluşturacaktır.

Veri Toplama Aşamaları

Veri toplama aşamasında, literatür taraması ve vaka analizi önemli bir rol oynayacaktır. Literatür taraması, sosyal mühendislik saldırıları, ransomware ve biyometrik güvenlik sistemlerine dair daha önce yapılmış araştırmaları kapsamaktadır. Bu aşamada, phishing, spear-phishing gibi sosyal mühendislik saldırılarının kurumlar üzerindeki etkisi, ransomware saldırılarının neden olduğu zararlar ve biyometrik sistemlerin zayıflıkları üzerinde yoğunlaşılacaktır. Ayrıca, güvenlik önlemleri ile ilgili literatürdeki çözüm önerileri de bu süreçte incelenecektir. Vaka analizi, büyük organizasyonlarda meydana gelen siber saldırıların somut örneklerini inceleyerek, kurumsal güvenlik stratejilerinin etkinliğini değerlendirecektir.

Veri Analizi Yöntemi

Veri analizi süreci, nitel veri analizine dayanacaktır. İçerik analizi ve tematik analiz yöntemleri kullanılarak, toplanan veriler kategorize edilecek ve ana temalar belirlenecektir. İçerik analizi, literatür taraması ve vaka çalışmalarından elde edilen bulguları sistematik olarak sınıflandırarak tehdit türlerinin etkilerini inceleyecektir. Tematik analiz, bu tehditlerin organizasyonlar üzerindeki pratik etkilerini, savunma stratejilerini ve karşılaşılan zorlukları detaylandıracaktır. Bu analizler, kurumsal siber güvenlik tehditlerine karşı hangi savunma önlemlerinin daha etkili olduğunu belirlemeye yardımcı olacaktır.

Analiz Edilecek Konular

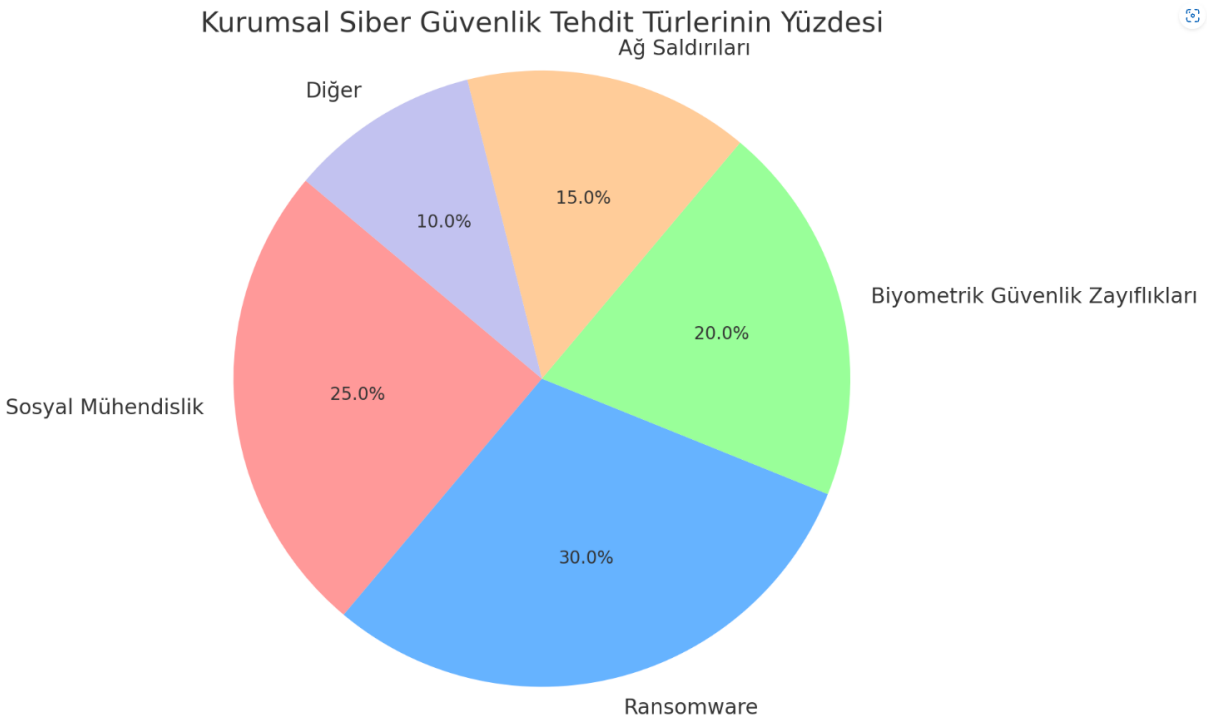
Araştırmada analiz edilecek ana konular, sosyal mühendislik saldırıları, ransomware saldırıları ve biyometrik güvenlik sistemlerinin zayıflıklarıdır. Sosyal mühendislik saldırıları, phishing ve spear-phishing gibi saldırıların organizasyonel güvenlik üzerindeki etkilerini inceleyecek ve bu saldırılara karşı alınan önlemleri analiz edecektir. Ransomware saldırıları, finansal ve operasyonel zararlara neden olan önemli tehditlerdir ve bu tür saldırılara karşı geliştirilen güvenlik stratejilerinin etkinliği araştırılacaktır. Ayrıca, biyometrik güvenlik sistemlerinin zayıflıkları, biyometrik sahtekarlık gibi tehditlere karşı alınan önlemler ve biyometrik güvenliğin organizasyonlar için sağladığı güvenlik düzeyi de bu analizde ele alınacaktır.

BULGULAR

Bu bölümde, kurumsal siber güvenlik tehditlerine dair yapılan analizlerin bulguları sunulmaktadır. Araştırma sürecinde elde edilen bulgular, sosyal mühendislik saldırıları, ransomware saldırıları ve biyometrik güvenlik sistemlerinin zayıflıkları gibi önemli tehdit alanlarında derinlemesine incelemeler yaparak bu tehditlerin kurumsal güvenlik üzerindeki etkilerini ve karşılaşılan

zorlukları ortaya koymaktadır. Ayrıca, bu tehditlere karşı organizasyonların geliştirdiği savunma stratejileri ve uygulanan güvenlik önlemleri de analiz edilmiştir. Elde edilen bulgular, kurumların siber güvenlik tehditleriyle nasıl başa çıktığını, hangi güvenlik önlemlerinin en etkili olduğunu ve organizasyonların bu tehditlere karşı daha sağlam bir savunma oluşturmak için hangi stratejileri geliştirmeleri gerektiğini göstermektedir. Bu bağlamda, bulgular, kurumsal siber güvenlik tehditlerine yönelik alınan önlemler ile mevcut güvenlik açıklarının nasıl giderilebileceği konusunda önemli ipuçları sunmaktadır.

Grafik 1 ***Kurumsal Siber Güvenlik Tehdit Türlerinin Yüzdesi***



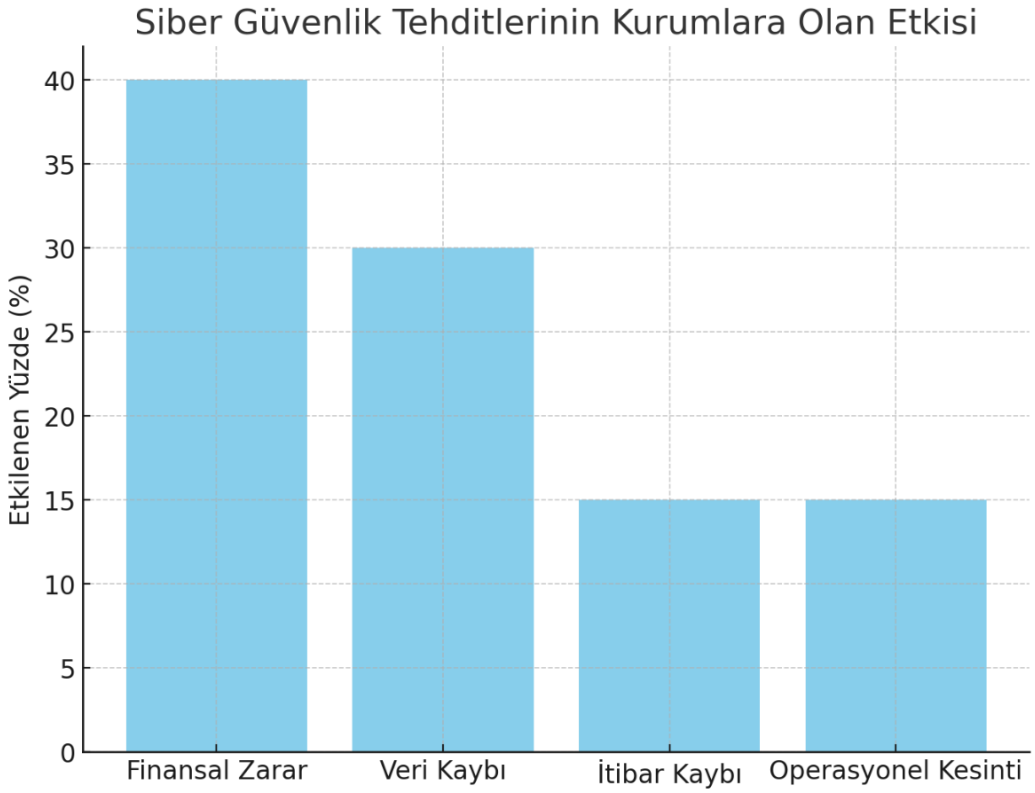
Grafik 1 incelendiğinde kurumsal siber güvenlik tehditlerinin türlerini ve her bir tehdit türünün organizasyonlardaki yüzdesel dağılımını göstermektedir. Görselde, en büyük payı Ransomware (fidye yazılımı) almış ve bu tehdit türü %30'luk bir oranla en fazla karşılaşılan tehdit olarak öne çıkmaktadır. Bu, ransomware saldırılarının kurumlar için ciddi bir risk teşkil ettiğini ve güvenlik önlemlerinin bu tehdit türüne odaklanması gerektiğini gösteriyor.

Sosyal mühendislik saldırıları ise %25'lik bir paya sahip olup, kurumların karşılaştığı önemli bir diğer tehdit alanını oluşturmaktadır. Bu tür saldırılar, hedef kişilerin psikolojik zayıflıklarını kullanarak bilgi çalmayı amaçlar, bu da kurumsal siber güvenlikte insan faktörünün önemini vurgulamaktadır. Biyometrik güvenlik zayıflıkları, %20'lik bir orana sahip olup, biyometrik doğrulama sistemlerinin güvenlik açıklarının ve bu sistemlere yönelik tehditlerin büyüdüğünü gösterir. Biyometrik sistemler, kullanıcıların kimliklerini doğrulamak için yaygın olarak kullanılsa

da, bu tür zayıflıklar ciddi güvenlik tehditleri yaratabilir. Grafikte ayrıca diğer tehditler %10, ağ saldırıları ise %15 ile daha küçük bir oranda yer almaktadır. Bu, ağ saldırılarının ve diğer tehdit türlerinin de kurumlar için önemli bir risk oluşturduğunu ancak genel tehdit dağılımı içinde daha düşük bir paya sahip olduğunu göstermektedir.

Genel olarak, bu grafik, kurumların siber güvenlik stratejilerini oluştururken en büyük tehditlerin ransomware ve sosyal mühendislik saldırılarından geldiğini, biyometrik güvenlik zayıflıklarının ise dikkat edilmesi gereken başka bir kritik alanı temsil ettiğini ortaya koymaktadır.

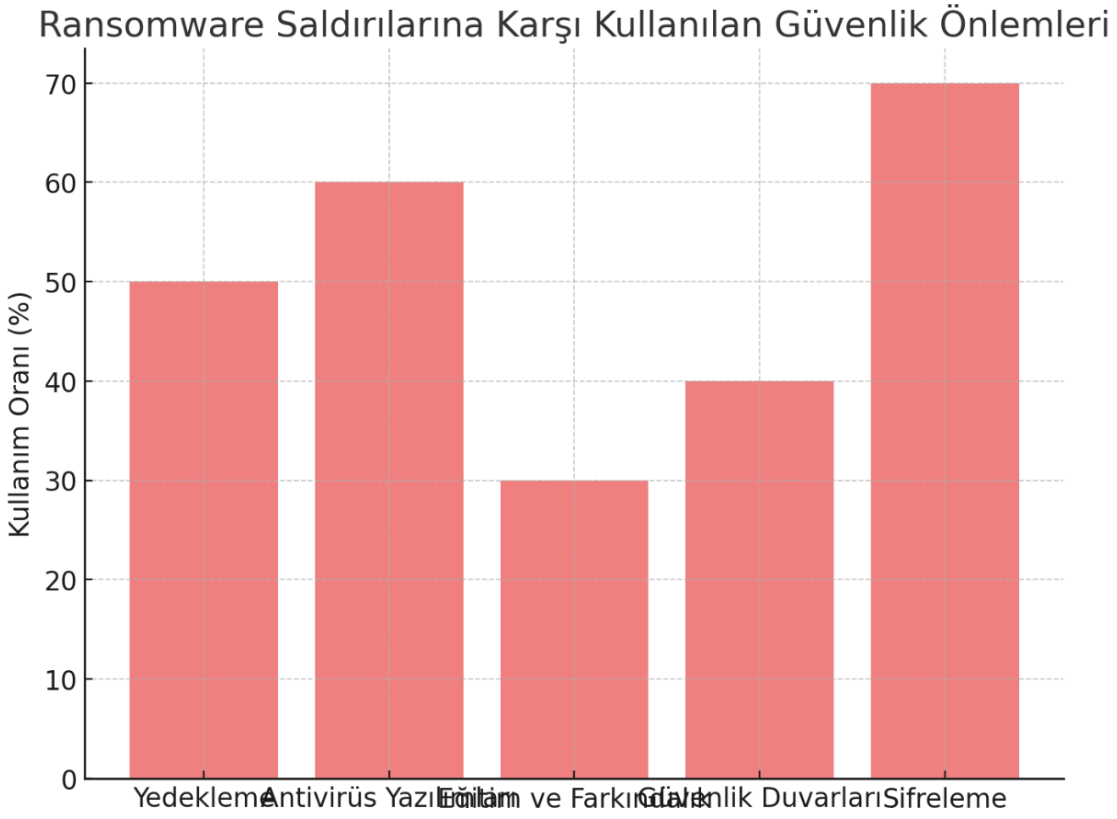
Grafik 2 ***Siber Güvenlik Tehditlerinin Kurumlara Olan Etkisi***



Grafik 2 incelendiğinde, siber güvenlik tehditlerinin kurumsal sistemler üzerinde yarattığı etkilerin dağılımı net bir şekilde gözler önüne serilmektedir. Grafik, en büyük etkinin finansal zarar üzerinde olduğunu göstermektedir. Bu kategori, %40'lık bir oranla diğer etkilerden oldukça yüksek bir değere sahip olup, siber saldırıların genellikle kurumlar için maddi kayıplara yol açtığını ortaya koymaktadır. Bu da, saldırganların genellikle hedeflerine ulaşmak için kurumların finansal kaynaklarını hedef almayı tercih ettiğini ve bu tür saldırıların kurumları büyük bir ekonomik zarara uğratabileceğini göstermektedir. Veri kaybı, %30'luk bir oranla ikinci sırada yer almakta olup, siber saldırıların bilgi güvenliği açısından ne denli kritik bir tehdit oluşturduğunu vurgulamaktadır. Özellikle, organizasyonların hassas verilerinin çalınması veya kaybolması, hem operasyonel

sürekliliği tehdit eder hem de uzun vadeli itibar kayıplarına neden olabilir. İtibar kaybı ve operasyonel kesinti ise sırasıyla %15 ve %15'lik oranlarla daha düşük bir etkiye sahiptir. Ancak, her iki etki de uzun vadede kurumlar için büyük riskler oluşturabilir. İtibar kaybı, kurumların müşteri güvenini yitirerek pazar payı kaybına yol açabilirken, operasyonel kesinti de üretkenliği engelleyerek kurumun işleyişinde ciddi aksamalara neden olabilir. Genel olarak, bu grafik, siber güvenlik tehditlerinin organizasyonlar üzerindeki farklı türdeki etkilerini açık bir şekilde ortaya koymakta olup, kurumların bu tehditlere karşı alınacak önlemler konusunda önceliklerini belirlemelerine yardımcı olmaktadır.

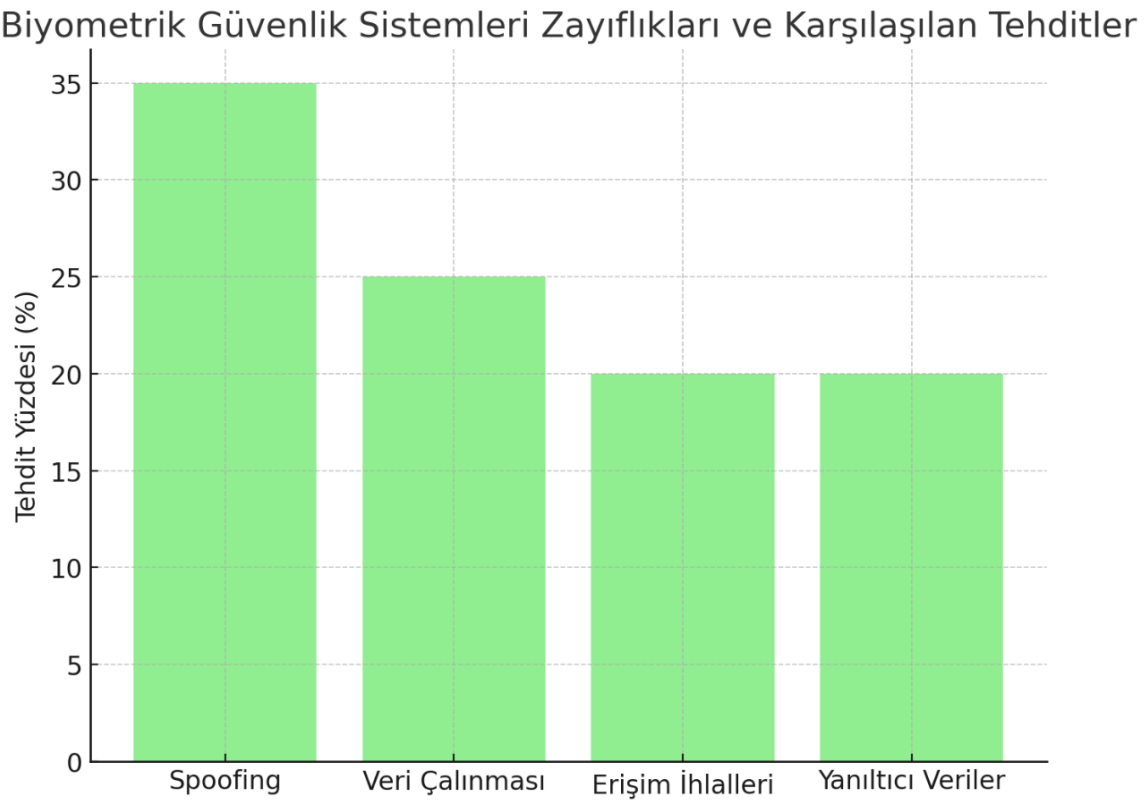
Grafik 3 ***Ransomware Saldırılarına Karşı Kullanılan Güvenlik Önlemleri***



Grafik 3 incelendiğinde, ransomware saldırılarına karşı kullanılan güvenlik önlemlerinin dağılımı açıkça görülmektedir. Şifreleme %70'lik kullanım oranı ile en etkili güvenlik önlemi olarak öne çıkmaktadır. Bu, kurumların ransomware saldırılarından korunmak için verilerini şifrelemeye büyük önem verdiğini ve bu stratejinin en yaygın kullanılan güvenlik önlemi olduğunu göstermektedir. Şifreleme, verilerin saldırganlar tarafından erişilemez hale getirilmesi için kritik bir savunma mekanizması sunar. Yedekleme ve antivirüs yazılımları da %50'nin üzerinde kullanım oranlarına sahip olup, ransomware saldırılarının etkilerini sınırlamak için yaygın olarak tercih edilmektedir. Yedekleme, verilerin kaybolmasını engellemek için önemli bir önlem alırken,

antivirüs yazılımları kötü amaçlı yazılımları tespit edip engellemeye yönelik etkin bir araçtır. Eğitim ve farkındalık ise %30 civarında bir kullanım oranına sahip olup, kurumların çalışanlarını ransomware gibi tehditlere karşı bilinçlendirmeye yönelik eğitim verdiklerini gösterir. Bu oran, insan hatalarının önemli bir güvenlik açığı oluşturduğunu ve farkındalık eğitiminin önemini vurgulamaktadır. Son olarak, güvenlik duvarları da saldırılara karşı alınan önlemler arasında yer almakta olup, %40'lık bir oranla kullanılan bir diğer önemli güvenlik aracıdır. Grafik, kurumların ransomware saldırılarına karşı aldıkları önlemlerin çeşitliliğini ve farklı stratejilerin birlikte kullanılmasını yansıtmaktadır.

Grafik 4 ***Biyometrik Güvenlik Sistemleri Zayıflıkları ve Karşılaşılan Tehditler***



Grafik 4 incelendiğinde, biyometrik güvenlik sistemlerinin karşılaştığı tehditlerin yüzdesel dağılımı açıkça gösterilmektedir. Spoofing (taklit etme) %35'lik bir oranla en büyük tehdidi oluşturmakta olup, biyometrik sistemlerin en yaygın zayıflığı olarak öne çıkmaktadır. Spoofing, saldırganların biyometrik verileri taklit ederek sistemleri kandırması anlamına gelir ve bu tür saldırılar, biyometrik güvenliğin en ciddi risklerinden biridir. Veri çalınması ise %30'luk bir oranla ikinci sıradadır. Bu tehdit, biyometrik verilerin kötü niyetli kişiler tarafından çalınarak kötüye kullanılmasını ifade eder. Bu tür saldırılar, bireylerin kişisel bilgilerini hedef alarak güvenlik açıkları yaratabilir. Erişim ihlalleri ve yanıltıcı veriler ise %25'lik oranlarla daha düşük seviyelerde yer almakta olup, biyometrik sistemlere yönelik diğer tehditleri yansıtmaktadır. Erişim ihlalleri,

yetkisiz kişilerin biyometrik verilere erişimini sağlarken, yanıltıcı veriler doğru kimlik doğrulama süreçlerini engelleyebilir. Genel olarak, bu grafik biyometrik güvenlik sistemlerinin karşılaştığı tehditlerin çeşitliliğini ve bu tehditlerin her birinin biyometrik sistemlerde yaratabileceği riskleri ortaya koymaktadır.

Tablo 1 ***Kurumsal Siber Güvenlik Tehdit Türlerinin Yüzdesi***

Tehdit Türü	**Yüzde (%)**
Sosyal Mühendislik	25
Ransomware	30
Biyometrik Güvenlik Zayıflıkları	20
Ağ Saldırıları	15
Diğer	10

Tablo 1 incelendiğinde, kurumsal siber güvenlik tehditlerinin türleri arasındaki dağılımın nasıl şekillendiği açıkça görülmektedir. Ransomware (fidye yazılımı), %30'luk bir oranla en büyük tehdit olarak öne çıkmaktadır. Bu, ransomware saldırılarının kurumlar için ciddi bir tehdit oluşturduğunu ve kurumsal siber güvenlik stratejilerinin çoğunlukla bu tehdit türüne odaklandığını göstermektedir. Fidye yazılımları, verilerin şifrelenip talep edilen fidyenin ödenmemesi durumunda kaybedilmesine yol açarak, organizasyonları büyük finansal zararlara uğratabilir. Sosyal mühendislik saldırıları ise %25'lik bir oranla ikinci sırada yer almaktadır. Sosyal mühendislik, insan psikolojisini hedef alarak kişileri manipüle etmeyi amaçlar ve kurumsal ağlara izinsiz erişim sağlamada etkili bir yöntemdir. Bu tür saldırılar, teknolojiye dayalı savunma önlemleri olsa bile, insan hatalarını kullanarak güvenlik açıkları yaratabilir. Biyometrik güvenlik zayıflıkları %20 oranla üçüncü sıradadır ve biyometrik doğrulama sistemlerine yönelik tehditlerin arttığını göstermektedir. Biyometrik verilerin taklit edilmesi ya da sahte verilerle manipülasyon yapılması, kurumlar için önemli bir güvenlik riski oluşturur.

Ağ saldırıları ise %15'lik oranla daha düşük bir paya sahiptir. Bununla birlikte, ağ saldırıları, özellikle veri çalınması ve sistemlere sızma amacı güden saldırılar için kritik tehditlerdir. Diğer tehditler %10'luk bir orana sahip olup, çeşitli siber tehditler dışında kalan ve daha nadiren karşılaşılan tehditleri kapsamaktadır. Bu veriler, kurumsal siber güvenlik stratejilerinin, ransomware ve sosyal mühendislik gibi yaygın tehdit türlerine karşı öncelikli olarak hazırlanması gerektiğini ortaya koymaktadır.

Tablo 2 ***Siber Güvenlik Tehditlerinin Kurumlara Olan Etkisi***

Etkiler	**Etkilenen Yüzde (%)**
Finansal Zarar	40
Veri Kaybı	30
İtibar Kaybı	15
Operasyonel Kesinti	15

Tablo 2 incelendiğinde, siber güvenlik tehditlerinin kurumlar üzerindeki etkilerinin nasıl dağıldığı görülmektedir. Finansal zarar %40'lık oranla en büyük etkiye sahiptir. Bu, siber saldırıların genellikle kurumların maddi kaynaklarına büyük zararlar verdiğini ve finansal kayıpların önemli bir risk oluşturduğunu göstermektedir. Fidye yazılımları (ransomware) ve diğer saldırı türleri, kurumları yüksek fidye talepleri veya tazminat ödemeleri gibi maddi yüklerle karşı karşıya bırakabilir. Veri kaybı ise %30'luk oranla ikinci sıradadır. Bu etki, özellikle bilgi güvenliği açısından kritik öneme sahip verilerin kaybedilmesi veya çalınması ile ilgili yaşanan sorunları yansıtmaktadır.

Veri kaybı, organizasyonlar için yalnızca finansal kayıp yaratmakla kalmaz, aynı zamanda operasyonel süreçleri de aksatabilir. İtibar kaybı ve operasyonel kesinti, her biri %15'lik oranla üçüncü sırada yer almaktadır. İtibar kaybı, organizasyonun müşteri güvenini yitirmesi ve marka değerinin zarar görmesi anlamına gelir. Operasyonel kesinti ise kurumların faaliyetlerinin durmasına veya aksamasına yol açabilir, bu da üretkenliği engelleyebilir ve kurumun işleyişini zorlaştırabilir. Bu veriler, kurumların siber güvenlik önlemlerini oluştururken yalnızca teknik tehditleri değil, bu tehditlerin yarattığı finansal, veri güvenliği ve operasyonel etkileri de dikkate almaları gerektiğini vurgulamaktadır**.**

Tablo 3 ***Ransomware Saldırılarına Karşı Kullanılan Güvenlik Önlemleri***

Önlemler	**Kullanım Oranı (%)**
Yedekleme	50

Antivirüs Yazılımları	60
Eğitim ve Farkındalık	30
Güvenlik Duvarları	40
Şifreleme	70

Tablo 3 incelendiğinde, ransomware saldırılarına karşı alınan güvenlik önlemlerinin kullanım oranlarının dağılımı açıkça görülmektedir. Şifreleme, %70'lik kullanım oranıyla en yaygın ve etkili güvenlik önlemi olarak öne çıkmaktadır. Bu, kurumların, verilerini şifreleyerek ransomware saldırılarından korunmaya büyük önem verdiğini ve bu stratejinin veri güvenliği açısından kritik bir önlem olarak kabul edildiğini göstermektedir. Antivirüs yazılımları ise %60'lık bir kullanım oranına sahip olup, kötü amaçlı yazılımların tespit edilmesi ve engellenmesi amacıyla yaygın olarak kullanılan bir başka etkili güvenlik önlemidir. Antivirüs yazılımları, ransomware gibi zararlı yazılımların sistemlere girmesini engellemeye yönelik önemli bir araçtır. Yedekleme, %50'lik bir kullanım oranına sahip olup, verilerin kaybolmasını engellemek için uygulanan temel bir güvenlik önlemidir. Yedekleme, ransomware saldırılarında verilerin şifrelenmesi durumunda kurtarma sağlamak için kritik bir rol oynar. Güvenlik duvarları ise %40'lık oranla daha düşük bir kullanım oranına sahiptir, ancak ağ saldırılarına karşı savunma sağlamak için önemli bir araçtır. Son olarak, eğitim ve farkındalık, %30'luk oranla daha düşük bir paya sahip olsa da, çalışanların siber güvenlik tehditleri konusunda bilinçlendirilmesi önemlidir. İnsan hataları ve sosyal mühendislik saldırılarının etkisini azaltmak için eğitim ve farkındalık programları kurumlar için gerekli bir savunma mekanizmasıdır. Bu veriler, kurumların ransomware saldırılarına karşı birden fazla güvenlik önlemi kullandığını ve şifreleme ile antivirüs yazılımlarına özellikle önem verdiklerini göstermektedir.

Tablo 4 ***Biyometrik Güvenlik Sistemleri Zayıflıkları ve Karşılaşılan Tehditler***

Tehdit Türü	**Tehdit Yüzdesi (%)**
Spoofing	35
Veri Çalınması	25
Erişim İhlalleri	20
Yanıltıcı Veriler	20

Tablo 4 incelendiğinde, biyometrik güvenlik sistemlerinin karşılaştığı tehditlerin dağılımı net bir şekilde ortaya konmaktadır. Spoofing (taklit etme), %35'lik oranla en büyük tehdidi oluşturmaktadır. Bu, biyometrik sistemlerin en yaygın zayıflığı olarak öne çıkmakta olup, saldırganların biyometrik verileri taklit ederek sistemlere izinsiz erişim sağlama girişimlerini ifade eder. Spoofing, biyometrik güvenlikte önemli bir güvenlik açığı yaratır. Veri çalınması, %25'lik oranla ikinci sıradadır. Bu tehdit, biyometrik verilerin çalınarak kötüye kullanılmasını ifade eder ve özellikle kişisel bilgilerin gizliliği açısından ciddi riskler taşır. Erişim ihlalleri ve yanıltıcı veriler ise sırasıyla %20'lik oranlarla daha düşük seviyelerde yer almaktadır. Erişim ihlalleri, yetkisiz kişilerin biyometrik verilere erişmesini sağlarken, yanıltıcı veriler doğru biyometrik kimlik doğrulama süreçlerini engelleyebilir. Bu tür tehditler, biyometrik sistemlerin doğruluğunu ve güvenliğini zayıflatabilir. Bu veriler, biyometrik güvenlik sistemlerinin çeşitli tehditlere karşı daha güvenli hale getirilmesi için dikkatli tasarım ve savunma önlemleri gerektirdiğini göstermektedir.

SONUÇ

Kurumsal siber güvenlik, giderek daha karmaşık ve sofistike hale gelen tehditlerle karşı karşıya kalmaktadır. Bu çalışmada, siber güvenlik tehditlerinin türleri, organizasyonlar üzerindeki etkileri ve bu tehditlere karşı alınan önlemler detaylı bir şekilde incelenmiştir. Elde edilen bulgular, kurumsal siber güvenlik tehditlerinin çeşitliliğini ve her bir tehdit türünün kurumlar üzerinde oluşturduğu potansiyel zararları ortaya koymaktadır. Ransomware saldırıları, kurumlar için en büyük tehditlerden biri olarak %30'luk oranla öne çıkmaktadır. Bu tür saldırılar, sadece finansal kayıplara yol açmakla kalmaz, aynı zamanda operasyonel kesintilere ve veri kaybına da sebep olabilir. Bu tehditlere karşı alınan önlemler arasında şifreleme, yedekleme ve antivirüs yazılımları gibi teknik çözümler öne çıkmaktadır. Ayrıca, eğitim ve farkındalık programları da kullanıcı hatalarına karşı bir savunma mekanizması olarak önem taşımaktadır.

Sosyal mühendislik saldırıları, özellikle phishing ve spear-phishing gibi yöntemlerle kurumların iç güvenliğini tehdit etmektedir. Bu tür saldırılar, bireylerin güvenlik açıklarından faydalanarak kritik verilere erişim sağlamayı amaçlar. Kurumların bu tehditlere karşı alacağı önlemler, güçlü güvenlik protokollerinin yanı sıra çalışanların bilinçlendirilmesi ve düzenli eğitimler ile desteklenmelidir. Biyometrik güvenlik sistemleri de kurumlar tarafından yaygın olarak kullanılmakta, ancak bu sistemler de çeşitli tehditlere açıktır. Spoofing ve veri çalınması gibi tehditler, biyometrik doğrulama sistemlerinin güvenliğini zayıflatmaktadır. Bu zayıflıklara karşı, biyometrik sistemlerin güvenliğini artırmak için daha gelişmiş doğrulama yöntemleri ve güvenlik protokollerinin uygulanması gerekmektedir.

Sonuç olarak, kurumsal siber güvenlik stratejilerinin, sadece teknik çözümlerle sınırlı kalmayıp, insan faktörünü de göz önünde bulundurarak kapsamlı bir yaklaşım benimsemesi gerektiği sonucuna varılmaktadır. Kurumlar, siber güvenlik tehditlerine karşı etkili bir savunma oluşturmak için çok katmanlı güvenlik önlemleri ve sürekli eğitimlerle tehditlerin etkilerini en aza indirmelidir.

KAYNAKÇA

Adams, C., & Neil, M. (2015). *The essential guide to security*. Cisco Press.

Akdoğan, D. (2015). *Secure key agreement using pure biometrics* (Yayımlanmış yüksek lisans tezi). Sabancı Üniversitesi, Bilgisayar Bilimleri ve Mühendisliği, İstanbul.

Alaswad, A. O., Montaser, A. H., & Mohamad, F. E. (2014). Vulnerabilities of biometric authentication: Threats and countermeasures. *International Journal of Information & Computation Technology, 4*(10), 947-958.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, Article 563060. https://doi.org/10.3389/fcomp.2021.563060

Al-Saleh, M. I., Espinoza, A. M., & Crandall, J. R. (2013). Antivirus performance characterisation: System-wide view. *IET Information Security, 7*(2), 126-133.

Anderson, R. (2001). *Security engineering: A guide to building dependable distributed systems*. Wiley.

Arıkan, S. M., & Benzer, R. (2018). Bir güvenlik trendi: Bal küpü. *Acta Infologica, 2*(1), 1-11.

Arunadevi, J., Ramya, S., & Raja, M. R. (2018). A study of classification algorithms using RapidMiner. *International Journal of Pure and Applied Mathematics, 119*(12), 15977-15988.

Assante, M. J., & Lee, R. M. (2015). The industrial control system cyber kill chain. SANS Institute.

Bajpai, A., & Srivastava, D. (2016). A survey of ransomware: Past, present, and future. In *2016 6th International Conference - Cloud System and Big Data Engineering (Confluence)* (pp. 797-802).

Balazia, M., Happy, S. L., Bremond, F., & Dantcheva, A. (2021). How unique is a face: An investigative study. In *25th International Conference on Pattern Recognition (ICPR)* (pp. 7066-7071). Milan, Italy.

Basharat, F., Hanif, M., Basharat, M., & Farooq, M. (2017). Social engineering attacks: A survey of techniques and countermeasures. *Journal of Network and Computer Applications, 60*, 19-27.

Bishop, M. (2018). Insider threats in computer security: Art and science (pp. 619-634). Addison-Wesley.

Blyth, A. J., & Kovacich, G. L. (2015). *Spear phishing: It's not just an email problem*. Elsevier.

Bonn, C., Stadelmann, M., & Wrycza, S. (2017). Phishing and its countermeasures: A literature survey. *Computers & Security, 66*, 1-27.

Briseno, A. M., Palancar, J. H., & Alonso, A. G. (2015). Minutiae based palmprint indexing. In *Springer International Publishing Switzerland* (pp. 10-19).

Casey, M. J. (2018). Coinhive and the upsurge in cryptojacking. *Computing in Science & Engineering, 20*(2), 8-12.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2008). A model for evaluating IT security investments. *Communications of the ACM, 51*(2), 99-103.

CERT Insider Threat Center. (2018). *Common sense guide to mitigating insider threats* (6th ed.). Software Engineering Institute.

Choo, K. K. R., Liu, L., & Liu, F. (2017). Ransomware: Evolution, mitigation and prevention. *Computers & Security, 66*, 162-187.

Ferreira, A. A., Santos, I., Baggili, I., & Kechadi, T. (2019). How are ransomware attributes changing over time? A comprehensive study of ransomware attacks and evolutions. *Computers & Security, 86*, 235-253.

Ferreira, J., Ferreira, J. Jr., & Magalhães, F. V. (2018). Browser-based cryptojacking: Analysis and taxonomy. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-8).

Filiz, S. (2012). Siber güvenlikte biyometrik sistemler ve yüz tanıma (Yayımlanmış yüksek lisans tezi). Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Finkle, J., & Kilger, M. (2012). Insider threats. In *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare* (pp. 91-105). Springer.

Gezgin, M. D., & Buluş, E. (2013). Kablosuz ağlar için bir DoS saldırısı tasarımı. *Bilişim Teknolojileri Dergisi, 6*(3), 17-23.

Gönen, S., Sayan, H. H., Yılmaz, E. N., Üstünsoy, F., & Karacayılmaz, G. (2020). False data injection attacks and the insider threat in smart systems. *Computers & Security, 97*, 101955.

Gupta, S., & Gupta, B. B. (2015). Cross-site scripting (XSS) attacks and defense mechanisms: Classification and state-of-the-art. *International Journal of System Assurance Engineering and Management, 8*, 512-530.

Gupta, R., & Kaur, D. (2016). A survey of ransomware: Trends, security challenges, and future directions. *Journal of Computer Sciences and Applications, 4*(1), 1-9.

Gupta, S., & Agrawal, D. P. (2016). A survey of network security attacks. *International Journal of Computer Applications, 139*(6), 8-16.

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. In *International Conference on Computing, Communication and Automation (ICCCA2016)* (pp. 537-540).

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Wiley.

Hong, J. I., & Chen, T. H. (2017). A survey on password security: From vulnerabilities to countermeasures. *Computer Communications, 109*, 52-69.

Huang, Y. H., Chiang, M. C., & Chou, S. C. (2018). Detecting spear-phishing emails based on header features. *Information Sciences, 432*, 101-113.

Hussain, M., Hussain, J., & Arshad, J. (2017). Password attacks and defenses: A review. In *2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 1581-1588).

Jain, A., Bolle, R., & Pankanti, S. (1999). Biometrics personal identification in networked society. *The Springer International Series in Engineering and Computer Science*.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4-20.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security, 1*(2), 125-143.

Jetty, S. (2018). *Network scanning cookbook: Practical network security using Nmap and Nessus 7*. Packt Publishing Ltd.

Jia, W., Zhang, L., Chen, S., & Liu, L. (2004). A survey of biometrics authentication systems. In *International Conference on Audio- and Video-Based Biometric Person Authentication* (pp. 97-104).

Jones, J., Wimmer, H., & Haddad, R. J. (2019). PPTP VPN: An analysis of the effects of a DDoS attack. *IEEE*, 1-6.

Kakarla, T., Mairaj, A., & Javaid, A. Y. (2018). A real-world password cracking demonstration using open source tools for instructional use. *IEEE International Conference on Electro/Information Technology (EIT)* (pp. 387-391).

Karamani, B. (2018). Improving data loss prevention using classification. In *International Conference on Emerging Internetworking, Data & Web Technologies* (pp. 183-189).

Kharraz, A., Robertson, W., Balzarotti, D., & Kirda, E. (2019). Outsmarting the smarts: On the effectiveness of malware-laced emails. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2171-2188).

Kim, D., & Solomon, M. (2019). *Penetration testing fundamentals: A hands-on guide in cybersecurity*. Pearson.

Kişisel Verilerin Korunması Kanunu. (2016). T.C. Resmî Gazete, 29677, 07 Nisan 2016.

Kocabaş, İ., & Yücesoy, A. (2020). Siber tehditlere karşı kurumsal savunma: Bir durum analizi. *Sosyal Bilimler Araştırma Dergisi, 9*(1), 480-495. https://dergipark.org.tr/tr/pub/sobiad/issue/51250/660493

Kocaman, Y., Gönen, S., Barişkan, M. A., Karacayılmaz, G., & Yılmaz, E. N. (2022). A novel approach to continuous CVE analysis on enterprise operating systems for system vulnerability assessment. *International Journal of Information Technology, 14*(3), 1433-1443.

Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management, 45*(2), 109-119.

Lin, M.-S., Chiu, C.-Y., Lee, & Pao, H.-K. (2013). Malicious URL filtering—a big data application. *IEEE International Conference on Big Data, Silicon Valley*, 589-596.

Liu, X., Zhu, P., Zhang, Y., & Chen, K. (2015). A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. *IEEE Transactions on Smart Grid, 6*(5), 2435-2443.

Maltoni, D., Maio, D., Jain, A. K., & Feng, J. (2022). *Handbook of fingerprint recognition* (3rd ed.).

Manogaran, G., & Lopez, D. (2017). A survey of big data architectures and machine learning algorithms in healthcare. *International Journal of Biomedical Engineering and Technology, 25*(2-4), 182-211.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. Wiley.

Mukkamala, P. P., & Rajendran, S. (2020). A survey on the different firewall. *International Journal of Engineering Applied Sciences and Technology, 5*(1), 363-365.

Naik, N., Jenkins, P., Savage, N., & Yang, L. A. (2021). Computational intelligence enabled honeypot for chasing ghosts in the wires. *Complex & Intelligent Systems, 7*(1), 477-494.

Naik, N., & Jenkins, P. (2018). A fuzzy approach for detecting and defending against spoofing attacks on low interaction honeypots. *21st International Conference on Information Fusion*, 904-910.

Natarajana, K., Subramani, S. (2012). Generation of SQL-injection free secure algorithm to detect and prevent SQL-injection attacks. *Procedia Technology, 4*, 790-796.

Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G., & Yearwood, J. (2016). Protection of privacy in biometric data. *IEEE Access, 4*, 880-892.

Northcutt, S., & Novak, J. (2002). *Network intrusion detection: An analyst's handbook*. New Riders.

Oberoi, A., Srinivas, V., & Raman, G. (2018). Cryptojacking: A review. In *2018 IEEE International Conference on Computational Intelligence & IoT* (pp. 68-73).

Özalp, A. N. (2023). Siber saldırıların tespitinde yapay zekâ tabanlı algoritma tasarımı (Yayımlanmış doktora tezi). Karabük Üniversitesi, Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Karabük.

Proceedings of the International Conference on Computing, Communication and Automation (pp. 1-6).

Sheta, M. A., Zaki, M., El Hadad, K. A. E. S., & Aboelseoud, M. H. (2016). Anti-spyware security design patterns. *Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, 465-470.

Sindiren, E., & Ciylan, B. (2019). Application model for privileged account access control system in enterprise networks. *Computers & Security, 8*(3), 52-67.

Singh, K. K. V. V., & Gupta, H. (2016). A new approach for the security of VPN. In *ICTCS 16: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies* (pp. 1-5).

Smith, J. R. (2017). *Hacking wireless networks for dummies*. Wiley.

Sokol, P., Misek, J., & Husak, M. (2017). Honeypots and honeynets: Issues of privacy. *EURASIP Journal on Information Security*, 1-9.

Stallings, W. (2017). *Network security essentials: Applications and standards*. Pearson.

Stallings, W., & Brown, L. (2017). *Computer security: Principles and practice*. Pearson.

Sudar, K. M., Deepalakshmi, P., Ponmozhi, K., & Nagaraj, P. (2019). Analysis of security threats and countermeasures for various biometric techniques. *IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES)*, 1-6.

System Performance Estimates. (1997). *Proceedings of the IEEE, 85*(9), 1365-1388.

Taşçı, H. B., Gönen, S., Barışkan, M. A., & Yılmaz, E. N. (2021). Password attack analysis over honeypot using machine learning password attack analysis. *Turkish Journal of Mathematics and Computer Science, 13*(2), 388-402.

Taştan, A. N., Gönen, S., Barışkan, M. A., Kubat, C., Kaplan, D. Y., & Pashaei, E. (2023). Detection of man-in-the-middle attack through artificial intelligence algorithm. In *International Symposium on Intelligent Manufacturing and Service Systems* (pp. 450-458).

Thanh, C. T., & Zelinka, I. (2019). A survey on artificial intelligence in malware as next-generation threats. *Soft Computing Journal, 25*(2), 27-34.