A, Tuncay ve A, Hasan (2025). Dünya Çapında Ünlü Hacker Olaylarının Analizi ve Önemli Güvenlik Önerileri. İstanbul Arel Üniversitesi İletişim Çalışmaları Dergisi, (27), 26-48.
ISSN: 2146-4162

*Araştırma Makalesi*

# DÜNYA ÇAPINDA ÜNLÜ HACKER OLAYLARININ ANALİZİ VE ÖNEMLİ GÜVENLİK ÖNERİLERİ

**Tuncay AKDEMİR***

**Hasan ALTİNCİK****

## Özet

Siber güvenlik, günümüzde giderek artan bir öneme sahiptir ve kurumlar için hayati bir konudur. Siber güvenliğin sadece teknik önlemlerle sınırlı kalmaması, aynı zamanda kurumsal yönetim, eğitim, olay müdahalesi ve uluslararası iş birliği gibi alanları da kapsaması gerekmektedir. Hacker saldırıları, siber tehditlere karşı daha hazırlıklı olunması ve güvenlik açıklarını sürekli olarak tespit edip giderilmesi açısından önemli bir olgudur. Bu bağlamda makalede, siber güvenlik stratejilerinin ve politikalarının güçlendirilmesi gerektiği, kurumların etkin olay müdahale stratejileri geliştirmesi, düzenli eğitimler sağlaması ve güvenlik bilincini artırması gerektiği vurgulanmaktadır. Hacker gruplarının saldırıları kamusal imajı, kurumsal stratejileri ve kurumların güvenlik algılarını hedef kitleler nezdinde olumsuz etkilemektedir. Bu eylemler sıklıkla yasalara aykırı olduğundan, etik ve hukuki tartışmalara da yol açabilmektedir. Bu felsefeden hareketle çalışmada, son dönemde yaşanan Kaseya ve Colonial Pipeline fidye yazılımı saldırılarının ışığında siber güvenlik önlemlerinin gerekliliği ve önemi tartışılmaktadır. Hackerlar, sosyal veya politik amaçlar için bilgisayar sistemlerini kullanarak toplumu etkilemekte ve siber aktivizmde bulunmaktadırlar. Bundan dolayı çalışma çerçevesinde kurumların alabilecekleri güvenlik önerileri ele alınmakta, siber güvenlik birimlerinin iş birliği yaparak en iyi uygulamaları paylaşması ve karşılaşılan tehditlere hızlı ve etkili yanıt vermesi gerektiği ifade edilmektedir. Ayrıca bu tür siber saldırılara karşılık bütüncül bir yaklaşım sergilenmesinin gelecekteki tehditleri önlemek açısından daha iyi hazırlanılmasını ve olası negatif etkilerin sınırlandırmasını sağlayacağı açıklanmaktadır.

***Anahtar Kelimeler:*** *Fiber yazılım, güvenlik önlemleri, hacker, siber güvenlik, siber saldırı*

**Yüksek Lisans Öğrencisi, tuncayakdemirtr@gmail.com ORCID: 0009-0009-3279-3010*

***Doç. Dr., Dicle Üniversitesi, hasanaltincik@gmail.com ORCID: 0000-0002-3528-2680*

Gönderim Tarihi: 28.01.2025

Kabul Tarihi: 15.04.2025

A, Tuncay ve A, Hasan (2025). Dünya Çapında Ünlü Hacker Olaylarının Analizi ve Önemli Güvenlik Önerileri. İstanbul Arel Üniversitesi İletişim Çalışmaları Dergisi, (27), 26-48.
ISSN: 2146-4162

*Research Paper*

# ANALYSIS OF WORLD-FAMOUS HACKER INCIDENTS AND KEY SECURITY RECOMMENDATIONS

**Tuncay AKDEMİR***

**Hasan ALTİNCİK****

## Abstract

Cyber security is of increasing importance today and is a vital issue for organizations. Cybersecurity should not only be limited to technical measures, but should also cover areas such as corporate governance, training, incident response and international cooperation. Hacker attacks are an important phenomenon in terms of being more prepared against cyber threats and continuously identifying and eliminating security vulnerabilities. In this context, the article emphasizes that cybersecurity strategies and policies should be strengthened, institutions should develop effective incident response strategies, provide regular trainings and increase security awareness. Attacks by hacker groups negatively affect public image, corporate strategies and security perceptions of organizations in the eyes of target audiences. Since these actions are often against the law, they can also lead to ethical and legal debates. Based on this philosophy, this study discusses the necessity and importance of cyber security measures in light of the recent Kaseya and Colonial Pipeline ransomware attacks. Hackers use computer systems for social or political purposes to influence society and engage in cyber activism. Therefore, the study discusses the security recommendations that organizations can take, and states that cyber security units should cooperate to share best practices and respond quickly and effectively to the threats encountered. It is also explained that taking a holistic approach to such cyber-attacks will ensure better preparation to prevent future threats and limit possible negative effects.

***Keywords:*** *Syber attack, cyber security, fiber software, hacker, security measures*

**Master's Student, tuncayakdemirtr@gmail.com ORCID: 0009-0009-3279-3010*

***Assoc. Prof. Dr., Dicle University, hasanaltincik@gmail.com ORCID: 0000-0002-3528-2680*

Received: 28.01.2025

Accepted: 15.04.2025

A, Tuncay ve A, Hasan (2025). Dünya Çapında Ünlü Hacker Olaylarının Analizi ve Önemli Güvenlik Önerileri. İstanbul Arel Üniversitesi İletişim Çalışmaları Dergisi, (27), 26-48.
ISSN: 2146-4162

# DÜNYA ÇAPINDA ÜNLÜ HACKER OLAYLARININ ANALİZİ VE ÖNEMLİ GÜVENLİK ÖNERİLERİ

## GİRİŞ

Günümüzde hacker terimi bilgisayar sistemlerine yetkisi olmadığı halde erişen, sistemden bilgi alan, işleyişi değiştiren veya sonlandıran kişiler olarak tanımlanmaktadır (Akdeniz, 2013: 9). Hacker saldırıları, terörizm ve çevresel riskler gibi faktörler, güvenlik politikalarının ve stratejilerinin sürekli olarak yeniden düşünülmesini ve geliştirilmesini gerektirmektedir. Küresel ölçekteki siber tehditlerin artması, güvenlik önlemlerine duyulan acil ihtiyacı vurgulamaktadır. Bu nedenle, güvenlik stratejilerinin sürekli olarak güncellenmesi ve aynı zamanda bilinçlendirme ve eğitim programlarının güçlendirilmesi, siber tehditlere karşı etkili bir mücadele için temel unsurlardır.

"*Fidye yazılımı, bilgisayara belirli bölümlere erişimi kısıtlayan (örneğin verilerini şifreleyerek) ve işlevselliğin tekrar kazanılması için mağdurdan ödeme talep eden, özellikle zararlı bir kötü amaçlı yazılım biçimidir*" (Hıdıroğlu, 2023: 6). Bu yazılım ciddi bir tehdit oluşturmakta ve siber suçlular tarafından hayati bilgilere erişilerek kurumlardan haraç almak amacıyla kullanıldığı için genellikle önemli veri kayıplarına yol açmaktadır. Fidye yazılımı saldırıları, siber güvenlikteki eksiklikleri ve önlemlerin önemini bir kez daha vurgulamaktadır. Günümüzde siber tehditler, teknoloji kurumlarının ve kritik altyapı sağlayıcılarının güvenlik önlemlerini sıkılaştırmalarını gerektiren ciddi bir endişe kaynağıdır.

2021 yılında, kötü amaçlı e-postaların önemli bir kısmı, veri bütünlüğünü tehlikeye atma ve depolanan bilgiler üzerinde kontrol sağlama kapasitesine sahip fidye yazılımı saldırılarını içermekteydi. (Balyemez, 2022). Kaseya'nın VSA yazılımında ortaya çıkan güvenlik açığına dayalı fidye yazılımı saldırısı ile Colonial Pipeline fidye yazılımı saldırısıyla bir kez daha açıkça görülmüştür. Bu çalışmada saldırının niteliği, etkileri, müdahale süreci, siber güvenlik açısından çıkarılan dersler ve gelecekte alınabilecek önlemler detaylı bir şekilde ele alınmıştır. Ayrıca, bu saldırıyla, siber güvenlikte iş birliği ve bilgi paylaşımının kritik önemi de gözler önüne serilmiştir. İki farklı saldırı olayının detaylı analizi, siber güvenlik alanında alınması gereken önlemlerin ve gelecekteki tehditlere karşı hazırlıklı olmanın önemini vurgulamaktadır. Bu analiz, siber güvenlik bilincinin

artırılmasına ve kurumların daha güvenli dijital ortamlar oluşturmasına katkı sağlayacaktır.

Dijital ve küresel boyutlara yayılan yeni tehditlerle güvenlik kavramı da karmaşıklaşmıştır. Devletler, kurumlar ve bireyler için siber güvenlik, verilerin çevrimiçi tehditlere karşı korumasının önemli bir unsuru haline gelmiştir. Bu bağlamda, bilgi teknolojilerinin güvenlik önlemleri de giderek daha fazla önem kazanmaktadır. Bu çalışmanın ilk bölümünde hacker kavramının tanımına ve kökenine inilmiş olup sosyal yaşamdaki yerleri hakkında bilgi verilmiştir. Ayrıca hacktivist grupların amaçlarına ve hedeflerine değinilmiş ve incelenmiştir. Çalışmanın ikinci bölümünde ise kurumlar için bir takım önemli güvenlik önerileri sunulmuş ve bu konudaki toplum bilincini artırmada devletin rolü ele alınmıştır. Çalışmanın üçüncü bölümünün oluşturan araştırma kısmında ise 2021 yılında gerçekleşen Kaseya ve Colonial Pipeline saldırıları örnek vaka analizi yöntemiyle değerlendirilmiştir. Kurumlar için hacker saldırılarına karşı alınacak önlemlerin önemi vurgulanmıştır.

## Hacker Kavramı ve Önemi

"*"Hacker" terimi, 1960'ların başlarında Massachusetts Teknoloji Enstitüsü'ndeki (MIT) bir grup tutkulu programcının bu kelimeyi kendi aralarında kullanmaya başlamasıyla ortaya çıkmış ve zamanla literatürde yerini almıştır.*" (Çoban, 2020: 45). Dolayısıyla, 1960'ların başlarındaki hacker kültürü ve MIT'deki (Massachusetts Teknoloji Enstitüsü) hacker gruplarının bilgisayar sistemlerine olan merakı, günümüzde hacktivizmin temellerini oluşturan unsurlardan biri olarak görülebilmektedir. Hackerlar, hacktivist olarak adlandırıldıklarında, belirli bir sosyal veya politik amacı desteklemek için bilgisayar sistemlerini kullanır ve bu şekilde siber aktivizmde bulunmaktadırlar. Hacktivizm bağlamında, yazılımların geliştirilmesinin ana hedefi, bireylerin bilgiye güvenli bir şekilde erişimini temin etmektir. Güvenlik, sıklıkla anonimlik ile özdeşleştirilir ya da anonimlik, güvenliğin sağlanmasında en kolay ve etkili yöntem olarak kabul edilir; dolayısıyla anonimlik, aynı zamanda mahremiyetin korunmasını da ifade eder (Öztürk, 2017: 178). Genellikle tipik bilgisayar korsanlarından farklı olarak, bu bilgisayar uzmanları bireysel olarak değil, gruplar halinde çalışmaktadır. Bu gruplar genellikle dünya çapında herhangi bir merkezi olmayan ağlar olarak örgütlenmektedirler.

Hacktivist grupların toplumu etkileme yollarından biri yolsuzluğu ve adaletsizliği açığa çıkarmaktır. Hacktivist eylemler alışılagelmiş protesto

yöntemleri kadar yaygın olmasa da özellikle kendisine geniş bir destekçi kitlesi bulduğundan yarattığı etki oldukça geniştir (Demirkıran, 2013: 27). Bu tür eylemler, bilgi sızıntıları, web sitelerinin devre dışı bırakılması veya veri korsanlığı gibi çeşitli yöntemlerle gerçekleştirilebilmektedir. Ancak, bu eylemler sıklıkla yasalara aykırı olduğundan, etik ve hukuki tartışmalara yol açabilir ve bu grupların amaçlarıyla ilgili geniş çapta görüş ayrılıklarına neden olabilmektedir. Bununla birlikte, hacktivist gruplar, toplumda farkındalık yaratmak ve değişim talep etmek için diğer protesto yöntemlerine alternatif olarak kullanılmaktadır.

Hacker grupların toplumu etkileme yöntemlerinden biri de ifade özgürlüğünü ve mahremiyeti teşvik etmektir. Mahremiyeti altı temel ilke üzerinden tanımlanır; 1) yalnız kalma hakkı, 2) kişinin kendine ulaşımı sınırlandırması, 3) gizlilik, 4) kişisel bilgi üzerinde kontrol sahibi olmak, 5) baskıdan uzaklaşarak kendi otonomi ve saygınlığını kazanmış bir birey olma, 6) yakın ilişki ve samimiyet (Yiğitbaşı ve Çelik, 2023: 850). Bu ilkeler, çevrimiçi özgürlük ve gizlilik konularında daha fazla farkındalık oluşturmuş ve insanları eyleme geçirmiştir. Ancak, hacktivist grupların hizmet aksatması ve zarar verme potansiyeli de bilinmektedir. DDoS (Distributed Denial of Service) saldırıları ve diğer siber saldırılar, hükümet ve kurumsal web sitelerine zarar vermiş ve bireylere hizmet aksamasına yol açmıştır. Aktivizm ile suç davranışı arasındaki çizgi genellikle belirsiz olmaktadır. Bu tür eylemlerin önemli konulara dikkat çekmek için gerekli olduğunu savunanlar olduğu gibi, bunları zararlı ve ters etki olarak görenler de bulunmaktadır. Kimileri onları kahramanlar ve sosyal adaletin savunucuları olarak görürken, diğerleri onları suçlu ve güvenlik tehdidi olarak algılamaktadır.

Hacker gruplarının kamusal imajı, değişim üzerinde etki yaratma güçlerini ve eylemlerinin farklı kitlelerce nasıl algılandığını etkileyebileceği düşünülebilmektedir. Bu nedenle, bu grupların devletler ve toplumlardaki algısını anlamak ve değerlendirmek önem arz etmektedir. Hükümetler, uzun zamandır ulusal güvenlik gerekliliği altında bilgiye erişmenin ve korumanın önemine ekonomik ve askeri olarak da değer vermektedir (Ersanel, 2001: 2). Hacker grupların eylemleri bazen önemli konulara dikkat çekerken sosyal değişime de yol açabilmekte ve aynı zamanda zarara da neden olabilmektedir. Eylemlerin faydalarını ve dezavantajlarını değerlendirmek, kamuoyu algısının etkilerini gözlemlemek ve olası sonuçları öngörmek gerekmektedir. Bu tür

çalışmalar, hacktivist grupların etkisinin geniş bir perspektiften anlaşılmasına yardımcı olabilmektedir.

Her alanda olduğu gibi hacktivizm dünyasında da etik olmak önemli olmaktadır. Hacker, yükümlülüklerinin ağırlığının farkındadır ve çabaları boyunca etik standartlara özenle bağlı kalmaktadır. Etik bilgisayar korsanlığı alanında, uyulması gereken bir dizi ilke bulunmaktadır. Bu ilkeler arasında en önemlisi, etik bilgisayar korsanının, sistemin sahibi olan kuruluştan açık rıza ve yetki alması gerekliliğidir (Maawi, 2021: 62). Hackerlıkta etik ilkelere bağlı kalmak, sistemdeki zayıflıkları inceleyip tespit ederek güvenlik önlemlerinin geliştirilmesini mümkün kılmaktadır. Etik hackerlar, güvenlik sistemlerinin test edilmesinin yanı sıra, kötü niyetli aktörlere karşı bir kalkan görevi de görmektedir. Bu sayede, kuruluş içerisindeki bireyleri veya işletmeleri hedef alan istismar girişimleri engellenerek, şantaj ve yetkisiz erişim olasılığı önemli ölçüde azaltılmaktadır.

## Kurumlar İçin Önemli Güvenlik Önerileri

Tarihin derinliklerinden günümüze kadar, insanlık varoluş mücadelesinde güvenlik olgusuna büyük bir önem vermiştir. Güvenlik, insanın hayatta kalması ve yaşamını sürdürmesi için temel bir gerekliliktir. Beslenme, barınma gibi fiziksel ihtiyaçların yanı sıra, güvenlik de insanın yaşamının vazgeçilmez bir parçasıdır (Özer, 2023: 73). Zamanla medeniyetler ilerlemiş ve güvenlik kavramı evrimleşmiştir. Günümüzde ise güvenlik kavramı, yalnızca fiziksel tehditlerle sınırlı kalmamakta; aynı zamanda dijital ve küresel boyutlara da yayılmaktadır. Siber saldırılar, terörizm ve çevresel riskler gibi yeni tehditler ortaya çıkmış ve bu da güvenlik politikalarının ve stratejilerinin sürekli olarak geliştirilmesini zorunlu kılmıştır.

Devletler, kurumlar ve insanların kişisel verileri için siber güvenlik alanı, bir kuruluşu, işgücünü ve varlıklarını çevrimiçi tehditlerden korumayı amaçlayan kapsamlı bir dizi önlemin uygulanmasını gerektirmektedir. Siber güvenlik, elektronik sistemler, bilgisayarlar, mobil cihazlar, sunucular, ağlar ve içerdikleri veriler dahil olmak üzere teknolojik cihazların ve altyapıların siber tehditlere karşı korunmasını içerir (Elmas, 2023: 21). Siber saldırılar daha sık hale geldikçe ve kurumsal ağlar karmaşıklaştıkça, bu risklerin etkisini azaltmak için bir dizi siber güvenlik çözümünün uygulanması önem arz etmektedir. Günümüzün dijital ortamında, işletmeler için bilginin önemi göz ardı edilmemektedir. Bu

nedenle, tehditlerin boyutunu ve bunların yansımalarını ölçmek için bir bilgi teknolojilerinin güvenlik risk analizi yapmak zorunlu hale gelmektedir.

Küresel siber tehditler, devamlı olarak değişen bir ortamda evrim geçiriyor ve dünya genelindeki kurumlar için büyük bir sorun haline gelmektedir. Veri ihlallerinin sıklığı her yıl artarak endişe verici bir eğilim göstermektedir. 2019'un ilk dokuz ayında 7,9 milyar kayıt veri ihlallerine maruz kalmıştır. Bu rakam, 2018'in ilgili dönemine kıyasla %112'lik önemli bir artışı temsil etmekte ve siber tehditlerin artan ciddiyeti ile güçlü siber güvenlik önlemlerine duyulan gerekliliği vurgulamaktadır (Kaspersky, tarih yok). Bu durum, siber tehditlerin giderek artan ciddiyetinin ve sağlam siber güvenlik önlemlerine olan acil ihtiyacın altını çizmektedir. Bu nedenle, kurumların güvenliklerini güçlendirmek için sürekli olarak yeni stratejiler ve teknolojiler geliştirmeleri ve uygulamaları gerekmektedir. Ayrıca, bilinçlendirme ve eğitim programlarının güçlendirilmesi de siber tehditlere karşı daha etkili bir mücadele için önemli bir adım olacaktır.

### Güncel Sistemlerin Önemi

Siber saldırıların kesin olarak önlenmesi zor olmaya devam etse de etkilerinin azaltılması ve olası zararların en aza indirilmesi için sağlam savunma stratejilerinin uygulanması gerekmektedir. Siber saldırganlar, eski sürümleri kullanan ve güncellemeleri yapılmamış sistemleri hedef alarak güvenlik açıklarından faydalanmaktadırlar. Bu nedenle, sistem güvenliğini sağlamak amacıyla güvenilir ve doğru kaynaktan düzenli güncellemelerin yapılması büyük önem taşımaktadır. Kurumların, yama ve güncelleme yönetimi için belirli bir program izlemeleri önerilmektedir. ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), bu tür zafiyetlere dayalı saldırıların oranını ise %29 olarak belirlemiştir. (Çavuş, 2018). Koruma için ileri teknolojiye geçiş, doğru şekilde uygulanmadığı takdirde gerçekten de etkisiz hale gelebilmekte ve genellikle geleneksel yöntemlerin önemini vurgulamaktadır. Bireylerin, güvenlik açıklarını azaltmak için sağlam parolalar kullanmanın ve cihaz uygulamalarını düzenli olarak güncellemenin önemini anlamaları gerekmektedir. Bunu yaparak yetkisiz erişimi engelleyebilir ve cihazlarını olası ihlallere karşı koruyabilmektedirler.

### İki Faktörlü Kimlik Doğrulamanın Önemi

Günümüzün dijital ortamında, çok sayıda platform iki faktörlü kimlik doğrulamayı etkinleştirme seçeneği sunarak hesaplarınızın güvenliğini

artırmaktadır. Bu ek koruma, kimliğinizin doğrulanmasına hizmet ederek hesabınıza erişen kişinin gerçekten yetkili olmasını sağlamaktadır (TitanFile, 2021). Bu koruma katmanı, sadece şifrenizi değil, aynı zamanda hesabınıza erişim için ek bir doğrulama adımı gerektirerek hesabınızı daha da güvende tutmaktadır. Örneğin cep telefonlarına gelen bir doğrulama kodu güvenliği artırmaya yardımcı olmaktadır.

### Kart Tabanlı Geçiş Sistemlerinin Önemi

Teknolojinin hızla ilerlediği günümüzde, güvenliği artırmak ve erişimi kontrol altında tutmak amacıyla kullanılan emniyet sistemleri ve kilitlerde büyük değişiklikler yaşanmaktadır. Kart tabanlı geçiş sistemleri, gündelik yaşamımızın pek çok alanında yaygın olarak kullanılmaktadır. Kamu kurumları, otobüsler, üniversiteler, hastaneler, yemekhaneler, eğlence merkezleri, oteller ve benzeri birçok yerde kartlı geçiş teknolojisi entegre edilmiştir (Nacaroğlu, 2023: 11). Bu sistemler, fiziksel anahtarların yerine geçerek daha güvenli ve esnek bir erişim sağlamaktadır. Bu sayede, güvenlik önlemleri güçlendirilirken kullanım kolaylığı da artmaktadır.

### Kurum Liderlerinin Siber Güvenlik Farkındalığı

Siber tehditlerin artan sayısı ve siber saldırıların yaygın etkilerine rağmen, araştırmacılar sıkça, kurum liderlerinin genellikle siber güvenlik tehditleri ve gereksinimleri hakkında yeterince farkında olmadıklarını belirtmektedirler (WaterISAC, 2016). Siber tehditlerin karmaşıklığı ve hızla değişen doğası, yöneticilerin bu konudaki güncel bilgilere ayak uydurmasını zorlaştırmaktadır. Yöneticilerin siber güvenlik stratejilerine daha fazla katılımı teşvik edilmeli ve bu konuda daha fazla sorumluluk almaları sağlanmalıdır. Bu şekilde, kurumlar siber tehditlere karşı daha hazırlıklı olabilir ve güvenliklerini daha etkin bir şekilde gerçekleştirebilirler.

### Asimetrik Şifreleme ve Dijital İmza

Asimetrik şifreleme, matematiksel teoremlerle desteklenen karmaşık algoritmaları temel alır. Örneğin, Diffie-Hellman protokolü, ortak gizli anahtar oluşturmak için ayrık logaritma problemini kullanır. Benzer şekilde, RSA (Rivest-Shamir-Adleman) şifreleme algoritması da ayrık logaritma problemine dayanır ve geliştirilmiş bir yöntem sunar (Yerlikaya vd., 2007: 2). Bu yöntem, anahtar değişimi sürecinde güvenlik sağlar ve tarafların gizli bir anahtarı paylaşmasına olanak tanır. Bu şekilde, güvenli iletişim ve dijital imza oluşturma gibi çeşitli

uygulamalarda yaygın olarak kullanılmaktadır.

Dijital imzaların oluşturulması genellikle asimetrik şifrelemede kullanılanlara benzer matematiksel algoritmaların kullanılmasına dayanmaktadır (AL-Hawamleh, 2023: 804). Asimetrik şifreleme, dijital imzaların güvenilirliğini sağlamak için kullanılan bir yöntemdir. Gönderen, özel anahtarıyla bir dijital imza oluşturur ve bu imza, alıcıya mesajın gerçekten gönderen tarafından oluşturulduğunu ve üzerinde değişiklik yapılmadığını kanıtlamaktadır. Bu yöntem, güvenli iletişimde ve dijital belgelerin güvenli bir şekilde imzalanmasında yaygın olarak kullanılmaktadır.

## Toplumların Güvenliğini Sağlamak İçin Adımlar

Siber güvenlik, kurumları ve devletleri kapsayan oldukça geniş bir çalışma alanı olmakla birlikte birçok devlet, uluslararası örgüt ve önemli ağ teknolojisi firmaları tarafından bir ulusal öncelik olarak kabul edilmektedir (Güntay, 2019: 109). Siber güvenlik, ulusal güvenliği, kamu hizmetlerini ve vatandaşların mahremiyetini tehlikeye attığına dair göz önüne alındığında, devletler için büyük bir endişe kaynağı olmaktadır. Devletlerin, kurumların ve bireylerin siber tehditlere karşı korunması, veri güvenliğinin sağlanması ve dijital altyapının güçlendirilmesi, modern toplumların sürdürülebilirliği için önem taşımaktadır. Birçok devlet, siber güvenliği ulusal bir öncelik olarak kabul etmiş ve bu alanda stratejiler geliştirmişlerdir.

Toplumun bilgi teknolojilerine olan bağımlılığı giderek arttığından dolayı, kritik altyapıların korunması ve kullanılabilirliği, ulusal çıkarlar açısından hayati bir öneme sahiptir. Bu nedenle, siber güvenlik artık toplumun her seviyesini etkileyen bir ulusal mesele olarak kabul edilmektedir (Ada ve Çakır, 2017: 632). Kamu siber güvenlik departmanları, çalışanlara ve yetkililere siber güvenlikle ilgili düzenli eğitimler vererek bu çabada önemli bir rol oynamaktadır. Bu uygulamalar arasında sağlam parolalar kullanmak, kimlik avı e-postalarından uzak durmak ve yazılımları güncel tutmak yer almaktadır. Ayrıca, kamu siber güvenlik birimleri siber tehditler ve bunların potansiyel sonuçları konusunda kamu bilincinin artırılmasına aktif olarak katılmalıdır. Buna ek olarak, siber güvenlik birimleri ağ ve sistemlerindeki siber riskleri ve güvenlik açıklarını dikkatle izlemeli ve değerlendirmelidir.

Bir diğer önemli tedbir de kamu kurumları ve daha geniş halk kitleleri arasında siber güvenlik farkındalığı ve eğitimi kültürünün geliştirilmesidir. Siber

güvenlik, yalnızca tek bir kişinin veya kurumun sorumluluğunda değildir. Her birey, internete bağlı cihazları kullanırken siber güvenlik konusunda sorumluluk sahibi olmaktadır. Bireysel davranışlarımızın, genel siber güvenlik durumunu etkilediği unutulmamalıdır (Ankara Üniversitesi Bilgi İşlem Daire Başkanlığı, 2018). Bu nedenle vatandaşları kişisel cihazlarında ve çevrimiçi faaliyetlerinde siber güvenlik önlemlerini benimsemeye teşvik etmek son derece önemlidir. Buna ek olarak, devletin siber güvenlik departmanlarının, siber güvenlik sorunlarına karşı hazırlıklarını ve müdahalelerini artırmayı amaçlayan ortak tatbikatlar ve girişimlerde bulunmaları tavsiye edilmektedir. Bunlar, siber tehditlere karşı savunmayı güçlendirmek için siber güvenlik departmanları tarafından alınan çeşitli önlemleri temsil etmektedir. Bu tedbirlerin benimsenmesi yoluyla devlet ulusal çıkarlarını ve değerlerini siber düşmanlardan koruyabilmektedir.

## Kaseya ve Colonial Pipeline Hacker Saldırılarına Yönelik Analiz

### Araştırmanın Konusu

Bu araştırma, 2021 yılında gerçekleşen önemli hacker olaylarından Kaseya ve Colonial Pipeline'a yönelik fidye yazılımı saldırılarının incelenmesini ve bu olaylara karşı alınabilecek güvenlik önlemlerinin analiz edilmesini konu almaktadır.

### Araştırmanın Önemi

Bu araştırma, siber saldırıların artan yaygınlığı ve karmaşıklığı göz önüne alındığında önem arz etmektedir. Hacker olayları hem bireysel hem de kurumsal düzeyde ciddi mali kayıplara, itibar zedelenmesine ve gizlilik ihlallerine yol açabilmektedir. Bu nedenle, hacker saldırılarına karşı etkili güvenlik önlemlerinin belirlenmesi, siber güvenlik stratejilerinin geliştirilmesi ve uygulanması bir gerekliliktir. Araştırma, bu alandaki bilgi eksikliğini gidermeyi ve ilgili taraflara rehberlik etmeyi amaçlamaktadır.

### Araştırmanın Sınırlılıkları

Bu çalışma 7 Mayıs 2021 Coloniel Pipeline ve 2 Temmuz 2021 Kaseya siber saldırılarının tarihleriyle sınırlandırılmıştır. Bu çalışma için hacker saldırılarına yönelik çıkan haberler ve blog sayfalarda konuyla ilgili yazılan yazılar incelenmiş ve analiz edilmiştir.

### Araştırmanın Yöntemi

Araştırmada örnek vaka analizi yapılmaktadır. Örnek vaka çalışmaları, bir

program, bir kişi, bir işlem, bir süreç, bir kurum ya da bir sosyal grup gibi belirli bir olguyu detaylı bir şekilde incelemek için oldukça uygun bir yöntemdir. Bu çalışmalar, belirli bir durumu anlamak, iç mekanizmalarını ortaya çıkarmak, etkilerini değerlendirmek ve genellikle teorik çerçevelerle ilişkilendirmek amacıyla kullanılır. Örnek vaka çalışmaları, derinlemesine analiz yapma fırsatı sağlar ve genellikle nitel araştırma yöntemleriyle gerçekleştirilir (Merriam, 1988: 6).

Bu araştırmada, Kaseya ve Colonial Pipeline saldırılarının neden-sonuç ilişkileri ele alınarak siber güvenlik ihlallerinin sistematik etkileri incelenmiştir. Nedensel etkiyi belirlemek için şu sorulara odaklanılmıştır:

Bu saldırılar neden gerçekleşti?

(Bağımsız değişkenler: güvenlik açıkları, fidye yazılım gruplarının stratejileri, zayıf kriz yönetimi)

Ne tür sonuçlar doğurdu?

(Bağımlı değişkenler: ekonomik kayıplar, operasyonel kesintiler, regülasyon değişiklikleri)

Benzer sonuçlara neden olan ortak faktörler nelerdi?

Her iki vakada da saldırganların sistemlerdeki güvenlik açıklarını tespit edip fidye yazılımı yayarak operasyonel kesintiye yol açtıkları görülmektedir. Ancak Kaseya saldırısında bir tedarik zinciri saldırısı gerçekleşmiş, yani hizmet sağlayıcının güvenlik açığı kullanılarak binlerce müşteri etkilenmiştir. Colonial Pipeline saldırısında ise kritik enerji altyapısı hedef alınarak bölgesel bir ekonomik kriz yaratılmıştır.

Bu iki farklı bağlamda gerçekleşen saldırılar, siber güvenlik açıklarının küresel ekonomiyi ve kamu düzenini nasıl etkilediğini gösteren nedensel bir bağlam sunmaktadır. Bu doğrultuda, çalışmada siber güvenlik saldırılarının kurumsal zafiyetleri nasıl istismar ettiğini açıklanmakta, vakalar arasında ortak nedensel faktörleri belirleyerek siber güvenlik politikalarının eksikliklerini ortaya koyulmakta ve teorik olarak, fidye yazılımı saldırılarının şirketler ve ulusal güvenlik için oluşturduğu riskleri analiz edilmektedir.

Bu çalışmada, örnek vaka analizi (Case Study Analysis) yöntemi benimsenmiş olup, analiz edilen Kaseya ve Colonial Pipeline saldırıları, benzerlik yöntemi (Method of Agreement) çerçevesinde ele alınmıştır. Benzerlik

yöntemi, bağımsız değişkenlerin farklılık gösterdiği ancak bağımlı değişkenin aynı olduğu durumlarda, bağımlı değişkenin nedenlerini anlamaya yönelik bir strateji sunar (Bennet, 2004: 19-55). Bu yöntemde, seçilen vakalar birbirlerinden oldukça farklıdır; ancak, her iki olay da siber güvenlik zafiyetleri ve fidye yazılımı saldırıları ile sonuçlanmıştır. Bu bağlamda, çalışmada kullanılan yöntem, "Aynı Sonucu Doğuran En Farklı (ASEF)" veya "En Farklı Sistemler Tasarımı (EFST)" olarak da adlandırılan yaklaşımla örtüşmektedir (Przeworski & Teune, 1970: 33-48). Przeworski ve Teune (1970), En Farklı Sistemler Tasarımı (EFST) yaklaşımında, farklı sosyo-politik ya da kurumsal bağlamlara sahip vakaların, ortak bir sonuç üretmesi durumunda, bu sonucun ardındaki belirleyici faktörlerin tespit edilebileceğini savunmaktadır. Çalışmada ele alınan Kaseya ve Colonial Pipeline saldırıları, operasyonel bağlam, hedeflenen sektörler ve saldırı teknikleri açısından farklılık gösterse de her ikisi de kritik altyapıyı hedef alan fidye yazılımı saldırıları olarak aynı sonucu doğurmuştur. Bu çerçevede, her iki saldırının siber güvenlik açısından temel zafiyetleri nasıl ortaya çıkardığını analiz etmek, yöntemsel olarak benzerlik yöntemi ile uyum göstermektedir.

Lijphart, az sayıda vaka ile çok fazla bağımsız değişkenin bulunmasının araştırmanın geçerliliğini riske atabileceğini öne sürmektedir (Lijphart, 1971: 685). Ancak, bu çalışmada uygulanan yöntem, Lijphart'ın eleştirisini bertaraf eden bir yapıya sahiptir. Çünkü çalışma, bağımsız değişkenleri çeşitlendirmeye değil, bağımlı değişkenin benzerliği üzerinden analiz yapmaya odaklanmaktadır. Anckar, da bu noktada, farklı sistemlerde test edilen tek bir bulgunun, araştırmanın iç tutarlılığını artırdığını ve metodolojik sağlamlığı desteklediğini belirtmektedir (Anckar, 2008: 395). Çalışmada, iki farklı vaka üzerinden aynı sonuca yol açan faktörler incelendiği için, bu eleştiri geçerliliğini yitirmektedir.

Sonuç olarak, kullanılan yöntem benzerlik yönteminin akademik temelleriyle örtüşmekte ve hem Przeworski & Teune (1970) hem de Anckar (2008) tarafından metodolojik açıdan güçlü bir yaklaşım olarak tanımlanan bir çerçeveye oturmaktadır. Böylece, araştırmanın siber güvenlik bağlamında vaka analizleri üzerinden sağlam bir nedensel çıkarım yapmasına olanak tanıdığı ifade edilebilir.

### Araştırmanın Analiz Birimi ve Kapsamı

Bu araştırmanın analizi, fidye yazılım saldırılarına maruz kalan kurumlar ve onların siber güvenlik stratejileri olarak belirlenmiştir. Örnek vaka analizi yöntemi doğrultusunda, 2021 yılında gerçekleşen Kaseya ve Colonial Pipeline

fidye yazılım saldırıları, siber güvenlik bağlamında kurumsal tepkiler ve alınan önlemler açısından ele alınmıştır. Analiz birimi olarak bu iki olayın seçilmesinin temel nedeni, farklı sektörlerde faaliyet göstermelerine rağmen benzer siber güvenlik tehditlerine maruz kalmaları ve saldırıların kurumsal süreçler üzerinde yarattığı etkilerin karşılaştırılabilir olmasıdır. Araştırmada analiz birimi çerçevesinde şu unsurlar ele alınmaktadır:

- Saldırıların hedef aldığı kurumlar ve güvenlik altyapıları
- Hacker gruplarının saldırı stratejileri ve kullanılan yöntemler
- Kurumların kriz yönetimi süreçleri ve müdahale stratejileri
- Siber güvenlik politikaları ve geleceğe yönelik çıkarılan dersler

Bu kapsam doğrultusunda, vaka analizinde kurumsal siber güvenlik stratejilerinin etkinliği ve fidye yazılım saldırılarının neden olduğu yapısal zafiyetler detaylı bir şekilde incelenmiştir. Analiz biriminin netleştirilmesi, çalışmanın araştırma sorunsalı ile daha güçlü bir bağ kurmasını sağlayarak, kurumsal düzeyde alınması gereken güvenlik önlemlerine dair kapsamlı bir değerlendirme sunmaktadır.

### Kaseya Hacker Saldırısına Yönelik Analiz

Kaseya, 2000 yılında teknoloji girişimcileri Mark Sutherland ve Paul Wong tarafından kuruldu ve küçük ile orta ölçekli işletmeler (KOBİ'ler) ile yönetilen hizmet sağlayıcıları (MSP'ler) için kapsamlı IT ve güvenlik yönetimi yazılımları geliştiren bir şirkettir (Kaseya, tarih yok). Şirket, kuruluşundan bu yana birçok önemli satın alım gerçekleştirmiştir. Bu alımlar, Kaseya'nın portföyünü güçlendirip, sektördeki lider konumuna gelmesini sağlamıştır (Kaseya, tarih yok).

2 Temmuz 2021 tarihinde Rusya destekli REvil fidye yazılım grubu, Kaseya'nın VSA (Sanal Sistem Yöneticisi) yazılımında bulunan bir Zero-Day yararlanarak bir dizi yönetilen hizmet sağlayıcısına ve bunların müşterilerine yönelik bir tedarik zinciri fidye yazılımı saldırısı gerçekleştirmiştir (Usta, 2021). Zero-Day (Sıfır Gün) açığı, yazılım geliştiricileri tarafından henüz keşfedilmemiş veya düzeltilmemiş güvenlik açıklarını ifade etmektedir. Bu tür açıklar, saldırganlara sistemlere yetkisiz erişim sağlama imkânı tanır ve tespit edilmeleri zordur (Turhost Blog, tarih yok) Hackerlar, Kaseya'nın yazılımını tehlikeye atarak birden

fazla müşterisinin sistemlerine fidye yazılımı dağıtmak için kullanmıştır. Saldırı karmaşık güvenlik açıklarından yararlanmayı içermekte ve bu da saldırganların yüksek düzeyde teknik yeterliliğe sahip olduğunu göstermektedir. Bu durum, yazılım güvenliğinin kritik önemini ve karmaşık yazılım sistemlerindeki güvenlik açıklarını gözden kaçırmanın kaçınılmaz sonuçlarını vurgulamaktadır.

İsveç'te bir süpermarket zinciri, 800 mağazasını kapattırmıştır. Tahminlere göre, bu durumun 800 ila 1.500 arasında işletmeyi olumsuz yönde etkilemiş olabileceği gözlemlenmektedir (Sade, 2021). Saldırının etkisi yaygın olmakla birlikte yalnızca Kaseya'nın doğrudan müşterilerini değil, aynı zamanda Kaseya'nın yazılımını kullanan binlerce küçük ve orta ölçekli işletmeyi etkilediği görülmekte olup birçok kurumunda faaliyetlerini kesintiye uğratmıştır.

Kaseya, 4 Temmuz'daki bilgi hırsızlığına karşı çözüm olarak evrensel bir şifre çözücü edinmiştir. Bu sayede REvil siber suç grubunun gerçekleştirdiği fidye yazılımı saldırısının mağdurları, dosyalarını ücretsiz olarak kurtarabileceklerdir (Olmos, 2021). Kaseya, müşterileri hızlı bir şekilde bilgilendirip, VSA sunucularını kapatarak ve bazı kurumlardan olay müdahale ekiplerini devreye sokarak saldırıya yanıt vermiştir. Kurum olayı araştırmak ve hizmetleri geri yüklemek için gece gündüz çalışmış ancak kurtarma sürecinde gecikmeler yaşanmıştır. Kaseya'nın saldırıya müdahalesi, etkilenen sunucuların derhal kapatılmasını, siber güvenlik uzmanlarıyla iş birliğini, ihlalini kontrol altına almak ve hizmetleri geri yüklemek için devam eden soruşturmaları içermektedir. Hızlı müdahale, iletişim stratejileri, kolluk kuvvetleri ve düzenleyici kurumlarla koordinasyon dahil olmak üzere olaya müdahale planlamasının önemini vurgulamaktadır. Etkili olay yönetimi, siber saldırıların etkisini en aza indirmek ve etkilenen sistemlere olan güveni yeniden tesis etmek için çok önemlidir.

Bu hacker saldırısı, siber güvenlik ortamında tedarik zinciri saldırılarının artan tehdidini vurgulamaktadır. Saldırganların Kaseya gibi bir satıcıyı hedef alarak eylemlerinin etkisini artırabilir ve çok sayıda kuruluşu etkileyebilmektedir. "*Bu saldırının her kurbanından talep edilen ödeme, her vaka için farklı olup, bazı araştırmacıların gördüğünü iddia ettiği en yüksek miktar olan 5 milyon dolara ulaşmaktadır*" (Harran, 2021). Bu olay aynı zamanda hem satıcılar hem de müşterileri için siber güvenlik hazırlığının öneminin altını çizmektedir. Ayrıca, Rusya ile bağlantılı olduğu iddia edilen REvil/Sodinokibi fidye yazılım grubunun olaya dahil olması, uluslararası siber güvenlik iş birliği ve ulus devletlerin siber tehditlerle mücadeledeki önemini vurgulamaktadır.

Kaseya, kötü amaçlı yazılımların müşterilere ulaşmasını önlemek amacıyla Sanal Sistem Yöneticisi (VSA) SaaS platformunu askıya almıştır. Ayrıca, tüm müşterilere bilgi yayma sorumluluğunu da üstlenmiştir (Cyvatar, 2022). Zorluklara rağmen Kaseya, yazılımların geliştirilmesi, dağıtılması ve üçüncü taraf güvenlik uzmanlarıyla iş birliği de dahil olmak üzere kurtarma sürecini hızlandırmak için çaba sarf etmiştir. Bu olay, siber tehditler karşısında mücadele vermenin zorluklarını vurgulamaktadır. Kaseya'nın yazılım iyileştirme, hizmetleri geri yükleme ve etkilenen müşterileri destekleme çabaları, siber düşmanlara karşı devam eden savaşı göstermektedir. Siber güvenlik duruşunu geliştirmek, sağlam yedekleme ve kurtarma mekanizmaları uygulamak, tehdit istihbaratı ve tespit yeteneklerine yatırım yapmak, gelecekteki riskleri azaltmak ve siber esneklik oluşturmak için gereklidir.

Bu çalışmada Kaseya siber saldırısı, yazılım tedarik zincirlerine yönelik fidye yazılımı saldırılarının etkilerini değerlendirmek amacıyla seçilmiştir. Vaka seçimi, olayın küresel ölçekte çok sayıda işletmeyi etkilemesi, siber güvenlik stratejileri açısından kritik bir örnek teşkil etmesi ve saldırının teknik ve operasyonel boyutlarıyla geniş çapta belgelenmiş olması gibi kriterlere dayanmaktadır. Analizde kullanılan temel değişkenler; saldırının yayılım mekanizması, etkilenen kurumların siber güvenlik önlemleri, müdahale süreci ve saldırının ekonomik ve operasyonel sonuçları olarak belirlenmiştir. Bu değişkenlerin incelenmesi, siber güvenlik alanında politika yapıcılara ve kurumsal aktörlere yönelik çıkarımlarda bulunmayı amaçlamaktadır. Kurumların risk yönetimi stratejilerini yeniden değerlendirmeleri ve gelecekte benzer olayları önlemek için daha güçlü güvenlik önlemlerine yatırım yapmaları gerekmektedir. Bu olay aynı zamanda siber tehditlerle etkin bir şekilde mücadele etmek için uluslararası iş birliği ve kolektif eylem ihtiyacını da hatırlatmaktadır.

Bu bağlamda, Kaseya siber saldırısı, siber güvenlik ve etkilenen kurumlar için geniş kapsamlı sonuçları olan önemli bir olayı temsil etmektedir. Bu olay, siber tehditlerin değişen doğasının risklerini azaltmak ve gelecekteki saldırılara karşı korunmanın altını çizmektedir. Kaseya'ya yönelik siber saldırı, siber güvenlik sorunlarının çok yönlü tehditlerini önleme, tespit ve müdahaleye yönelik bütüncül bir yaklaşıma duyulan ihtiyacın altını çizmektedir. Kurumlar siber olayların teknik, operasyonel ve politika boyutlarını anlayarak gelecekteki saldırılara daha iyi hazırlanabilir ve etkilerini azaltabileceklerdir. Devletler,

kurumlar ve siber güvenlik uzmanları arasındaki iş birliği, gelişen tehditleri ele almak ve dijital ekosistemleri korumak için gereklidir.

### Colonial Pipeline Hacker Saldırısına Yönelik Analiz

Colonial Pipeline, ABD'nin en büyük rafine petrol ürünleri boru hattı sistemidir. Şirket, 1961 yılında dokuz büyük petrol rafinerisi tarafından kurulmuştur. Şirketin ilk adı Suwannee Pipeline Company olarak belirlenmiş, ancak 1962 yılında Colonial Pipeline Company olarak değiştirilmiştir. Boru hattının inşaatına 1962 yılında başlanmış ve 1964'te tamamlanmıştır. Houston, Texas'tan New York Limanı'na kadar uzanan bu hat, ABD'nin güney ve doğu bölgelerindeki topluluklara ve işletmelere günlük milyonlarca galon benzin, ev ısınma yakıtı, havacılık yakıtı ve diğer rafine petrol ürünlerini taşımaktadır. Şirketin hissedarları arasında Koch Industries, Güney Kore Ulusal Emeklilik Servisi, Kohlberg Kravis Roberts, Caisse de dépôt et placement du Québec, Royal Dutch Shell ve IFM Investors yer almaktadır. (Colonial Pipeline, tarih yok).

7 Mayıs 2021 tarihinde DarkSide adlı bir hacker grubunun bilgisayar korsanları, ABD'nin en büyük boru hattını işleten Colonial Pipeline kurumunun sistemlerine sızarak akaryakıt transferinin durmasına yol açmıştır. Colonial Boru Hattı, Houston, Teksas'tan New York da dahil olmak üzere çeşitli güneydoğu eyaletlerine benzin, dizel ve jet yakıtı taşımaktan sorumlu, Amerika Birleşik Devletleri'ndeki önemli bir petrol boru hattı sistemidir (Russon, 2021). Colonial Boru Hattına yönelik saldırı, önceki güçlü siber saldırıların ardından, kritik altyapının siber tehditlere karşı savunmasızlığına ilişkin artan endişelerin ortasında meydana gelmiştir.

Colonial Pipeline siber saldırısının temel nedenleri, bilgisayar korsanları tarafından istismar edilen çeşitli teknik güvenlik açıklarına kadar izlenebilmesidir. Etkin olmayan bir VPN (Virtual Private Network) hesabının kullanılması, ağa yetkisiz girişi önlemek için uzaktan erişim sistemlerinin sürekli izlenmesi ve yönetilmesi gerektiğinin altını çizmektedir. İki faktörlü kimlik doğrulamanın olmaması, saldırıyı kolaylaştıran bir diğer kritik faktördür (GovTech, 2021). İki faktörlü kimlik doğrulaması, kullanıcıların hassas sistemlere veya verilere erişim sağlamadan önce birden fazla doğrulama biçimi sunmalarını gerektirerek ek bir güvenlik katmanı eklemektedir.

Colonial Pipeline siber saldırısının etkisi çok geniş kapsamlı olmuş, sadece kurumun kendisini etkilemekle kalmamış, aynı zamanda Amerika Birleşik

Devletleri'ndeki yakıt tedarikinde ve ekonomik faaliyetlerde aksamalara neden olmuştur. Dolayısıyla bu sıradan bir saldırı değil, belirli bir hedefi olan bir saldırıdır. İtibar açısından saldırı, Colonial Pipeline'ın siber güvenlik önlemlerinin yetersiz olduğu yönünde bir algı oluşturmuş ve kamuoyu nezdinde güven kaybına yol açmıştır (Securefors, 2021). Mali açıdan ise şirketin operasyonlarını durdurması nedeniyle doğrudan gelir kaybına uğradığı tahmin edilmekle birlikte, kesin miktar kamuya açıklanmamıştır. Bununla birlikte, operasyonların hızla yeniden başlatılabilmesi amacıyla Colonial Pipeline'ın saldırganlara yaklaşık 4,4 milyon dolar fidye ödediği bilinmektedir (Mobildev, 2021). Zararın sorumlusu olarak tanımlanan DarkSide grubu, hedefini belirledikten sonra onları korkutan, makinelerine fidye yazılımı yerleştiren ve sistemlerini kilitlemeden önce verilerini çalan bir suç çetesi olarak tanımlanmaktadır (Rockwell Automation, 2021). Bilgisayar korsanlarına fidye ödeme kararı, saldırının ciddiyetini ve fidye yazılımı tehditleriyle başa çıkmada kurumların karşılaştığı zorlukları daha da vurgulamıştır. Saldırıya yanıt olarak, olağanüstü hâl ilanı, ulaşım kısıtlamalarının geçici olarak askıya alınması ve fidye ödemelerinin geri alınmasına yönelik çabalar da dahil olmak üzere çeşitli tedbirler uygulanmıştır. Fidyenin bir kısmının Adalet Bakanlığı tarafından geri alınması, hükümetin siber suçluları sorumlu tutma ve bu tür saldırıların mali etkilerini azaltma konusundaki kararlılığını göstermiştir.

Colonial Pipeline saldırısı açık bir mesajın altını çizmektedir: fidye yazılımları tüm kuruluşlar için yakın ve büyüyen bir tehdit oluşturmaktadır ve bunun gibi yüksek profilli saldırılara verilen özel yanıt ne olursa olsun, felaketle sonuçlanabilecek sonuçları önlemek için proaktif koruma önlemleri şarttır (Montini, 2021). Colonial Pipeline siber saldırısı hem teknik güvenlik açıkları hem de kurumsal hazırlık açısından siber güvenlik için birkaç önemli sonucu vurgulamıştır. İlk olarak, saldırı düzenli güvenlik denetimleri, güvenlik açığı değerlendirmeleri ve çalışan eğitim programları da dahil olmak üzere siber güvenlik önlemlerinin öneminin altını çizmiştir. Kurumlar, gelecekteki siber saldırıları önlemek için güvenlik zayıflıklarını belirleme ve ele alma konusunda her daim olmalıdır. İkinci olarak, saldırı, etkili iletişim protokolleri, kolluk kuvvetleriyle koordinasyon ve bir saldırının ardından operasyonları hızla eski haline getirme becerisi dahil olmak üzere sağlam olay müdahale yeteneklerine duyulan ihtiyacı vurgulamıştır. Üçüncü olarak, saldırı siber güvenlikte iş birliği ve bilgi paylaşımının kritik rolü konusunda farkındalık yaratmıştır. Kurumlar, tehdit istihbaratını ve en iyi uygulamaları paylaşarak siber güvenlik savunmalarını

kolektif olarak geliştirebilir ve ortaya çıkan tehditlere karşı daha iyi koruma sağlayabileceklerdir.

Colonial Pipeline fidye yazılımı saldırısı, dünya çapında altyapıların karşı karşıya olduğu siber tehditleri keskin bir şekilde hatırlatmaktadır. Siber güvenlik önlemlerinin, etkili olay müdahale stratejilerinin ve siber suçlarla mücadelede uluslararası iş birliğinin öneminin altını çizmektedir. Kurumlar gelişen siber tehditlerle çatışmaya devam ederken, bu olaydan çıkarılan dersler, altyapıyı ve ulusal güvenliği korumak için gelecekteki siber güvenlik uygulamalarını ve politikalarını şekillendirecektir. Colonial Pipeline fidye yazılımı saldırısının sadece tekil bir olay olmadığı, giderek dijitalleşen bir dünyada siber güvenlik esnekliği ve altyapının korunmasına ilişkin daha geniş tartışmalara yol açacak bir hacker saldırısı olmuştur. Genel olarak, Colonial Pipeline siber saldırısı, siber risklerin azaltılmasında teknik kontrollerin, kurumsal hazırlığın ve iş birliğinin önemini vurgulayarak siber güvenliğe yönelik bütüncül bir yaklaşımın gerekliliğini ortaya koymuştur.

## SONUÇ VE ÖNERİLER

Kaseya ve Colonial Pipeline gibi son dönemde yaşanan fidye yazılımı saldırıları, siber güvenlik alanında daha kapsamlı ve etkin önlemlerin alınması gerekliliğini bir kez daha vurgulamaktadır. Bu saldırılar, kurumların siber tehditlere karşı daha iyi hazırlıklı olmaları, güvenlik açıklarını tespit etmek ve gidermek için sürekli olarak çaba sarf etmeleri gerektiğini göstermektedir. Siber güvenlik, artık sadece teknik önlemlerle sınırlı kalmamakta, aynı zamanda kurumsal yönetim, eğitim, olay müdahalesi ve uluslararası iş birliği gibi alanları da kapsamaktadır.

Çalışmada örnek vaka analizi ile iki farklı sektör üzerinden siber güvenlik politikalarının etkinliği değerlendirilmiştir. Benzerlik yöntemi kullanılarak, farklı kurumsal yapıların benzer tehditlere nasıl tepki verdiği incelenmiştir. Çalışmada, örnek vaka analizleri yoluyla, fidye yazılımı saldırılarının kurumsal güvenlik açıklarını nasıl hedef aldığı, farklı sektörlerde gerçekleşen saldırıların ortak noktaları ve farklılıkları, siber güvenlik politikalarının eksiklikleri ve kriz yönetimi süreçlerindeki hatalar, gelecekte benzer saldırılara karşı daha dirençli güvenlik stratejileri geliştirilmesi gerektiği temel bulgularına ulaşmıştır. Siber güvenlik stratejilerinin hem teknik hem de kurumsal boyutta ele alınması gerektiği aynı zamanda incelenen olaylar ekseninde siber güvenlik politikaları

geliştiren kurumlar, şirket yöneticileri ve politika yapıcılar için önemli dersler sunduğu söylenebilir.

Bu olaylardan çıkarılacak dersler, siber güvenlik stratejilerinin ve politikalarının daha da güçlendirilmesi gerektiğini göstermektedir. Teknik kontrollerin yanı sıra, kurumlar etkin bir olay müdahale stratejisi geliştirmeli, çalışanlarına düzenli eğitimler sağlamalı ve güvenlik bilincini artırmalıdır. Ayrıca, kurumların siber güvenlik birimleri en iyi uygulamaları paylaşarak birlikte çalışmalı ve karşılaşılan tehditlere daha hızlı ve etkili bir şekilde yanıt vermeyi sağlayacak ortak savunma birimleri oluşturmalıdır.

Kaseya ve Colonial Pipeline saldırıları, siber güvenlik alanında sürekli bir çabanın ve bütüncül bir yaklaşımın önemini vurgulamaktadır. Kurumlar, teknolojiyi kullanırken güvenliklerini en üst düzeyde tutmalı ve siber tehditlere karşı sürekli olarak tetikte olmalıdır. Ayrıca, uluslararası iş birliği ve bilgi paylaşımı, siber suçlarla mücadelede daha etkili bir strateji oluşturmak için önemlidir. Bu şekilde, gelecekteki hacker saldırılarına karşı daha iyi hazırlanabilir ve etkilerini en aza indirebileceklerdir. Dijital dünyada güvenliğin yalnızca bir teknik sorun olmadığını, aynı zamanda kurumsal kültür, sürekli eğitim ve uluslararası koordinasyon gerektiren çok boyutlu bir mücadelenin olduğunu göstermektedir. Kurumların, siber güvenlik stratejilerini sürekli gözden geçirip güncellemeleri, yeni tehditlere karşı esnek ve adaptif olmaları gerekmektedir. Bu, sadece mevcut sistemlerin korunması için değil, aynı zamanda inovasyon ve rekabet avantajını sürdürebilmek için de kritik olmaktadır.

Siber güvenlikte başarı, teknolojiye yapılan yatırımlarla birlikte insan faktörünün de göz ardı edilmemesiyle mümkündür. Çalışanların bilinçlendirilmesi, sürekli eğitim programları ve tatbikatlarla desteklenmeli, aynı zamanda kurum içi ve kurumlar arası iş birliği teşvik edilmelidir. Bu bütüncül yaklaşımlar hem bireysel hem de kurumsal düzeyde siber dayanıklılığı artırarak, gelecekteki siber tehditlerle daha etkili bir şekilde başa çıkılmasını sağlayacaktır.

## Kaynakça

Ada, M., & Çakır, H. (2017). Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 5*(2), 632-656.

Akdeniz, G. (2013). Hacker Etiği. A. R. Keleş, & Y. Sal içinde, *Hack Kültürü ve Hactivizm: Yeni Bir Siyaset Biçimi*. İstanbul: Alternatif Bilişim.

AL-Hawamleh, A. M. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science and Applications, 14*(2), 804.

Anckar, C. (2008). On the applicability of the most similar systems design. 395.

Ankara Üniversitesi Bilgi İşlem Daire Başkanlığı. (2018). *Siber Güvenlik Farkındalığı*. Ankara Üniversitesi: https://bid.ankara.edu.tr/2018/10/02/siber-guvenlik-farkindaligi/ adresinden alındı

Balyemez, O. (2022, Ocak 5). *2021'in öne çıkan fidye yazılım saldırıları*. Siberbülten: https://siberbulten.com/siber-saldirilar-2/2021in-one-cikan-fidye-yazilim-saldirilari/ adresinden alındı

Bennet, A. (2004). Case Study Methods: Design, Use, and Comparative Advantages. 19-55.

Colonial Pipeline. (tarih yok). *Our History*. Colonial Pipeline: https://www.colpipe.com/about-us/history/ adresinden alındı

Cyvatar. (2022). *Kaseya Ransomware Attack: Top MSPs affected, its impact & lessons learnt*. cyvatarai: https://cyvatar.ai/kaseya-ransomware-attacks/ adresinden alındı

Çavuş, M. (2018, Haziran 27). *Siber Saldırılara Karşı 7 Etkin Savunma*. Nisan 5, 2024 tarihinde btGünlüğü: https://www.btgunlugu.com/siber-saldirilar-a-karsi-7-etkin-savunma/ adresinden alındı

Çoban, S. (2020). Hackerlık Kavramı, Modeller ve Medyada Hackerlığın Sunumu. *11*(40), 45.

Demirkıran, P. (2013). Hacktivizim. A. R. Keleş, & Y. Sal içinde, *Hack Kültürü ve Hacktivizim*. İstanbul: Alternatif Bilişim Yayınları.

Elmas, E. (2023). Cybersecurıty and Rısk Assessment in Payment System in the Digital. 21. İstanbul: Marmara Üniversitesi, Fen Bilimleri Enstitüsü.

Ersanel, N. (2001). *Siber İstihbarat - Sanal ve Dijital Casusluğun Anatomisi*. Ankara: ASAM Yayınları.

GovTech. (2021). *Back to Basics: A Deeper Look at the Colonial Pipeline Hack*. Government Technology: https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack adresinden alındı

Güntay, V. (2019). 21. Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk. *Novus Orbis: Siyaset Bilimi Ve Uluslararası İlişkiler Dergisi, 1*(2), 87-109.

Harran, J. M. (2021). *Ataque masivo del ransomware REvil comprometió más de 1000 compañías en mundo*. welivesecurity.com: https://www.welivesecurity.com/la-es/2021/07/05/ataque-masivo-ransomware-revil-comprometio-mas-1000-companias-mundo/ adresinden alındı

Hıdıroğlu, B. (2023). İşletmelerin Dijitalleşme Sürecinde Siber Güvenlik: Sosyal Ağ Analizine Dayalı Hazır Bulunuşluk Ölçeğinin Geliştirilmesi. İzmir: Ege Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi.

Kaseya. (tarih yok). *Fred Voccola*. Kaseya: https://www.kaseya.com/company/fred-voccola/ adresinden alındı

Kaseya. (tarih yok). *Our story*. Kaseya: https://www.kaseya.com/careers/our-story/ adresinden alındı

Kaspersky. (tarih yok). *Siber Güvenlik Nedir?* Nisan 9, 2024 tarihinde Kaspersky: https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security adresinden alındı

Lijphart, A. (1971). Comparative politics and the comparative method. 685.

Maawi, M. H. (2021). *Computer Engineering and Computer Science and Control*. İstanbul: Altınbaş Üniversitesi Yüksek Lisans Tezi.

Merriam, S. B. (1988). *Case Study Research in Education: A Qualitative Approach*. Jossey-Bass.

Mobildev. (2021, Mayıs 25). *Fidye yazılım musibeti*. Mobildev: https://www.mobildev.com/blog/fidye-yazilim-musibeti adresinden alındı

Montini, H. (2021). *Colonial Pipeline Ransomware Attack: Why it Matters*. provendata: https://www.provendata.com/blog/colonial-pipeline-ransomware-attack/ adresinden alındı

Nacaroğlu, M. (2023). *Kurumlarda Siber Güvenlik Tabanlı Ziyaretçi Kontrol Sistemi Tasarımı ve Uygulaması*. İzmir: Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisan Tezi.

Olmos, F. G. (2021). *Cómo Kaseya recuperó la información tras el ciberataque de REvil*. Expansion: https://expansion.mx/tecnologia/2021/07/26/cronica-como-kaseya-recupero-la-informacion-tras-el-ciberataque-de-revil adresinden alındı

Özer, M. O. (2023). *Ulusal ve Uluslararası Güvenlik Politikaları Temelinde Dijitalleşme ve Siber Güvenlik: Hukuksal ve Yönetsel Bir Değerlendirme*. Hatay: Hatay Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi.

Öztürk, Ö. Ç. (2017). *Toplumsal Hareketler Bağlamında Hack ve Hacktivizm*. İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü Doktora Tezi.

Przeworski, A., & Teune, H. (1970). The logic of comparative social inquiry. 33-48. New York: Wiley.

Rockwell Automation. (2021). *Las lecciones del ciberataque a Colonial Pipeline*. Rockweller Automatin: https://www.rockwellautomation.com/es-mx/company/news/articles/lecciones-del-ciberataque-a-colonial-pipeline.html adresinden alındı

Russon, M.-A. (2021). *ABD'de siber saldırı: Bilgisayar korsanları ülkenin en büyük boru hattını devre dışı bıraktı, akaryakıt karayoluyla taşınacak*. BBC News Türkçe: https://www.bbc.com/turkce/haberler-dunya-57056048 adresinden alındı

Sade, G. (2021). *Tarihin en büyük' fidye yazılım saldırısında İsveç'te 800 market kepenk kapattı*. Euronews: https://tr.euronews.com/2021/07/04/tarihin-en-buyuk-fidye-yaz-l-m-sald-r-s-nda-isvec-te-800-market-kepenk-kapatt adresinden alındı

Securefors. (2021, Haziran 10). *Siber öldürme zincirinde en zayıf halka: İnsan*. Securefors: https://www.securefors.com/siber-oldurme-zincirinde-en-zayif-halka-insan adresinden alındı

TitanFile. (2021). *Cyber security tips & best practices*. Titanfile: https://www.titanfile.com/blog/cyber-security-tips-best-practices/ adresinden alındı

Turhost Blog. (tarih yok). *Sıfır gün açığı nedir?* Turhost: https://www.turhost.com/blog/sifir-gun-acigi-nedir/ adresinden alındı

Usta, O. (2021). *Tarihin en büyük fidye yazılım saldırısı Kaseya hakkında bilmeniz gereken 5 şey*. Siberbülten: https://siberbulten.com/dijital-guvenlik/tarihin-en-buyuk-fidye-yazilim-saldirisi-kaseya-hakkinda-bilmeniz-gereken-5-sey/ adresinden alındı

WaterISAC. (2016). *10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks*. Waterisac: https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_Oct2016%5B2%5D.pdf adresinden alındı

Yerlikaya, T., Buluş, E., & Buluş, N. (2007). Asimetrik Şifreleme Algoritmalarında Anahtar. *IX. Akademik Bilişim Konferansı Bildirileri*. Kütahya: Akademik Bilişim.

Yiğitbaşı, K. G., & Çelik, S. (2023). Dijital Dünyada Mahremiyet, Ebeveynlik ve Çocuklar: Afyonkarahisar Örneği. *TRT Akademi, 8*(19), 850.