YÖNETİM BİLİŞİM SİSTEMLERİ & SİBER GÜVENLİK

Editör
Recep BENZER

ISBN
978-625-8399-33-2

Kitap Adı
Yönetim Bilişim Sistemleri & Siber Güvenlik

Editör
Recep BENZER
ORCID iD: 0000-0002-5339-0554

Yayın Koordinatörü
Yasin DİLMEN

Sayfa ve Kapak Tasarımı
Akademisyen Dizgi Ünitesi

Yayıncı Sertifika No
47518

Baskı ve Cilt
Vadi Matbaatbacılık

Bisac Code
COM088000

DOI
10.37609/akya.1249

GENEL DAĞITIM

Akademisyen Kitabevi A. Ş.

Halk Sokak 5 / A
Yenişehir / Ankara
Tel: 0312 431 16 33
siparis@akademisyen.com

www.akademisyen.com

ÖNSÖZ

Yönetim Bilişim Sistemi, insan ve bilgisayardan oluşan, bilgilerin toplanması, iletilmesi, saklanması ve işlenmesinde kullanılabilen bir sistemdir. Yönetim Bilişim Sistemi, bilgisayar donanımı, yazılımı, yapay zekâ, karar modeli ve veri tabanını kullanan, organizasyonun işleyişi, yönetimi ve karar vermesi için bilgi desteği sağlayan bir insan-makine sistemidir.

Siber Güvenlik, yazılımlara, bilgisayarlara ve ağlara yönelik kötü niyetli saldırı riskini azaltmayı içerir. Siber Güvenlik, izinsiz girişleri tespit etmek, virüsleri durdurmak, kötü niyetli erişimi engellemek, kimlik doğrulamasını zorlamak, şifreli iletişimleri etkinleştirmek ve devam etmek için kullanılan araçları içerir.

Yönetim Bilişim Sistemleri & Siber Güvenlik, yönetim bilişim sistemleri ve siber güvenlik alanındaki araştırmacılar için yazılmıştır. Yönetim Bilişim Sistemleri & Siber Güvenlik kitabı ile ele alınan bölümlerde, mevcut ve bilimsel tartışmayı teşvik etmenin yanı sıra yönetim bilişim sistemleri ile siber güvenlik alanlarındaki uzmanlar arasında fikir ve deneyim alışverişi için bir forum sağlamaktır.

Yönetim Bilişim Sistemleri & Siber Güvenlik, önemli konuların kapsamlı bir şekilde kapsanmasını sağlayan sekiz (8) ayrı bölüm halinde düzenlenmiştir. (1) Güvenlik Orkestrasyon, Otomasyon ve Olaylara Müdahale (SOAR), (2) İlköğretim Müfredatında Siber Güvenlik Konularının İncelenmesi, (3) Tallinn Manual 2.0 (Tallinn Kılavuzu) ile Siber Savaşta Uygulanacak Uluslararası Hukuk Kurallarına Genel Bakış, (4) Siber Saldırılardan Yeni Nesil Korunma Teknikleri, (5) Sızma Testi ve Uygulama, (6) Web Uygulamalarına Yapılan Ataklar ve Uygulama, (7) Bilişim Terörü ve Bilişim Suçları, (8) Yapay Zekâ Yöntemi ile Reaktif Güç Kompanzasyonu Tekniği.

Kitabımızın ortaya çıkmasında sabır ve fedakârlık gösteren ailelerimize, desteklerinden dolayı öğrencilerimize ve Akademisyen yayınevi personeline teşekkür eder, eserin akademisyenlere, eğitimcilere, öğrencilere ve konuya ilgi duyan herkese faydalı olmasını dilerim.

Doç.Dr. Recep BENZER

İÇİNDEKİLER

YAZARLAR

Tezsiz YL Öğrencisi, Mehmet Alptunga GÖNÜLLÜ
Gazi Üniversitesi, Adli Bilişim, Ankara, Türkiye,
ORCID iD: 0000-0001-7472-9898

Doç. Dr. Recep BENZER
Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim, Ankara, Türkiye
ORCID iD: 0000-0002-5339-0554

Prof. Dr. Aslıhan TÜFEKÇİ
Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim, Ankara, Türkiye
ORCID iD: 0000-0002-8669-276X

Tezsiz YL Öğrencisi Dilara GELEN
Ahmet Yesevi Üniversitesi, Siber Güvenlik, Ankara, Türkiye
ORCID iD: 000-0003-0488-3077

Tezsiz YL Öğrencisi Haluk ÇATAL
Milli Savunma Üniversitesi, Havacılık ve Uzay Teknolojileri Enstitüsü, Bilgisayar Mühendisliği, İstanbul, Türkiye
ORCID iD: 0000-0003-3369-681X

YL Öğrencisi Kemal KARAÇUHA
İstanbul Teknik Üniversitesi, Bilişim Enstiüsü, İstanbul, Türkiye
ORCID iD: 0000-0001-9641-7035

Dr. Öğr. Üyesi Nafiz ÜNLÜ
İstanbul Teknik Üniversitesi, Bilişim Enstiüsü, İstanbul, Türkiye
ORCID iD: 0000-0002-2094-8080

Tezsiz YL Öğrencisi Ahmet SOLAK
Ahmet Yesevi Üniversitesi, Siber Güvenlik, Ankara, Türkiye
ORCID iD: 0000-0003-1543-9721

Tezsiz YL Öğrencisi Eser SOLMAZ
Ahmet Yesevi Üniversitesi, Siber Güvenlik, Ankara, Türkiye
ORCID iD: 0000-0003-4865-1219

Tezsiz YL Öğrencisi Elif DEMİRLİ
Gazi Üniversitesi Adli Bilişim, Ankara, Türkiye
ORCID iD: 0000-0002-0414-6037

BÖLÜM 1

GÜVENLİK ORKESTRASYON, OTOMASYON VE OLAYLARA MÜDAHALE (SOAR)

Mehmet Alptunga GÖNÜLLÜ[1]
Recep BENZER[2]
Aslıhan TÜFEKÇİ[3]

1. GİRİŞ

Bilişim teknolojilerinde son yıllarda çok büyük gelişmeler yaşanmıştır. Bu gelişmelerin getirdiği rahatlıklar ve faydalar, bilgi paylaşımı ve iletişim kanallarının çeşitliliğinin artmasına, ticaret, finans ve kamu hizmetlerinin sanal ortama taşınmasına olanak sağlamıştır (Kırışık ve Sezer, 2015). Ülkeler için kritik seviyede öneme sahip olan ve çeşitli sektörler artık bilgi sistem otomasyonları ile yönetilmektedir. Bilişim teknolojisinin ilerlemesine paralel olarak bilişim alanındaki bu gelişmelere ve yeniliklere yönelik tehdit, zafiyet ve riskler de artmaktadır. Teknolojideki gelişmeler ekonomik büyümenin temel etmeni olmakla birlikte, aynı zamanda siber saldırıların daha çok görülmesine yol açmıştır. Bu yüzden siber güvenlik denilen kavram son yıllarda en fazla tartışılan konulardan birisi haline gelmiştir. Siber güvenlik; bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma olarak tanımlanabilir. Dünya çapında her kurum, kuruluş topluluk kendi siber güvenliğini bir şekilde sağlamayı amaçlar. Siber güvenliğin sağlanması için çeşitli araçlar ve yapılar mevcuttur (Kiiveri, 2021). Bu araçlardan birisi de SOAR (Security Orchestration Automation and Response – Güvenlik Orkestrasyon, Otomasyon ve Olaylara Müdahale) adı verilen bir otomasyon yazılımıdır.

1.1. Problem Durumu / Konunun Tanımı

SOAR, Güvenlik Orkestrasyon, Otomasyon ve Olaylara Müdahale anlamına gelmektedir. Bu terim, üç yazılım özelliğini tanımlamak için kullanılır. Tehdit ve Güvenlik Açığı Yönetimi, Güvenlik Olayına Müdahale ve Güvenlik İşlemleri Oto-

[1] Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim, Tezsiz Y. Lisans Dönem Projesi çalışmasıdır. Tezsiz YL Öğrencisi, Gazi Üniversitesi, Adli Bilişim, Ankara, Türkiye, alptungagonullu@gmail.com
[2] Doç.Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim, Ankara, Türkiye, rbenzer@gazi.edu.tr
[3] Prof. Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Yönetim Bilişim Sistemleri, Ankara, Türkiye, asli@gazi.edu.tr

gelişen ve karmaşık siber tehditler nedeniyle, SIEM ortamları, SGOM analistlerine ağır iş yükleri ve yorgunluk yüklemektedir.

SGOM analistlerinin yüklerini azaltmak ve yorgunluk derecelerini düşürmek adına ayrıca güvenlik otomasyonu sağlamak adına SOAR sistemleri ortaya çıkmıştır. SOAR sistemleri, siber tehdit algılama, azaltma ve SGOM analistlerini güçlendirmek üzere tasarlanmıştır. SOAR, güvenlik personelinin iş yükünü azaltır, böylece rutin görevlere harcanan saat miktarı, bunun yerine kuruluşun mevcut güvenlik ortamının değerlendirilmesi ve iyileştirilmesi gibi daha üretken görevlerde kullanılabilir. Bu çalışmada, SOAR güvenlik otomasyonu yöntemleri ve çeşitli kullanım durumları ve faydaları hakkında temel düzeyde bir anlayış sunulmuştur. Siber güvenlik otomasyonu, SOAR platformlarının kullanımı, çeşitli tehditlere doğru ve etkili yanıtlar vererek, düzenleme ve otomasyon ile güvenlik tehditlerine tutarlı yanıtlar sağlamaktadır.

Kurumlar, Devletler ve birçok özel kuruluş Siber dünyada güvenliklerini sağlamak için log yönetimi gibi ilkel teknolojiler kullanmaktadır. Bazıları ise bu logları toplayarak SIEM'e entegre eder ve güvenliklerini SIEM'lerden takip eder ve güvenlik ürünlerinden olaylara aksiyon alır. SOAR ise bunların tamamını tek başına yapabilir. Olayları loğlar, izler ve aksiyon alır. Günümüzde kurum ve kuruluşlar hala SOAR'a geçmeyi başaramamış olsalar da yakın gelecekte tüm Siber Güvenlik olaylarına SOAR ile aksiyon alacaklar ve bu nedenle SOAR kullanmaya başlayacaklar.

KAYNAKLAR

Acartürk, C., Ulubay, M., & Erdur, E. (2021). Continuous improvement on maturity and capability of Security Operation Centres. *IET Information Security*. 2020, 1-17.

Brewer, R. (2019). Could SOAR save skills-short SOCs?. Computer Fraud & Security, 2019(10), 8-11.

Dorigo, S. (2012). *Security information and event management*. Radboud University, Nijmegen.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (siem): Analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14), 4759.

Hekim, H. & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikalari. *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2), 135-158.

İnternet: Abhishek, I. (2019). Introducing Demisto v5.0: SOAR Just Got Better URL: https://www.paloaltonetworks.com/blog/2019/10/cortex-demisto-v5-soar/

İnternet: BGA Security (2018). SOME ve SOC Ekipleri için Açık Kaynak Çözümler URL: https://www.bgasecurity.com/makale/some-ve-soc-ekipleri-icin-acik-kaynak-cozumler/

İnternet: Choudhury, S. (2021). Log4j Vulnerability Explanation In Details URL: https://infosecwriteups.com/log4j-vulnerability-explanation-in-details-73f7556c5ff1

İnternet: Cook, A. (2021). Recon›s Soar Playbook To Detect Log4j Exploitatıon. URL: https://blog.reconinfosec.com/recons-soar-playbook-to-detect-the-log4j-exploit/

İnternet: Demirel, F. (2017). Yerli siber güvenlik girişimi ATAR Labs, Diffusion Capital Partners yatırımıyla dünyaya açılacak URL: https://webrazzi.com/2017/09/25/atar-yatirim/

İnternet: Dilay Merve Özdemir, (2021). SOAR Çözümleri Bölüm-1. URL: https://www.mshowto.org/acik-kaynak-soar-cozumleri-bolum-1.html

İnternet: EM360 Tech (2020). Top 10 SOAR Companies to Watch in 2021 URL: https://em360tech.com/top-10/top-10-soar-companies-watch-2021

İnternet: Engelbrecht, S. (2018). The Evolution of SOAR Platforms URL: https://www.securityweek.com/evolution-soar-platforms

İnternet: Gartner (2020) URL: Security Information and Event Management (SIEM) Reviews and Ratings, https://www.gartner.com/reviews/market/security-information-event-management

İnternet: Kaspersky (2021). Sıfır Gün Saldırısı nedir? URL: https://www.kaspersky.com.tr/resource-center/definitions/zero-day-exploit

İnternet: Kirtley, E. (2020). What is SOAR vs SIEM: Security Solutions Explained URL: https://swimlane.com/blog/siem-soar/

İnternet: Lostar (2021). Kritik Log4J Zafiyeti. URL: https://lostar.com.tr/2021/12/kritik-log4j-zafiyeti.html

İnternet: N-able (2020). Top SIEM Benefits URL: https://www.solarwindsmsp.com/blog/top-siem-benefits

İnternet: NetSmart, (2020). SIEM vs SOAR. URL: https://www.netsmart.com.tr/2020/09/02/siem-vs-soar/

İnternet: Olgun, Y. (2020). SIEM, EDR ve SOAR ürünleri ile bir APT tespiti nasıl yapılabilir? URL: https://muhammedyusufolgun.blogspot.com/p/siem-edr-ve-soar-urunleri-ile-bir-apt.html

İnternet: Pazoğlu, E. (2020). SOAR B.2: Kavramlar ve Bileşenler. URL: https://evrenbey.medium.com/soar-b-2-kavramlar-ve-bile%C5%9Fenler-85c60b5feb1a

İnternet: Sumo Logic. (2021). The difference between siem and soar why do i need-soar-if-i-have-siem URL: https://www.dflabs.com/resources/blog/the-difference-between-siem-and-soar-why-do-i-need-soar-if-i-have-siem/

İnternet: Yüzük, E. (2019). SOAR (Security Orchestration Automation and Responce) Nedir? URL: https://www.ercanyuzuk.com/2019/11/soar-security-orchestration-automation.html

Kiiveri, K. (2021). *Automation in cyber security*. Yüksek Lisans Tezi. Turku University of Applied Sciences.

Kinyua, J. & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intell. Autom. Soft Comput*. 28(2), 527-545.

Kırışık, F., & Sezer, Ö. (2015). Bilgi ve İletişim Teknolojilerinin Kamu Politikası Oluşturma Sürecindeki Rolü. *Ekonomik ve Sosyal Araştırmalar Dergisi*, 11(2), 199-215.

Morozov, V. & Miloslavskaya, N. (2020). Technical to Psychological Aspects Ratio in the Specialized Information Security Training Content. *Procedia Computer Science*, 169, 90-95.

Purujoki, J. (2020). *SOAR Playbook Implementation-Incident Deduplication and Its Effects*. Yüksek Lisans Tezi. JAMK University of Applied Sciences.

Singh, K. (2020). *Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 Computer Lab* (Doctoral dissertation, Marquette University).

BÖLÜM 2

İLKÖĞRETİM MÜFREDATINDA SİBER GÜVENLİK KONULARININ İNCELENMESİ[1]

Dilara GELEN[2]
Recep BENZER[3]

1. GİRİŞ

İnternet ve bilgisayar teknolojileri ile tanışmamızın üzerinden yarım asır bile geçmemiş olmasına rağmen, bu teknolojileri sahiplenme hızımız büyük bir ivme ile her geçen yıl artış göstermektedir. Türkiye İstatistik Kurumunun 2021 yılında yayınladığı rapora göre Türkiye' de 2021 yılında internete erişim hane oranı %92, İnternet kullanım oranı 16-74 yaş grubundaki bireylerde %82,6 olmuştur (TUİK, 2021). 2011 yılı kullanım oranı %42,9 iken sadece 10 yılda %92 oranına ulaşarak, neredeyse tüm toplumumuzun hayatına etki etmeye başlayan popüler teknoloji internet, sağladığı birçok olanağın yanı sıra çeşitli güvenlik sorunlarını da beraberinde getirmiştir. Zararlı yazılımlar, kimlik hırsızlığı, istenmeyen mesajlar (spam), korsanlık faaliyetleri (hacking), oltalama (phishing), siber zorbalık, istismar, terör ve gizlilik ihlalleri gibi tehditler bu çevrimiçi risklerden yalnızca bazılarıdır.

Araştırmalar çevrimiçi risklerle karşılaşma oranlarının internet kullanımlarının paralelinde yükseldiğini göstermektedir (Livingstone, Haddon, Görzig ve Olafsson, 2011). Nesnelerin Internet'i (Internet of Things, – IoT) kavramı ile internete bağlanan cihaz sayısının çok daha artması, bu cihazların insanların hayatına daha fazla dâhil olmasıyla çevrimiçi risklerle karşılaşma oranımız her geçen gün daha fazla artmaktadır. Bunun yanında, gerekli e-okuryazarlıkları henüz sağlayamamış teknoloji kullanıcılarının bu karşılaşmalardan zarar görme olasılıklarının daha yüksek olduğu ortadadır.

Akamai güvenlik şirketinin hazırladığı rapora göre (Temmuz 2020); ülkemiz, web uygulamaları saldırılarında 105874601 saldırı ile küresel sıralamada 21. sırada yer almaktadır. Bu durum internet ortamında, siber suçlarla karşılaşma olasılığımızın yüksek olduğunu ve bilinçli teknoloji okuryazarlığının önemini ortaya

[1] Ahmet Yesevi Üniversitesi, Siber Güvenlik YL Dönem Projesi çalışmasıdır.

[2] Tezsiz YL Öğrencisi, Ahmet Yesevi Üniversitesi, Siber Güvenlik, Ankara, Türkiye, dilaragelen35@gmail.com

[3] Doç.Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim, Ankara, Türkiye, rbenzer@gazi.edu.tr

hurbaşkanlığı Dijital Dönüşüm Ofisi tarafından 2020 yılından itibaren Siber Zekâ Bilgi Yarışması düzenlenmektedir. 2021 Ekim ayında ikincisi düzenlenen yarışmaya; 1 milyonun üzerinde öğrenci katılmıştır. Sorularının kademelere göre değişiklik gösterdiği yarışmada, ilkokul öğrencileri için 25 soru, ortaokul öğrencileri için 40 soru, lise öğrencilerini ise 50 soru yer almaktadır. En çok doğru cevabı en kısa sürede verip dereceye giren öğrenciler, sürpriz hediyeler kazanabilmektedir. Siber vatanımızın güvenliğini gelecekte emanet edeceğimiz çocuklarımıza, siber güvenliğin önemine dair farkındalık oluşturmak için hazırlanan bu yarışmalar, ülkemizdeki Siber Güvenlik eğitimleri için çok önemli ve dikkate değerdir. Öğrencilerin motivasyonlarını arttırıp, dikkatlerini çeken bu tarz yarışma, organizasyon ve fuarların arttırılmasının, çocuklarımızın siber bilgi, kapasite ve becerilerini arttırılacağı düşünülmektedir.

Eğitim sadece "bilme (düşünce)" için değil, "hissetme (duygu)" ve "yapma (eylem)" için de verilir; dolayısıyla bu ders için sadece bilişsel ölçümler yeterli kabul edilmemelidir. Öğrencide bilişim etiği, sorumlu teknoloji kullanımı kazanımlarını güçlendirmek için; " bireysel ve grup aktivite davranışı, bilgi teknolojilerine yönelik iyi tutum, coşku ve okul ortamında görgü kuralları " gibi kriterlerin değerlendirilmesinin olumlu olacağı düşünülmektedir.

KAYNAKLAR

Barut, E., Kuzu, A. (2017). Türkiye ve İngiltere Bilişim Teknolojileri Öğretim Programlarının Amaç, Kazanım, Etkinlik, Ölçme ve Değerlendirme Süreçleri Açısından Karşılaştırılması. *Trakya Üniversitesi Eğitim Fakültesi Dergisi*, 7, (2), 721-745

Daggett, W. R. (2010). Preparing students for their technological future. International Center for Leadership in Education, 1-14

Göksu, M. (2020). 5. Sınıf geometri öğretiminde eba destekli matematik eğitiminin öğrenci başarısına ve görüşlerine etkisi (Yayınlanmamış yüksek lisans tezi). Giresun Üniversitesi Fen bilimleri Enstitüsü, Giresun.

İnternet: Bilişim Teknolojileri Eğitimcileri Derneği [BTE]. (2013). Türkiye'de İlk ve Ortaokullarda (İlköğretim) Okutulan Bilişim Teknolojileri Derslerinin Tarihi. Web: https://bte.org.tr/wp-content/uploads/2020/12/btderslerinin_tarihi_ilk-ortaokul_ilkogretim.pdf 10 Ekim 2021 tarihinde alınmıştır.

İnternet: Çin Eğitim Sistemi – Doç.Dr. İsmail Gelen (2016) https://avys.omu.edu.tr/storage/app/public/ismailgelen/57388/-%C3%87in%20Egitim%20Sistemi%20IG.pdf 5 Aralık 2021 tarihinde alınmıştır.

İnternet: Department for Education. (2014a). The national curriculum in England Framework document. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/381344/Master_final_national_curriculum_28_Nov.pdf adresinden 30 Ekim 2021 tarihinde alınmıştır.

İnternet: Department for Education. (2014b). Assessment Principles. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/304602/Assessment_Principles.pdf adresinden 30 Ekim 2021 tarihinde alınmıştır.

İnternet: Milli Eğitim Bakanlığı (2012). Fatih Projesi Çalıştay Raporu. https://yegitek.meb.gov.tr/www/egitim-teknolojileri-gelistirme-ve-projeler-daire-baskanliginda-yapilan-arastirmalar/icerik/3035 19 Aralık tarihinde alınmıştır.

İnternet: Milli Eğitim Bakanlığı (2018a). Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (İlkokul 1, 2, 3 ve 4. Sınıflar). https://mufredat.meb.gov.tr/Dosyalar/2018813171732131-4-2018-91%20Bili%C5%9Fim%20Teknolojileri%20ve%20Yaz%C4%B1l%C4%B1m%20(1-4.%20S%C4%B1n%C4%B1flar).pdf adresinden 30 Ekim 2021 tarihinde alınmıştır.

İnternet: Milli Eğitim Bakanlığı (2018b). Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (Ortaokul 5 ve 6. Sınıflar) https://mufredat.meb.gov.tr/Dosyalar/2018124103559587-Bili%C5%9Fim%20Teknolojileri%20ve%20Yaz%C4%B1l%C4%B1m%205-6.%20S%C4%B1n%C4%B1flar.pdf adresinden 30 Ekim 2021 tarihinde alınmıştır.

İnternet: Milli Eğitim Bakanlığı (2018c). Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (Ortaokul ve İmam Hatip Ortaokulu 7 ve 8. Sınıflar) https://mufredat.meb.gov.tr/Dosyalar/2018813171426130-2-201881Bili%C5%9Fim%20Teknolojileri%20ve%20Yaz%C4%B1l%C4%B1m%20Dersi%20(7%20ve%208.%20S%C4%B1n%C4%B1flar).pdf adresinden 30 Ekim 2021 tarihinde alınmıştır.

İnternet: National Center for Education Statistics [NCES]. (2018d). Uluslararası Bilgisayar Ve Bilgi Okuryazarlığı Çalışması (ICILS),2018 https://nces.ed.gov/surveys/icils/icils2018/theme1.asp 31 Ekim 2021 tarihinde alınmıştır.

İnternet: T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). Ulusal Siber Güvenlik Stratejisi 2020-2023. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf 6 Aralık tarihinde alınmıştır.

İnternet: Tayland Akademik İşler ve Eğitim Standartları Ofisi (The Basic Education Core Curriculum B.E. 2551 A.D. (2008). Temel Eğitim Çekirdek Müfredatı 2008) http://academic.obec.go.th/images/document/1525235513_d_1.pdf adresinden 27 Kasım 2021 tarihinde alınmıştır.

İnternet: Türkiye İstatistik Kurumu Veri Portalı [TUİK]. (2021). Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2021. https://data.tuik.gov.tr/Bulten/Index?p=Survey-on-Information-and-Communication-Technology-(ICT)-Usage-in-Households-and-by-Individuals-2021-37437#:~:text=%C4%B0nternete%20eri%C5%9Fim%20imkan%C4%B1%20olan%20hane%20oran%C4%B1%20%92%2C0%20oldu&text=Bu%20oran%20ge%C3%A7en%20y%C4%B1l%20%90,Konya%2C%20Karaman)%20b%C3%B6lgesi%20izledi. 10 Ekim 2021 tarihinde alınmıştır.

Livingstone, S., Haddon, L., Görzig, A. ve Olafsson, K. (2011). EU Kids Online Final Report. London: EU Kids Online: LSE.

Özbek, Y. (2019). Öğretmen Adaylarının Siber Güvenlik Farkındalıklarının İncelenmesi, Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi, Konya.

Özkan, Ö. (2004). Veri güvenliğinde saldırı ve savunma yöntemleri, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, Isparta.

Özseven T. (2012). Bilgisayar Ağları, Murathan Yayınevi, ss. 227-259

Şenol, M. (2017). Türkiye'de siber saldırılara karşı caydırıcılık. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 3(2), S:1-9

Topuz, A. C. (2010). Bilgisayar öğretmenlerinin meslek hayatında karşılaştıkları sorunlara yönelik nitel bir araştırma. Yayınlanmamış yüksek lisans tezi, Marmara Üniversitesi, İstanbul.

Yeşiltepe, G. M., & Erdoğan, M. (2013). İlköğretim bilişim teknolojileri öğretmenlerinin mesleğe yönelik sorunları, bu sorunların nedenleri ve çözüm önerileri. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi*, 33(3), 495-590.

BÖLÜM 3

TALLINN MANUAL 2.0 (TALLINN KILAVUZU) ile SİBER SAVAŞTA UYGULANACAK ULUSLARARASI HUKUK KURALLARINA GENEL BAKIŞ

Haluk ÇATAL[1]

1. GİRİŞ

Gelişen teknoloji ile Siber Uzayın savaş ve üstünlük kurma aracı haline gelmesine ragmen uluslararası hukukta siber saldırıların bir takım hak ve yükümlülükler bağlamında nasıl düzenleneceği, bazı istisnalar haricinde BM şartnamesiyle yasaklanmasına rağmen egemen devletin diğeri ülkelerin bütünlüğüne ve siyasi bağımsızlığına karşı kuvvet kullanmaması, klasik kuvvet kullanma ile aynı sonuçları doğurabilecek siber savaşların, yöntem ve sonuçları açısından uluslararası hukukun nasıl işletileceği belirsizliğini korumaktadır.

Mevcut durumda uluslararası düzeyde, Avrupa Konseyi Siber Suçlar Sözleşmesi, bir kısım NATO düzenlemeleri ve Shanghai İş Birliği Örgütü çalışmaları dışında mutabakat sağlanmış uluslararası bir mekanizma olmadığından ülkeler kendi iç hukuklarında siber suç ve suçlularla mücadele kapsamında bir kısım düzenlemeler oluşturmuş, taraf oldukları birlik ve örgütlerin normları dahilinde dar kapsamlı düzenlemeleri benimsemişlerdir. Ancak bu çabaların muhtemel bir siber savaşın yaratacağı yıkıcı etkileri önlemekte yetersiz kalacağı aşikadrdır.

Çalışmanın ilk bölümünde Siber Güvenlik, Siber Savaş ve Huhuki boyutuna değinilerek, savaşta ve barista siber alanın kullanıldığı örnekler verilmiş, siber savaşın hukuki boyutu değerlendirilmiştir. İkinci bölümde Tallin Manual ve tarihsel gelişim sürecine yer verilerek Tallinn Manual 2.0 kılavzuna genel bir bakış yapılarak uluslararası normlar çerçevesinde oluşturulan kurallar incelenmiştir. Çalışmanın son bölümünde sonuç ve değerlendirmelere yer verilmiştir.

2. SİBER GÜVENLİK / SİBER SAVAŞ VE HUKUKİ BOYUTU

Güvenlik kavramı, içinde bulunduğumuz çağın gerçekliklerine göre konumlanarak anlam kazanmış, gelişim ve değişimle birlikte dönüşüme uğramıştır. Teknoloji

[1] Tezsiz YL Öğrencisi, Milli Savunma Üniversitesi, Havacılık ve Uzay Teknolojileri Enstitüsü, Bilgisayar Mühendisliği, İstanbul, Türkiye, catal.haluk@gmail.com

Kılavuz ayrıca tıbbi koşullarımızdan cinsel tercihlerimize ve genetik yapımıza kadar en mahrem ayrıntıların dijitalleştirildiğini ve bu bilgilerin geniş veri tabanlarında mevcut olduğunu, bu varlıklarında yasalarla korunması gerektiğini belirtmektedir.

6. SONUÇ VE DEĞERLENDİRME

Tallinn 2.0, önümüzdeki birkaç yıl ve belki de daha uzun bir süre için tartışmanın başlangıç noktası olacak. Kapsamlı yapısı, bilgiye dayalı analiz ve sonuçları ile hem devlet hem de uzman yorumlarının dahil edilmesi, kılavuzu siber operasyonların uluslararası hukuk üzerine geliştirdiği bir tartışma için en değerli referans ve başlangıç noktası yapmaktadır.

Tallinn Kılavuzlarını yazan Uzmanlar arasında bile hala birçok anlaşmazlık ve netlik eksikliği bulunmaktadır. Devletlerin siber operasyonlar konusunda kamuoyu önünde konuşmadığı veya hareket etmediği birçok durum da mevcuttur. Siber operasyonlar, hukukun hala büyüyen bir alanıdır ve mevcut sorunlara yeni yaklaşımlar yaratmak için iç görü ve anlayışa büyük ihtiyaç duyulmaktadır. Ancak, bu aşamada devletler tutumlarını netleştirene kadar, Tallinn 2.0 siber operasyonlar yasasında ilerlemek için bir başlangıç noktası olarak hizmet edecektir.

KAYNAKLAR

Şenol, M. (2018). Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık, Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık, 2018, 181-214.

Meyers, A. (2022). Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units, Crowdstrike Blog, (https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/), [Erişim tarihi 07 Ocak 2022].

Bakır, E. (2011). İnternet Güvenliğinin Tarihçesi, *TUBİTAK Bilgem Dergisi,* 16. Sayısı, 2011.

Clarke, A.R., & Knarke, R. K. (2011). Siber Savaş (Cyber War) (Çeviren:Murat Erduran), İstanbul Kültür Üniversitesi, 2011.

Yayla, M. (2013). Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma, *TBB Dergisi*, 2013 (107).

Thomas R. (2012). Cyber War will not Take Place in, Strategic Studies, V.35, I.1, 2012, s.5-32; Ryan Singel, "White House Cyber Czar: There is no Cyber War", Wired, http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ erişim tarihi 09.01.2022

Birleşmiş Milletler Antlaşması (1945). 4801 Sayılı Onay Kanunu 24 Ağustos 1945 gün ve 6902 Sayılı Resmi Gazete.

Güreşçi, R. (2019). Siber Saldırıların Uluslararası Hukuktaki Güç Kullanımı Kapsamında Değerlendirmesi, *Savunma Bilimleri Dergisi The Journal of Defense Sciences* Mayıs/May 2019, Cilt/Volume 18, Sayı/Issue 1.

Çaycı, S. (1995). Silahlı Kuvvetlerin Kullanılması, Genelkurmay Basımevi, Ankara,1995, s.38.

Tikk E. & Kaska K. Legal Cooperation to Investigate Cyber Incidents Estonian Case Study and_Lessons, CCDCOE, 2010

Schmitt. M.N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

BÖLÜM 4

SİBER SALDIRILARDAN YENİ NESİL KORUNMA TEKNİKLERİ

Kemal KARAÇUHA[1]
Nafiz ÜNLÜ[2]

1. GİRİŞ

Son yıllarda insanlar internet teknolojisine giderek daha fazla bağımlı hale gelmektedir. Bilgisayarlar dünyanın bir çok yerinde insan yaşamının var olduğu her yerde hayatın her yönüne etki ederek insanları ve insanların kullandığı cihazları birbirine bağlamaktadır. Finans ve kamu kuruluşlarında, eğitim sektöründe, endüstriyel alanlarda, bireysel kullanımda ve diğer tüm alanlarda tüm işlemler internet altyapısına dönüştürülmüş ve hayatın tümü internete entegre olarak sürdürülmektedir. Yaşamı kolaylaştıran ve daha verimli kılan bu teknoloji, aynı zamanda çok büyük güvenlik açıklarına ve tehditlere yol açtığından dolayı, aynı zamanda güvenlik için büyük bir endişe kaynağı olmuştur.

Özellikle geçmiş son 25 yıl göz önünde bulundurulduğunda değişen teknoloji ve kullanılan sistemlerin değişmesi, internet altyapısı ve ağa bağlı cihazların teknolojilerinin değişmesi ile yeni saldırı yöntemleri geliştirilmiş ve evrimleşmiştir. Korsan diye tabir ettiğimiz bu sistemlerin açıklarını arayarak, sistemlere zarar veren, bilgi hırsızlığı yapan saldırganlar, nesiller ve teknolojiler geliştikçe yeni yöntemler keşfetmektedir. Bu keşiflerle beraber dijital dünyada siber güvenliğin sağlanması, bu saldırıların etki alanları hakkında bilgi sahibi olmak oldukça önemlidir.

Siber saldırı kavramı, bir şahıs tarafından veya bir topluluk tarafından yine bir başka şahıs veya topluluğa karşı bilgi sisteminin ihlaliyle sonuçlanan kötü niyetli bir girişimdir.

Günümüzde gerçekleştirilen ve günümüz teknolojisine uyarlanmış siber saldırıların gelişme süreci, teknolojinin gelişiminden daha hızlıdır. Saldırıların seviyesinin yükselmesinin, gelişen teknolojinin güvenlik altyapılarından daha ileride gitmesinin sebebi basit bir mantıkla açıklanabilmektedir; Saldırganlara karşı bir

[1] YL Öğrencisi, İstanbul Teknik Üniversitesi, Bilişim Enstiüsü, İstanbul, Türkiye, karacuha19@itu.edu.tr
[2] Dr.Öğrt.Üyesi, İstanbul Teknik Üniversitesi, Bilişim Enstiüsü, İstanbul, Türkiye, unluna@itu.edu.tr

5. SONUÇ

Son 30 yılda, bilgisayar ve teknolojinin hayatımıza girmesiyle beraber insanlar için vazgeçilmez olan siber teknoloji hayatımızı kolaylaştırdığı kadar da tehlike arz etmektedir. Bu gelişme ile siber tehditler ve bu tehditlerin evrimsel sürecini inceledik. Bu zamana kadar yaşanan siber saldırı olaylarını ve ağırlıklı olarak dönemsel zayıflıkları incelediğimiz bu makalede görüyoruz ki, günün şartlarına uygun, zamanın teknolojisine ayak uyduracak saldırılar düzenlenmekte ve gün geçtikçe saldırıların boyutu ve kapsamı korkunç boyutlara ulaşmaktadır. İçinde bulunduğumuz 2017 sonrası dönemde yapılan birkaç kitlesel spesifik saldırı bile bizlere o kadar koruma çözümü olmasına rağmen bir saldırının bu kadar büyük kitlelere ulaşabileceğini göstermiştir. Bir önceki dönemlere kıyasla hareket ettiğimizde bu saldırılara karşı çözümlerimiz evrimleşmiş ve teknolojiyi daha iyi kullanarak sonuç odaklı çözümlere yoğunlaşmaktayız. Genel bağlamda bakacak olursak kullanıcının, sistemin en büyük zafiyeti olduğunu söylememiz yanlış olmayacaktır. Bu konuda alınabilecek en büyük önlem toplumda bilinç sağlamak ve koruma mekanizmaları ne kadar gelişirse gelişsin, geçmişte ve gelecek dönemde de sosyal mühendislik ile saldırı kavramı her zaman karşımıza çıkacaktır.

KAYNAKLAR

Checkpoint (2018). security report. 2018. Available Online: https://www.checkpoint. c o m / downloads/product – related/report/2018 – security-report.pdf.

Checkpoint (2022). Check Point History. https://www.checkpoint.com/about-us/check-point-history/

Checkpoint (2022). Stepping Up to Gen V (5th Generation) of Cyber Security. https://www.checkpoint.com/downloads/product-related/brochure/gen_v_brochure-.pdf

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, Symantec Corp., Security Response, 5(6), 29.

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. Wired, August, 22.

Hern, A., Gibbs, S. (2017). What is 'WanaCrypt0r 2.0' ransomware and why is it attacking the NHS?. The Guardian. Londra. ISSN 0261-3077.

Kaspersky (2022). A Brief History of Computer Viruses & What the Future Holds. https://www.kaspersky.com.tr/resource-center/threats/a-brief – history-of-computer-viruses-and-what-the-future-holds

Kushner, D. (2013). The real story of stuxnet. ieee Spectrum, 50(3), 48-53.

Leyden, J. (2003). Slammer: Why security benefits from proof of concept code". Register. Retrieved 29 November 2008.

Lika, R. A., Murugiah, D., Brohi, S. N., & Ramasamy, D. (2018, July). NotPetya: cyber attack prevention through awareness via gamification. In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 1-6). IEEE.

Maynor, D.(2011). Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research. Elsevier. p. 218. ISBN 978-0-08-054925-5.

Mcafee (2022). Eugene Kaspersky görüşleri. https://expertsmirnov.ru/tr/windows-10/evgenii-kasperskii-s-ironiei-otozvalsya-o-mcafee-kakoi-antivirus.html

McAlpine, K. B. (2018). Bits and Pieces: A history of Chiptunes. Oxford University Press, USA.
Nichols, S., Thomson, I. (2009). Top ten worst viruses. http://www.pcauthority.com.au/News/143993,top-ten-worst-viruses.aspx,
Özer, M. C. (2015). Bilgisayar müziği dillerinin tarihçesi. Ege Üniversitesi Devlet Türk Musikisi Konservatuvarı Dergisi, 6, 47-59.
Parker, R. (2018). ILOVEYOU!. Medium. Retrieved 2021-07-28.
Poulsen, K. (2000). May 4, 2000: Tainted 'Love' Infects Computers. Wired. ISSN 1059-1028. Retrieved 2021-07-28.
Serazzi, G.; Zanero, S. (2004). Computer Virus Propagation Models (PDF). In Calzarossa, Maria Carla; Gelenbe, Erol (eds.). Performance Tools and Applications to Networked Systems. Lecture Notes in Computer Science. Vol. 2965. pp. 26–50.
Spafford, E. (1988). An analysis of the worm (PDF). Purdue University. Retrieved October 30, 2019.
Wong, J. C. Solon, O. (2017). Massive ransomware cyber-attack hits 74 countries around the world. The Guardian. Londra.

BÖLÜM 5

SIZMA TESTİ VE UYGULAMA

Ahmet SOLAK[1]
Recep BENZER[2]

1. GİRİŞ

Siber güvenlik ve siber savaşlar klasik savaş metotlarını geride bırakarak çağın yeni nesil harp yöntemleri içinde yerini almıştır. Bu bağlamda giderek şiddetini arttıran siber saldırıların etkisi göz ardı edilemez. İnternetin ilk defa askeri sahada ABD'de haberleşme teknolojisiyle doğuşundan sonra sivil mecrada kullanımı ile dünyanın kültürel ve ekonomik yapısı giderek bilişim merkezli şekilde değişmiştir. Buradaki değişim internetin tersine, ilk defa sivil aktörlerin bilişim teknolojilerini saldırı amaçlı olarak veyahut da sabote aracı halinde kullanması ile başlamıştı (Ünver, Canbay ve Özkan, 2010: 54). Sonraki noktada gelişen süreçte devletler siber güvenliğin kazanımını kavramış ve buna bağlı savunma yatırımları ve savunma stratejileri ilerletmeye başlamışlardır. Siber saldırıların yerini devlet seviyesinde olan siber saldırılar almıştır. Ancak bu varsayıma tezat bir biçimde siber saldırılar da değerini kaybetmemiştir (Yılmaz ve Sağıroğlu, 2013: 84). Çıkışı bireyler düzeyinde olan siber saldırıların oyuncularının sayıları devletlerin siber komutanlıkları veya Siber Olaylara Müdahale (SOM) kurumlarında bulunan çalışanlarından fazladır. Bu vaziyet siber saldırı örneklerinin siber savaş olanlarına göre daha çok sık görülmesine sebep olmaktadır (Karabacak, 2011: 76). Lakin siber saldırılar sık görünmelerine rağmen tesirleri siber savaşları unutturacak seviyede yıkıcı olabilmektedir.

Siber güvensizliğin getireceği maliyetin bu sahada yapılacak harcamalardan çok daha fazla olabileceği dikkate alınırsa siber savunmaya çok daha fazlaca yatırım yapılması gerektiği açıkça önemli görülmektedir. Hizmetlerinin etkin ve verimli bir şekilde verilebilmesi için e-Devlet yaşam döngüsünün sürekliliği bir amaç olarak karşımıza çıkmaktadır. Bahsedilen yaşam döngüsünün en önemli bacaklarından birisi de bilgi güvenliğidir (Koçak ve Memiş, 2018). Bilgi güvenliğinin temel amacı bireylerin verilerine müdahale edebilecek yetkisiz erişimlerin

[1] Ahmet Yesevi Üniversitesi, Siber Güvenlik Tezsiz Y.Lisans Dönem Projesi kapsamında yapılan çalışmadır. Tezsiz YL Öğrencisi, Ahmet Yesevi Üniversitesi, Siber Güvenlik, Ankara, Türkiye, ahmetsolak@outlook.com
[2] Doç.Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim, Ankara, Türkiye, rbenzer@gazi.edu.tr

4. SONUÇ

Bu çalışmada sızma testi programı kurulumu ve Deauthentication Saldırısı (Ağdan Düşürme) örneği ekran görüntüleri ile açıklanmıştır.

Alacağımız önlemler, saldırı yüzeylerini azaltmada ve siber saldırıları önlemede kullanıcılara önemli faydalar sağlayacaktır.

4.1. Öneriler

- Web uygulamalarda en önemli zafiyet insan faktörü olduğu unutulmamalıdır. Farkındalık hususu tam olarak kullanıcılara verilmelidir.
- Alt yapıda kullanılan tüm elemanların güvenlik sıkıştırmaları yamaları ile yapılmalıdır.
- Tüm güncellemeler zamanında yapılmalıdır.
- Güvenlik duvarı kullanılmalı ve yapılandırılması uzman kişiler tarafından uygun şekilde yapılmalıdır.
- Web uygulamalarında ssl inspection özellikleri aktif olmalıdır.
- Saldırı emaresi olabilecek ip adresi, alan adı ya da domain bilgisi içeren trafik engellenmelidir.
- Uygun korelasyonlar kullanılarak olası saldırıların önüne geçilmesi sağlanmalıdır.

KAYNAKLAR

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.

Akkaya, M. U. (2014). Siber Güvenlik Standartları ve Belgelendirmeleri. 2. Uluslararası İstanbul Akıllı Şebekeler Kongre ve Fuarı, 48-52.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi.

Atasever, S., Özçelik, İ., ve Sağıroğlu, Ş. (2019). Siber Terör ve DDoS. Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23(1), 238-244.

Bıçakcı, S. (2014). NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. Uluslararası İlişkiler Dergisi, 10(40), 100-130.

Bıçakcı, S., Ergun, F. D., ve Çelikpala, M. (2016). Türkiye'de Siber Güvenlik, 1. Baskı, İstanbul: İmak Ofset Basım Yayın, 28-73.

Bolat C. (2020). Siber Saldırılara Karşı Meşru Müdafaa Hakkının Uluslararası Hukuk Açısından İncelenmesi, (Doktora Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Çelikkol, M. (2015). Ağ ve Bilgi Güvenliği Sempozyumu Kritik Altyapılar: Elektrik Üretim Ve Dağıtım Sistemleri Scada Güvenliği. Bildiriler Kitabı, 19.

Ermiş, U. & Özdal, B. (2015). Siber caydırıcılık kavramının nükleer caydırıcılık olgusu ile karşılaştırmalı analizi, Yüksek Lisans Tezi, Uludağ Üniversitesi/Sosyal Bilimler Enstitüsü/Uluslararası İlişkiler Anabilim Dalı, Bursa, 69-80

Göçoğlu, V. (2018). Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi. Yayınlanmamış Doktora Tezi, Ankara: Hacettepe Üniversitesi Sosyal BİIimler Enstitüsü.

Göçoğlu, V., & Aydın, M. D. (2011). Siber Güvenlik Politikası: Abd, Rusya ve Çin Üzerine Karşılaştırmalı Bir Analiz. Güvenlik Bilimleri Dergisi, 8(2), 229-252.

Gürkaynak, M., ve İren, A. A. (2011). Reel dünyada sanal açmaz: Siber alanda uluslararası ilişkiler. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 16(2), 263-279.

Hatipoğlu, C. (2017). Teknolojik Savaşlar: Siber Terörizm Tehditleri. In Icpess (International Congress On Politic, Economic And Social Studies) (No. 3).

Hatipoğlu, C. (2017). Teknolojik Savaşlar: Siber Terörizm Tehditleri. In ICPESS (International Congress on Politic, Economic and Social Studies) (No. 3).

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar Ve Türkiye'nin Siber Güvenlik Politikalari. Uluslararası Güvenlik ve Terörizm Dergisi, 135-158.

Hekim, H., ve Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nİn Sİber Güvenlİk PolİtİkalarI. Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), 135-158.

https://www.kali.org/get-kali/ Erişim: 1012.2021

Karabacak, B. (2011). Kritik Altyapılara Yönelik Siber Tehditler Ve Türkiye İçin Siber Güvenlik Önerileri. Siber Güvenlik Çalıştayı, Bilgi Güvenliği Derneği, 29.

Kartal, Atahan Birol. (2018) Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye'de DAEŞ ve YPG Örneği". Güvenlik Stratejileri Dergisi, 14(27): 39-77.

Kınık, H., & Güntay, V. (2016). Siber Güvenlik Temelinde Kritik Altyapılar Ve Hazar Havzası. Journal of International Social Research, 9(47).

Kurnaz, S., & Karatepe, S. (2017). Kamusal Kritik Tesislerin Güvenliği Kapsamında Türkiyedeki Hava Alanlarının Siber Güvenliği. Assam Uluslararası Hakemli Dergi, 119-129.

Öğün, M. N., & Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi Ve Alınabilecek Tedbirler. Security Strategies Journal, 9(18).

Sertçelik, A. (2015). Siber Olaylar Ekseninde Siber Güvenliği Anlamak. Medeniyet Araştırmaları Dergisi, 2(3), 25-42.

Şahinaslan, E., Şahinaslan, Ö., & Selimli, S. (2016). Siber Saldırıların Kritik Altyapılar Üzerindeki Etkileri. Bilişim Teknolojileri Dergisi, 8(3), 133-149.

Şenol, M. (2017). Türkiye'de Siber Saldırılara Karşı Caydırıcılık. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 3(2), 1-9.

Tarık, A. (2014). İç Güvenlik Yönetimi Açısından Kritik Altyapılarını Korunması. Assam Uluslararası Hakemli Dergi, 42-51.

Ünver, M., Canbay, A. (2009). Uluslararası Kuruluşların Siber Güvenlin Faaliyetleri. Uluslararası İlişkiler Dergisi, 9(4), 102-180.

Ünver, M., Canbay, C., & Özkan, H. B. (2010). Kritik Altyapıların Korunması. Bilgi Tennolojileri Ve Koordinasyon Dairesi Başnanlığı, Mayıs. Kritik Enerji Altyapı Güvenliği El Kitabı.

Yayla, M. (2013). Hukuki Bir Terim Olarak Siber Savaş. Tbb Dergisi, 104, 194-198.

Yılmaz, E., Halil, U. & Gönen, S. (2015). Bilgi Toplumuna Geçiş ve Siber Güvenlik. Bilişim Teknolojileri Dergisi, 8(3), 133.

Yılmaz, S., & Sağıroğlu, Ş. (2013). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri. 6. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı Bildiriler Kitabı, 158-166.

BÖLÜM 6

WEB UYGULAMALARINA YAPILAN ATAKLAR VE UYGULAMA

Eser SOLMAZ[1]
Recep BENZER[2]

1. GİRİŞ

Günümüz ortamında internetin vazgeçilemez derecede yaygın kullanılması ve bilgiye her yerden ulaşılmak istenmesi ile bilirlikte web teknolojileri çok yaygın bir şekilde kullanılmaktadır. Web teknolojileri ile ulaşılmak istenen bilgilerin sınırsızlığı ve bu bilgiler üzerinde yapılmak istenen işlemlerin sonunun gelmemesi ile web teknolojilerin de her geçen gün yenilenmesine sebep olmaktadır (Çağlayan, 2004; Sarısakal ve Uysal, 2001).

1.2. Web Teknolojilerinde Güvenlik İhtiyacı

Web uygulamalarının vazgeçilemez olması ve kullanım yoğunluğu da web tehditlerini beraberinde getirmiştir. Web uygulamalarının internet ya da intranet ortamları ile erişilebilir olduğu sürece geliştirici hataları ya da mantık hataları ile zafiyet oluşturma ihtimalini her zaman taşımaktadır. Oluşabilecek bu zafiyetleri ya da kötü niyetli kişiler tarafından web uygulamalarına yapılabilecek saldırıları engelleme ihtiyacı vardır ve ihtiyaç artarak çoğalmaktadır (Çağlayan, 2004; Gülnaz, 2010).

1.3. Web Teknolojilerine Yönelik Tehdit ve Saldırılar

Web teknolojilerine yönelik saldırılar için literatür taraması yapıldığı zaman OWASP (Open Web Application Security Project) kuruluşunun web uygulama güvenlik uzmanları tarafından gelişimi desteklenen en iyi içeriği sahip bilgi kaynağı olarak görebiliyoruz. Aşağıda OWASP TOP10 projesinin 2021 yılı içerisinde web uygulamalarına karşı en çok yapılan 10 saldırı yöntemini detaylandırıyor olacağız (Çağlayan, 2004; Owasp1, 2021, Owasp2, 2021).

SQL enjeksiyon ve Siteler arası betik çalıştırma gibi en tehlikeli web saldırıları uygun filtreleme ve doğrulama olmadan kaynağı belirsiz verileri kabul ede-

1 Ahmet Yesevi Üniversitesi, Siber Güvenlik Tezsiz Y.Lisans Dönem Projesi kapsamında yapılan çalışmadır. Tezsiz YL Öğrencisi, Ahmet Yesevi Üniversitesi, Siber Güvenlik, Ankara, Türkiye, esersolmaz@gmail.com
2 Doç.Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim, Ankara, Türkiye, rbenzer@gazi.edu.tr

dan şifreleme (ssl inspection) özelliklerin aktif olması gereklidir.

- Web uygulamalara gelebilecek saldırıları tespit edebilmek web uygulamalarının çalışması için gerekli olan bütün noktalardaki olay günlüklerinin merkezi log yönetim sistemlerine aktarılarak oluşabilecek bütün saldırı tipleri için ilgili kuralların yazılması gereklidir.
- Günümüzde güvenlik üreticisi firmalarının müşterileri ile paylaştıkları saldırı emarelerini (IOC) sistemlerimizde kullanabilir olarak ayarları yapmalıyız ve bu şekilde saldırı emaresi barındıran ip adresi, alan adı ya da domain bilgisi içeren trafiğin engellenmesi sağlanabilir.
- Olay yönetim sistemi korelasyonu ile algılanmış saldırılar yada korelasyon kuralları ile saldırı seviyesi yükseltilmiş saldırılar için otomatik cevap verebilecek sistemlerin kurulumu ve kullanımı mutlaka yapılmalıdır.

KAYNAKÇA

Aslan, B. (2007). Web 2.0, teknikleri ve uygulamaları. XII.Türkiye'de İnternet Konferansı Bildirileri, 8-10.

Avcı, İ., Koca, M., & Atasoy, M. (2021). Windows Tabanlı Uygulamalarda SQL Enjeksiyon Siber Saldırı Senaryosu ve Güvenlik Önlemleri. *Avrupa Bilim ve Teknoloji Dergisi*, 213-219.

Baykara, M., Daş, R, & Tuna, G. (2016). Web Sunucu Erişim Kütüklerinden Web Ataklarının Tespitine Yönelik Web Tabanlı Log Analiz Platformu. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi,* 291-302.

Çağlayan, İ. (2004). Yeni web teknolojileri ve web uygulamaları (Doctoral dissertation, İstanbul Kültür Üniversitesi/Fen Bilimleri Enstitüsü/Bilgisayar Mühendisliği Anabilim Dalı). 5-15

Çakmak, A. (2018). Web güvenliğinde SSL/TLS kriptografik protokolü: açıklıklar, saldırılar ve güvenlik önlemleri (Master›s thesis, İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü). 63 – 98

Çınar, I., & Bilge, H. Ş. (2016). Web Madenciliği Yöntemleri ile Web Loglarının İstatistiksel Analizi ve Saldırı Tespiti. *Bilişim Teknolojileri Dergisi*, 9(2), 125.

Çiftçi, H. (2013). Her Yönüyle Siber Savaş. TÜBİTAK,

Demirol, D., Daş, R., & Baykara, M. (2013). SQL enjeksiyon saldırı uygulaması ve güvenlik önerileri. In 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu) 62-66.

Gaissecurity (2021). Bkz.https://gaissecurity.com/bilgi/ssrf-server-side-request-forgery environments (Erişim: 01 Aralık 2021).

Gülnaz, M. (2010). Kamusal Web Güvenliği (Türkiyede Kamu Kurumlarına ve Özel Şirketlere Ait Web Sitelerinin Web Güvenliği Açısından Değerlendirilmesi Üzerine Bir Araştırma) (Doctoral dissertation, Marmara Universitesi (Turkey)). 65-146

Karaarslan, E. (2008). Web saldırı saptama sistemlerinin etkinleştirilmesi için sistem farkındalığı ve çok katmanlı güvenlik önlemlerinin gerçekleştirilmesi. (Doktora Tezi, Ege Üniversitesi Fen Bilimleri Enstitüse Bilgisayar Mühendisliği Anabilim Dalı, İzmir) 67-91

Karaaslan, E., Tuğlular, T., & Şengonca, H. (2008). Kurumsal web güvenliği yapısı. *Akademik Bilişim,* 237-246.

Mitropoulos, D., Louridas, P., Polychronakis, M., & Keromytis, A. D. (2017). Defending against web application attacks: approaches, challenges and implications. *IEEE Transactions on Dependable and Secure Computing*, 188-203.

Of, M. (2019). Siber Güvenlik Üzerine Bir Araştırma: Yazılım Güvenliği. *Bayburt Üniversitesi Fen Bilimleri Dergisi*, 2(2), 254-260.

Owasp1 (2021). Bkz.https://owasp.org/www-project-top-ten (Erişim Tarihi: 01.12.2021)

Owasp10 (2021). Bkz.https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_(SSRF) (Erişim: 01 Aralık 2021).

Owasp2 (2021). Bkz.https://trendmicro.com/en_us/devops/21/k/overview-owasp-top-10-2021.html (Erişim: 01 Aralık 2021).

Owasp3 (2021). Bkz.https://owasp.org/Top10/A01_2021-Broken_Access_Control (Erişim: 01 Aralık 2021).

Owasp4 (2021). Bkz.https://owasp.org/Top10/A04_2021-Insecure_Design (Erişim: 01 Aralık 2021)

Owasp5 (2021). Bkz.https://owasp.org/Top10/A05_2021-Security_Misconfiguration (Erişim: 01 Aralık 2021)

Owasp6 (2021). Bkz.https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components (Erişim: 01 Aralık 2021).

Owasp7 (2021). Bkz.https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures (Erişim: 01 Aralık 2021)

Owasp8 (2021). Bkz.https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures (Erişim: 01 Aralık 2021).

Owasp9 (2021). Bkz.https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures (Erişim: 01 Aralık 2021).

Özbek, M., (2019). Mikroservis Tabanlı Ağ Uygulamalarında Zararlı Davranışların Saptanması (Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Bilgisayar Mühendisliği Anabilim Dalı, İstanbul)

Sağıroğlu, Ş., & Alkan, M. (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Grafiker Yayınları

Sarısakal, N., & Uysal, M. (2001). Web teknolojilerindeki hızlı gelişmelerin ve web programlama araçlarının incelenmesi. *Istanbul University-Journal of Electrical ve Electronics Engineering*, 2-4.

Securityintelligence (2021). Bkz.https://securityintelligence.com/posts/x-force-report-hacking-cloud-environments (Erişim: 01 Aralık 2021).

Sevri, M. (2016). Web saldırılarının tespitine yönelik yapay zeka tabanlı bir güvenlik modülü geliştirilmesi (Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü Bilişim Sistemleri Ana Bilim Dalı, Ankara)

Tekerek, A., Gemci, C., & Bay, Ö. F. (2016). Web tabanlı saldırı önleme sistemi tasarımı ve gerçekleştirilmesi: yeni bir hibrit model. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 645-653.

W3techs (2021). Bkz.https://w3techs.com/technologies/details/ce-httpsdefault (Erişim: 01 Aralık 2021).

Yalçınkaya, M. A., & Küçülsille, E. (2021). Web Uygulama Sızma Testlerinde Kapsam Genişletme İşlemi İçin Metodoloji Geliştirilmesi ve Uygulanması. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi,* 25(1), 16-27.

BÖLÜM 7

BİLİŞİM TERÖRÜ VE BİLİŞİM SUÇLARI

Elif DEMİRLİ[1]
Recep BENZER[2]

1. GİRİŞ

Tarihin en eski dönemlerinden beri var olan iki kurum insanlığın gidişatına belki de en çok şekil verenlerdir. Bunlardan ilki paradır. Gerçekten de dünyanın adım atılmadık hiçbir bölgesi yoktur ki paranın izlerine rastlanılmasın. Fakat varlığını paradan dahi öncesine götürebileceğimiz bir kurum vardır ki nefes alan ilk iki insanın yan yana gelmesi, onun varlığı için kafidir. Bu hukuktan başkası değildir. İnsanlar bir arada yaşamaya karar vermekle tarihteki ilk sözleşmenin temelini atmışlardır. Nitekim nasıl her sözleşme beraberinde muhtemel bir ihlal de getiriyorsa toplum sözleşmesi de içerisinde bu ihlalin potansiyelini barındırır. Bunun önüne geçilmelidir zira sözleşmenin sürekliliği insan yaşamının idamesi(!) için zaruri bir ihtiyaçtır. O halde sözleşmenin sürekli kılınabilmesi birtakım yaptırımlar da devreye sokulmalıdır ve böylelikle yeni ihlallerin önüne geçilecektir. Ayrıca modern olmayan hukuk düzenindeki yaklaşımla ihlalciler dönemlerince sakıncalı olarak kabul edilen bu hareketlerinin bedelini de ödemelidirler. Burada hukuk kurumunun beraberinde taşıdığı "suç" ve "ceza" kavramlarıyla karşılaşmaktayız. Hukuktan kastımız yalnızca yazılı normlar değildir. Biz burada yazılı yahut yazısız, düzeni teşkil etmek iddiasıyla yaşayan her türlü kuralı ifade ediyoruz. Zira hukuk ne monoteist bir dinin ürünüdür ne Rönesans'ın ne de bir devletin. Onun mevcudiyet kazanması için iki insanın bir araya gelmesi yeterlidir.

Herakleitos'un o meşhur ifadesi ile nasıl değişmeyen tek şey değişimin kendisi ise adli bakımdan suç ve beraberinde de hukuk da değişmektedir. 1641 yılında o ünlü Leviathan'ı yazan Hobbes için yalnızca bir hayalden ibaret makineler günümüzün her alanına doğrudan temas eden birer hakikat oldukları düşünüldüğünde suçun içerisinde makinelerin de yer almaması düşünülemez. İşte bilişim suçları ve bilişim suçlarının bir alt başlığı olarak değerlendirilebilecek ancak şahsına münhasır özelliklere de sahip olan bilişim terörizmi bu gelişmelerin ürünüdür.

[1] Gazi Üniversitesi, Bilişim Enstitüsü, Uzaktan Eğitim, Bilişim Suçları ve Mücadele Dersi proje çalışmasıdır. Tezsiz YL Öğrencisi, Gazi Üniversitesi Adli Bilişim, Ankara, Türkiye, elifdemirli-90@hotmail.com

[2] Doç.Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim, Ankara, Türkiye, rbenzer@gazi.edu.tr

KAYNAKLAR

Akarslan, H. (2015). *Bilişim Suçları*. Ankara: Seçkin Yayıncılık.

Akbulut, B. (2017). *Bilişim Alanında Suçlar*. Ankara: Adalet Yayınevi.

Akhgar, B., Staniforth, A., & Bosco, F. (2014). *Cyber Crime and Cyber Terrorism Investigator's Handbook*. E. Luiijf içinde, Definitions of Cyber Terrorism (s. 11-17). Waltham, Massachusetts: Elsevier.

Aydın, N. (2011). *Kırmızı Kitap Milli Güvenlik Politikası*. İstanbul: Paraf Yayınları.

Balkan, C. (2006). *Soğuk Savaş Sonrasında Türkiyenin Ulusal Güvenlik Sorunları*. İstanbul: Toplumsal Dönüşüm Yayınları.

BM Enformasyon Merkezi (2016). *Birleşmiş Milletler'in Terörle Mücadelesi ve Terörle Mücadele Eylem Planı*. 10.12.2021 tarihinde BM Enformasyon Merkezi Ankara, Türkiye http://www.unicankara.org.tr/language/tr/birlesmis-milletlerin-terorle-mucadelesi-terorle – mucadele-eylem-plani/#.Xel3FZMzbIU

Ceza-bb.adalet.gov.tr. (2021). *TCK Kanun Gerekçesi*. 10.12.2021 http://ceza – bb.adalet.gov.tr

Colarik, A. (2006). *Cyber Terrorism: Political and Economic Implications*. London: Idea Group Publishing.

Dedeoğlu, B. (2014). *Uluslararası Güvenlik ve Strateji*. İstanbul: Yeniyüzyıl Yayınları.

Dülger, M. (2018). *Bilişim Suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin Yayıncılık.

Ertan, B. (2015). *Terörizm ve Türkiye*. İstanbul: Toplumsal Dönüşüm Yayınları.

Hatipoğlu, C. (2017). *Teknolojik Savaşlar: Siber Terörizm Tehditleri*. 3nd International Congress on Political, Economic and Social Studies (ICPESS), (s. 157-168).

Ankara. hurriyet.com.tr. (2017). Türkiye'nin 21 bin siber güvenlik askeri olacak! 15.12.2021 http://www.hurriyet.com.tr/teknoloji/turkiyenin-21-bin-siber-guvenlik-askeri-olacak

İç İşleri Bakanlığı. (2017). *Güvenlik Terimleri Sözlüğü*. Ankara: Uluslararası Piri Reis Kültür Ajansı.

Kara, O., Aydın, Ü., & Oğuz, A. (2013). *Ağ Ekonomisinin Karanlık Yüzü: Siber Terör*. https://istihbaratsahasi.files.wordpress.com/2013/10/a-ekonomsnn-karanlik-yz-sber-terr.pdf

Kaspersky.com. (2021). Botnet Nedir? https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks

Langner, R. (2013). *To Kill a Centrifuge*. Munich: The Langner Group.

Lendman, S. (2020). Trump Regime Electricity War in Venezuela More Serious than First Believed. Global Research: https://www.globalresearch.ca/trump-regime electricity-war-venezuela/5670970

NATO Centre of Excellence Defence Against Terrorism (2008). NATO and Cyber Terrorism. P. Everard içinde, Responses to Cyber Terrorism (s. 118-127). Amsterdam: IOS Press.

Özbek, V. (2002). İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 4(1), 101-158.

Pazarcı, H. (2008). *Uluslararası Hukuk*. Ankara: Turhan Kitabevi.

Schmid, A., & Easson, J. (2011). 250-plus Academic, Governmental and Intergovernmental Definitions. A. Schmid içinde, The Routledge Handbook of Terrorism Research (s.99-157). New York: Routledge.

Simpson, D. (2019). States of Terror: History,Theory, Literature. Chicago: The University of Chicago Press. state.gov. (2021, December 12). Joint Statement on Advancing Responsible State Behavior in Cyberspace. U.S. Department of State: https://www.state.gov/joint-statement-on – advancing-responsible-state-behavior-in-cyberspace/

T.C. Dış İşleri Bakanlığı. Türkiye'nin Uluslararası Toplumun Terörle Mücadele Çabalarına Katkıları. (2021) T.C. Dış İşleri Bakanlığı:http:www.mfa.gov.tr/turkiye_nin-uluslararasi-toplumun-terorle-mucadele-cabalarina-katkilari.tr.mfa

Türkiye Barolar Birliği. (2006). *Türkiye ve Terörizm*. Ankara: TBB Yayınları. UITSEC. (2016). Siber Güvenlik Cep Sözlüğü. İstanbul: UTI SEC Teknoloji A.Ş.

Ünver, Y. (2001). TCK ve CK Tasarısının İnternet Açısından Değerlendirilmesi. *İstanbul Üniversitesi Hukuk Fakültesi Dergisi,* 59(1-2), 51-153.

Winterfeld, S., & Andress, J. (2013). The Basics of Cyber Warfare. Waltham: Syngress.

WWW Siberbülten (2018). Kritik Altyapıların Siber Güvenliğine Ayrılan Bütçe 125 Milyar Dolara Çıkacak. Siber Bülten: https:siberbulten.com/kritik-altyapi-guvenligi/kritik-altyapilarin-siber-guvenligine-ayrilan-butce-125-milyar-dolara-cikacak/

Zetter, K. (2014). *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.

BÖLÜM 8

YAPAY ZEKÂ YÖNTEMİ İLE REAKTİF GÜÇ KOMPANZASYONU TEKNİĞİ[1]

Nafiz ÜNLÜ[2]

1. YAPAY ZEKÂ NEDİR?

Yapay zeka (AI), tipik olarak insan zekası ile yapılan işleri akıllı bilgisayar ve robotlar tasarlayarak gerçekleştirmeyi planlayan bilgisayar biliminin geniş kapsamlı bir dalıdır. İnsanların düşünme ve hareket etme biçiminin modellenmesi ve simülasyonudur (PK, 1984; Fetzer, 1990; Winston, 1992; Boden, 1996). AI, felsefe, matematik, ekonomi, sinirbilim, psikoloji, dilbilim ve bilgisayar mühendisliği dahil olmak üzere çeşitli disiplinlerin araştırma ve geliştirmesinden yararlanır (Bilgilioğlu, 2018). İnsanların düşünme ve hareket etme şeklini simüle ederek, insanların karşılaştığı birçok sorunu çözmemize yardımcı olacak makineleri kullanabiliriz.

Son birkaç on yılda bir dizi yapay zeka tanımı ortaya çıkmış olsa da, Yapay zeka (AI) sözcüğünü ve LISP yazılım dili buluşunu yapanlardan biri olan John McCarthy, yapay zekayı şu şekilde anlatmaktadır (Karabulut, 2021): "Özellikle akıllı bilgisayar programları yapan akıllı makinelerdir. Bu, insan zekasını anlamak için bilgisayarları kullanma göreviyle benzer bir görevdir, ancak yapay zekanın kendisini biyolojik olarak gözlemlenebilir yöntemlerle sınırlaması gerekmez." Ancak bu tanımdan on yıllar önce, yapay zeka sohbetinin doğuşu Alan Turing'in çığır açan çalışması, 1950'de yayınlanan "Bilgisayar Makineleri ve Zeka" makalesinde belirtilmişti. Turing'in bu makalesinden sonra gerçekleşitirilen Turing Testi, yapay zekanın belirlenen temel amacını ve görünümünü ortaya koydu. Test bugün için geçerliliğini koruyor ve AI'nın doğal dil işleme, makine öğrenmesi, robotik gibi alt disiplinlerini tanımlıyor. Yapay zekanın en gelişmiş misyonu, içeriği,birçok soru ve tartışmayı da beraberinde getirmiştir. Sonuçta bu tartışma tek bir tanım üzerinde ortak bir görüşün ortaya çıkmasını da engellemiştir. İngiliz matematikçi, bilgisayar bilimcisi , kriptolog, Turing, şu soruyu soruyor: "Makineler düşünebilir mi?". Ardından bir insan sorgulayıcısının, bir bilgisayar ve insan metin yanıtını ayırt etmeye çalışacağı, şimdi ünlü olarak "Turing Testi" olarak bilinen bir testi sunuyor. Bu test, yayımlanmasından bu yana çok fazla incelemeden geçmiş olsa

[1] Yüksek Lisans Tezinin bir bölümüdür.

[2] Dr.Öğrt.Üyesi, İstanbul Teknik Üniversitesi, Bilişim Enstiüsü, İstanbul, Türkiye, unluna@itu.edu.tr

Reaktif güç kompanzasyonun tüketici açısından faydaları ise;

1. Hem tüketici hem de İşletme maliyetlerini azaltır,
2. Kalitesiz enerji kaynaklı arıza riskini azaltır.
3. Enerji kalitesi artığı için imalat kalitesi de artar.
4. Müşteri, güç faktörünü düzelterek şebekeden düşük miktarda reaktif güç çekerek daha az ödeme yapar.
5. Enerji kalitesi arttıkça üretim kalitesi de artar.

5. SONUÇ

Bu bölümde, bir yapay sinir ağı (YSA) akım denetleyicisini, performansını ve aktif güç filtreleri için geçerliliğini göstermektedir. Burada sistemin nasıl çalışması ve modellenmesi açıklanmıştır. Simülasyon sonuçları harmonikleri ve reaktif güç bileşenlerini ortadan kaldırmak için oldukça tatmin edici bulunmuştur.

Elde edilen veriler ANN'yi eğitmek için kullanılır, böylece ANN, yük değiştiğinde hangi kapasitörün bağlanacağını veya ayrılacağını göstererek yeterli kapasitör için 0 veya 1 çıkış verecek ve böylece kayıplar minimum olacak ve ağırlıklar elde edilecektir. Kondansatörler ayrıca, herhangi bir kondansatör arıza nedeniyle AÇIK konuma geçemezse, reaktif gücü telafi etmek için bitişik kondansatör AÇIK konuma getirilecek şekilde kontrol edilir.

Ayrıca bu çalışmada, güç kompanzasyonu da Levenberg-Marquardt (LM) öğrenme algoritması ile düşürülerek ve YSA ile performansı yüksek ve iyi sonuçlara ulaşılabilir. Ayrıca YSA'nın uygun bir şekilde modellenmesine ihtiyaç duymadan kompanzasyon işlemi yapılabilmektedir.

KAYNAKLAR

Winston, P. H. (1992). Artificial intelligence. Addison-Wesley Longman Publishing Co., Inc..

Boden, M. A. (Ed.). (1996). Artificial intelligence. Elsevier.

PK, F. A. (1984). What is Artificial Intelligence?. "Success is no accident. It is hard work, perseverance, learning, studying, sacrifice and most of all, love of what you are doing or learning to do"., 65.

Fetzer, J. H. (1990). What is artificial intelligence?. In Artificial intelligence: its scope and limits (pp. 3-27). Springer, Dordrecht.

Bilgilioğlu, S. S. (2018). Makine öğrenmesi teknikleri ile mekansal karar destek sistemlerinin geliştirilmesi: Aksaray ili örneği. Yüksek lisans Tezi, Aksaray Üniversitesi.

Karabulut, B. (2021). Yapay Zeka Bağlamında Yaratıcılık Ve Görsel Tasarımın Geleceği. Elektronik Sosyal Bilimler Dergisi, 20(79), 1516-1539.

Russell, S., & Norvig, P. (2002). Artificial intelligence: a modern approach.

Coşkun, F, and Gülleroğlu, H.D. (2021). Yapay Zekanın Tarih İçindeki Gelişimi ve Eğitimde Kullanılması. Ankara University Journal of Faculty of Educational Sciences (JFES) (2021): 1-20.

Bhatia, P., Khurana, N., & Sharma, N. (2013). Intuitive approach to use intelligent database for prediction. International Journal of Computer Applications, 83(15).

Evgeniou, T., & Pontil, M. (1999, July). Support vector machines: Theory and applications. In Advanced Course on Artificial Intelligence (pp. 249-257). Springer, Berlin, Heidelberg.

Hwang, R. C., Chen, Y. J., & Huang, H. C. (2010). Artificial intelligent analyzer for mechanical properties of rolled steel bar by using neural networks. Expert Systems with Applications, 37(4), 3136-3139.

Bennett, C. C., & Hauser, K. (2013). Artificial intelligence framework for simulating clinical decision-making: A Markov decision process approach. Artificial intelligence in medicine, 57(1), 9-19.

Dale, R., Moisl, H., & Somers, H. (Eds.). (2000). Handbook of natural language processing. CRC press

Dixon, J., Moran, L., Rodriguez, J., & Domke, R. (2005). Reactive power compensation technologies: State-of-the-art review. Proceedings of the IEEE, 93(12), 2144-2164.

Şekkeli, M., & Tarkan, N. (2010). Reaktif güç kontrol rölesinde minimum anahtarlama sayısı ve optimal reaktif güç seçimi. İTÜ Dergisi/d, 4(6).

Özdemir, Ş., & Kuşdoğan, Ş. (2005). Doğrusal olmayan yüklerde aktif güç filtresi ile harmoniklerin filtrelenmesi ve reaktif güç kompanzasyonu. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 20(2).

Gelgün, E. (2015). Elektrik Dağıtım Sistemlerinde Genetik Algoritma İle Kayıpların Azaltılması İçin Reaktif Güç Yönetimi (Doctoral dissertation, Fen Bilimleri Enstitüsü).

Kakilli, A., Tunçalp, K., & Sucu, M. (2008). Harmoniklerin Reaktif Güç Kompanzasyon Sistemlerine Etkilerinin incelenmesi ve Simülasyonu. Fırat Üniv. Fen ve Müh. Bil. Dergisi, 20(1), 109-115.

Bayındır, R., Sağıroğlu, Ş., & Çolak, İ. (2007). Yapay sinir ağları tabanlı reaktif güç kompanzasyonu. Politeknik Dergisi, 10(2), 129-135.

Öztemel, E. (2003). Yapay sinir ağlari. PapatyaYayincilik, Istanbul.

Kocabaş, E. (2006). Reaktif Güç Kompanzasyonu ve Simülasyonu (Doctoral dissertation, Marmara Universitesi (Turkey)).

WEB LİNK

https://www.ibm.com/cloud/learn/neural-networks

https://www.cmpe.boun.edu.tr/~akin/papers/beyin.pdf

https://www.ncbi.nlm.nih.gov/books/NBK225562/

https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

https://builtin.com/artificial-intelligence

https://dergipark.org.tr/tr/download/article-file/384629

https://dspace.gazi.edu.tr/bitstream/handle/20.500.12602/149890/alper_gorgun_tez.pdf;jsessionid=A1E86C871F95ABFEAFFC3722556F7AFF?sequence=1

https://www.accessscience.com/content/reactive-power-compensation-technology/YB084380#:~:text=Reactive%20power%20compensation%20is%20defined,to%20load%20and%20voltage%20support.

https://electrical-engineering-portal.com/how-reactive-power-is-helpful-to-maintain-a-system-healthy#:~:text=When%20reactive%20power%20supply%20lower,and%20potentially%20causing%20cascading%20failures.

https://electrical-engineering-portal.com/the-case-of-real-time-reactive-compensation

https://www.sektorumdergisi.com/kompanzasyon/

http://acikerisim.harran.edu.tr:8080/jspui/bitstream/11513/2352/1/610450.pdf