SİBER GÜVENLİK SİSTEMLERİNDE MODERN TEHDİDLER VE KORUMA MEKANİZMALARININ GELİŞİMİ

Xusenov Shoxrux Sherali oğlu
Muhammed el-Harezmi adını taşıyan Taşkent Bilgi Teknolojileri Üniversitesi Yazılım Mühendisliği Fakültesi 4. sınıf öğrencisi
Xusenova Nigina Sherali kızı
Çirçik Devlet Pedagoji Üniversitesi Turizm Fakültesi, Yabancı Dil ve Edebiyat Bölümü, 2. sınıf öğrencisi xusenovshoxrux7@gmail.com

Özet: *Bu makalede siber güvenlik sistemlerinde karşılaşılan modern tehditler, bunların ortaya çıkış nedenleri ve bu tehditlere karşı geliştirilen koruma mekanizmalarının evrim süreci analiz edilmektedir. Dijital dönüşüm sürecinde bilgi güvenliğinin sağlanmasının önemi temellendirilmiştir. Araştırma sonuçları, siber güvenliğin sağlanmasında bütüncül bir yaklaşımın ve ileri teknolojilerin kullanımının büyük önem taşıdığını göstermektedir.*

Anahtar Kelimeler: *siber güvenlik, bilgi güvenliği, zararlı yazılım, oltalama (phishing), fidye yazılımı (ransomware), Zero Trust, kimlik doğrulama, veri gizliliği*

Giriş: *Dijital teknolojilerin hızlı gelişimi, küresel ölçekte bilgi alışverişinin ve veri akışının önemli ölçüde artmasına neden olmuştur. Kamu yönetimi, bankacılık ve finans sistemi, sağlık, eğitim ve sanayi alanlarının dijitalleşmesiyle birlikte siber güvenlik konusu stratejik bir önem kazanmıştır.*

Son yıllarda siber saldırıların sayısı ve karmaşıklığı artış göstermektedir. Özellikle uzaktan çalışma modelinin yaygınlaşması, bulut teknolojilerinin benimsenmesi ve IoT cihazlarının çoğalması bilgi güvenliği sistemleri için yeni tehditler ortaya çıkarmıştır. Bu nedenle, modern tehditlerin tespit edilmesi ve etkili koruma mekanizmalarının geliştirilmesi önemli bir görev haline gelmiştir.

Modern tehditler, geleneksel virüslerden farklı olarak karmaşık, çok aşamalı ve hedef odaklı bir yapıya sahiptir. Bunlar arasında en yaygın olanlar şunlardır:

Modern Tehdit Türleri

1. Zararlı Yazılımlar (Malware)

Zararlı yazılımlar, bilgisayar sistemlerine yetkisiz erişim sağlamak, veri çalmak veya sistem işleyişini bozmak amacıyla geliştirilir. Türleri şunlardır:

- Virüsler
- Truva atı (Trojan) yazılımlar
- Casus yazılımlar (Spyware)
- Fidye yazılımları (Ransomware)

Özellikle fidye yazılımları son derece tehlikelidir; verileri şifreleyerek geri yükleme karşılığında ödeme talep ederler.

2. Oltalama (Phishing) Saldırıları

Phishing, kullanıcıların kişisel bilgilerini (kullanıcı adı, parola, banka bilgileri vb.) ele geçirmeye yönelik bir sosyal mühendislik yöntemidir. Genellikle e-posta, sahte web siteleri veya mesajlaşma uygulamaları aracılığıyla gerçekleştirilir.

3. DDoS Saldırıları

Dağıtılmış Hizmet Engelleme (Distributed Denial of Service – DDoS) saldırıları, sunucu veya ağ kaynaklarını aşırı isteklerle meşgul ederek hizmetin durmasına neden olmayı amaçlar.

4. Sıfır Gün (Zero-day) Açıkları

Zero-day açıkları, yazılım geliştiriciler tarafından henüz tespit edilmemiş güvenlik açıklarından yararlanır. Bu tür saldırılar, tespit edilmelerinin zor olması nedeniyle son derece risklidir.

Koruma Mekanizmalarının Gelişimi

Siber güvenlik alanındaki koruma mekanizmaları, tehditlerin evrimine paralel olarak gelişmektedir.

Geleneksel Koruma Araçları

- Antivirüs yazılımları
- Güvenlik duvarı (Firewall)
- IDS/IPS sistemleri (Saldırı Tespit ve Önleme Sistemleri)

Bu araçlar temel güvenlik katmanını oluşturmaktadır.

Kriptografik Koruma - Veri şifreleme, siber güvenliğin temel bileşenlerinden biridir. Modern sistemlerde AES, RSA gibi algoritmalar yaygın olarak kullanılmaktadır. Şifreleme, verilerin gizliliğini ve bütünlüğünü sağlamaktadır.

Çok Faktörlü Kimlik Doğrulama (MFA) - MFA sistemleri, kullanıcı doğrulamasında birden fazla kimlik doğrulama faktörü kullanır (parola, SMS kodu, biyometrik veri vb.). Bu yöntem, yetkisiz erişim riskini önemli ölçüde azaltmaktadır.

Zero Trust Modeli - Modern güvenlik yaklaşımlarından biri olan Zero Trust modeli, "kimseye güvenme, her zaman doğrula" prensibine dayanmaktadır. Bu modelde iç ağ dahi potansiyel tehdit kaynağı olarak değerlendirilir ve tüm erişimler sıkı denetime tabi tutulur.

Yapay Zekâ Tabanlı Koruma - Yapay zekâ teknolojileri, tehditlerin gerçek zamanlı olarak tespit edilmesini ve tahmin edilmesini mümkün kılmaktadır. Makine öğrenmesi algoritmaları, ağ trafiğindeki anormal faaliyetleri yüksek doğruluk oranıyla belirleyebilmektedir.

Dijital ekonomi koşullarında bilgi kaynakları en değerli varlıklardan biri haline gelmiştir. Bankacılık sektörü, e-devlet sistemleri ve sanayi altyapıları doğrudan siber güvenlik seviyesine bağlıdır.

Siber saldırılar yalnızca mali kayıplara değil, aynı zamanda itibar zedelenmesine, veri sızıntılarına ve ulusal güvenlik tehditlerine yol açabilmektedir. Bu nedenle siber güvenliğin sağlanması devlet politikası düzeyinde öncelikli bir alan haline gelmiştir.

Şirketler açısından ise "Security by Design" yaklaşımı, yani güvenliğin sistem tasarım aşamasından itibaren entegre edilmesi, büyük önem taşımaktadır.

Gelecekte siber güvenlik alanında şu gelişmelerin öne çıkması beklenmektedir:

- Yapay zekâ destekli otomatik güvenlik operasyonları
- Kuantum kriptografisi
- Bulut tabanlı güvenlik hizmetleri (Security as a Service)
- IoT güvenliğini artırmaya yönelik teknolojiler

Tehditlerin karmaşıklığı arttıkça koruma mekanizmaları da daha akıllı ve uyarlanabilir hale gelecektir.

İstatistiksel Veriler ve Analiz

Son yıllarda siber tehditler küresel ekonomiye ciddi zararlar vermektedir. Uluslararası analizlere göre, 2018 yılında küresel siber suçların yol açtığı zarar yaklaşık 0,6 trilyon ABD doları iken, 2024 yılına gelindiğinde bu rakam 9 trilyon doları aşmıştır.

Özellikle 2021–2023 döneminde zarar miktarında hızlı bir artış gözlenmiştir. Bunun başlıca nedenleri şunlardır:

- Fidye yazılımı saldırılarındaki artış
- Bulut altyapılarına yönelik saldırılar
- IoT cihazlarının yetersiz güvenliği
- Sosyal mühendislik (phishing) yöntemlerinin gelişmesi

Araştırmalara göre:

- 2023 yılında kuruluşların %60'ından fazlası en az bir siber saldırıya maruz kalmıştır;
- Veri ihlallerinin ortalama maliyeti 4 milyon doları aşmıştır;
- Çok faktörlü kimlik doğrulama uygulanan sistemlerde yetkisiz erişim riski %70'e kadar azalmıştır;
- Yapay zekâ tabanlı tehdit tespit sistemleri, saldırı tespit süresini %50 oranında kısaltmıştır.

Bu göstergeler, siber güvenliğe yatırım yapmanın stratejik bir zorunluluk olduğunu açıkça ortaya koymaktadır.

Sonuç

Analizler, modern siber tehditlerin çok boyutlu ve karmaşık bir yapıya sahip olduğunu göstermektedir. Bu tehditlerle etkili şekilde mücadele edebilmek için teknik, organizasyonel ve hukuki önlemleri bir arada içeren bütüncül bir yaklaşım gereklidir.

Modern koruma mekanizmalarının uygulanması, yapay zekâ tabanlı analiz araçlarının kullanılması ve kullanıcıların siber güvenlik bilincinin artırılması, dijital toplumun sürdürülebilir gelişimini güvence altına alacaktır.

KAYNAKÇA:

1. William Stallings. Network Security Essentials: Applications and Standards. Pearson, 2020.
2. Bruce Schneier. Applied Cryptography. Wiley, 2015.
3. IBM. Cost of a Data Breach Report 2023.

4. Cisco. Cybersecurity Threat Trends Report, 2024.
5. ENISA. Threat Landscape Report 2023.
6. World Economic Forum. Global Cybersecurity Outlook 2024.
7. NIST. Cybersecurity Framework 2.0, 2023.
8. Kaspersky. IT Threat Evolution Report, 2023.
9. McKinsey & Company. Cybersecurity as a Strategic Priority, 2022.
10. OECD. Digital Security Risk Management, 2021.