

BÖLÜM A

Günümüzde siber saldırılar yalnızca dışardan yapılan saldırılarla sınırlı değildir. Bir saldırgan sisteme girdikten sonra uzun süre o sistemde fark edilmeden hareket edebilir. Bu yüzden güvenlik mimarisi sadece saldırıyı engellemeyi değil tespit etmeyi ve müdahale etmeyi de yapabilmeklidir.

Firewall sistemleri, ağ ile internet arasındaki trafiği kontrol ederek erişimleri kontrol eder. Yetkisiz olanları engeller. Fakat firewall sistemleri bu trafiğin içeriğini bilmez ve sisteme önceden sızan bir saldırıyı fark edemez. Firewall'dan sonraki durak ise IDS(Intrusion Detection System) ve IPS(Intrusion Prevention System)'dir. IDS şüpheli trafiği tespit eder, IPS ise bu şüpheli trafiği otomatik olarak engeller.

Olduda saldırgan içeriye sızdı ve ağ içerisinde dolaşabiliyor. Bu noktada NDR(Network Detection and Response) devreye girer. NDR, içerideki anormallığı fark eder. Bu anormallikleri analiz eder ve tehditleri ortaya çıkarır. Eğerki saldırgan sistemin içine zararlı yazılım bıraktı. Burda ise EDR(Endpoint Detection and Response) çalışır. Bilgisayardaki çalışan zararlı yazılımları tespit ve şüpheli işlemleri tespit eder.

Tüm bu alanlardan gelen şüpheli davranışlar SOC (Security Operations Center)'a iletilir. SOC bir nevi beyindir. Farklı güvenlik sistemlerinden gelen verileri birleştirir ve karar vererek müdahale eder. SIEM ise SOC'a gelen bilgileri derleyen, toplayan ,alarm oluşturan ve SOC'a ileten kısımdır.

SOAR ise refleks gibidir. Önceden yaşanmış saldırılara otomatik olarak tepki verir ve engeller. Bu eylem her seferinde aynı olayların yaşanmasını engeller ve diğer güvenlik sistemlerinin iş yükünü azaltır.

Bunlarla ek olarak NDR ve EDR sistemlerinin birleşerek evrimleşmiş hali olan XDR(Extended Detection and Response) vardır. XDR sadece loglara bakmaz. E-posta, bulut sistemleri, ağ ve uç noktaları tek bir platformdan yönetir. Peki farkı nedir? SIEM pasif olarak veri toplarken, XDR aktif olarak tehdit toplar ve bu tehditlere yanıt verir.

Birde MDR(Managed Detection and Response) vardır. MDR bir cihaz veya yazılım değil , siber tehditlerin 7/24 uzmanlar tarafından izlendiği, avlandığı ve saldırı anında doğrudan müdahale edildiği bir güvenlik hizmetidir. Bu teknoloji ile insan uzmanlığını birleştirerek kurumun güvenlik açıklarını profesyonel bir şekilde kapatmayı sağlar.

Eğer genel bu sistemi hikayeleştirecek olursak: Hastane güvenliği üzerinden anlatabiliriz. Firewall, hastaneye giren araçları ve yayaları kontrol eden ana nizamiyedir. Kaydı olmayan veya yasaklı plakaların içeri girmesini en başta engeller. IDS/IPS, kapıdan girenlerin üstünü arayan dedektörlerdir. Şüpheli bir cisim (bıçak/zararlı kod) gördüğünde alarm verir (IDS) ve güvenliğe haber vererek içeri girmesini engeller (IPS). NDR, bir kişi içeri girdikten sonra, yetkisi olmadığı halde ameliyathaneye veya eczane deposuna girmeye çalışırsa, NDR bu anormal hareketliliği koridorlardaki sensörlerle fark eder. EDR, saldırgan tüm engelleri aşır

bir doktorun bilgisayarına veya ilaç dolabına ulaştığında devreye girer. İlaçların (verilerin) izinsiz alınmasını veya değiştirilmesini engeller. SIEM, tüm kameraların, giriş-çıkış kayıtlarının ve sensör verilerinin tek bir ekranda toplandığı dev ekranlı odadır. Dağınık bilgileri birleştirerek "Aynı kişi hem eczaneye hem laboratuvara girmeye çalıştı" diye uyarı verir. SOC, O ekranların başında 7/24 nöbet tutan, alarm geldiğinde telsizle müdahale emri veren profesyonel ekiptir. SOAR, bir sızıntı tespit edildiğinde, kimsenin düğmeye basmasına gerek kalmadan ilgili katın kapılarını otomatik kilitleyen ve asansörleri durduran "refleks" sistemidir. XDR, hastane güvenliği, hasta kayıt sistemi ve bina yönetiminin tek bir akıllı panelde birleşmesidir. Sadece hırsız değil, onun hangi hasta kaydına baktığını da anında ilişkilendirir. MDR, hastanenin kendi güvenliği yerine, dünyanın en iyi güvenlik şirketinden bir ekibin gelip 7/24 tüm bu sistemleri yönetmesidir.

BÖLÜM B

1. Temel Yapıtaşları ve Ağ

Transistör ve Bilgisayar Arasındaki Bağ: Transistörlerin 0 ve 1 durumları, mantık kapılarını oluşturur ve bu kapılar birleşerek işlemciyi meydana getirir. İşletim sistemleri de en temelde bu donanım üzerinde çalışan yazılımlardır.

OSI ve TCP/IP Modelleri: OSI modeli ağ iletişimini her aşamasıyla açıklayan 7 katmanlı akademik bir referans haritasıdır ve öğrenmek için şarttır; TCP/IP bu işin "pratik uygulama rehberidir". OSI'deki 7 katmanı daha basit 4 katmana indirir. Gerçek dünya standartıdır.

Kriptografi ve Bilgi Güvenliği: Kriptografi, sadece veriyi kilitlemek değildir. verileri matematiksel yöntemlerle şifreleyerek sadece yetkili tarafların okumasını (Gizlilik) sağlarken; "Hash" gibi tekniklerle verinin yolda değiştirilmediğini de (Bütünlük) ispatlayan bir güvenlik bilimidir.

2. Saldırı Vektörleri (Offensive Terminology)

Sosyal Mühendislik ve Phishing: İnsanlar teknik sistemlere göre daha kolay kandırılabilirliği için sosyal mühendislik saldırıları daha etkilidir. Phishing sahte içerikle kullanıcıyı kandırırken, e-mail spoofing teknik olarak e-postanın gönderici bilgisini sahte gösterir.

Malware ve Ransomware: Malware, sisteme zarar veren tüm zararlı yazılımların genel adıdır. Ransomware ise verileri şifreleyip fidye talep eden özel bir malware türüdür.

Zero-Day: Zero-Day zafiyetleri henüz bilinmediği ve yamalanmadığı için savunma sistemleri tarafından önceden engellenemez. Bu durum savunma tarafını hazırlıksız bırakır.

3. Savunma Mekanizmaları (Defensive Terminology)

Patch Yönetimi: Patch uygulanmayan sistemlerde bilinen güvenlik açıkları kapatılamaz ve bu açıklar saldırganlar tarafından istismar edilir. Bu nedenle yama yönetimi doğrudan güvenlik

seviyesiyle ilişkilidir.

Kimlik ve Erişim – 2FA: Parola tek başına ele geçirilebilir olduğu için yeterli değildir. 2FA, ikinci bir doğrulama faktörü ekleyerek saldırganın başarılı olma olasılığını matematiksel olarak ciddi biçimde düşürür.

VPN & SSL/TLS: VPN kullanıcı ile hedef ağ arasında şifreli bir tünel oluşturur ancak kullanıcıyı tamamen görünmez yapmaz. SSL/TLS ise bu iletişim sırasında verinin güvenli şekilde şifrelenmesini sağlar.

4. Standartlar ve Süreçler

Zafiyet Taraması & Pentest: Zafiyet taraması otomatik araçlarla bilinen açıkları tespit ederken, pentest bu açıkların gerçekten istismar edilip edilemeyeceğini manuel olarak test eder. Pentest saldırgan:: bakış açısını simüle eder.

ISO 27001, NIST, GDPR: Bu standartlar teknik araçlardan çok birer güvenlik yönetim çerçevesidir. Bir mühendisin bunları bilmesi, teknik çözümleri yasal ve kurumsal gereksinimlere uygun tasarlamasını sağlar. Yani bir mühendis sadece kod yazmamalı, veriyi korumanın yasal kurallarını da bilmeli ki şirket ceza yemesin.

BÖLÜM C

1. Adım: Pasif İstihbarat Toplama (CTI)

Öncelikle verilen IP adresini(45.128.232.67) VirusTotal kullanarak inceledim.

Kimlik tespiti: Bu IP adresi Hollanda'da bir sunucuda bulunmaktadır. AS50053 (Anton Levin) isimli bir servis sağlayıcıya aittir.

Sicil Kaydı: Verilere göre bu IP, Malware (Zararlı Yazılım) dağıtımı ve Phishing (Oltalama) faaliyetleri ile ilişkilendirilmiştir. BitDefender ve G-Data gibi global servisler tarafından Phishing olarak damgalanmıştır.

Zaman Çizelgesi: İncelediğim kısımda "Last Analysis Date" göre bu IP ile ilgili raporlamalar en son 1 ay öncedir. Ancak topluluk yorumları, bunun bilinen ve aktif bir tehdit olduğunu gösteriyor.

2. Adım: Terminoloji ve Yapılandırma

IOC (Indicator of Compromise/Uzlaşma Göstergesi): Buradaki ana IOC IP adresi 45.128.232.67 'dir. IOC yalnızca IP adresi ile sınırlı değildir. Saldırgan altyapısına ait URL'ler, domain isimleri veya zararlı dosya hash'leri de IOC olarak değerlendirilebilir.

CTI (Cyber Threat Intelligence): IP adresinin Hollanda da bulunması bir veri niteliği taşır ve tek başına tehdit unsuru barındırmaz. Bu IP'nin geçmişte zararlı yazılım dağıtımı ve C2

(Command and Control) altyapısı olarak kullanıldığına dair güvenlik raporları bulunması, bu veriyi tehdiye dönüştürür.

MISP: MISP tehdit bilgisini herkes için erken uyarıya çevirir. Olurda bu IP yeni bir Fidyeye cüzdanında kullanıldığı MISP de paylaşılsa güvenlik ekiplerinin bu tehdidi erken aşamada fark etmesini sağlar. Bu erken fark edilme durumu Blue Team ekiplerinin firewall ve SIEM sistemlerine bu IOC'yi ekleyerek önlem almasını sağlar. Böylece fidye yazılımının daha çok yayılması engellenmiş olur.

3. Adım: Karar ve Aksiyon

Karar: Engelle

Gerekçe: Yapılan CTI analizi sonucunda 45.128.232.67 IP adresinin geçmişte phishing ve zararlı yazılım dağıtımı ile ilişkilendirildiği ve C2 altyapısı olarak kullanıldığına dair bulgular bulunmuştur. Bu IP ile ağıımız arasında kurulabilecek herhangi bir iletişim, sistemlerimizde uzaktan komut çalıştırma ve veri sızdırma riskleri oluşturabileceğinden, engellenmesi uygun görülmüştür.

BÖLÜM D

1. Senaryo: Fidyeye Yazılım (Ransomware) Saldırısı

Acil Müdahale

- 1) Etkilenen bilgisayarın ethernet kablosunu çıkarıp Wi-Fi bağlantısını kapatırdım. Böylece fidye yazılımının ağda yayılmasını engellerdim.
- 2) Bilgisayarı kapatmak yerine kullanıcı etkileşimini durdururdum. RAM deki önemli verilerin kaybolmasını engellerdim.
- 3) Çalıştığım ekibi bilgilendirir ve benzer olay yaşayan sistemlere bakardım.

Analiz

İlk bakacağım log Mail logları olur. Phishing ile şüpheli ek veya link varmı kontrol ederim. Sonrasında EDR loglarına bakarım. Şüpheli bir uygulama çalıştırma var mı bakarım. Firewall loglarına da bakarım. Şüpheli bir IP veya C2 bağlantısı kurulmuş mu kontrol ederim.

2. Senaryo: Phishing (Oltalama) E-Postası Analizi

Teknik İnceleme: İlk önce gelen mailin içeriğine bakıp sosyal mühendislik dili kullanılmış mı (acil, hemen, gizli vb.) bakarım. Sonra gönderici IP'ye bakar ve gerçek domain üzerinden mi gönderilmiş teyit ederim. URL yapısını kontrol eder ve kısaltılmış link, sahte domain, HTTPS taklidi var mı incelerim.

Önlem: Email Gateway üzerinde ilgili domain, IP ve URL için engelleme kuralı yazarım. SIEM'e IOC ekler, aynı e-postayı alan diğer kullanıcıları tespit ederim.

3. Süreç ve İletişim

Standartlar: Ben olay müdahale sürecimi NIST'e dayandırırım:

Hazırlık → Tespit → Sınırlama → Temizleme → Kurtarma

Herşey sıralı ve ne yapacağım bellidir. Böylece paniğim azalır.

Kriz İletişimi: Yönetimi teknik detay boğmadan, net risk ve etkiyle bilgilendiririm. Ekibe durum kontrol altında, şu adımdayız, şunu yapıyoruz mesajı verir ve paniği azaltırım.

4. Vizyon: Güncel Kalma Sanatı

Kendimi güncel tutmak için teknik zafiyetleri NVD üzerinden, pratik tehdit istihbaratını VirusTotal üzerinden, sektörel gelişmeleri ise çoğunlukla güvenlik araştırmacılarının paylaşımlarıyla takip ederim.