Hafta 1 : Dijital Savaş Alanı ve CTI (Tehdit İstihbaratı)

Görev 1 : Gölge Analist Raporu

Bölüm A : Savunma Mimarisi ve Teknoloji Entegrasyonu

1. Ağ ve Çevre Güvenliği (Sınır Hattı)

- Firewall & IDS/IPS: Kapıdaki kilit (Firewall) ile harekete duyarlı alarm (IDS/IPS) arasındaki farkı ve iş birliğini açıklayın. Biri engellerken diğeri neden sadece izler ?

Firewall 'u bir bodyguard gibi düşünelim. Sadece izin verilen tipteki insanları(IP/PORT) içeriye alıyor . Ama kapıda kıyafeti tamemen uyan ama cebinde bıçak ,silah...(Payload ve Zararlı Yazılım) taşıyan insanlar da var ve bunları gizledikleri için göremiyor ve içeriye alıyor . Burada devreye güvenlik kameralarımız devreye giriyor yani IDS . IDS ise içeriye giren insanların içlerine bakıyor yani izliyor ve eğer bir şey görürse sadece alarm çaldırıyor (yani Log/Alarm üretiyor.). Ama dikkat edelim ,herhangi bir müdahalede bulunmuyor. Neden ? Eğer ki sorun olduğu durumda tüm girişleri durdurursa şirkette büyük bir problem çıkabilir. Bu yüzden sadece uyarıyor . Yani gerisini şirket sorumlusuna bırakıyor. IPS ise IDS 'den gelen bilgiye göre zararlı kişiyi durduran / engelleyen bir özel timdir. Sorumluluğu büyüktür. Müdahale hızlı olmak zorundadır . Bu da kendi içnde bir risk barındırır . Yanlış bir müdahale tüm alımları durdurabilir ya da doğru ifadeyle tüm şirketin internetini kesebilir.

- NDR (Network Detection and Response): Trafik şifreli olsa bile veya Firewall atlatılsa bile, NDR ağ içindeki anormallikleri (Örn: Yan ağa sıçrama) nasıl yakalar ?

NDR , hani bazı insanlar vardır ben insanın içinin kötü olup olmadığını yürüyüşünden bile tanırım diyen tiptir. NDR biraz farklı çalışır , normalde şirket bilgisayarında x kişisine veriler sürekli parça parça geliyodur. Bir gece aniden dışarıda bilinmeyen bir IP' ye gitmeye başlarsa NDR alarm verir .Çünkü bu sıradışı bir şeydir. Bazen ise işlemlerin sıklığından anlar .Mesela şirket cihazından sürekli belirli aralıklarla şifreli bir paket gidiyor. BUnun bir Heartbeat sinyali olduğunu anlar.Bazen ise şifreli bağlantı kurulurken handshake olayından anlar . Çünkü her uygulamanın handshake'i farklıdır. Firewall (internet-şirket içi) iken NDR (Bilgisayar A -Sunucu B) trafiğini izler. X çalışanın bilgisayarı sadece yazıcı ve M sunucusuyla konuşuyo olsun aniden Yazılım Ekibinin Veritabanı Sunucusuna RDP (Uzak Masaüstü) veya SSH yapmaya çalışıyor ise NDR burada anormalilik olduğu söyler ve yakalar.

2. Uç Nokta Savunması (Son Kale)

- Antivirüs vs EDR: Klasik bir Antivirüs imza tabanlı çalışırken, EDR (Endpoint Detection and Response) davranışsal olarak nasıl fark yaratır? "Dosyasız saldırıları" (Fileless Malware) hangisi yakalar ?

Antivirüs' ü bir suçlunun parmak izine benzetelim . Parmak izlerimiz burada hash oluyor . Eğer sistemde parmak izi varsa bu içeriye alınmıyor. Ama şöyle bir durum var: Parmak izlerimiz hafif bir deforme olduğu zaman sistem okuyamıyor ve içeri rahatça girebiliyoruz. Yani zararlı yazılım kodunda tek bir virgül bile değiştirse içeri girebliyor. Burada devreye EDR sistemi giriyor .EDR , bir sivil dedektif çünkü sistemde herhangi bir anomali bir davranış

olduğu zaman onu engelliyor veya öldürüyor . Onun haricinde suçlunun sisteme nereden , ne zaman , nasıl girdiğini ve neler yaptığını listeliyor. Eğer ki sorunun yanıtına gelecek olursak "Dosyasız Saldırıları " (Fileless Malware) EDR tarafından durdurulur. Neden ? Çünkü Çünkü Fileless Malware (Dosyasız Zararlı), sabit diske .exe gibi bir dosya olarak kaydedilmez. Doğrudan RAM'e (Hafıza) yerleşir ve Windows'un kendi araçlarını (PowerShell, WMI) kullanır. Antivirüs tarayacak bir dosya bulamadığı için "Temiz" raporu verir.

EDR Yakalar: EDR, RAM'i ve çalışan süreçleri (Process) izler. Saldırgan, dosya indirmeden PowerShell üzerinden bir kod çalıştırdığında, EDR "PowerShell'in bu komutu çalıştırması normal değil" diyerek davranışı tespit eder.

3. Operasyon Merkezi ve Görünürlük (Beyin Takımı)

- SOC & SIEM: Firewall, EDR ve Sunuculardan gelen binlerce log (kayıt), SIEM üzerinde nasıl anlamlı bir alarma dönüşür? SOC analisti bu ekranda ne görür ?

Saniyede firewall 500 log , EDR 200 log ,sunucular ise 300 log üretiyor olsun . Bu bir günde milyonlarca satır yazı demek . Bunu bir yapboz gibi düşünelim. SİEM bu yapbozları ilk önce anlaşılan tek bir dile (yani örnek vereyim Windows sunucusu başarısız (IP)sözcüğünü x diye kodlasın , linux y , firewall m . SİEM tüm tanımlamaları gördüğü zaman bu sözcük(IP) m dir diyor.) çevirip bir senaryo oluşturuyor. Buna ilişkilendirme (correlation) da denir. Bir senaryoda dışarıdan bir IP şirketin VPN kapısını zorluyor. Aynı IP 1 dakikada 50 başarısız yanlış şifre girişi yapıyor 51.de açılıyor ve sonrasında cmd.exe çalıştırılıyor olsun. SİEM buna şöyle yorum yapıyor : BRUTE FORCE !!! saldırgan içeride . SOC analisti ekranda : “Alarm düştüğünde ekranda şunları görür:

Olayın Adı: “Successful Brute Force Attack followed by Suspicious Process” (Kırmızı ve yanıp sönen bir başlık).

Önem Derecesi (Severity): Critical / High.

Saldırgan (Attacker): 192.168.1.50 (Rusya IP’si).

Kurban (Victim): Muhasebe Sunucusu (Ahmet kullanıcısı).

Zaman Çizelgesi: Saldırı ne zaman başladı, ne zaman bitti?

Kanıtlar: Hangi loglar bu alarmı tetikledi? “ bunu görüyor. SOC analisti saldırı yapılan bilgisiyarın sahibine bilgi veriyor ve durumu öğrenip IP ‘yi engelliyor.

- SOAR: Tespit edilen bir tehdide (Örn: Phishing maili) insan müdahalesi olmadan otomatik cevap vermek (IP engellemek, kullanıcıyı izole etmek) için SOAR nasıl kullanılır ?

SİEM yangın sırasında itfayeyi arayan kişiyse SOAR ise gelen itfayecidir. SOAR temelinde akış şemaları yatan bir robottur .Diyelim ki SİEM bir mailde zararlı bir link olduğu konusunda alarm çalmış olsun , sonrasında SOAR devreye girer. API (Yazılımların birbiriyle konuşma dili) yardımıyla sırasıyla güvenlik limanlarına(Virustotal, Talos,Sandbox…) gönderip bilgi alır bir sıkıntı var mı diye ? Sorun yoksa kullanıcıya sorun olmadığına dair bir mail gönderir. Sorun varsa müdahale aşamasına geçer. Müdahale aşamasında sırasıyla :Mail Sunucusu (Exchange/O365) ile Konuşur:

“Bu zararlı mail, şirkette başka kime gitmiş? Ahmet’e, Ayşe’ye ve Mehmet’e. Hepsini bul ve Gelen Kutusundan Sil (Purge).” (Böylece kimse tıklayamaz).

Firewall ile Konuşur:

“Saldırganın IP adresini (1.2.3.4) engellenenler listesine ekle.”

Active Directory ile Konuşur:

“Bu maili açan kullanıcının şifresini Zorla Sıfırla ve hesabını geçici olarak kilitle.”

EDR ile Konuşur:

“Kullanıcı linke tıkladıysa, o bilgisayarı ağdan İzole Et (İnterneti kes, sadece benimle konuşabilsin).” En son ise kullanıcıyı sorun hakkında bilgilendirir ve sorunun giderildiğini söyler.

4. Genişletilmiş ve Yönetilen Hizmetler

- XDR (Extended Detection and Response): EDR sadece bilgisayara, NDR sadece ağa bakarken; XDR bu ikisini ve daha fazlasını (E-mail, Cloud) nasıl birleştirir ?

Bir şirket düşünelim XDR bu şirketin müdürüdür. EDR(Bilgisayar) , NDR(Ağ) , Email güvenliği , Cloud(Bulut) vb. ise şirket içinde çalışan depatmanlardır. Her departmandan farklı bilgiler gelir ve XDR bu gelen bilgileri yapay zeka yardımıyla birleştirir. Eğer gönderilen bilgiler belirli bir uyum içindeyse şüphelenir ve yöneticiye bildirir . Yönetici ise tek bir komutla örnek vereyim : "saldırıyı durdur" XDR 'ye yapması gerekeni söyler. XDR ise departmanlara gidip emirler yağdırarak durumu kontrol altına alır.

- MDR (Managed Detection and Response): Şirketin kendi SOC ekibi yoksa veya yetersizse, MDR hizmeti bu boşluğu
  insan kaynağı ve uzmanlık olarak nasıl doldurur ?

  Şirketimizde evet bir müdür (XDR) var ama diyelim ki şirket krize(saldırı) girdi bu durumda size danışması gereken(Ne yapmalıyım saldırı oluyor) kısımlar oldu ama siz ise

tatildesiniz . Bu durumda sizin şirketlerin kriz yönetimi konusunda uzman (SOC analistleri) olan kişileri tutuyorsunuz . başka bir açıklamayla ise sizin şirket sisteminiz koruyacak bir siber güvenlik uzmanı çalıştırmanız gerekiyor. Büyük bir şirketin sistemlerini koruyan 4-5 tane siber güvenlik uzmanı olur ve her birine düzenli olarak maaş vermek zorundasınızdır. Ama MDR(Nerede oladuğu farketmeksizin sizin sistemlerinizi 7/24 koruyan uzman siber güvenliklerden oluşan bir şirket sistemi) kullanırsanız bunu hem daha uyguna getirmiş oluyorsunuz hem de alanında uzman olan siber güvenlik uzmanlarından destek almış oluyorsunuz.

Bölüm B: Teknik Sözlük ve Kavram Avı

1. Temel Yapıtaşları ve Ağ

- Transistör & Bilgisayar: En temelden başlarsak; transistörlerin açılıp kapanması (0-1) ile modern işletim sistemlerinin çalışması arasındaki bağı nasıl kurarsınız ?

Transistörler, elektriği geçirip (1) veya keserek (0) bilgisayarın en temel dili olan ikili (binary) kodu fiziksel olarak oluşturur. Bu milyarlarca 0 ve 1, birleşip mantık kapılarını ve işlemci komutlarını oluşturarak en tepedeki İşletim Sistemi'nin senin tıklamalarını anlamasını sağlar.

- OSI vs TCP/IP: OSI modeli teorik bir referans iken, TCP/IP neden günümüz internetinin pratik temelidir ?

OSI modeli akademik ve detaylı bir harita olarak kalırken, TCP/IP daha az katmanlı ve esnek yapısıyla sahada çalışan ilk

protokol olduğu için standart savaşını kazandı. Yani OSI "nasıl olmalı"yı anlatır, TCP/IP ise "işin nasıl yapıldığını".

- Kriptografi: Veriyi şifrelemek neden sadece gizlilik için değil, aynı zamanda veri bütünlüğü (integrity) için de önemlidir ?

Şifreleme algoritmaları (özellikle Hashing ve Dijital İmza), veriye özel matematiksel bir "parmak izi" ekler; yolda verinin tek bir harfi bile değiştirilirse bu parmak izi uyuşmaz ve hile anında anlaşılır. Böylece sadece mesajın gizli kalmasını değil, aynı zamanda gönderildiği haliyle bozulmadan bize ulaştığını da garanti etmiş oluruz.

2. Saldırı Vektörleri (Offensive Terminology)

- Sosyal Mühendislik & Phishing: Bir sistemi hacklemek yerine insanı hacklemek (Social Engineering) neden daha kolaydır ?Phishing ve E-mail Spoofing arasındaki teknik fark nedir ?

- Milyon dolarlık güvenlik duvarlarında açık bulmak çok zordur ama insanların duyguları (korku, merak, güven) her zaman sömürülebilir ve "yaması olmayan" en zayıf halkadır. Bir şifreyi kırmak süper bilgisayarlarla yıllar sürebilirken, çalışanı kandırıp o şifreyi istemek sadece saniyeler alır.

- Phishing, seni kandırıp bilgilerini çalmayı amaçlayan saldırının (senaryonun) genel adıdır. Spoofing ise bu saldırıda inandırıcı olmak için gönderici kimliğini (örneğin "admin@google.com") teknik olarak taklit eden yöntemdir.

- Malware Dünyası: Genel bir terim olan Malware ile özel bir tehdit olan Ransomware (Fidye Yazılımı) arasındaki fark nedir ?

Malware, bilgisayara zarar veren tüm kötü amaçlı yazılımların (virüs, trojan, casus yazılım) genel adıdır**.** Ransomware ise bu ailenin, dosyalarını şifreleyip rehin alan ve geri vermek için para isteyen özel bir türüdür.

- Zero-Day (Sıfır Gün): Bir zafiyetin "Zero-Day" olarak adlandırılması, savunma tarafı için neden bir kabustur ?

"Zero-Day" denmesinin sebebi, geliştiricinin sorunu düzeltmek için sıfır günü (hiç vakti) olmasıdır; yani saldırgan açığı bulmuştur ama yama henüz yoktur. Savunma için kabustur çünkü ortada bir "ilaç" olmadığı için sistemler saldırıya tamamen açıktır ve güncelleme yapmak işe yaramaz.

3. Savunma Mekanizmaları (Defensive Terminology)

- Yama (Patch) Yönetimi: Güvenlik güncellemelerini (Patch) zamanında yapmamak ile Güvenlik Açığı (Vulnerability) oluşması arasında nasıl bir ilişki vardır ?

Yama yayınlandığı an o güvenlik açığı herkese ifşa olur ve saldırganlar için artık "bilinen bir hedef" (N-Day) haline gelir. Güncellemeyi yapmamak, kilidi bozuk bir kapıda "Burada Hata Var" tabelasıyla oturmak gibidir; saldırı kaçınılmaz olur.

- Kimlik ve Erişim: Parola neden yetmez ? İki Faktörlü Kimlik Doğrulama (2FA) güvenliği matematiksel olarak nasıl artırır ?

Parolalar statik ve çalınabilir oldukları için "Tek Nokta Hatası" (Single Point of Failure) yaratır; biri ele geçirildiğinde kapı sonuna kadar açılır. 2FA ise güvenliği toplama işlemiyle değil çarpma işlemiyle artırır; saldırganın hem şifreni bilme olasılığı (p1) hem de telefonuna fiziksel erişim olasılığı (p2) birleştiğinde, kırılma riski (p1*p2) matematiksel olarak neredeyse imkansız hale gelir.

- Tünelleme ve Gizlilik: VPN (Sanal Özel Ağ) kullanmak bizi internette tamamen görünmez yapar mı, yoksa sadece tünel mi oluşturur ?SSL/TLS protokolü bu tünelin neresindedir ?

VPN bizi tamamen görünmez yapmaz, sadece trafiğimizi şifreli bir tünelden geçirerek servis sağlayıcımızdan (ISP) saklar ama VPN sağlayıcısı her şeyi görebilir. SSL/TLS ise bu tünelin içindeki veriyi ayrıca şifreleyen ikinci bir zırh gibidir; yani VPN tünelin dış duvarıysa, SSL/TLS içindeki çelik kasadır.

4. Standartlar ve Süreçler

- Zafiyet Taraması: Ağ zafiyet taraması yapmak ile Sızma Testi (Pentest) yapmak arasındaki temel fark nedir? (Biri otomatik, biri manuel mi ?)

Zafiyet taraması, sistemdeki olası açıkların röntgenini çeken ve sadece "burada sorun olabilir" diyen otomatik bir işlemdir. Pentest ise bu açıkları gerçekten sömürerek (exploit) sisteme sızan ve riskin boyutunu kanıtlayan manuel bir saldırı simülasyonudur.

- Regülasyonlar: ISO 27001, NIST veya GDPR gibi standartlar teknik birer araç mıdır, yoksa bir yönetim anlayışı mıdır ? Bir mühendis neden bunları bilmelidir ?

Bu standartlar teknik birer araç değil, güvenliğin sürdürülebilir olması için kuralları koyan stratejik bir yönetim çerçevesidir (Framework). Bir mühendis bunları bilmelidir çünkü yazdığı kodun veya kurduğu sistemin yasalara (GDPR) uygun olması, teknik olarak çalışmasından çok daha kritiktir.

Bölüm C: CTI ve İstihbarat Odaklı Vaka Analizi

- Senaryo: SOC ekibindeki nöbetiniz sırasında, sorumluluğunuzdaki kritik bir sunucunun 45.128.232.67 IP adresi ile şüpheli bir trafik oluşturduğunu tespit ettiniz.

  🚨 Kritik Kural (OpSec): Şüpheli IP adresiyle ASLA doğrudan etkileşime girmeyin (Ping atmayın, tarayıcıda açmayın). Bu, saldırganı uyarabilir.

1. Adım: Pasif İstihbarat Toplama (CTI)

- Kimlik Tespiti: Bu IP adresi hangi ülkeye ve hangi organizasyona (ISP/ASN) aittir ?

Pasif bilgi toplama araçlarına (Whois, RIPE) göre bu IP adresi Hollanda lokasyonlu görünmektedir. Ağ sahipliği (ASN) ise saldırganların gizlenmek için sıkça tercih ettiği " IE-Anton-Levin " firmasına aittir.

- Sicil Kaydı: Bu IP daha önce hangi saldırı türleriyle (Brute Force, Phishing, Port Scan vb.) veya hangi zararlı yazılım aileleriyle (Malware Families) ilişkilendirilmiş ?

Bu IP, özellikle SSH Brute Force (kaba kuvvet ile şifre kırma) saldırıları yapmasıyla tanınan sabıkalı bir adres. Ayrıca

BitDefender ve G-Data gibi otoriteler, bu kaynağı Phishing (oltalama) ve genel Malware (zararlı yazılım) dağıtıcısı olarak işaretlemiş.

2. Adım: Terminoloji ve Yapılandırma (Applied Concepts)

- IOC (Indicator of Compromise): Bu senaryodaki "IOC" tam olarak nedir? Sadece IP adresi midir, yoksa URL veya dosya hash'i de olabilir mi ? Bu vakadaki IOC verisini teknik bir formatta yazın.

IOC (Indicator of Compromise), bir saldırıdan geriye kalan dijital parmak izleridir ve bu senaryoda gördüğümüz gibi sadece IP adresi değil, URL, dosya özeti (Hash) veya alan adı da birer IOC olabilir.

Açıklama: SOC analisti olarak rapor yazarken veya ekip arkadaşlarımıza bilgi verirken asla tıklanabilir link (http://...) paylaşamayız. Yanlışlıkla biri tıklar ve şirketi saldırgan bizi hackleyebilir .Çünkü zararlı yazılım tarayıcımız tıkladığımız zaman otomatik olarak çalıştırılır.

Bunun yerine "Defanging" (Zararsızlaştırma) tekniğini kullanırız:

http yerine hxxp yazarız.

. (nokta) yerine [.] yazarız.Yani:

IP Adresi: 45[.]128[.]232[.]67

URL: hxxp://45[.]128[.]232[.]67/

Tehdit Türü: Phishing, Malware, SSH Brute Force

- CTI (Cyber Threat Intelligence): Sadece "IP adresi Rusya'da" demek bir Veri (Data)'dir. Bunu İstihbarat (Intelligence)'a dönüştüren şey nedir ? Bu IP'nin

şirketiniz için neden tehdit oluşturduğunu "Bağlam" (Context) katarak açıklayın.

Veriyi istihbarata dönüştüren şey, o bilginin bizim sistemimizdeki hangi açığı hedef aldığını ve niyetini (Context) ortaya koymasıdır. Örneğin "IP Rusya'da" demek boş bir bilgiyken; "Bu IP, bizim kullandığımız VPN sürümündeki açığı sömüren bir fidye yazılımı çetesi" demek, aksiyon almamızı sağlayan gerçek bir istihbarattır.

- MISP (Malware Information Sharing Platform): Diyelim ki bu IP'nin yeni bir Fidye Yazılımı (Ransomware) yaydığını keşfettiniz. Bu bilgiyi MISP gibi bir platformda paylaşmak, diğer kurumların savunmasına (Mavi Takım) nasıl yardımcı olur ?

MISP'te paylaştığın an, diğer kurumların güvenlik sistemleri bu veriyi (IOC) otomatik olarak çekip kendi duvarlarına ekler. Böylece saldırgan henüz onlara ulaşmadan kapılar yüzüne kapanır.

3. Adım: Karar ve Aksiyon (Actionable Intelligence)

- Karar:

Tehdit istihbaratı kaynaklarınca 45.128.232.67 adresinin aktif bir SSH Brute Force ve Phishing kaynağı olduğu teyit edilmiştir. Risk eliminasyonu için bu IP'nin derhal Firewall üzerinde bloklanmasını ve hedef sunucuda geriye dönük başarılı giriş (log) analizi başlatılmasını onayınıza sunarım.

- Gerekçe: "VirusTotal skoru X olduğu için..." gibi basit değil, "Bu IP, Cobalt Strike C2 sunucusu olarak bilindiği ve sunucumuzla iletişim kurmaya çalıştığı için..." şeklinde teknik bir gerekçe sunun.

Söz konusu IP adresi, kurumumuzun dışa açık servislerine yönelik sistematik SSH Brute Force (Kaba Kuvvet) saldırıları gerçekleştirmekte ve global istihbarat verilerine göre Mirai Botnet altyapısının aktif bir düğümü olarak İlk Erişim (Initial Access) sağlamaya çalışmaktadır; bu nedenle ağımızda yatay hareket (Lateral Movement) riskini elimine etmek için engellenmesi elzemdir.

Bölüm D: Kriz Yönetimi ve Olay Müdahale Refleksleri

- 1. Senaryo: Fidye Yazılımı (Ransomware) Kıyameti Şirketin finans departmanından bir kullanıcı aradı ve "Ekranımda kırmızı bir kilit resmi var, dosyalarım açılmıyor" dedi. Bu bir fidye yazılımı saldırısıdır.
- Acil Müdahale: Panik yapmadan atacağınız ilk 3 teknik adım nedir? (İpucu: Fişi çekmek veri kaybına yol açabilir mi? Ağı izole etmek daha mı mantıklı?)

Fişi çekmek, RAM'deki delilleri (saldırganın parmak izlerini) yok ettiği için en büyük hatadır: Ben şöyle ilerlerim :

Sunucuyu kapatmadan sadece ağ bağlantısını keserim (sanal ise vSwitch'i kapatırım, fiziksel ise kabloyu çekerim) ki saldırgan dışarı çıkamasın ve deliller silinmesin. Sonrasında kurumsal güvenlik duvarında (Firewall) 45.128.232.67 adresini hem Inbound hem Outbound yönünde kalıcı olarak yasaklarım . Sistem hala çalışıyorken uçucu belleğin (RAM) ve aktif bağlantıların (Netstat) imajını alarak saldırının anlık fotoğrafını kaydederim.

- Analiz: Bu zararlının sisteme nasıl girdiğini bulmak için hangi loglara bakarsınız ?

Sisteme giriş kapısı genellikle kimlik doğrulama olduğu için öncelikle Linux'ta /var/log/auth.log (başarılı/başarısız girişler)

dosyasına bakardım. Eğer saldırı web üzerinden geldiyse, hangi dosyaların çağrıldığını görmek için web sunucusunun access.log kayıtlarını incelerdim.

- 2. Senaryo: Oltalama (Phishing) Dedektifliği CEO'dan geldiği iddia edilen "Acil Fatura Ödemesi" konulu şüpheli bir e-posta inceliyorsunuz.
- Teknik İnceleme: E-postanın sahte olduğunu kanıtlamak için hangi teknik parametrelere (Header analizi, Gönderici IP, URL yapısı vb.) bakarsınız ?

İlk iş olarak e-postanın "dijital imzası" olan SPF, DKIM ve DMARC kayıtlarının "Fail" (Başarısız) verip vermediğine bakarım; çünkü bu protokoller göndericinin taklit edilip edilmediğini matematiksel olarak kanıtlar. Ayrıca görünen gönderici adresiyle teknik Return-Path (yanıt adresi) uyuşmazlığı ve linklerin hedefi ile metni arasındaki farklar sahteciliğin en net teknik delilleridir.

- Önlem: Bu saldırının diğer çalışanlara ulaşmasını engellemek için hangi güvenlik cihazında (Email Gateway, Firewall vb.) kural yazarsınız ?

E-postanın kullanıcılara hiç ulaşmamasını sağlamak için ana müdahale noktası Secure Email Gateway (SEG) cihazıdır; burada gönderici (Sender), konu (Subject) veya zararlı dosya özetini (Hash) kara listeye eklerdim. Sonra ekstra güvenlik katmanı olarak, dışarıdan gelen bu IP trafiğini ağ seviyesinde tamamen kesmek için ise Firewall üzerinde de bir engelleme kuralı yazmak şarttır.

3. Süreç ve İletişim: "Mavi Takım" Ruhu

- Standartlar: Olay müdahale sürecinizi (Hazırlık -> Tespit -> Sınırlama -> Temizleme -> Kurtarma) hangi

uluslararası standarda (Örn: NIST veya ISO 27001) dayandırırsınız?

Yukarıdaki adımlar NIST SP 800-61 (Bilgisayar Güvenliği Olay Müdahale Rehberi) standardının adımlarıdır. ISO 27001 daha çok genel yönetim çatısını (ISMS) kurarken, NIST 800-61 olayın teknik olarak nasıl yönetileceğinin operasyonel kılavuzudur. Bu yüzden NIST SP 800-61 standardına dayandırırdım.

- Kriz İletişimi: Saldırı devam ederken yönetim sizden sürekli bilgi istiyor ve ortam çok gergin. Ekip içindeki paniği önlemek ve yönetimi doğru bilgilendirmek için nasıl bir iletişim stratejisi izlersiniz?

Teknik ekibi yönetim baskısından izole etmek için bir Kriz İletişim Sorumlusu (SPOC) atarım ve yönetime sadece bu kişi üzerinden, belirlenen periyotlarla (örn. her 30 dakikada bir) durumu özetleyen net "Durum Raporları" (SitRep) sunarım. Paniği engellemek için ise asla tahmini konuşmam; sadece doğrulanmış bulguları ve bunların iş süreçlerine etkisini (Business Impact) paylaşarak beklentiyi yönetirim.

4. Vizyon: Güncel Kalma Sanatı

Tuncay Erol , sausiber , candeger