CYBER KİLL CHAİN

Hazırlayan: Esra Akteke
Tarih: 07.02.2025

Giriş

Siber güvenlik giderek daha karmaşık hale gelen tehditlerle başa çıkmayı gerektiren bir alan haline gelmiştir. Bu bağlamda siber saldırıları anlamak, tespit etmek ve bunlara etkili bir şekilde müdahale etmek için stratejik araçlara ihtiyaç duyulmaktadır. Cyber Kill Chain ise bu noktada devreye giriyor. Bu raporun amacı Cyber Kill Chain modelinin ne olduğunu, siber saldırıların yaşam döngüsünü nasıl tanımladığını ve bu modeli kullanarak güvenlik operasyon merkezlerinin etkinliğini nasıl artırabileceklerini incelemektir.

Cyber Kill Chain (Siber Öldürme Zinciri) Nedir?

Cyber Kill Chain siber saldırıların bir hedefe ulaşmadan önce geçtiği aşamaları tanımlayan bir modeldir. Bu model saldırganların kullandığı teknikleri, yöntemleri ve adımları analiz ederek güvenlik ekiplerine saldırıların erken aşamalarında tespit ve müdahale etme imkanı sunuyor. Siber güvenlik savunmalarını güçlendirmek için proaktif bir yaklaşım sağlar. Her bir aşamanın anlaşılması güvenlik ekiplerinin potansiyel tehditleri daha etkili bir şekilde önleyebilmesi ve saldırılara karşı direnç geliştirebilmesi açısından büyük önem taşımaktadır.

Cyber Kill Chain Aşamaları

Cyber Kill Chain aşamaları bir siber saldırının her aşamasını sistematik olarak tanımlamaktadır. Bu aşamalar saldırganın hedefe ulaşmadan önce geçirdiği süreçleri anlamak ve her bir adımda müdahale ederek saldırıyı engellemek için kritik öneme sahiptir.

Keşif (Reconnaissance)

Siber Öldürme Zinciri'nin ilk aşaması saldırganın hedef sistem hakkında bilgi topladığı keşif sürecini tanımlar. Bu aşamanın temel amacı hedef sistemin savunma açıklarını belirlemek ve sızma yollarını keşfetmektir diyebiliriz. Saldırgan; hedefin IP adreslerini, çalışan bilgilerini, güvenlik yapılarını ve diğer kritik verileri toplayarak hedefin zayıf noktalarını analiz eder. Keşif aşaması genellikle iki farklı yöntemle gerçekleştirilir:

Aktif Keşif

Saldırgan, hedef sistemlerini tarar ve ağ yapılarını, açık portları, yazılım açıklıklarını ve diğer potansiyel zayıf noktaları tespit etmeye çalışır. Bu tür bilgi toplama genellikle hedefe doğrudan bağlanmayı gerektirir ve saldırganın izlerinin daha kolay fark edilmesine neden olabilir.

Pasif Keşif

Saldırgan bu keşif türünde hedef hakkında çevrimiçi kaynaklardan bilgi toplamaktadır. Bu kaynaklardan örnek vermek gerekirse halka açık web siteleri, sosyal medya hesapları, forumlar, Whois veritabanları ve daha fazlası yer alır. Pasif bilgi toplama saldırganın hedefin kimlik bilgilerini veya güvenlik önlemleri hakkında herhangi bir tespit olmadan bilgi edinmesini sağlar.

Siber Keşif

Siber keşif saldırganların hedefler hakkında bilgi toplamak için çeşitli stratejiler kullandığı bir süreçtir. Bu stratejiler arasında;

-**Sosyal mühendislik:** İnsanları manipüle ederek gizli bilgilere ulaşmayı amaçlayan psikolojik bir tekniktir. Bu strateji genellikle kullanıcıları kandırmak veya onları belirli bir şekilde davranmaya zorlamak için kullanılır.

-**Açık kaynak istihbaratı (OSINT**): İnternette yayımlanan kamuya açık verilerin toplanıp işlenmesiyle hedefe dair önemli bilgiler edinmeyi sağlamaktadır.

-**Sosyal medya platformları**: Kullanıcıların paylaştığı kişisel ve profesyonel bilgilerden faydalanarak daha fazla içgörü edinmeye olanak tanımaktadır. Bu da saldırganların hedefin güvenlik zayıflıklarını belirlemesine yardımcı olabilmektedir.

Silahlanma (Weaponization)

Silahlanma aşaması bir siber saldırının önemli bir parçasıdır ve saldırganın hedefe ulaşmak için kullanacağı zararlı araçları hazırladığı adımdır. Bu aşama saldırganın keşif sürecinde elde ettiği bilgiler ışığında hedefi daha kolay şekilde ihlal edebilmek amacıyla zararlı yazılımlar veya özel saldırı araçları oluşturmasına dayanıyor. Genellikle güvenlik açıkları kullanılarak sistemin güvenliğini aşabilen exploit'ler ve zararlı kodlar geliştirilir. Bu yazılımlar hedefin sistemine zarar vermek, saldırganın sisteme tam erişim sağlamasını ya da gizli verilere ulaşmasını sağlamak için özelleştirilir. Saldırgan hazırladığı araçları hedefe etkili şekilde ulaştırabilmek için bu yazılımları dikkatlice test eder ve çalışır duruma getirir.

En yaygın saldırı vektörleri şunlardır:

-Zayıf veya çalınmış kimlik bilgileri
-Uzaktan erişim servisleri (RDP, SSH, VPN'ler)
-Dikkatsiz çalışanlar
-İçeriden gelen saldırganlar
-Zayıf veya hiç olmayan şifreleme
-Sistem yanlış yapılandırmaları

Teslimat (Delivery)
Teslimat aşaması bir siber saldırının önemli bir sürecidir ve bu adımda saldırganın daha önce hazırladığı zararlı yazılım hedef sisteme iletilir. Bu aşama saldırının hedefine ulaşmasını sağlamak amacıyla kullanılan çeşitli yöntemleri içermektedir. Saldırgan, zararlı yazılımı hedefe iletmek için sosyal mühendislik tekniklerini, kötü amaçlı e-posta eklerini, USB cihazlarını, güvenli olmayan ağları veya diğer yolları kullanabilir. Burada ki amaç hedefin farkında olmadan zararlı yazılımı almasını ve sisteme yüklemesini sağlamaktır.

İstismar (Exploitation)
İstismar aşaması saldırganın hedef sisteme zarar vermek veya erişim sağlamak için güvenlik açıklarından yararlandığı aşamadır. Bu noktada saldırgan daha önce keşif aşamasında belirlediği zayıf noktaları kullanarak hedefin sistemindeki güvenlik açığını tetikliyor. Zararlı yazılımın çalışması için gerekli ortamın oluşturulmasını sağlar ve hedefin savunmasız kalan noktalarından faydalanarak sisteme izinsiz erişim sağlanır. Bu adımda saldırgan güvenlik duvarları, antivirüs yazılımları veya diğer savunma mekanizmalarını aşmak için çeşitli teknikler kullanabilir. Bu aşama için saldırganın hedefe ilk kez doğrudan zarar vermeye başladığı, güvenlik önlemleri geçersiz kılındığı ve genellikle daha fazla zarar vermek için kurulum aşamasına geçişin sağlandığı kritik bir adımdır diyebiliriz.

Kurulum (Installation)
Kurulum aşaması saldırganın zararlı yazılımını hedef sisteme yerleştirdiği ve sistem üzerinde kalıcı bir erişim sağlamayı amaçladığı süreçtir. Bu aşama saldırganın hedef sisteme tam anlamıyla entegre olarak sistemde izinsiz bir şekilde uzun süreli kontrol elde etmesine olanak tanıyor. Kurulum, zararlı yazılımın hedef sistemde çalışmaya devam etmesini sağlayacak şekilde tasarlanıyor. Böylece sistemin yeniden başlatılması, güncellenmesi veya başka değişiklikler yapılması durumunda bile saldırganın kontrolü devam edebilmektedir. Bu aşama için saldırganın uzaktan erişim kurma, sistem üzerinde sürekli işlem yapabilme ve hedefteki diğer aşamaları gerçekleştirebilme yeteneklerini güçlendiriyor demek mümkündür.

Komuta ve Kontrol (C2)
Komuta ve Kontrol aşaması saldırganın hedef sisteme uzaktan erişim sağladığı ve bu erişimi sürekli hale getirdiği kritik bir adımdır. Bu aşamada saldırgan hedef üzerinde tam kontrol kurabilmek için zararlı yazılım aracılığıyla bir iletişim kanalı oluşturur. Bu kanal saldırganın sisteme komutlar göndermesine ve elde ettiği bilgileri geri almasına olanak tanıyor. Genellikle gizlenmiş ve şifrelenmiş bağlantılar üzerinden yürütülen bu iletişim, saldırının tespit edilmesini zorlaştırmak için özel olarak tasarlanır. Bu aşama başarılı olduğunda saldırganın hedef üzerindeki etkisi kalıcı hale gelir ve daha sonraki kötü amaçlı eylemler için bir zemin hazırlanır diyebiliriz.

Hedefteki Eylem (Actions on Objectives)

Hedefteki Eylem aşaması saldırının nihai amacı olan operasyonların gerçekleştirildiği son aşamadır. Bu noktada saldırgan sisteme tam erişim sağladıktan sonra belirlediği hedefleri yerine getirir. Bu hedefler hassas verilerin çalınması, sistemlerin sabote edilmesi, hizmetlerin devre dışı bırakılması veya fidye yazılımı gibi saldırılarla sistemin tamamen kilitlenmesi gibi farklı eylemleri kapsayabilir. Saldırganın amacına bağlı olarak bu aşamada veri sızdırma, kimlik bilgilerini ele geçirme ya da kritik altyapılara zarar verme gibi farklı operasyonlar yürütülebilir.

Saldırının hangi aşamada olduğunu analiz etmek, güvenlik ekiplerinin etkili bir şekilde müdahale etmesini sağlamak için kritik öneme sahiptir. Aşamalar arasındaki ilerlemeyi tespit etmek genellikle farklı izleme ve analiz tekniklerinin kullanılmasıyla yapılır. Bu analiz için kullanılan bazı yöntemler mevcuttur.

Log Analizi

Sistem ve ağ cihazlarından gelen loglar saldırının hangi aşamada olduğunu anlamak için en önemli kaynaklardan biridir. Örneğin izleme alanında olan bir e-posta sunucusunda şüpheli bir e-posta teslimatı veya sistemde bir exploit aktivitesinin tespit edilmesi analiz edilerek hangi noktada olunduğu belirlenebilir.

İzleme ve Alarm Sistemleri

SIEM sistemleri saldırıların aşamalarını izlemek için kullanılıyor. Bu araçlar saldırıya dair anormallikleri ve belirli güvenlik açığı exploitlerini tespit ederek saldırının hangi aşamada olduğunu belirlemede yardımcı olmaktadır. Örnek vermem gerekirse bir exploit kodunun çalışması istismar aşamasını zararlı yazılımın sisteme kurulması ise kurulum aşamasını işaret eder diyebiliriz.

Ağ Trafiği Analizi

Şüpheli ağ trafiği saldırının hangi aşamada olduğunu belirlemede önemli bir göstergedir. Örneğin bir saldırganın komuta ve kontrol sunucusuyla iletişim kurmaya başladığı durum, bir ağ trafiği analiziyle tespit edilmektedir. Aynı şekilde hedef ağdaki anormal trafik veya bilinmeyen dışa veri sızdırma çabaları Actions on Objectives aşamasının göstergeleri olabilir. Aşama tespiti anlamında çok önemlidir.

Yazılım ve Sistem Tarama

Kurulum aşaması tespit edildiyse zararlı yazılımın sistemde nasıl yerleştiği ve ne tür yazılımlar çalıştığına dair bir tarama yapılabilir. Örnek vermem gerekirse eğer zararlı yazılım bir exploit veya başka bir zafiyetten faydalanıyorsa bu durum istismar aşamasının bir belirtisidir. Sistem taraması esnasında tespiti kaçınılmazdır.

Kök Neden Analizi (Root Cause Analysis)

Saldırının hangi aşamada olduğunu anlamanın en kesin yolu saldırının önceki aşamalarına dair bıraktığı kalıcı izlerdir diyebiliriz. Örnek vermem gerekirse, silahlandırma aşamasına veya teslimat aşamasına dair izler, loglar ve olaylar incelenerek geriye doğru bir analiz yapılabilir ve bununla birlikte tespit sağlanarak gerekli aksiyonlar alınabilir.

Her Hacker Bu Akışı Takip Eder mi?

Her hacker siber saldırı süreçlerinde Cyber Kill Chain akışını birebir takip etmek zorunda değildir. Bu model özellikle organize ve planlı saldırılarda yaygın bir referans çerçevesi olarak kullanılır ancak saldırganların yetenekleri, hedefleri ve stratejileri farklılık gösterdiği için tüm saldırılar bu aşamalara sadık kalmayabilir. Bazı saldırganlar doğrudan bir güvenlik açığını hedef alırken diğerleri keşif veya silahlandırma adımlarını atlayabilir.

Bu nedenle, Cyber Kill Chain modeli her saldırıyı kapsayan sabit bir şablon değil, saldırıları daha iyi analiz etmek ve savunma stratejileri geliştirmek için bir rehber olarak değerlendirilmelidir diyebiliriz.

Siber Saldırı Zincirinin Siber Güvenliğe Etkisi

Siber saldırıların nasıl planlandığını ve gerçekleştirildiğini anlamak siber güvenlik uzmanları için kritik bir avantaj sağlamaktadır. Bu bilgi güvenlik ekiplerinin potansiyel zayıf noktaları tespit etmesine ve bu açıkları etkili bir şekilde kapatmasına yardımcı oluyor. Aynı zamanda saldırının erken aşamalarında şüpheli aktiviteleri ve tehlike sinyallerini daha hızlı fark etmelerini mümkün kılıyor. Pek çok kurum güvenlik stratejilerini daha proaktif hale getirmek ve olay müdahale süreçlerini iyileştirmek için Cyber Kill Chain modelini benimsemektedir.

Sonuç

Cyber Kill Chain modeli siber saldırıların sistematik olarak anlaşılmasını sağlayarak siber güvenlik alanında önemli bir rehber işlevi görmektedir. Bu raporda Cyber Kill Chain kavramını öğrenmek ve siber saldırıların yaşam döngüsünü kavramak, güvenlik tehditlerine daha bilinçli bir yaklaşımla müdahale etme becerisi kazandırmak amaçlanmıştır. Her aşamanın derinlemesine incelenmesi, bir saldırının hangi noktada olduğunu tespit edebilme ve gerekli adımları hızla atma yeteneğini geliştirmiştir.

Özellikle SOC analistleri için bu modelin sunduğu stratejik bakış açısı olayları daha erken tespit etmeye ve saldırılara etkin bir şekilde müdahale etmeye olanak tanımaktadır. Cyber Kill Chain'in gerçek dünya saldırı senaryolarında proaktif savunma mekanizmalarını güçlendirdiği ve tehditlerle mücadelede sağlam bir temel oluşturduğu görülmüştür. Bu bilgi ve deneyim, hem bireysel hem de kurumsal savunma stratejilerine büyük katkılar sunmaktadır.

Kaynakça

https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu

https://berqnet.com/blog/cyber-kill-chain

https://bbsteknoloji.com/cyber-kill-chain-nedir /

https://www.fortinet.com/blog/industry-trends/get-the-skills-to-defeat-the-cyber-kill-chain

https://www.securefors.com/cyber-kill-chain-nedir/

https://www.netskope.com/security-defined/cyber-security-kill-chain

https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain

https://www.proofpoint.com/us/threat-reference/cyber-kill-chain