2025

CYBER KILL CHAIN

BİLGEHAN BAYRAK

07/02/2025

İçindekiler Tablosu

1. GİRİŞ

Siber saldırılar günümüzde giderek karmaşık hale gelmektedir. Siber güvenlik uzmanları, saldırıları tespit etmek ve önlemek amacıyla çeşitli metodolojiler geliştirmiştir. Bu metodolojilerden biri de Cyber Kill Chain olarak adlandırılan ve Lockheed Martin tarafından geliştirilen bir çerçevedir. Bu raporda, Cyber Kill Chain'in aşamaları detaylı olarak ele alınacak ve saldırılara karşı etkili savunma stratejileri incelenecektir.

2. CYBER KİLL CHAİN NEDİR?

Cyber Kill Chain, siber saldırıların genellikle belirli bir dizi aşamadan geçerek hedeflerine ulaşmaya çalıştığını belirten bir modeldir. Bu model, saldırganların saldırılarını planlama ve uygulama süreçlerini yedi aşama halinde tanımlar. Cyber Kill Chain, her bir aşamanın ayrı ayrı analiz edilmesi gerektiğini savunur, böylece her aşamada müdahale edilerek saldırıların erken safhada tespit edilmesi ve önlenmesi mümkün hale gelir. Bu model, siber güvenlik uzmanlarına saldırıları daha etkin şekilde engelleme ve savunma stratejilerini oluşturma imkânı tanır.

3. CYBER KİLL CHAİN AŞAMALARI

Cyber Kill Chain, siber saldırıları önceden tahmin etmek ve önlemek için her bir aşamanın izlenmesini teşvik eder. Saldırganlar, belirli teknikleri kullanarak bu aşamalarda ilerler, ancak her bir aşama, güvenlik savunmalarının müdahale etmesi için bir fırsat sunar. Bu aşamalar şunlardır:

a. Keşif (Reconnaissance)

Bu aşama, saldırganın hedef hakkında bilgi toplama sürecidir. Keşif aşamasında saldırgan, hedefin zayıf noktalarını ve olası güvenlik açıklarını keşfetmeye çalışır.

- **Açık Kaynak İstihbarat (OSINT)**: Saldırganlar, halka açık olan her türlü kaynaktan bilgi toplar. Sosyal medya, internet siteleri, forumlar ve şirket verileri bu kaynaklardan bazılarıdır.
- **Zafiyet Tarama**: Hedef sistem veya ağ üzerinde güvenlik zafiyetlerini tespit etmek için araçlar kullanılır. Bu araçlar, sistemdeki açık portları, yazılım güncellemeleri ve eski sürümleri araştırır.
- **Sosyal Mühendislik**: Saldırganlar, hedef kullanıcıları aldatmaya yönelik stratejiler geliştirebilir. Örneğin, çalışanlardan şifre bilgilerini almak için taktikler kullanılabilir.

b. Silahlanma (Weaponization)

Keşif aşamasında elde edilen bilgilerin ardından, saldırganlar saldırı için gerekli araçları hazırlarlar. Bu aşama, saldırının tasarımının oluşturulduğu aşamadır.

- **Kötü Amaçlı Yazılım**: Bu aşamada, hedef sistemi etkilemek için virüsler, trojanlar, worm'lar veya diğer zararlı yazılımlar oluşturulur.
- **Saldırı Vektörleri Seçimi**: Saldırganlar, hedefi en etkili şekilde saldırmak için uygun araç ve yöntemleri seçer. Bu, e-posta ekleri, kötü amaçlı linkler veya USB cihazları gibi araçlar olabilir.
- **Saldırı Kodları**: Saldırganlar, sistemin zayıf noktalarını istismar edebilecek şekilde özelleştirilmiş saldırı kodları hazırlarlar.

c. Teslimat (Delivery)

Saldırganlar, silahlandıkları zararlı yazılımları hedef sisteme teslim ederler. Bu aşama, saldırının başlatıldığı andır.

- **Kimlik Avı (Phishing) E-postaları**: Saldırganlar, hedefe sahte e-postalar gönderir ve bu e-postalar aracılığıyla zararlı yazılımları iletmeye çalışırlar. E-posta ekleri veya kötü amaçlı bağlantılar üzerinden hedeflerin tıklaması beklenir.
- **USB ve Diğer Fiziksel Cihazlar**: Birçok durumda saldırganlar, USB bellekler veya taşınabilir diskler gibi fiziksel cihazlarla zararlı yazılım gönderirler.
- **Web Siteleri ve Sosyal Mühendislik**: Saldırganlar, kullanıcıları tuzaklara düşürmek için sahte web siteleri kurabilir veya sosyal mühendislik teknikleri kullanarak zararlı yazılımı yayabilir.

d. İstismar (Exploitation)

Bu aşamada saldırganlar, hedef sistemdeki güvenlik açıklarından faydalanarak aktif bir saldırı başlatırlar.

- **Kötü Amaçlı Kod Çalıştırma**: Hedef sisteme ulaşan zararlı yazılım, sistemde çalıştırılır ve bu yazılım, zafiyetlerden faydalanarak hedefi kontrol altına alır.
- **Zafiyetlerin İstismarı**: Saldırganlar, sistemdeki güvenlik açıklarını keşfederek, bu zafiyetleri kullanarak sisteme erişim sağlarlar.
- **Güvenlik Mekanizmalarının Aşılması**: Kullanıcıların güvenlik mekanizmaları (şifreler, kimlik doğrulama) aşılabilir. Örneğin, parola kırma saldırıları veya güvenlik yazılımlarını atlatma yöntemleri uygulanabilir.

e. Yükleme (Installation)

Bu aşama, saldırganların sisteme sürekli erişim sağlamayı hedeflediği aşamadır.

- **Arka Kapı (Backdoor) Kurulumu**: Saldırganlar, hedef sisteme bir "arka kapı" yüklerler. Bu, sisteme herhangi bir zamanda yeniden erişim sağlamak için kullanılan bir yazılımdır.
- **Rootkit veya Trojan Yükleme**: Saldırganlar, hedef sistemin yönetici (root) haklarına sahip olabilmek için rootkit veya trojan gibi zararlı yazılımlar yükler.
- **Sürekli Erişim Mekanizmaları**: Saldırganlar, hedef sistemde kalıcı bir erişim sağlamak için çeşitli teknikler kullanarak bu erişimi sürdürebilecek mekanizmalar oluştururlar.

f. Komuta ve Kontrol (Command and Control - C2)

Bu aşamada, saldırganlar, hedef sistem üzerinde uzaktan kontrol sağlamak için bir iletişim kanalı kurarlar.

- **Komut Sunucusuna Bağlanma**: Saldırganlar, hedef sisteme zarar vermek veya veri çalmak için bir komut ve kontrol (C2) sunucusuna bağlanırlar. Bu sunucu, zararlı yazılımı yönetir ve talimatlar verir.
- **Veri Sızdırma**: Saldırganlar, hedef sistemden hassas verileri toplar ve sızdırmaya başlarlar. Bu veriler şifreler, kişisel bilgiler veya finansal veriler olabilir.
- **Sistem Manipülasyonu**: Saldırganlar, hedef sistemi değiştirebilir veya bozulmasına yol açacak manipülasyonlar yapabilir.

g. Hedef Gerçekleştirme (Actions on Objectives)

Saldırganlar, nihai hedeflerine ulaşmak için bu aşamada aksiyon alırlar.

- **Veri Hırsızlığı**: Saldırganlar, hedef sistemdeki hassas bilgileri çalarlar. Bu veriler, kullanıcı verileri, finansal bilgiler veya kurumsal sırlar olabilir.
- **Şifreleme Saldırıları (Ransomware)**: Saldırganlar, hedef sistemdeki dosyaları şifreler ve kullanıcıdan fidye talep ederler. Bu tür saldırılarda, verilerin geri alınabilmesi için ödeme yapılması istenir.
- **Sistem Zarar Verme**: Hedef sistemdeki kritik işlevleri bozarak, organizasyonların operasyonlarını aksatabilirler. Bu tür saldırılar, servis dışı bırakma (DoS) veya ransomware türünde olabilir.

4. CYBER KİLL CHAİN'İN ÖNEMİ

Cyber Kill Chain, siber güvenliğin daha proaktif bir yaklaşım gerektirdiğini vurgular. Bu model sayesinde, savunma ekipleri sadece bir saldırı gerçekleştiğinde yanıt vermek yerine, her aşamada aktif olarak saldırıyı engellemeye çalışabilirler. Böylece, bir saldırının önceden tespit edilmesi ve etkisiz hale getirilmesi sağlanır.

Sonuç olarak, Cyber Kill Chain sadece bir saldırının nasıl işlediğini anlamakla kalmaz, aynı zamanda siber güvenlik uzmanlarının her bir aşamayı hedefleyerek, sistemleri daha iyi korumalarına olanak tanır.

5. ALINABİLECEK ÖNLEMLER VE SAVUNMA STRATEJİLERİ

Cyber Kill Chain modeline karşı etkili savunma stratejileri, her aşamada saldırıları önleyici ve tespit edici önlemleri içermelidir. Aşağıda bu stratejiler detaylandırılmıştır:

a) Keşif Aşamasına Karşı Önlemler

Keşif aşaması, saldırganların hedef hakkında bilgi topladığı aşamadır. Bu aşama, genellikle açık kaynaklardan (OSINT) veya sosyal mühendislik tekniklerinden faydalanılarak yapılır.

Savunma Stratejileri:

- **OSINT Tarama Engelleme**: Organizasyonlar, dışarıya bilgi sızdıran unsurları tespit etmek için ağlarında aktif taramalar yapmalıdır. Ayrıca, kritik bilgilerin halka açık kaynaklardan toplanmasını engellemek için, şirket politikaları ve güvenlik protokolleri uygulanmalıdır.
- **Sosyal Mühendislik Saldırılarına Karşı Korunma**: Çalışanlar, phishing ve diğer sosyal mühendislik saldırıları konusunda eğitim almalıdır. Şirket içindeki hassas bilgiler, yalnızca yetkili kişilerle paylaşılmalıdır.
- **Güvenlik Duvarı ve SIEM Kullanımı**: Güvenlik duvarları, şüpheli trafiği engelleyerek dışarıdan yapılacak keşif girişimlerini sınırlayabilir. Ayrıca, SIEM sistemleri, ağda şüpheli aktiviteleri tespit edip gerçek zamanlı izleme yaparak erken uyarılar verir.

b) Silahlanma Aşamasına Karşı Önlemler

Bu aşama, saldırganın hedefi etkileyecek zararlı yazılımı hazırladığı aşamadır. Saldırganlar, hedefi etkili şekilde ele geçirmek için yazılım araçlarını oluşturur ve çoğu zaman özel saldırı vektörleri kullanırlar.

Savunma Stratejileri:

- **Zararlı Yazılım Analizi ve Tehdit İstihbaratı**: Şirketler, zararlı yazılımların örneklerini analiz ederek potansiyel tehditler hakkında bilgi edinmeli ve tehdit istihbaratına dayalı önlemler almalıdır. Bu, yeni tehditler ve saldırı tekniklerinin tespit edilmesine yardımcı olur.
- **Yazılım Yaması Yönetimi**: Yazılımın güvenlik açıklarını kapatmak için düzenli olarak güncellemeler ve yamalar yapılmalıdır. Güvenlik açıkları, saldırganların silahlanma aşamasında kullanabileceği araçlar haline gelebilir.
- **Şüpheli Dosya Ekleri ve Bağlantıların Otomatik Tarama**: E-posta ve diğer iletişim kanallarındaki şüpheli dosya ekleri, bağlantılar ve içerikler, otomatik güvenlik yazılımlarıyla taranmalı ve tehlikeli içerikler engellenmelidir.

c) Teslimat Aşamasına Karşı Önlemler

Saldırganlar, zararlı yazılımları bu aşamada hedef sisteme teslim ederler. Genellikle e-posta, web siteleri veya sosyal mühendislik teknikleri ile bu teslimat yapılır.

Savunma Stratejileri:

- **Kimlik Avı Saldırılarına Karşı Eğitim**: Çalışanlar, phishing ve sosyal mühendislik saldırılarına karşı eğitilmelidir. Onlara, şüpheli e-postaları tanımayı ve zararlı bağlantılara tıklamama konusunda rehberlik edilmelidir.
- **E-posta Güvenlik Filtreleri**: Güvenli e-posta filtreleme çözümleri, zararlı ekler ve bağlantılar içeren e-postaları engellemek için kullanılmalıdır.
- **Zararlı Web Sitelerinin Engellenmesi**: Güvenlik yazılımları, zararlı yazılımlar barındıran web sitelerinin ziyaret edilmesini engellemeli, ayrıca web proxy çözümleri ile trafiğin denetlenmesi sağlanmalıdır.

d) İstismar Aşamasına Karşı Önlemler

İstismar aşamasında, saldırganlar sistemdeki güvenlik açıklarından yararlanarak sisteme girmeye çalışırlar.

Savunma Stratejileri:

- **Gelişmiş Tehdit Algılama Sistemleri (IDS/IPS)**: Sistemler, anormal etkinlikleri tespit etmek için IDS ve IPS çözümleri ile donatılmalıdır. Bu sistemler, şüpheli davranışları analiz ederek girişimlere hızlıca tepki verir.
- **Proaktif Güvenlik Açığı Tarama**: Ağ ve sistemlerdeki güvenlik açıklarını düzenli olarak taramak ve yamalar yapmak, saldırganların istismar aşamasında kullanabileceği zafiyetlerin ortadan kaldırılmasına yardımcı olur.
- **En Az Yetki İlkesinin Uygulanması**: Kullanıcılar ve uygulamalara yalnızca gerekli olan en düşük erişim izinleri verilmelidir. Böylece, bir saldırgan sistemde yer alsa bile, daha fazla hasar veremeden tespit edilebilir.

e) Yükleme Aşamasına Karşı Önlemler

Bu aşamada, saldırganlar hedef sisteme zararlı yazılım yükleyerek sürekli erişim sağlamaya çalışırlar.

Savunma Stratejileri:

- **Anti-Virüs ve EDR Çözümleri**: Anti-virüs yazılımları ve EDR çözümleri, kötü amaçlı yazılımların otomatik olarak tespit edilmesini ve kaldırılmasını sağlar.
- **Kötü Amaçlı Yazılımların Otomatik Tespiti**: Sistemler, yüklenen zararlı yazılımları otomatik olarak tespit edip kaldıracak şekilde yapılandırılmalıdır.
- **Uygulama Beyaz Listeleme**: Kullanıcıların yalnızca yetkili ve güvenilir uygulamaları çalıştırmasına izin verilmesi, zararlı yazılımların sisteme yüklenmesini engeller.

f) Komuta ve Kontrol Aşamasına Karşı Önlemler

Saldırganlar, hedef sistemi uzaktan kontrol etmek için komut ve kontrol (C2) altyapılarını kullanırlar.

Savunma Stratejileri:

- **Anormal Trafik Akışları Tespiti**: SIEM sistemleri ve IDS/IPS çözümleri, ağda şüpheli ve anormal trafik akışlarını tespit ederek bu tür komut ve kontrol trafiğini engellemeye yardımcı olur.

- **Ağ Segmentasyonu ve Erişim Kontrolü**: Ağda segmentasyon yapılmalı ve her segment arasında erişim kontrolü sağlanmalıdır. Bu, saldırganın C2 altyapısına bağlanmasını zorlaştırır.
- **C2 Altyapılarının Engellenmesi**: Güvenlik duvarları ve ağ izleme araçları, bilinen komut ve kontrol sunucularına yapılan bağlantıları engellemeli ve trafik akışlarını analiz etmelidir.

g) Hedef Gerçekleştirme Aşamasına Karşı Önlemler

Son aşamada, saldırganlar hedeflerine ulaşır ve verileri çalar, sistemleri şifreler veya başka zararlı eylemler gerçekleştirir.

Savunma Stratejileri:

- **Veri Şifreleme**: Hassas veriler, şifreleme teknikleri ile korunmalıdır. Bu, verilerin çalınsa bile okunamaz hale gelmesini sağlar.
- **Sistem Yedekleme**: Düzenli olarak yedekleme yapılarak, saldırganların şifrelemesi veya silmesi durumunda veriler geri alınabilir.
- **İç Tehditlerin İzlenmesi**: İç kullanıcılar üzerinde izleme yaparak, şüpheli aktiviteleri tespit etmek ve anomalileri raporlamak, içeriden gelebilecek tehditlere karşı bir önlem almayı sağlar.

6. SONUÇ

Cyber Kill Chain modeli, siber saldırıları anlamak ve önlemek için güçlü bir çerçeve sunmaktadır. Bu model sayesinde güvenlik ekipleri, saldırıların her aşamasında önlem alarak tehditleri daha etkin bir şekilde yönetebilirler. Savunma stratejileri, saldırının keşif aşamasından nihai hedefine kadar her adımda uygulanarak saldırıların başarılı olma ihtimalini minimize eder. Güvenlik farkındalığı eğitimleri, tehdit istihbaratı ve gelişmiş güvenlik çözümleri, Cyber Kill Chain çerçevesinde uygulanabilecek en kritik önlemler arasındadır. Gelecekte siber tehditlerin daha karmaşık hale gelmesi beklenirken, proaktif savunma stratejileri her zamankinden daha önemli olacaktır.

7. KAYNAKÇA

1. https://chatgpt.com
2. https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu
3. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
4. https://socradar.io/using-cyber-kill-chain-for-threat-intelligence/

5. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-kill-chain/
6. https://www.proofpoint.com/us/threat-reference/cyber-kill-chain
7. https://attack.mitre.org/
8. https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html