

**Cyber Kill Chain**

**Hazırlayan:** Hilal ŞAHİN

**Tarih:** Şubat 2025

1. **Giriş**

Siber saldırıların nasıl gerçekleştiğini anlamak ve bunlara karşı alınan savunma stratejilerinde **Cyber Kill Chain** önemli bir rol oynar. Siber saldırı aşamalarını sistematik bir şekilde açıklar. Saldırganların saldırıyı başlatmasından, hedefe ulaşana kadar geçen süreci ayrıntılı olarak ele alır. Saldırı aşamasında alınan tedbirleri belirlemeye yardımcı olur. Bu rapor, **Cyber Kill Chain** modelini ele alarak, siber saldırıların detaylarını inceleyecek ve modelin her aşamasına yönelik savunma stratejilerini açıklayacaktır. Amacımız, organizasyonların etkili siber güvenlik çözümleri geliştirmesine katkı sağlamaktır.

1. **Ana Bölümler**

Bu raporda, **Cyber Kill Chain** modeli detaylı bir şekilde ele alınacaktır. Siber saldırıların aşamalarını anlamak ve bu aşamalara karşı alınabilecek savunma stratejilerini belirlemek adına modelin temel yapısı incelenecektir. **Cyber Kill Chain,** saldırganların saldırıyı başlatmasından hedefe ulaşana kadar geçen süreci açıklamakta ve her aşamada uygulanabilecek savunma yöntemlerini belirlemeye yardımcı olmaktadır. Rapor kapsamında, **Cyber Kill Chain** modelinin aşamaları detaylandırılacak ve organizasyonların siber tehditlere karşı nasıl savunma sağlayabileceği analiz edilecektir.

1. **Cyber Kill Chain Nedir?**

Siber saldırıları analiz edebilmek için çeşitli modellerden birisi olan ve Locheed Martin firması tarafından geliştirilen Cyber Kill Chain, keşif aşamasından saldırı aşamasına kadar tanımlayan ve bu saldırıyı gerçekleştirmek veya önlemek amacıyla oluşturulan 7 aşamalı bir modeldir.

Cyber Kill Chain, siber saldırılarının çeşitli aşamalarını belirleyerek çalışır. Her aşama, saldırı yapan kişinin belirli bir hedefe ulaşmak için gerçekleştirdiği adımları temsil etmektedir. Yapılan saldırının aşamalarını anlamak için, savunma ekiplerinin saldırganı erken tespit edip saldırıyı engellemesine yardımcı olur. Kısaca Cyber Kill Chain’in temel amacı, saldırganın faaliyetlerini erken aşamalarda durdurarak saldırının tamamlanmasını önlemektir.



**Şekil 1** Cyber Kill Chain adımları

* 1. **Cyber Kill Chain Aşamaları** 
     1. **Reconnaissance**

Saldırı yapılmadan önce keşif ve bilgi toplama aşamasıdır. Saldırı yapan taraf; hedef sistem ve sistem üzerinde çeşitli taramalar yaparak zafiyetleri tespit etmeye çalışır. Çalışanların isimleri, ip adresleri, görevleri, e-mail adresleri gibi eylemleri aktif ve pasif bilgi toplama araçlarıyla yapar. Sosyal medya hesaplarından (iş ilanları, linkedln, facebook, X, instagram gibi) hedef hakkında sosyal mühendislik yöntemleri ile bilgiler toplar.

* + - 1. **Pasif Bilgi Toplama**

Hedef ile direkt olarak temasa geçmeden bilgi toplama işidir.

* + - 1. **Aktif Bilgi Toplama**

Hedefe direkt olarak temasa geçerek bilgi toplar.

* + 1. **Weaponization**

Keşif yaparken bulunan zafiyetlerin sömürülmesi için kullanılan yöntemleri belirlemesi ve uygun araçları hazırlama olarak tanımlanan aşamadır. Bu aşama zafiyete uygun exploitler, zafiyetin istismar edilmesi için kullanılabilecek payloadlar olabileceği gibi zararlı dosyalar ve dökümanlar, oltalama saldırısında kullanılabilecek sahte epostalar gibi birçok yöntem kullanılarak sızma işlemi yapılır.

* + 1. **Delivery**

Hazırlanmış olan zararlının ve belirlenmiş yöntemin hedefe ulaşmasıdır. Açık kaynak kodlu yazılımlar, sosyal networkler, phishing gibi yöntemler kullanılabileceği gibi, güvenlik çalışanların sosyal mühendisliklere veya phising saldırılarına karşı farkındalıkları, çalışanların hangi donanımların kurum ağına bağlanabileceği veya bağlanamadığı konusunda bilgilendirilmesi, bilinen zararlı web sitesinin erişim bloklarını kontrol edilmesi bu aşamayı önler.

* + 1. **Exploitation**

Oluşan zararlı ve belirlenen atak vektörünü kullanarak hedefin zafiyetinin sömürüldüğü aşamadır. Exploit hazırlanıp hedefe iletildikten sonra bu aşama, zararlı kodu çalıştırır. bunu önlemek amacıyla yazılımlar ne sıklıkla güncellendiği, sistemdeki zafiyetlerin tespit edilmesi için güvenlik denetimlerinin yapılıp yapılmadığını kontrol eder.

* + 1. **Installation**

Hedef sömürüldükten sonra, kalıcı bir tehdit oluşturmak amacıyla, güvenlik sisteminin ötesinde sistemin başarılı bir şekilde kontrol edilmesi sağlanır. Bu aşamada, zararlı yazılımın sistemde kalacağı süreyi mümkün olduğunca uzatmak hedeflenir.

* + 1. **Command and Control**

Sisteme yerleşen zararlının çalışmasını uzaktan kontrol eden ve sistemin ele geçirildiği aşamadır. Saldırıyı engelleyen firewall ve IPS'in devrede olup olmadığı, iyi bir şekilde konfigüre edilip edilmediği ve güvenlik cihazlarının monitör edilebilirliği, bu aşamanın aksamasını engellemek adına önemli unsurlardır.

* + 1. **Actions on Objectives**

Bütün aşamalar gerçekleştirildikten sonra saldırgan, kuruma erişim sağlar. Bu aşamada, veri değiştirme, veri çalma, silme, şifreleme ve sisteme zarar verme gibi eylemler gerçekleştirilir. Önlem olarak, iç ağdan dışarıya yapılan veri akışının sınıflandırılması ve sadece bilinen sunuculara veri akışının sağlanması durumunda saldırı engellenebilir. Ayrıca, bu süre boyunca tehdit altındaki verilerin yedeklerinin önceden alınması ve bir sistem devre dışı kaldığında hizmet verebilecek yedek sistemlerin bulunması, saldırının etkilerini azaltmaya yardımcı olur.

1. **Sonuç**

Cyber Kill Chain modeli, siber saldırıların aşamalarını sistematik bir şekilde analiz ederek, organizasyonların saldırılara karşı daha etkili savunma stratejileri geliştirmesine yardımcı olmaktadır. Modelin sunduğu çerçeve sayesinde, saldırı süreci keşif aşamasından başlayarak, hedef sistemin ele geçirilmesine kadar detaylı bir şekilde incelenmektedir. Bu raporda, Cyber Kill Chain’in yedi aşaması ele alınmış ve her aşamaya karşı uygulanabilecek güvenlik önlemleri açıklanmıştır. Reconnaissance (Keşif) aşamasında saldırganların hedef hakkında bilgi toplama süreçleri değerlendirilmiş, Weaponization (Silahlandırma) ve Delivery (Teslimat) aşamalarında saldırı yöntemlerinin belirlenmesi ve zararlı yazılımın hedefe ulaştırılması incelenmiştir. Exploitation (Sömürü) ve Installation (Kurulum) aşamalarında, saldırganların hedef sistem üzerindeki kontrollerini güçlendirme yöntemleri tartışılmıştır. Command and Control (Komuta ve Kontrol) ile Actions on Objectives (Hedef Üzerinde Eylemler) aşamalarında ise saldırganların sistem üzerindeki yetkilerini nasıl kullandıkları ve olası etkileri değerlendirilmiştir.

Sonuç olarak, Cyber Kill Chain modeli, siber güvenlik uzmanlarının saldırıların her aşamasını daha iyi anlamalarına ve saldırıları erken tespit edip önlemelerine yardımcı olmaktadır. Organizasyonların güvenlik önlemlerini bu modele uygun şekilde belirlemesi, siber tehditlere karşı daha güçlü bir savunma oluşturmasını sağlayacaktır. Özellikle, keşif aşamasında proaktif güvenlik önlemleri almak, zararlı yazılımların sistemlere bulaşmasını önlemek ve saldırganların hedeflerine ulaşmasını engellemek için etkin bir güvenlik stratejisi oluşturmak kritik öneme sahiptir.

Bu bağlamda, Cyber Kill Chain modelinin siber güvenlikteki önemi göz önüne alındığında, kurumların saldırı öncesi, saldırı sırasında ve sonrasında uygulayabilecekleri güvenlik politikalarını sürekli olarak güncellemeleri ve geliştirmeleri gerekmektedir.

1. **Kaynakça**

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

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