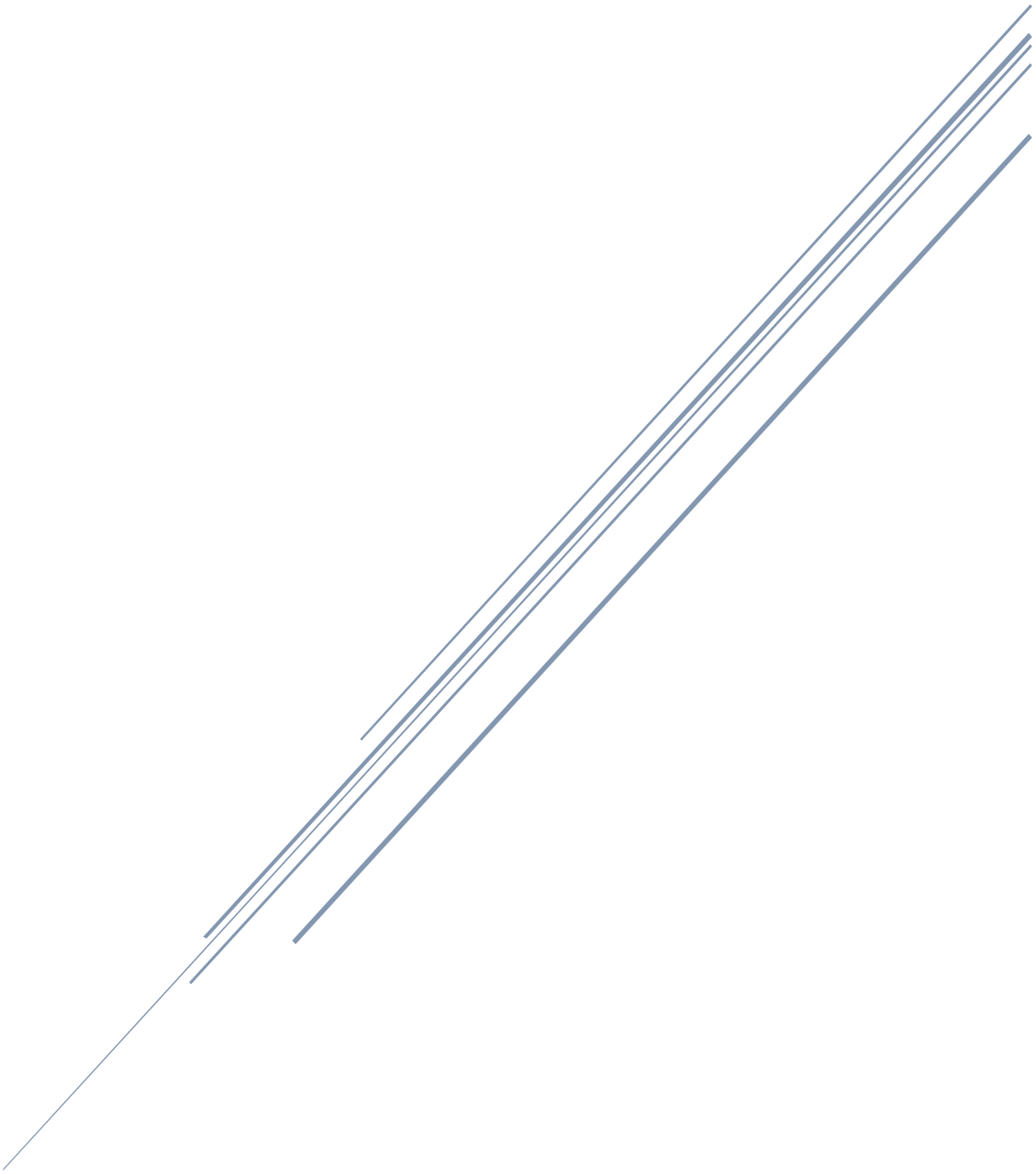
Cyber Kill Chain

Hazırlayan: Sinan Kocagöz

Tarih: 07.02.2025



İçindekiler

1. Giriş

Siber güvenlik tehditleri günümüzde hızla artmakta ve saldırganlar giderek daha sofistike yöntemler geliştirmektedir. Bunlardan biri de Cyber Kill Chain olarak adlandırılır.
Cyber Kill Chain, 2011 yılında Lockheed Martin tarafından geliştirilen ve keşif aşamasından saldırı aşamasına kadar tanımlayan ve bu saldırıyı gerçekleştirmek veya önlemek amacıyla oluşturulan 7 aşamalı bir modeldir. Bu model, saldırıların nasıl gerçekleştirildiğini anlamaya yardımcı olurken aynı zamanda savunma stratejilerinin geliştirilmesine de katkı sağlar. Cyber Kill Chain, saldırı sürecini adım adım açıklayarak güvenlik ekiplerine erken müdahale etme fırsatı sunmaktadır.

Bu raporda, Cyber Kill Chain modeli ayrıntılı bir şekilde incelenecek ve siber güvenlik süreçlerindeki önemi ele alınacaktır. Raporda ayrıca, Cyber Kill Chain modelinin avantajları ve sınırlamaları incelenecek, siber saldırılara karşı nasıl etkili bir savunma sağlayabileceğimizi anlatılacak.

2. Cyber Kill Chain(Siber Öldürme Zinciri) Nedir?

Cyber kill chain, saldırıyı birden fazla aşamaya bölerek karmaşık siber saldırıları tespit etmek ve durdurmak için tasarlanmış bir güvenlik çerçevesidir. Bu model, güvenlik ekiplerinin saldırıları bir kuruluşu etkilemeden önce tanımasına veya engellemesine yardımcı olur.
Cyber kill chain amacı, bir organizasyonun gelişmiş kalıcı tehditlere (APT'ler) karşı savunmasını güçlendirmektir, ayrıca karmaşık siber saldırılar olarak da bilinir.
Bu tehditler genellikle şunları içerir:

- **Malware(Zararlı Yazılım):**
  Zararlı yazılım, programlanabilir herhangi bir aygıta, hizmete veya ağa zarar vermek veya bunlardan yararlanmak üzere tasarlanmış her türlü zararlı yazılım için kullanılan kapsamlı bir terimdir. Siber suçlular genellikle bunu, mali kazanç için kurbanlardan veri elde ederek baskı yapmak üzere kullanır. Bu veriler finansal verilerden sağlık kayıtlarına, e-postalara ve parolalara kadar değişebilir. Kötüye kullanılabilecek bilgi türü sonsuzdur.
  Çeşitleri:
  - Virüsler
  - Fidye Yazılımı
  - Scareware
  - Solucanlar
  - Reklam yazılımı
  - Casus yazılım
  - Dosyasız zararlı yazılım
  - Truva atı

- **Ransomware(Fidye Yazılımları):**
  Fidye yazılımı, fidye ödenene kadar sizi sisteminizden kilitleyen veya dosyalarınıza erişimi engelleyen bir kötü amaçlı yazılım türüdür. Bu kötü amaçlı yazılım, bilgisayar sistemlerine çeşitli yollarla sızar, örneğin:
  - Kimlik avı
  - Kötü amaçlı web siteleri
  - İndirmeler

  Fidye yazılımı sisteminize eriştiğinde dosyalarınıza erişmenizi engeller veya bilgisayar ekranınızı kilitler ve erişimi geri yüklemek için fidye ister. Modern fidye yazılımları genellikle Bitcoin gibi kripto paralarla ödeme talep eder ve fidye miktarları hedefe bağlı olarak milyonlarca dolara ulaşır.

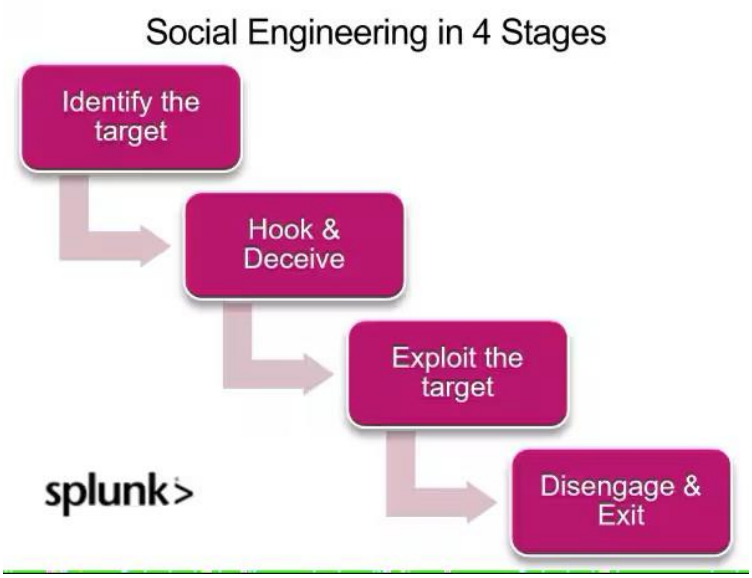
- **Trojan horses(Truva Atı):**
  Truva Atı, bir bilgisayar sistemine erişim sağlamak için kendisini meşru bir yazılım gibi gizleyen bir tür kötü amaçlı yazılımdır. Truva atları kurulduktan sonra hassas verileri çalmak, kullanıcı etkinliğini izlemek ve siber suçlular için yetkisiz uzaktan erişim sağlamak gibi çeşitli kötü amaçlı faaliyetler gerçekleştirebilir. Bilgisayar virüsleri veya solucanlar gibi diğer kötü amaçlı yazılım türlerinin aksine, Truva atları kendi kendini çoğaltmaz. Bunun yerine,

dağıtım için sosyal mühendislik taktiklerine ve kullanıcı etkileşimine güvenirler. Örneğin, görünüşte zararsız e-posta eklerinde gizlenebilir veya sahte yazılım güncellemelerine yerleştirilebilirler.
Truva atları şu anda en sık rastlanan zararlı yazılım kategorisidir. Arka kapılar açmak, etkilenen cihazın kontrolünü ele geçirmek, kullanıcı verilerini süzmek ve saldırgana göndermek, etkilenen sisteme diğer zararlı yazılımları indirmek ve çalıştırmak ve diğer birçok kötü amaç için kullanılırlar.

- **Phishing(Kimlik avı):**
  Kimlik avı, bilgisayar korsanlarının kendilerini güvenilir kimlikler olarak tanıtarak hassas verilerinizi paylaşmanız için sizi kandırdığı bir siber saldırıdır. Ayrıca hassas verilerinizi veya paranızı çalmak için bilgisayarınıza veya cihazınıza kötü amaçlı yazılım yüklemeniz için sizi kandırabilirler.
  - Sosyal mühendislik
  - Bağlantı manipülasyonu
  - Sesli oltalama
  - LNK oltalama
  - Zıpkınla oltalama
  - Klon oltalama

  Kimlik avı tamamen hileyle ilgilidir. Saldırgan, kullanıcıyı istenen eylemleri yapmaya ikna etmek için meşru bir varlığı taklit eder. Kimlik avı girişimleri genellikle hedefler hakkında fazla bağlam olmadan şüphelenmeyen kullanıcıları hedefler. Genellikle, kurbanlar güvenlik farkındalığı eksikliği nedeniyle kimlik avı girişimlerinin kurbanı olurlar.

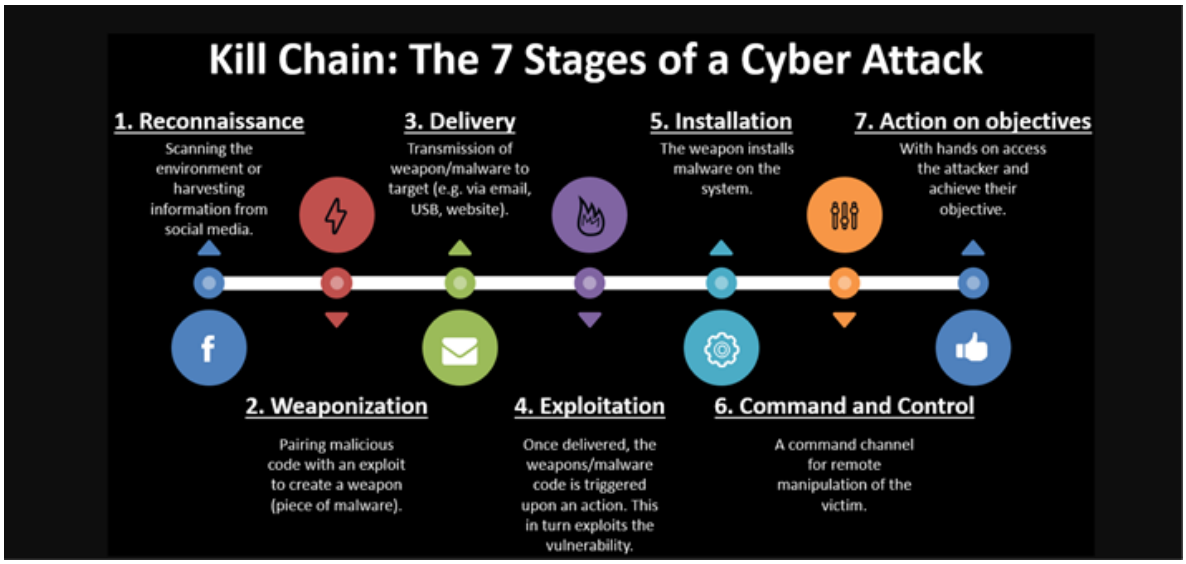
- **Other social engineering techniques(Sosyal Mühendislik):**
  Ancak gerçekte, siber suç olaylarının çoğu insan unsurunu kullanır Cyber kill chainin en zayıf halkası. Sosyal mühendislik, hassas bilgileri elde etmek için insan hatalarını/zayıflıklarını istismar etmeyi içeren kötü niyetli faaliyetleri tanımlayan toplu bir terimdir. Saldırganlar, kurbanlarını onlarla doğrudan etkileşim kurarak kendilerini tehlikeye atmaya ikna eder.
  Bu süreç dört aşamadan oluşur:
  Aşama 1. Hedef Tanımlama: Bu, saldırganın kurbanları hakkında ilgili arka plan bilgilerini topladığı ilk aşamadır. Saldırganlar, kurbanları hakkında toplanan bilgileri potansiyel giriş noktalarını belirlemek için kullanırlar.
  Aşama 2. Kanca/Aldatmaca: Bu aşamada saldırgan, hedefleriyle etkileşime girmek için sosyal mühendislik tekniklerinden birini kullanır. Saldırgan bu aşamada kurbanının güvenini kazanmaya çalışır.
  Aşama 3. İstismar: Bu aşamada, kurban saldırgana güvenmiştir ve saldırgan kurbanın zayıflığından haberdardır. Saldırgan bu zayıflığa dayanarak kontrolü ele geçirir ve kurbanın hesap bilgilerini paylaşma, tehlikeli dosyaları indirme veya banka kartı bilgilerini paylaşma gibi tehlikeye atacak eylemler gerçekleştirmesini sağlar.
  Aşama 4. Ayrılma/Çıkış: Saldırı bu noktaya gelirse, saldırgan istediğini başarmış demektir. Saldırgan etkileşimi sonlandırır ve izlerini örter.



3. Cyber Kill Chain 7 Aşaması

Bu, sektörde en sık başvurulan çerçevedir.7 aşamalı siber öldürme zinciri, bir siber suçlunun metodolojisini ve motivasyonunu tüm saldırı zaman çizelgesi boyunca inceler ve kuruluşların tehditleri anlamalarına ve bunlarla mücadele etmelerine yardımcı olur. Bu yedi aşama şunlardır:

1. Keşif
2. Silahlanma
3. Teslimat
4. Sömürü
5. Kurulum
6. Komuta ve Kontrol
7. Eylem



3.1. Keşif

Saldırı gerçekleşmeden veya bir istismar yaratılmadan önce keşif ve bilgi toplama aşamasıdır. Saldıran taraf; hedef sistem veya sistemler üzerinde çeşitli taramalar gerçekleştirerek zafiyetleri tespit etmeye çalışır ayrıca çalışanların isimleri, görevleri, e-mail adresleri, ip adresleri, ağ haritası çıkarma gibi eylemleri aktif ve pasif bilgi toplama araçlarıyla yapabildiği gibi, iş ilanları, linkedln, twitter, facebook, instagram gibi sosyal medya aracılığıyla hedef hakkında sosyal mühendislik yöntemleri ile bilgiler toplayabilir.

Pasif Bilgi Toplama: Hedef ile direkt olarak temasa geçilmeden bilgi toplama çeşitidir. (Shodan, Whoıs ve Dns, Osınt Araçları vb.)
Aktif Bilgi Toplama: Hedef ile direkt olarak temasa geçilen bilgi toplama çeşitidir. (Port Scan, Ağ Tarama, SQLMap vb.)

3.2. Silahlanma

Keşif sırasında bulunan zafiyetlerin sömürülmesi için kullanılacak yöntemlerin belirlenmesi ve uygun araçları hazırlama olarak tanımlanan aşamadır. Bu aşamada zafiyete uygun exploitler, zafiyetin istismar edilmesi için kullanılabilecek payloadlar olabileceği gibi zararlı dosyalar ve dokümanlar, oltalama saldırısında kullanılabilecek sahte epostalar gibi birçok yöntem kullanılarak sızma işlemi gerçekleştirilebilir.

3.3. Teslimat

Hazırlanan zararlının ve belirlenen yöntemle hedefe iletilmesi bu aşamadadır. Çeşitli açık kaynak kodlu yazılımlar, phishing, sosyal networkler veya tünellemeler gibi yöntemler kullanılabileceği gibi, güvenlik olarak çalışanların sosyal mühendisliklere veya phishing saldırılarına karşı farkındalıkları, çalışanların hangi donanımların kurum ağına bağlanabildiği veya bağlanamadığı konusunda bilgilendirmesi, bilinen zararlı veya şüpheli web sitelerinin erişim bloklarının kontrol edilmesi bu aşamayı önleyebilir.

3.4. Sömürü

Oluşturulan zararlı ve belirlenen atak vektörünü kullanarak hedefin zafiyetinin sömürüldüğü aşamadır. Exploit hazırlanıp hedefe iletildikten sonra bu aşamada zararlı kod çalıştırılır. Genellikle sistemler arasında yatay olarak hareket ederek daha fazla potansiyel giriş noktası ve zayıflık belirlerler.
Bunu önlemek amacıyla yazılımlar ne sıklıkla güncellendiği, sistemdeki zafiyetlerin tespit edilmesi için güvenlik denetimleri yapılıp yapılmadığı kontrol edilebilir.

3.5. Kurulum

Hedefin sömürülmesi ardından, kalıcı bir tehdit haline gelmek, güvenlik sisteminin ötesinde sistem başarılı bir şekilde kontrol edilebilmesi için hedefe asıl zararlı yazılımın indirilmesi, zararlı yazılımın sistemde kalacağı süreyi mümkün olduğunca arttırmayı hedefleyen aşamadır.
Sistemde çalışan bilgisayarlarla yüklenen yazılımların denetlenmesi, kullanıcıların istedikleri yazılımları bilgisayarlara yükleyebilirlikleri, whitelisting ve blacklisting oluşturma bu aşamayı önleyebilir.

3.6. Komuta ve Kontrol

Sisteme yerleşmiş olan zararlının çalışması uzaktan kontrol edilebildiği ve sistemin ele geçirildiği aşamadır. İzlerini örtmek için karartma teknikleri ve güvenlik ekiplerini saldırının temel hedeflerinden uzaklaştırmak için hizmet reddi (DoS) taktikleri kullanırlar.

Bu aşama için saldırıyı engelleyebilecek firewall ve ips'in devrede olup olmadığı iyi konfigüre edilip edilmediği ve güvenlik cihazlarının monitör edilebilirliği bu aşamayı aksatmak için önemli unsur taşımakta.

3.7. Eylem

Bütün aşamaları gerçekleştiren saldırgan kuruma erişim sağlamıştır ve bu aşamada, veri çalma, veri değiştirme, veri silme, veri şifreleme, sisteme zarar verme gibi eylemleri gerçekleştirebilir.

Önlem olarak iç ağdan dışarı yapılan veri akışı sınırlandırılması, sadece bilinen sunuculara veri akışını sağlama (whitelisting) oluşturulduğunda saldırı engellenebilir. Bu süreçte tehdit altındaki verilerin yedeklerinin önceden alınması, bir sistem devre dışı kaldığında hizmet verebilecek yedek sistemin olması bu saldırının etkilerini azaltabilir.

4. Siber Saldırıları Önleme

Siber saldırıları önlemek, sadece belirli güvenlik önlemlerini uygulamakla sınırlı kalmaz; sürekli güncellenen, çok katmanlı ve proaktif bir güvenlik yaklaşımı gerektirir. Günümüzde tehdit aktörleri giderek daha sofistike saldırı yöntemleri geliştirdiğinden, kuruluşların güvenlik önlemlerini sürekli olarak gözden geçirmesi ve güncellemesi gerekmektedir.

İşte kuruluşunuzun savunmasını geliştirmek için stratejiler:

4.1. Gelişmiş tehdit algılama araçları

Saldırı algılama sistemleri (IDS), saldırı önleme sistemleri (IPS) ve uç nokta algılama ve yanıt (EDR) çözümleri gibi araçları dağıtın. Bu araçlar tehditleri gerçek zamanlı olarak belirleyip azaltabilir ve saldırganlar için fırsat penceresini daraltabilir.

4.2. Düzenli zafiyet değerlendirmeleri ve penetrasyon testleri

Saldırganlar bunları istismar etmeden önce güvenlik zafiyetlerini belirlemek ve düzeltmek için düzenli zafiyet değerlendirmeleri ve penetrasyon testleri gerçekleştirin. Bu hem otomatik taramaları hem de yetenekli güvenlik uzmanları tarafından yapılan manuel testleri içermelidir.

4.3. Yama yönetimi

İşletim sistemleri, uygulamalar ve güvenlik araçları dahil tüm yazılımların en son yamalar ve güncellemelerle güncel olduğundan emin olun. Bu, saldırganların bilinen güvenlik açıklarını istismar etme riskini azaltır.

4.4. Ağ segmentasyonu

Saldırganların ağınız içindeki hareketini sınırlamak için ağ segmentasyonunu uygulayın. Ağınızı daha küçük, izole segmentlere bölerek ihlalleri sınırlayabilir ve saldırganların hassas alanlara erişmesini önleyebilirsiniz.

4.5. Çok faktörlü kimlik doğrulama (MFA)

Özellikle hassas bilgilere ve kritik sistemlere erişimi olanlar olmak üzere tüm kullanıcı hesapları için çok faktörlü kimlik doğrulaması gerektirir. MFA, saldırganların yetkisiz erişim elde etmesini zorlaştırarak ekstra bir güvenlik katmanı ekler.

4.6. Çalışan eğitimi ve farkındalık programları

Çalışanlar için düzenli siber güvenlik eğitimi ve farkındalık programları yürütün. Onlara kimlik avı girişimlerini, sosyal mühendislik saldırılarını ve güvenli çevrimiçi uygulamaları tanıma konusunda eğitim verin. Bilgili bir iş gücü, siber tehditlere karşı kritik bir savunma hattıdır.

4.7. Olay müdahale planlaması

Kapsamlı bir olay müdahale planı geliştirin ve sürdürün. Bu plan, roller ve sorumluluklar, iletişim protokolleri ve kurtarma prosedürleri dahil olmak üzere bir güvenlik ihlali durumunda atılacak adımları ana hatlarıyla belirtmelidir. Etkinliğini sağlamak için planı düzenli olarak test edin ve güncelleyin.

4.8. Davranışsal analiz

Ağınızdaki anormallikleri ve alışılmadık etkinlik kalıplarını tespit etmek için davranışsal analizden yararlanın. Normal davranışın bir taban çizgisini oluşturarak, geleneksel güvenlik önlemlerinin gözden kaçırabileceği potansiyel tehditleri belirleyebilirsiniz.

4.9. Sıfır güven mimarisi

"Asla güvenme, her zaman doğrula" ilkesiyle çalışan sıfır güven güvenlik modelini benimseyin. Bu yaklaşım, erişim izni vermeden önce hem ağın içinde hem de dışında tüm kullanıcıların, cihazların ve uygulamaların sürekli olarak doğrulanmasını gerektirir.

4.10.Düzenli veri yedeklemeleri.

Tüm kritik verilerin düzenli yedeklemelerini gerçekleştirin ve yedekleme sistemlerinin güvenli ve test edilmiş olduğundan emin olun. Bir fidye yazılımı saldırısı veya veri kaybı durumunda, güvenilir yedeklemelere sahip olmak hızlı kurtarmayı kolaylaştırabilir ve kesinti süresini en aza indirebilir.

5. Sonuç

Cyber Kill Chain modeli, siber güvenlik alanında önemli bir çerçeve sunmaktadır. Bu çalışmada incelenen yedi aşamalı model, modern siber saldırıların karmaşık yapısını anlamak ve bunlara karşı etkili savunma stratejileri geliştirmek için değerli bir araç olduğunu göstermiştir. Cyber Kill Chain, mevcut stratejideki kusurları belirleyerek veya halihazırda iyi işleyen şeyleri doğrulayarak bir işletmenin siber güvenlik stratejisine rehberlik edebilir.
Örneğin, aşağıdakiler gibi hizmetlerin ve çözümlerin benimsenmesini teşvik edebilir:

- Uç nokta koruma yazılımı
- VPN'ler
- Çalışan eğitimi

Modelin en güçlü yanı, siber saldırıların aşamalarını sistematik bir şekilde tanımlayarak, kuruluşların her aşamada alabilecekleri önlemleri belirlemelerine olanak sağlamasıdır. Bununla birlikte, teknolojinin hızla gelişmesi ve siber tehditlerin evrimleşmesi, modelin bazı sınırlamalarını da ortaya çıkarmıştır.

Özellikle iç tehditler, dosyasız zararlı yazılımlar ve modern saldırı tekniklerine karşı modelin yetersiz kalması, güvenlik stratejilerinin MITRE ATT&CK gibi tamamlayıcı çerçevelerle desteklenmesi gerektiğini göstermektedir. Ayrıca, bulut bilişim, IoT ve yapay zeka gibi yeni teknolojilerin getirdiği güvenlik zorlukları, modelin sürekli olarak güncellenmesi ve geliştirilmesi ihtiyacını ortaya koymaktadır.

Sonuç olarak, Cyber Kill Chain modeli tek başına yeterli olmasa da, siber güvenlik stratejilerinin temel yapı taşlarından biri olmaya devam etmektedir. Kuruluşların bu modeli diğer güvenlik çerçeveleriyle birlikte kullanması, çok katmanlı bir savunma stratejisi geliştirmesi ve sürekli olarak güncel tehdit trendlerini takip etmesi, siber saldırılara karşı etkili bir koruma sağlamanın anahtarıdır.

Kaynakça

https://www.mcafee.com/tr-tr/antivirus/malware.html
https://www.splunk.com/en_us/blog/learn/social-engineering-attacks.html
https://www.splunk.com/en_us/blog/learn/phishing-scams-attacks.html
https://www.splunk.com/en_us/blog/learn/ransomware-attack-types.html
https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html
https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu