CYBER STRUGGLE
TASK - Incident Handling and Response Overview

Hazırlayan:

DCS001 Hakan ŞEN

Ekim 2023

Ankara

İÇİNDEKİLER

Task 1: Explain the differences between an Event and an Incident.

Bir event, bir sistem veya ağda gözlemlenebilen herhangi bir oluşumdur. Bir kullanıcının bir dosya paylaşımına bağlanması, bir sunucunun web isteği alması, bir kullanıcının e-posta göndermesi ve bir güvenlik duvarının bir bağlantı girişimini engellemesi gibi durumları içerir. Olumsuz event'ler sistem çökmeleri, paket flood saldırıları, hassas verilere izinsiz erişim ve verileri yok eden zararlı yazılım çalışıtırılması gibi gibi olumsuz sonuçları olan olaylardır.

Incident ise bilgisayar güvenliği politikalarının, kabul edilebilir kullanım politikalarının veya standart güvenlik uygulamalarının ihlali veya bu ihlalin yaklaşan bir tehdidi olarak kabul edilebilir. Incident örneği olarak;

- Bir saldırganın, elinde bulunan bir botnet ile web sunucuna yüksek miktarda bağlantı isteği göndererek çökmesine neden olmasıi
- Kullanıcıları yanıltarak aslında zararlı bir yazılım içeren epostayı açmasını sağlayıp, harici bir sistem ile bağlantı kurmasının sağlanması,
- Bir saldırganın organizasyona ait hassas verileri elde ederek fidye talebinde bulunması gibi olaylar incident olarak sayılabilir.

Incident'leri eventlerden ayırmak son derece önemlidir.

- Incident bir sistemin gizliliğini, bütünlüğünü ve kullanılabilirliğini kasıtlı olarak veya kazara tehdit eden veya olumsuz etkileyen siber faaliyetlerdir ve bunlara uygun kanallar aracılığı ile alarm verilir ve bildirilir.
- Event ise normal davranış veya ortamda meydana gelen değişikliklerdir.

İÇİNDEKİLER'E DÖN

Task 2: Explain the stages of incident handling contains

Olay müdahalesi genel olarak siber güvenlik olaylarına etkili bir şekilde tepki vermek, hafifletmek ve kurtarmak için bir dizi aşamayı içerir. Bu aşamalar, belirli bir olay yanıtı çerçevesinde veya modeline bağlı olarak değişiklik göstermektedir.

Olay müdahalesine ilişkin aşamalar NIST tarafından yayınlanan NIST SP 800-61 Computer Security Incident Handling Guide (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf) içeriğinde aşağıdaki şekilde tanımlanmıştır.

1. Hazırlık (Preparation)
2. Tanımlama ve Analiz (Detection and Analysis)
3. Kontrol, Yoketme ve Kurtarma (Containment, Eradication & Recovery)
4. Olay Sonrası Aktiviteler (Post-Incident Activity)

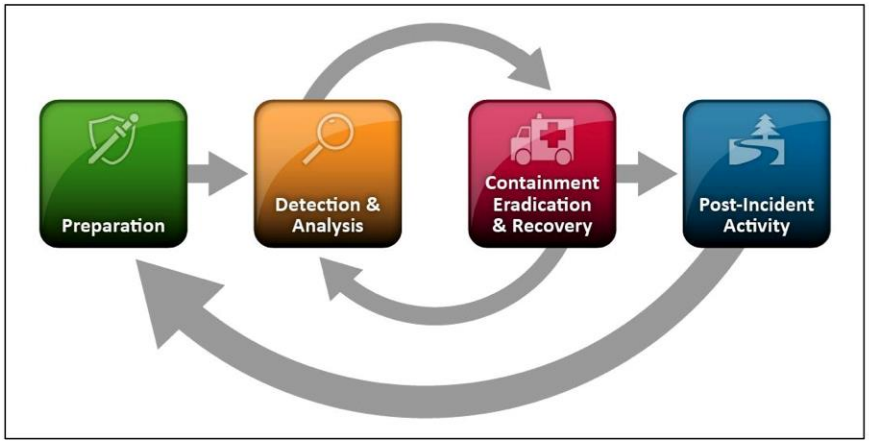

Figure 3-1. Incident Response Life Cycle

Öte yandan SANS'ın yayını olan SANS Incident Handler's Handbook 'ta (https://sansorg.egnyte.com/dl/6Btqoa63at) bir olayın çeşitli aşamalarında izlenecek önemli adımları vurgulayarak daha taktiksel ve prosedürel bir yaklaşım belirlemiştir. Belirtilen kaynakta olay müdahalesine yönelik aşamalar ise aşağıda verilmiştir.

1. Hazırlık (Preparation)
2. Tanımlama (Identification)
3. Kontrol (Containment)
4. Yok Etme (Eradiction)
5. Kurtarma (Recovery)
6. Edinilen Dersler (Lessons Learned)

İÇİNDEKİLER'E DÖN

Task 3: Explain the objective of each stage and what the main activities and aims to.

Bir önceki göreve verilen cevaplardan yola çıkarak SANS'ın Olay müdahale süreçlerinin amaçları ve yapılacak faaliyetler aşağıda çıkarılmıştır.

Hazırlık Aşaması:

-Amaç : Etkili olay yanıtı için temel oluşturmak.

-Faaliyetler:

* Olay müdahale politikası ve planı oluşturulması.
* Olay müdahale ekibi için roller ve sorumlulukların tanımlanması.
* Eğitim ve farkındalık programlarının düzenlenmesi.
* Olay tespiti ve yanıt için gerekli araçların ve teknolojilerin hazırlanması.
* Organizasyon dışı kuruluşlarla iletişim kanalarının ve koordinasyonun kurulması.

Tanımlama Aşaması:

- Amaç: Güvenlik olayının gerçekleştiğini tanımlamak ve doğrulamak.
- Faaliyetler :
  * Anormal veya şüpheli faaliyetleri izlemek için izleme sistemlerinin kullanılması.
  * Logların ve diğer ver kaynaklarının analiz edilerek potansiyel incidentlerın tanımlanması.
  * Bir incident'ın neyi içerdiğini tanımlamak için kriterlerin belirlenmesi

Kontrol Aşaması:

- Amaç: Olayın yayılmasını engellemek veya daha fazla zarar vermesini önlemek.
- Faaliyetler:
  * Etkilenen sistemlerin veya ağların izole edilmesi.
  * Ele geçirilmiş veya tehlikedeki kullanıcı hesabı veya servislerin devre dışı bırakılması.
  * Geçici çözümler ve yamaların uygulanması.

Yok Etme Aşaması:

- Amaç: Olayın köken nedenini belirlemek ve ortadan kaldırmak.
- Faaliyetler:
  * Saldırının kökeni ve yöntemlerini anlamak için kapsamlı soruşturma yapılması.
  * Olayın tekrarlanmasını önlemek için kalıcı düzeltmeler geliştirilmesi ve uygulanması.
  * Zararlı yazılımların veya izinsiz erişim noktalarının kaldırılması.

Kurtarma Aşaması:

- Amaç: Etkilenen sistemleri normal işlemlere geri döndürmek.
- Faaliyetler:
  * Uygulamanan düzeltmelerin etkinliğinin doğrulanması.
  * Yedeklerden veri ve yapılandırmaların geri yüklenmesi.
  * Sistemlerin herhangi bir kalıntı tehlikesi açısından izlenmesi.

Edinilen Dersler Aşaması:

- Amaç: Olay yanıtı sürecini analiz ederek gelecekteki yanıtları iyileştirmek.
- Faaliyetler:
  * Olay sonrası bir değerlendirme yaparak güçlü ve zayıf yönlerin belirlenmesi.
  * Öğrenilen derslerek dayanarak olay müdahale süreçlerinin güncellenmesi.
  * Olay müdahale ekibi ve genel olarak organizasyon ile bilgi ve deneyim paylaşımı.

NIST'in olay müdahale süreçlerinin amaçları ve icra ediecek faaliyetleri aşağıda çıkarılmıştır.

Hazırlık Aşaması:

- Amaç: Organizasyonun güvenlik olaylarına etkili bir şekilde yanıt verme ve kurtarma için hazırlıklı olmasını sağlamak. Bir olay müdahale yeteneği oluşturmak ve sürdürmek.
- Faaliyetler:
* Olay müdahale politikası ve planını geliştirme ve uygulama.
* Olay müdahale ekibi için farkındalık ve eğitim programları düzenleme.
* Olay müdahale ekibini kurma ve rolleri ile sorumlulukları tanımlama.
* Olay müdahale yeteneği oluşturma ve uygulama.

Tespit ve Analiz Aşaması:

- Amaç: Incidentleri hızlı bir şekilde tanımlamak ve etkili yanıt ve kurtarma sağlamak. Olayları zamanında tespit etmek ve etkilerini anlamak.
- Faaliyetler:
* İzleme ve tespit sistemlerini uygulama.
* Olayları analiz ederek kapsam ve etkilerini belirleme.
* Adli verileri toplama ve analiz etme.
* Bilgi paylaşımı ve harici kuruluşlarla iş birliği yapma.

Kontrol, Yok Etme ve Kurtarma Aşaması:

- Amaç: Zararı en aza indirmek, işlemleri geri yüklemek ve olayın tekrarını önlemek. Olayın etkilerini sınırlamak, kök nedeni ortadan kaldırmak ve normal işlemleri geri yüklemek.
- Faaliyetler:
* Olayı yayılmasını önlemek için kontrol etme.
* Olayın kök nedenini ortadan kaldırma.
* Etkilenen sistemleri ve verileri kurtarma.
* Gelecekteki olayları önlemek için düzeltici önlemleri uygulama.

Olay Sonrası Aktiviteler Aşaması:

- Amaç: Gerçekleşen olaylardan elde edilen bilgilerle olay müdahale süreçlerini, yeteneklerini ve genel güvenlik durumunu iyileştirmek. Olayları belgelemek ve sürekli iyileştirmek için öğrenmek.
- Faaliyetler:
* Olay ayrıntıları, yanıt eylemleri ve öğrenilen dersleri belgeleme.
* Olay sonrası bir değerlendirme ve analiz yapma.
* Olay müdahale planlarını ve yeteneklerini öğrenilen derslere dayanarak güncelleme.

İÇİNDEKİLER'E DÖN

Task 4: What are the prerequisites for a SOC in the preparation stage for an incident?

Güvenlik Operasyonları Merkezi (SOC) için olaya müdahale hazırlık aşamasındaki temel gereklilikleri aşağıda çıkarılmıştır.

1. Olay Müdahale Politikası ve Planı: Güvenlik olaylarına yanıt verme politikası ve planını. Olaylara yanıt verme yaklaşımını, rolleri, sorumlulukları ve olaylara yanıt verme prosedürlerini tanımlamalıdır.

2. Olay Müdahale Ekibi: Net rolleri ve sorumlulukları tanımlanan bir olay müdahale ekibi kurulmalıdırç Ekip üyelerinin eğitimi yeterli olduğundan ve olay sırasında görevlerini bilincinde olmalıdır.

3. İletişim ve Koordinasyon: SOC içinde ve dışındaki varlıklarla iletişim ve koordinasyon mekanizmalarını kurulmalıdır. Bu, olayların bildirilmesi, diğer ekiplerle iş birliği yapma ve ilgili paydaşlarla bilgi paylaşma için açık kanalları içermelidir.

4. Eğitim ve Farkındalık Programları:SOC personeli ve diğer ilgili personel için eğitim ve farkındalık programları düzenlenmelidir. Ekip üyelerinin olay yanıt planı, araçlar ve prosedürler konusunda iyi bilgi sahibi olmalıdır.

5. Araçlar ve Teknolojiler: Olay tespiti, analizi ve yanıt için gerekli araçları ve teknolojileri kurulmalı ve idamesi sağlanmalıdır. Bu, güvenlik bilgi ve etkinlik yönetimi (SIEM) sistemleri, sızma tespit/engelleme sistemleri ve diğer ilgili güvenlik araçlarını içerebilir.

6. Veri Toplama ve Saklama: Veri toplama ve saklama için bir strateji belirlenmelidir. Olay analizi için hangi türde verilerin toplanması gerektiğini belirleyin ve bu verilerin güvenli ve erişilebilir bir şekilde saklanması için prosedürler oluşturulmalıdır.

7. Hukuki ve Düzenleyici Uyumluluk: SOC'un ilgili hukuki ve düzenleyici gerekliliklere uygun olarak çalıştığından emin olunmalıdır. Bu, bildirim yükümlülüklerini anlama, gizlilik düşüncelerini ve olay yanıt faaliyetlerine yönelik herhangi bir yasal kısıtlamayı içerir.

8. Sürekli İyileştirme: Olay yanıt yeteneklerinin sürekli olarak iyileştirilmesi için bir süreç uygulanmlıdır. Bu, önceki olaylardan öğrenilen derslere dayalı olarak olay yanıt planları, prosedürleri ve araçları düzenli olarak gözden geçirme ve güncelleme içermelidir.

9. Test ve Egzersizler: Olay yanıt planının etkinliğini değerlendirmek için düzenli olarak test ve egzersizler yapılmalıdır. Farklı türde olayları işlemek için SOC ekibinin iyi hazırlandığından emin olmak için çeşitli senaryoları simüle edilmelidir.

10. Kaynak Tahsisi: Etkili olay yanıt faaliyetlerini desteklemek için yeterli kaynakları, hem personel hem de teknoloji açısından tahsis edilmelidir. SOC'un, organizasyonun güvenlik ihtiyaçlarını karşılamak için yeterli personelle ve donanımla donatılmalıdır.

11. Bilgi Paylaşımı: Tehdit istihbaratı ve bilgi paylaşımı için dış kuruluşlarla mekanizmaları kurulmalıdır. Bu, endüstri meslektaşlarıyla, devlet kurumlarıyla ve ilgili siber güvenlik topluluklarıyla bilgi paylaşımı için mekanizmalar içermelidir.

Bu gerekliliklere odaklanmak, bir SOC'un güvenlik olaylarına etkili bir şekilde yanıt vermesi ve organizasyonun genel siber güvenlik durumuna katkıda bulunması için temel oluşturacaktır. Bu hazırlık aşaması, güçlü ve etkili bir olay yanıt yeteneği oluşturmak için kritiktir.

İÇİNDEKİLER'E DÖN

Task 5: Explain the artifacts of an incident. What should it include?

Organizasyonların olay müdahale süreçleri boyunca göz önünde bulundurmaları gereken çeşitli artifactler bulunmaktadır. Bu artifactler güvenlik olaylarını anlama, yanıtlama ve öğrenme açısından kritik olan bilgi ve belgelerdir. Temel olarak olması gereken artifactler ve içerikleri aşağıda sunulmuştur.

1. Olay Kaydı:
   - Olayla ilgili temek bilgiler, olay kimliği, tarih,saat ve ilk değerlendirme
   - Olayı yöneten ve ilgili tarafların iletişim bilgileri
   - Olayın kısa açıklaması ve etkisi
2. Muhafaza Zinciri:
   - Delilin muhafaza ve işlenmesine dair belgeler
   - Delili elinde bulunduran kişilerin adları
   - Delil transferlerinin zaman damgaları ve detayları
3. Delil Kayıtları:
   - Toplanan tüm delillerle ilgili detaylı kayıtlar
   - Her bir delilin kaynağı yeri ve bağlamı hakkında bilgiler
   - Muhafaza ve işleme ayrıntıları
4. Tanık Beyanları:
   - Olayı gözlemleyen kişilerin beyanları
   - Tanıkların ne gözlemlediği veya yaşadığına dair açıklamalar
   - Tanıkların iletişim bilgileri
5. Adli Veri:
   - Etkilenen sistemler üzerinde yapılan adli analiz sonuçları.
   - Zararlı yazılımlar, izinsiz erişim izinleri veya diğer anormalliklere dair bilgiler.
   - Detaylı adli raporlar.
6. Uyarılar ve Bildirimler:
   - Olay sırasında tetiklenen uyarıların kopyaları
   - Olay müdahel ekipleri, yönetim veya diğer paydaşlara gönderilen bildirimler
   - Uyarıların meydana geldiği zaman damgaları veya detayları
7. İletişim Kayıtları:
   - Olay sırasında gerçekleşen iletişim kayıtları.
   - Olayla ilgili e-posta alışverişleri, sohbet kayıtları veya diğer iletişim biçimleri.
   - Alınan kararlar ve yapılan eylemler hakkında bilgiler.
8. Olay Analizi Raporları:
   - Olayın, kök nedenlerin ve etkilerin detaylı analizi.
   - Olaydan öğrenilen dersler ve iyileştirmeler için öneriler.
   - Organizasyonun bilgi tabanına katkıda bulunabilecek bilgiler.
9. Hukuki Belgeler:
   - Olayın hukuki yönleriyle ilgili belgeler.
   - Herhangi bir arama kararı, mahkeme kararı veya hukuki anlaşmalar.
   - Olay sonrası bildirim yükümlülüklerine ilişkin belgeler.
10. Olay Sonrası İnceleme:
    - Olay sonrası inceleme sürecine dair belgeler.
    - İncelenen bulgular, güçlü yönler ve iyileştirme alanlarından elde edilen sonuçlar.
    - İnceleme temelinde olay yanıt planlarının ve süreçlerinin güncellenmesi.

Belirtilen artifactler olay müdahale yaşam döngüsünde belirli bir amaca hizmet eder ve olayın ayrıntılı anlaşılmasına ve çözüm bulunması için katkıda bulunur.

İÇİNDEKİLER'E DÖN

Task 6: What are the differences between containment and eradication?

Kontrol Altına Alma (Containment):

- Kontrol altına alma, olayın yayılmasını engellemek ve organizasyonun sistemleri ve verileri üzerindeki etkisini sınırlamak için yapılan işlemleri içerir.
- Kontrol altına almanın temel amacı, etkilenen sistemleri izole etmek, daha fazla zararı önlemek ve olayın potansiyel zararını en aza indirmektir.
- Bu aşama, etkilenen sistemleri ağdan izole etmek, kötü amaçlı faaliyetleri engellemek, geçici düzeltmeler uygulamak veya olayın kapsamını sınırlamak için diğer önlemleri içerebilir.

Yok Etme (Eradiction):

- Yok etme, olayın köken sebebini organizasyonun sistemlerinden tamamen kaldırmayı hedefler. Olayın meydana gelmesine neden olan zayıflıkları ve eksiklikleri ortadan kaldırmayı amaçlar.
- Yok etmenin temel amacı, olayın temel nedenini ele alarak olayın tekrarlanmasını önlemektir. Bu, yazılım zayıflıklarını düzeltmek, kötü amaçlı yazılımları kaldırmak ve benzer olayların önüne geçmek için uzun vadeli çözümler uygulamayı içerir.
- Yok etme faaliyetleri, detaylı sistem analizi, zayıflık değerlendirmeleri ve sömürülen zayıflıkları ortadan kaldırmak için kalıcı düzeltmeler uygulamayı içerir.

Kontrol altına alma, olayın yayılmasını engellemek ve daha fazla zararı önlemekle ilgilidir, kökten yok etme ise olayın ilk meydana gelmesine neden olan kök sebepleri ve zayıflıkları ortadan kaldırmakla ilgilidir. Her iki aşama da olay yanıt sürecinde kritiktir ve genel hedef, normal işlemleri geri yüklemek ve gelecekteki olaylara karşı organizasyonun direncini artırmaktır.

Task 7: Give an example of short-term containment and long-term containment.

Kısa Vadeli Kontrol Altına Alma için örnek olarak; Bir ağ üzerinde yayılan kötü amaçlı yazılım için kısa vadeli olarak etkilenen sistemin ya da bölümün ağdan izole edilmesi, tehlikeye girmiş hesapların devre dışı bırakılması veya geçici olarak erişim kontrolleri uygulanması kötü amaçlı yazılımın kısa vadeli olarak daha fazla yayılmasını önleyebilir.

Uzun Vadeli Kontrol Almada olayın kök nedenlerini ortadan kaldırmak ve tekrarlanmasını önlemek için daha kapsamlı önlemleri içermektedir. Örnek olarak bir ihlal tespit edilmesini müteakip, güvenlik politikalarının gözden geçirilmesi ve buna yönelik olarak çalışanlara siber güvenlik eğitimi verilmesi verilebilir. Yine örnek olarak ağ mimarisi yeniden yapılandırılması ve tespit sistemlerinin eklenmesi örnek olaak verilebilir.

Kısa vadenin amacı tehdidi anında durdurmak ve etkisini sınırlamaktır, uzun vadeli ise olayın temel nedenlerini ele alarak gelecekte benzer olayların yaşanmaması için önlemeye odaklanmaktadır.

İÇİNDEKİLER'E DÖN

Task 8: Explain the Post-Incident Activity Stage, Why do we have to use this stage?

Olay sonrası aktivite aşaması, incident başarıyla kontrol altına alındığı, ortadan kaldırıldığı ve etkilenen sistemlerin normale dönmesi sonrası icra edilen faaliyetleri içeren aşamadır. Temel amacı olaydan çıkarılan derslere dayanarak organizasyonun genel siber güvenlik durumunu değerlendirmek ve iyileştirmektir.

Olay sonrası aktivite süreçleri değerlendirildiğinde;

Öğrenilen Dersler: Olay müdahalenin en önemli kısmından biri olmasının yanında sıklıkla atlanan kısımdır. Müdahale ekipleri, yeni tehditleri, gelişmiş teknolojiyi ve öğrenilen dersleri yansıtacak şekilde gelişmelidir. Olay sonrasında periyodik olarak olayın tüm tarafları ile öğrenilen dersler toplantısı düzenlemek, güvenlik önlemlerinin iyileştirilmesinde ve olay süreçlerinin geliştirilmesinde son derece yararlı olacaktır. Yapılacak toplantı yaşananları, müdahale için neler yapıldığını ve müdahalenin ne suretle işletildiği konularının gözden geçirilerek olaya ilişkin sonuca ulaşılmasını gerçekleştirme şansı sağlayacaktır.

Analiz ve Değerlendirme : olayın kapsamı, etkisi ve varsa saldırganların kullandığı tatkikleri anlamak için olayın detaylı bir şekilde incelenmesini kapsamaktadır. Bu analiz organizasyonun güvenlik altyapısındaki zayıflıkları ve güvenlik açıklarını belirlemede yardımcı olmaktadır.

Sürekli İyileştirme: olay sonrası elde edilen bilgiler güvenlik politikalarının prosedürlerin ve teknolojilerin sürekli olarak iyileştirilmesinde katkıda bulunur. Ortaya çıkan tehditlere ilişkin adapte olmayı ve genel güvenlik altyapısını güçlendirmeyi sağlayan yenilenen bir süreçtir.

Risk Yönetimi: Olayların kök nedenlerini anlamak ve bunlarla başa çıkmak gelecekte ortaya çıkabilecek riskleri yönetmede ve hafifletmede yardımcı olur.

Belgeleme ve Raporlama: olayın, zaman çizelgesinin, alınan önlemlerin ve sonuçların belgelenmesi önemlidir.

Olay sonrası aktiviteler sadece bir olaydan sonra olayın kapatılması ile ilgili değildir, aynı zamanda sürekli iyileştirmeyi, risk yönetimini ve daha dayanıklı bir siber güvenlik alt yapısını geliştirmeyi teşvik eden stratejik bir aşamadır. Olay müdahale yaşam döngüsünün kurum yada kuruluşun genel siber güvenlik olgubluğuna katkıda bulunan önemli bir parçasıdır.

İÇİNDEKİLER'E DÖN