DDoS SİBER OLAY YANIT PROSEDÜRÜ:

Prosedür Adı:	DDoS SİBER OLAY YANIT PROSEDÜRÜ
Doküman Kodu:	BGYS.PR.T.001.ATABAUM.BC
Doküman Sahibi:	BGYS Yöneticisi
Doküman Onay Tarihi:	05/12/2021
Gizlilik Sınıfı:	İç Kullanım

İçindekiler:

AMAÇ:

Bu prosedür, Kuruluş Bilgi Sistemlerine Yönelik bir DDoS (Dağıtık Hizmet Durdurma) veya DoS (Hizmet Durdurma) Saldırısı Meydana geldiğinde neler yapılması gerektiğini belirlemeyi amaçlar.

KAPSAM:

Kuruluş bünyesindeki İnternet Servisi, Sunucu İşletim Sistemleri, Haberleşme Protokolleri, Uygulama Yazılımlarını kapsar.

TANIMLAR:

SORUMLULAR:

İlgili Sorumluluklar SİBER OLAYLARA MÜDAHALE TABLOSU'nda tanımlanmıştır. Sorumluların ilgili Sistem Yöneticisi olmasına dikkat edilmiştir.

UYGULAMA:

Bu Prosedür Olası Saldırı Vektörleri (Tipleri) ve İlgili Bilgi Varlıkları SİBER OLAYLARA MÜDAHALE POLİTİKASINDA belirtilen "Siber Olay Tipleri" dikkate alınarak hazırlanmıştır.

SALDIRININ TESPİT EDİLMESİ AŞAMASI ve GEREKLİLİKLER AŞAMASI:

Saldırının tespit edilebilmesi için kullanılan mevcut kontroller:

1. Anormal Trafiğin Tespit edilebilmesinde Firewall Sistemi ile ilişkilendirilen SIEM Sistemi kullanılır. İlgili kayıtlar Firewall üzerinden yetkilendirilmiş olarak, UDP 514 (SYSLOG) portu ile alınır. Bu sistemden beklenen;

a. Yoğun Oturum (Session) Olay Kaydı. Bu olay kayıt sayısının belirlenebilmesi için SIEM sistemi üzerinde ilgili sistemlerin 14 günlük trafiği izlenerek eşik değerler belirlenir. Bu eşik değerlerin üzerinde olan olay sayıları için ilgili Sistem Yöneticisine Alarm üretilir. Alarm aralığı 10 dakika, tüm kayıtların saklanma süresi en az 1 yıldır.
b. İlgili Ağ Sistemine yönelik, Anormal Portlara ve Protokollere olan Erişim Denemeleri. Örneğin TCP 22, 22, 23, 2222, vb. Portlara erişim gibi.
c. İlgili Ağ Sisteminden iç Ağ ve İnternete yönelik Anormal Portlara ve Protokollere olan Erişim Denemeleri. Örneğin yoğun ICMP trafiği, DNS trafiği (UDP Port 53) gibi.

2. Anormal Trafiğin tespit edilebilmesi için ilgili Ağ Cihazı ile ilişkilendirilen SIEM Sistemi kullanılır. İlgili kayıtlar ilgili Ağ Cihazının destek vermesi durumunda yetkilendirilmiş olarak, Syslog, Port Mirroring, SNMP veya SSH üzerinden alınır.
    a. Yoğun Oturum (Session) Olay Kaydı. Bu olay kayıt sayısının belirlenebilmesi için SIEM sistemi üzerinde ilgili sistemlerin 14 günlük trafiği izlenerek eşik değerler belirlenir. Bu eşik değerlerin üzerinde olan olay sayıları için ilgili Sistem Yöneticisine Alarm üretilir. Alarm aralığı 10 dakika, tüm kayıtların saklanma süresi 1 yıldır.
    b. Desteklemesi durumunda, İlgili Ağ Sisteminden "SNMP v2" Protokolü ile alınan Bant Genişliği grafikleri ile 14 günlük trafiğin izlenmesi yapılarak Normal/Anormal Trafik seviyeleri belirlenir. Yüksek Upload/Download durumunda ilgili Bant Genişliği Takip Sistemi üzerinden alarm alınır, Sistem gerçek zamanlı bir monitörden izlenir.
    c. Desteklemesi durumunda, İlgili Ağ Sisteminden alınan Olay Günlüklerinden (Log) Yetkisiz Erişim Denemelerinin tespiti yapılır. Bilgiler SIEM sistemi üzerinden alınır. Yetkisiz Erişim Denemesi tespit edildiği takdirde ilgili Sistem Yöneticisine alarm üretilir. Alarm aralığı 10 dakika, tüm kayıtların saklanma süresi en az 1 yıldır.
    d. Desteklemesi durumunda, İlgili Ağ Sisteminden alınan günlüklerde Yoğun Yönetici (Administrator) Yetki kullanımının tespiti yapılır. İlgili Sistemde Yoğun Yönetici Hak Kullanımı tespit edildiği takdirde ilgili Sistem Yöneticisine alarm üretilir. Alarm aralığı 10 dakika, tüm kayıtların saklanma süresi 1 yıldır. Burada dikkat edilmesi gereken husus bu işlemin tespiti sonrasında ilgili sistemdeki logların güvenli, güvenilir olamayacağı ve ilgili sisteme erişilemeyebileceğidir.
    e. Ağ Sisteminde aşırı kaynak tüketimi incelenir. Ağ sistemlerinde aşırı CPU, RAM, I/O tüketimi durumunda ilgili Ağ Yöneticisine Alarm üretilir.

ACİL DURUMLARDA YAPILMASI GEREKEN İŞLEMLER:

Saldırı Tespiti Sonrası İlk Yanıt Aşaması:

Saldırının türünün bir "DDoS veya DoS" olarak tanımlanması durumunda, öncelikle saldırıya yanıt verecek personele ulaşılır. İletişim bilgisi SİBER OLAYLARA MÜDAHALE TABLOSU'nda bulunmaktadır.

1. Bir veya Birden Fazla Kaynaktan Büyük Boyutlu ICMP Paket Gönderme Sonucu Sunucunun Yanıt Veremez Duruma Gelmesi;
    a. Durum Tespiti SIEM ve Firewall Sistemi Üzerinden yapılabilir.
    b. İlgili Sisteme Gelen ICMP Paketleri Firewall üzerinden kapatılır.
    c. Firewall üzerinden kesilemediği durumlarda İşletim Sistemi Firewall Yazılımı üzerinden Gelen ICMP Trafiği kesilir.
    d. ICMP Paket büyüklüğü sunucu üzerinden kısıtlanarak erişime açılır.

    Not: Önemli bir ihtiyaç yoksa Dışarıdan İçeriye doğru gelen ICMP Trafiğinin Firewall tarafından engellenmesi gereklidir.

    Not: Kapatılan Servisin, işe Olan Etki Analizinin (Risk Analizinin) yapılması gereklidir.
2. UDP Flood Saldırısı:
    a. UDP Flood Saldırısı SIEM ve Firewall üzerinden tespit edilir. Saldırı SIEM sistemleri üzerinde ciddi bir olay yükü oluşturabilir. Bu etki ciddi disk kullanımlarına neden olabilir. SIEM sistemleri üzerinde olası "log" kayıplarının engellemesi için "Log Rotation" **uygulanmamalıdır** (bu durumun dezavantajı, Log Sistemini kayıt tutamaz duruma getirecek bir öncü saldırı olabileceğidir).
    b. İlgili Servis Sağlayıcı ile İletişime geçilerek, saldırının sınırlandırılması sağlanır. İletişim Bilgisi SİBER OLAYLARA MÜDAHALE TABLOSU'nda bulunur.
    c. Saldırının tüm servisleri etkilemesi durumunda, Saldırı yapılan Hedef Servis Firewall üzerinden geçici olarak kapatılır. Bu durum E-Posta, DNS Servisi için uygulanmaz. Bunun yerine İlgili Servis Sağlayıcı ile bağlantıya geçilerek "Mitigation" stratejisi uygulanır.
3. TCP Flood Saldırısı:
    a. Durum Tespiti SIEM ve Firewall Sistemi Üzerinden yapılabilir.

b. Kaynak IP yasaklanabilir (ancak Dağıtık olarak gelen bir saldırı tipinde (Botnet) IP yasaklama pek uygulanabilir değildir).
c. İlgili Servis Sağlayıcı ile İletişime geçilerek, saldırının sınırlandırılması sağlanır. İletişim Bilgisi SİBER OLAYLARA MÜDAHALE TABLOSU'nda bulunur.
d. Saldırının ülke dışından gelmesi durumunda geçici olarak Ülke bazlı sınırlandırma yöntemi kullanılabilir.
e. Saldırının tüm servisleri etkilemesi durumunda, Saldırı yapılan Hedef Servis Firewall üzerinden geçici olarak kapatılır. Bu durum E-Posta, DNS Servisi için uygulanmaz. Bunun yerine İlgili Servis Sağlayıcı ile bağlantıya geçilerek "Mitigation" stratejisi uygulanır.
f. "Mitigation" stratejisinin uygulanamadığı, ilişkili sistemlerin tamamını etkilenmesi ve etkinin yüksek olduğu durumlarda Servis geçici olarak kapatılarak işe olan etki azaltılabilir.

4. Uygulama Katmanına Yönelik Saldırılar (HTTP Flood):
   a. Durum Tespiti SIEM, WAF ve Firewall Sistemi üzerinden yapılabilir.
   b. Kaynak IP yasaklanabilir (ancak Dağıtık olarak gelen bir saldırı tipinde (Botnet) IP yasaklama pek uygulanabilir değildir).
   c. Saldırın alt türünün tanımlanması için Erişim (Access) günlüklerinden (Log) Hedef Adres incelenir. Zayıflık bir konfigürasyon veya kod hatasından kaynaklı ise Sistem, Yönetici ve Yazılım Geliştirici tarafından gerekli düzeltmeler yapılmalıdır.
   d. Saldırının tüm servisleri etkilemesi durumunda, Saldırı yapılan Hedef Servis Firewall üzerinden geçici olarak kapatılır. İlgili Servis Sağlayıcı ile bağlantıya geçilerek "Mitigation" stratejisi uygulanır.
   e. "Mitigation" stratejisinin uygulanamadığı, ilişkili sistemlerin tamamını etkilenmesi ve etkinin yüksek olduğu durumlarda Servis geçici olarak kapatılarak işe olan etki azaltılabilir.

İLK YANIT SONRASI SİSTEMİN TEKRAR KAZANILMASI AŞAMASI

1. Yüklenici bir firma var ise ilgili firmadan destek alınır.
2. İlgili Cihazlar, İşletim Sistemleri ve Yazılımlar ile ilgili güncel bir yama olup olmadığına Resmi Sitesinden bakılır.
3. İlişkili Sistemler ile ilgili bir zafiyet olup olmadığı aşağıdaki veya benzer kaynaklardan araştırılır.
   - https://nvd.nist.gov/vuln/search
   - https://cve.mitre.org/cve/search_cve_list.html

TAM KAZANIM:

1. Tam kazanım için SİBER OLAY KAYIT FORMLARI doldurulur.
2. Doldurulan Form ile olay takibi yapılarak gerekli faaliyetler tetiklenir.
3. Tam Kazanım amacı ile devreye alınan sistemler için;
   a. İşletim Sistemi Güncellemeleri yapılmalı.
   b. Servis Yazılım Güncellemeleri yapılmalı.
   c. Uygulama Yazılım Güncellemeleri ve ihtiyaç duyulan yamalar yapılmalı.
   d. Sistem Penetration Test'e tabi tutularak zayıflıkların durumu kontrol edilmelidir.
4. Ayrıca Dağıtık Hizmet Durdurma Saldırılarına için DDOS YANIT PROSEDÜRÜNE bakılmalıdır.
5. Zayıflığın Kaynağı bir "Sıfırıncı Gün Zayıflığından" Kaynaklı olması durumunda ZERO DAY OLAY YANIT PROSEDÜRÜNE bakılmalıdır.

Firewall, SIEM, DLP, MRTG, PRTG, vb. Kontrol Servislerinin Güvenliği:

İlgili Sistemler için;

1. Güncellemeleri yapılıyor olmalı.
2. Güvenli bir VLAN üzerinde olmalı.
3. Zayıflık taramasından geçmiş olmalı.
4. Zaman bilgisini bir NTP üzerinden alıyor olmalı.
5. Sadece ilgili kişiler, ilgili servislere erişiyor olmalı.
6. İlgili Sistemler, uygulanabilir durumlarda, kendi sistem kaynaklarında, kontrolü devre dışı bırakabilecek aşırı kaynak kullanımı gerçekleştiğinde ilgili Sistem Yöneticisine alarm üretiliyor olmalıdır.

İLGİLİ REFERANS DOKÜMANLAR VE KONTROL MADDELERİ:
REFERANS VERİLEN:

REFERANS ALINAN:
1. A.16.1.1 | İlişkili Kontroller: A.16.1.1
2. A.16.1.2 | İlişkili Kontroller: A.16.1.2
3. A.16.1.3 | İlişkili Kontroller: A.16.1.3
4. A.16.1.4 | İlişkili Kontroller: A.16.1.4
5. A.16.1.5 | İlişkili Kontroller: A.16.1.5
6. A.16.1.6 | İlişkili Kontroller: A.16.1.6
7. A.16.1.7 | İlişkili Kontroller: A.16.1.7

Bu sayfa son olarak 05 Aralık 2021 tarihinde ve 14.41 saatinde düzenlenmiştir.