AĞ SİSTEMLERİ SİBER OLAY YANIT PROSEDÜRÜ:

Prosedür Adı:	AĞ SİSTEMLERİ SİBER OLAY YANIT PROSEDÜRÜ
Doküman Kodu:	BGYS.PR.T.003.ATABAUM.BC
Doküman Sahibi:	BGYS Yöneticisi
Doküman Onay Tarihi:	05/12/2021
Gizlilik Sınıfı:	İç Kullanım

İçindekiler:

1. AMAÇ
2. KAPSAM
3. TANIMLAR
4. SORUMLULAR
5. UYGULAMA
    a. SALDIRININ TESPİT EDİLMESİ AŞAMASI ve GEREKLİLİKLER AŞAMASI
    Saldırının tespit edilebilmesi için kullanılan mevcut kontroller
    b. ACİL DURUMLARDA YAPILMASI GEREKEN İŞLEMLER
    Saldırı Tespiti Sonrası İlk Yanıt Aşaması
    c. İLK YANIT SONRASI SİSTEMİN TEKRAR KAZANILMASI AŞAMASI
    d. TAM KAZANIM
    e. Firewall, SIEM, DLP, MRTG, PRTG, vb. Kontrol Servislerin Güvenliği
6. İLGİLİ REFERANS DOKÜMANLAR VE KONTROL MADDELERİ
    a. REFERANS VERİLEN
    b. REFERANS ALINAN

AMAÇ:

Bu prosedür, Kuruluş Ağ Sistemlerine Yönelik bir Siber Saldırı Meydana Gelmesi Durumunda yapılacak iş adımlarını belirlemeyi amaçlar.

KAPSAM:

Tüm Modem, Router, Firewall, Switch, AP Controller, vb. Ağ Donanım ve Yazılımlarıdır.

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 POLİTİKASI'nda 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 AĞ SİSTEMLERİ SİBER OLAYI" olarak tanımlanması durumunda, öncelikle saldırıya yanıt verecek personele ulaşılır. İletişim bilgisi SİBER OLAYLARA MÜDAHALE TABLOSU'nda bulunmaktadır.

1. Bir Firewall'a, Yetkisiz Erişim yapıldığının tespiti durumunda;
    a. Firewall Sistemi Ağdan çıkarılır.
    b. Yüklenici bir firma var ise ilgili firmaya ulaşılır.
    c. Üzerindeki Mevcut Firmware ve konfigürasyonların yedeği alınır (bu yedek, yedekten geri dönülmesi için değil olay incelemesi için alınmaktadır).
2. Bir Modem, AP veya Router'a Yetkisiz Erişim yapıldığının Tespiti Durumunda;
    a. İlgili Modem Ağdan çıkarılır.
    b. Yüklenici bir firma var ise ilgili firmaya ulaşılır.
    c. Üzerindeki Mevcut Firmware ve konfigürasyonların yedeği alınır (bu yedek, yedekten geri dönülmesi için değil olay incelemesi için alınmaktadır).
3. Omurga veya Kenar Anahtarlama Cihazına Yetkisiz Erişim yapıldığının tespiti durumunda;
    a. İlgili Ağ Cihazına olan erişimlerin kısıtlanması için sistem portlarının tamamı fiziksel olarak çıkartılır.
    b. Yüklenici bir firma var ise ilgili firmaya ulaşılır.
    c. Üzerindeki Mevcut Firmware ve konfigürasyonların yedeği alınır (bu yedek, yedekten geri dönülmesi için değil olay incelemesi için alınmaktadır).

İLK YANIT SONRASI SİSTEMİN TEKRAR KAZANILMASI AŞAMASI:

1. Yüklenici bir firma var ise ilgili firmadan destek alınır,
2. İlk cevap sonrası Sisteme Yetkisiz Erişim yapan Kaynağın ve ilişkili sistemlerin tam olarak belirlenmesinden sonra, ilgili Sistem ağa dahil edilmeden önce Fabrika ayarlarına getirilir.

3. İlişkili Tüm Parolalar değiştirilir.
4. Daha önce alınmış güvenli bir konfigürasyon incelenerek konfigürasyondan kaynaklı bir zafiyet olup olmadığı incelenir. Konfigürasyon ile ilgili bir zafiyet **yoksa** Yedek, sisteme aktarılır.
5. Cihaz ile ilgili güncel bir yama (firmware) olup olmadığına resmi sitesinden bakılır.
6. Cihaz ile ilgili bir zafiyet olup olmadığı aşağıdaki veya benzer adreslerden araştırılır.
    a. https://nvd.nist.gov/vuln/search
    b. https://cve.mitre.org/cve/search_cve_list.html
7. Erişim kaynağı belirlenmeden sistem hizmete açılamaz!

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 Saldırıları için DDOS YANIT PROSEDÜRÜNE bakılmalıdır.

5. Zayıflığın Kaynağı bir "Sıfırıncı Gün Zayıflığından" Kaynaklı ise 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 Sunucu 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.