SUNUCU UYGULAMALARI SİBER OLAY YANIT PROSEDÜRÜ:

Prosedür Adı:	SUNUCU UYGULAMALARI SİBER OLAY YANIT PROSEDÜRÜ
Doküman Kodu:	BGYS.PR.T.005.ATABAUM.BC
Doküman Sahibi:	BGYS Yöneticisi
Doküman Onay Tarihi:	05/12/2021
Gizlilik Sınıfı:	İç Kullanım

İçindekiler:

AMAÇ:

Bu Prosedür Kuruluş Sunucu Sistemleri ve Uygulama Sistemlerine Yönelik bir Siber Saldırı Meydana Gelmesi Durumunda Yapılacakları belirler.

KAPSAM:

Kuruluş veya Kuruluş ile ilişkili Tüm Sunucu Sistemlerini (Web Sunucu, İlişkili Veritabanı Sistemleri, vb.) 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 ilişkilendirilmiş olan 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 trafik 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. Dışarıdan İçeriye (Sisteme) Anormal Portlara ve Protokollere olan erişim denemeleri. Örneğin TCP 80 ve TCP 443 açık olan sisteme UDP 6779 portundan erişim denemesi gibi. Sistem Yöneticisine Alarm üretilir. Alarm aralığı 10 dakika, tüm kayıtların saklanma süresi 1 yıldır.

c. İçeriden Dışarıya (Yerel Ağ veya İnternete) Anormal Portlara ve Protokollere olan erişim denemeleri. Örneğin güncelleme amacı ile TCP 80 ve TCP 443 açık olan sisteme UDP 6779 portundan erişim denemesi gibi. Alarm aralığı 10 dakika, tüm kayıtların saklanma süresi 1 yıldır.

2. Anormal Trafiğin Tespit edilebilmesinde ilgili Web Servisi ile ilişkilendirilen SIEM sistemi kullanılır. İlgili kayıtlar Web Sunucusu üzerinden yetkilendirilmiş is File Share kullanılabilir.
   a. Yoğun Oturum (Session) Olay Kaydı. Bu olay kayıt sayısının belirlenebilmesi için SIEM sistemi üzerinde ilgili sistemlerin 14 günlük trafik 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. Kritik Dosya ve Dizinlere erişim. Kritik dosya ve dizinler belirlenerek bu dizinlere bir erişim denemesi yapıldığında alarm üretilir.
   c. İlgili Sunucu Sisteminden dışarıya olan erişim Hedef IP adresleri kontrol edilir. Erişilmemesi gereken Hedef IP, Hedef Ülke Trafiği var ise Sistem Yöneticisine alarm üretilir. Bu Kontrolden Amaç Sahte Güncelleme (Rogue Update Attack), vb. saldırıların engellenmesidir.
3. Anormal Veri iletiminin tespit edilebilmesinde ilgili Web Servisi-Database Server ile ilişkilendirilen SIEM sistemi kullanılır. İlgili kayıtlar Web Sunucusu-Database Server üzerinden yetkilendirilmiş ise File Share kullanılabilir.
   a. Yoğun Oturum (Session) Olay Kaydı. Bu olay kayıt sayısının belirlenebilmesi için SIEM sistemi üzerinde ilgili sistemlerin 14 günlük trafik 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. Database sunucusunda kritik tablolara bir erişim denemesi meydana geldiğinde alarm üretilmelidir. Bu kritik tablolar ilgili Sistem Yöneticisi tarafından belirlenmelidir.
4. Sunucu Sistemlerinden alınan Bant Genişliği grafikleri ile 14 günlük trafik izlemesi yapılarak Normal/Anormal trafik seviyeleri belirlenir. Yüksek Upload/Download durumunda ilgili Bant Genişliği Takip Sistemi üzerinden alarm alınır, Sistem gerçek zamanlı bir monitörden izlenir.
5. Sunucu Sistemlerindeki Olay Günlüklerinden (Log) Yetkisiz Erişim Denemesinin tespiti. Bu bilgiler SIEM sistemi üzerinden alınır. Yetkisiz Erişim Denemesi tespit edildiği takdirde ilgili Sistem Yöneticisine alarm üretilir. Alarm aralığı 10 dakika, tüm kayıtların saklanma süresi 1 yıldır.
6. Sunucu Sistemlerindeki Olay Günlüklerinden Yoğun Yönetici (Administrator) Yetki kullanımının tespiti. 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 bu işlemin tespiti sonrasında ilgili sistemdeki logların güvenli/güvenilir olamayacağı ve ilgili sisteme erişilemeyebileceğidir.
7. Sunucu Sistemlerinde aşırı kaynak tüketimi incelenir. Sunucu sistemlerinde aşırı CPU, RAM, I/O tüketimi durumunda ilgili Sistem Yöneticisine Alarm üretilir.

ACİL DURUMLARDA YAPILMASI GEREKEN İŞLEMLER:

Saldırı Tespiti Sonrası İlk Yanıt Aşaması:

Saldırı türünün bir "UYGULAMA KATMAN SALDIRISI" olarak tanımlanması durumunda:

a. DMZ bölgesindeki Sisteme Saldırgan tarafından erişilmemişse:
   1- Saldırının kaynağı belirlenir. Bu kaynak; IP adresi, Kaynak Port, Hedef Port, İletişim Protokolü ve Kaynak Ülke bilgisidir.
   2- Saldırı tipi bir deneme yanılma saldırısı ise sadece IP Adresi engellenebilir. Ancak dışarıya açık ve kullanılan UDP Port engellemelerinin IP bazlı yapılması halinde ilişkili sistemlere olan erişimi bozulabilmektedir. Bu nedenle ilişkili sistemler gözden geçirildikten sonra gerekli engellemeler devreye alınabilir.

3- Saldırı Uygulama Katmanına (Layer-7) yönelik bir DDoS saldırısı ve Sisteme olan erişilebilirliği bozabilecek seviyede ise öncelikle IP adresi Firewall tarafından bloklanmalıdır. Bloklama işlemi UDP protokolü için uygulanmaz.
4- Sistem erişilebilirliği bozulmuş ve ilişkili diğer sistemleri de etkilemeye başlamışsa, Sistem Yöneticisi sistemin erişimi kapatıldığında mümkün olan etkiyi belirleyerek çıkış port ve protokolü dışarıya kapatabilir (bu analizin Risk Değerlendirmesinde yapılması gereklidir.)
5- Şayet saldırı Çıkış Bant Genişliğini etkileyebilecek seviyede ise İlgili Servis Sağlayıcı ile iletişime geçilerek destek alınır.

b. DMZ bölgesindeki Sisteme Saldırgan tarafından erişilmişse:
   1. Olası delillerin kaybedilmemesi için Sistem **kapatılmaz**.
   2. Sistem Kilitlenir (Lockdown), yani dışarı ve içeri olan erişimlerin tamamı Firewall üzerinden kapatılır.
   3. İç ağa ve diğer VLAN'lara olan erişimin engellenmesi için, Sistem Ağ Kartı geçici olarak kapatılır, Fiziksel sistem için Ağ Bağlantı Kablosu çıkartılır.
   4. Sisteme sadece Fiziksel olarak erişim yapılır.
   5. Sistem sanal bir sistem ise "Snapshot" alınır.
   6. Sistem gerçek bir sistem ise üzerindeki tüm veriler güvenli ve genel yedekleme ile ilişkisi olmayan bir alana yedeklenir. Bu yedekleme işleminde ikincil enfeksiyonların oluşmaması için ilişkisiz bir yedekleme yöntemi tercih edilmelidir.
   7. Sistem olan erişim seviyesi tespit edilir. Bu erişim seviyesi;
      a. İşletim sistemi seviyesinde bir kullanıcı oluşturmaya kadar ulaşmışsa. Tüm sistem enfekte kabul edilir. Sistemin kurtarılması temizlenmesi yerine yeni bir kurulum yapılarak var olan veri yedekleri aktarılabilir veya "Snapshot" kullanılarak geri dönülür. Sistem ile ilişkili tüm Parolalar değiştirilir. Tüm Erişim Yetkileri kontrol edilir.
      b. Sadece Uygulama yazılımına kullanıcı olarak erişilmiş ise, ilgili kullanıcı ve erişim vektörü belirlenir. Değişiklik yapılmış ise değişiklik incelenerek yedekten geri dönüşe gerek olup olmadığı belirlenir. Sistem ile ilişkili Tüm Yönetici Parolaları ve ilgili kullanıcı parolaları değiştirilir. Tüm Erişim Yetkileri kontrol edilir.
      c. Sadece Uygulama yazılımına "admin" olarak erişilmiş ise veritabanı ve uygulama yazılım dosyaları yedekten geri yüklenir.
      d. Sadece Uygulama yazılımına erişim yapılmış ve sadece Gizlilik bozulmuşsa erişim kaynağı belirlenir. Sistem ile ilişkili tüm Parolalar değiştirilir. Servis Seviyesindeki tüm Erişim Yetkileri kontrol edilir.
      e. İlgili uygulama Servis veya İşletim Sistemi üzerinden diğer sistemlere de yetkisiz erişim yapıldığı tespit edildiği takdirde bu sistemler için de yukarıdaki maddeler uygulanır.
   8. Tüm kayıtlar adli bir inceleme için yedeklenir, dış ve güvenli bir ortama alınır. Bu kayıtların saklanma süresi yasal bir soruşturma oluşturabileceği için 10 (on) yıldır.

c. İç sistemdeki (SSS-Secure Server Side VLAN) bir Sunucuya Saldırgan tarafından erişilmişse:
   1. Olası delillerin kaybedilmemesi için Sistem **kapatılmaz**.
   2. Sistem Kilitlenir (Lockdown) yani dışarı ve içeri olan erişimlerin tamamı Firewall üzerinden kapatılır.
   3. İç Ağa ve diğer VLAN'lara olan erişimin engellenmesi için, Sistem Ağ Kartı geçici olarak kapatılır, Fiziksel Sistem için Ağ Bağlantı Kablosu çıkartılır.
   4. Sistem sanal bir sistem ise "Snapshot" alınır. Amaç olası delillerin korunmasıdır.
   5. Sistem gerçek bir sistem ise üzerindeki tüm veriler güvenli ve genel yedekleme ile ilişkisi olmayan bir alana yedeklenir. Bu yedekleme işleminde, ikincil enfeksiyonların oluşmamasının engellenmesi için ilişkisiz bir yedekleme yöntemi tercih edilmelidir.
   6. Sisteme olan erişim seviyesi tespit edilir. Bu erişim seviyesi;

a. İşletim sistemi seviyesinde bir kullanıcı oluşturmaya kadar ulaşmışsa. Tüm sistem enfekte olarak kabul edilir. Sistemin kurtarılması temizlenmesi yerine yeni bir kurulum yapılır ve var olan veri yedekleri aktarılabilir veya güvenli "Snapshot" kullanılarak geri dönülür.
b. Sadece Uygulama yazılımına kullanıcı olarak erişilmiş ise, ilgili kullanıcı ve erişim vektörü belirlenir. Değişiklik yapılmış ise değişiklik incelenerek yedekten geri dönüşe gerek olup olmadığı belirlenir (yani değişikliğin sınırları belirlenir).
c. Sadece Uygulama yazılımına "admin" olarak erişilmiş ise Veritabanı ve uygulama yazılım dosyaları yedekten geri dönülür.
d. Sadece Uygulama yazılımına erişim yapılmış ve sadece Gizlilik bozulmuşsa erişim kaynağı belirlenir.
e. İlgili uygulama Servis veya İşletim Sistemi üzerinden diğer sistemlere de yetkisiz erişim yapıldığı tespit edildiği takdirde bu sistemler için de yukarıdaki maddeler uygulanır.

7. Tüm kayıtlar adli bir inceleme için yedeklenir, dış ve güvenli bir ortama alınır. Bu kayıtların saklanma süresi yasal bir soruşturma oluşturabileceği için 10 (on) yıldır.

İLK YANIT SONRASI SİSTEMİN TEKRAR KAZANILMASI AŞAMASI:

1. İlk Cevap sonrası sisteme olan erişime neden olan kaynağın tam olarak ve ne zaman erişildiğinin belirlenmesinden sonra SİSTEM SALDIRI TESPİTİ SONRASI İLK YANIT AŞAMASI bölümünde belirtilen kontroller dikkate alınarak erişime açılır.
2. **DİKKAT:** 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 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 5 Aralık 2021 tarihinde ve 11.50 saatinde düzenlenmiştir.