"ZERO DAY" SİBER OLAY YANIT PROSEDÜRÜ:

Prosedür Adı:	"ZERO DAY" SİBER OLAY YANIT PROSEDÜRÜ
Doküman Kodu:	BGYS.PR.T.007.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 Siber Saldırı olması ve Saldırının bir Sıfırıncı Gün (Zero Day) zafiyetinden kaynaklı olduğunun belirlenmesi durumunda neler yapılması gerektiğini amaçlar.

KAPSAM:

Kuruluş ve kuruluş ile ilişkili bilgi sistemlerini 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:

Bir saldırının Zero Day Zafiyeti/Açıklığı olarak tanımlanması için;

1. Saldırıya Hedef olan sistemlerde; Zafiyetin
    a. Donanımdan,
    b. İşletim Sisteminden,
    c. Bir yazılımdan kaynaklı olması ve

d. İlgili Sistemlerin aşağıdaki web adreslerinden sorgulandığında güncel bir açıklık/yama bulunup/bulunmadığına göre belirlenebilir.
   - https://nvd.nist.gov/vuln/search
   - https://cve.mitre.org/cve/search_cve_list.html

2. Zero Day Zafiyetini belirleme aşamasında aşağıdakiler kullanılabilir:
   a. SIEM sistemleri.
   b. MRTG/PRGT Sistemleri.
   c. Antivirüs Sistemleri.
   d. Personelin farkındalığı.

ACİL DURUMLARDA YAPILMASI GEREKEN İŞLEMLER:

Saldırı Tespiti Sonrası İlk Yanıt Aşaması:

Saldırının türünün bir Zero Day (Sıfırıncı Gün) açıklığı ile ilişkili olduğunun belirlenmesinin ardından, öncelikle saldırıya yanıt verecek personele ulaşılır. İletişim bilgisi SİBER OLAYLARA MÜDAHALE TABLOSU'nda bulunmaktadır.

Zero Day Zafiyeti Sunucu, İşletim Sistemi veya Servis Yazılımında bulunuyor ise;

a. Zero Day Zafiyeti gözlenen sisteme olan erişim, geçici olarak kısıtlanır veya erişim kaldırılır.
b. Zero Day Zafiyeti olduğu düşünülen aktivite, SIEM Sistemi veya ilgili Sistem günlüklerinden (log) incelenerek hangi sistemlere erişilebilir olduğu doğrulanır.

İLK YANIT SONRASI SİSTEMİN TEKRAR KAZANILMASI AŞAMASI

1. Yüklenici bir firma var ise ilgili firmadan destek alınır.
2. 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
3. Şayet zafiyetin etkisi sınırlandırılabiliyorsa kısıtlı erişim verilebilir. Örneğin yazma izninin geçici olarak kaldırılması ve sadece okuma izninin verilmesi gibi.
4. Sistem sadece Yerel Ağ ve Sistemlere açılır, Dış Ağ ve Ortamlara erişim geçici olarak Firewall üzerinden kısıtlanır.

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.

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.