ELEKTRONİK SİSTEMLER SİBER OLAY YANIT PROSEDÜRÜ:

Prosedür Adı:	ELEKTRONİK SİSTEMLER SİBER OLAY YANIT PROSEDÜRÜ
Doküman Kodu:	BGYS.PR.T.004.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 "Fiziksel Donanım Ekleme, Çıkartma" tespit edilmesi durumunda yapılması gerekenleri amaçlar.

KAPSAM:

Kuruluş bilgi varlıkları ile ilişkili tüm 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:

1. Ağ Cihazları SNMP v2.0 Protokolü üzerinden takip edilmekte ve izlenmektedir,
2. Ağ sistemlerine izin verilmeyen bir sistem eklenememektedir (RADIUS kullanılmaktadır).
3. Sisteme izinsiz bir cihaz eklendiği takdirde belirlenebilmekte ve ilişkili fiziksel port belirlenebilmektedir.

4. SIEM sistemi ile anormal aktiviteler tespit edilmektedir.
5. Personel Bilgi Güvenliği Farkındalık Eğitimlerinde İzinsiz Eklenen Donanım konusunda bilgilendirilmiştir.

ACİL DURUMLARDA YAPILMASI GEREKEN İŞLEMLER:
Saldırı Tespiti Sonrası İlk Yanıt Aşaması:
Saldırının türünün bir "Fiziksel Donanım çıkartma/ekleme yöntemi" olduğu tespit edildiğinde saldırıya yanıt verecek personele ulaşılır. İletişim bilgisi SİBER OLAYLARA MÜDAHALE TABLOSU'nda bulunmaktadır.

İzinsiz eklenen donanımın tespit edildiğinde donanım adli bir incelemede delil olabileceği için parmak izi bırakılmadan, donanım doğrulanarak ve olası tehlikeler göz önünde bulundurularak (patlayıcı, elektrik kaçağı, vb. tehditler) ağdan ayrılır.

İLK YANIT SONRASI SİSTEMİN TEKRAR KAZANILMASI AŞAMASI:
1. Sistem'den ilgili donanım ayrılır.
2. MAC adresi belirlenerek SIEM sisteminden aldığı IP adresinden hareketle eriştiği IP Adresleri ve Portlar bulunur. Eriştiği IP Adres ve Portlarda başka istemciler de mevcut ise bu istemcilerde IP ➔ MAC ➔ Fiziksel Port tespiti ile tespit edilerek 1. Aşama uygulanır.

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 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 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.