ZARARLI YAZILIM VE OLTALAMA SALDIRISI SİBER OLAY YANIT PROSEDÜRÜ:

Prosedür Adı:	ZARARLI YAZILIM VE OLTALAMA SALDIRISI SİBER OLAY YANIT PROSEDÜRÜ
Prosedü Kodu:	BGYS.PR.T.006.ATABAUM.BC
Prosedür Sahibi:	BGYS Yöneticisi
Prosedür İlk Yayın Tarihi:	05/12/2021
Gizlilik Sınıfı:	İç Kullanım

İçindekiler:

AMAÇ:

Bu prosedür Kuruluş personeli ve Kuruluş Bilgi Sistemlerine Yönelik bir Oltalama (Phishing) saldırısının tespit edilmesi durumunda yapılması gereken kontrolleri belirlemek amacı ile oluşturulmuştur.

KAPSAM:

Kuruluş personeli, ilgili II. Taraf Personel 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:

1. Personel Bilgi Güvenliği Farkındalık Eğitimlerinden şüpheli bağlantılara tıklamaması, şüpheli bir durumda "Bilgi Teknolojieri Departmanına" bilgi vermesi konusunda eğitim verilmektedir.

2. İstemci Antivirüs Sisteminden zararlı yazılım tespit edilmesi durumunda alarm üretilmekte ve günlük olarak raporlanmaktadır.

ACİL DURUMLARDA YAPILMASI GEREKEN İŞLEMLER:

Saldırı Tespiti Sonrası İlk Yanıt Aşaması:

Saldırının türünün bir "Oltalama (Phishing) Yöntemi" olduğu tespit edildiğinde saldırıya yanıt verecek personele ulaşılır. İletişim bilgisi SİBER OLAYLARA MÜDAHALE TABLOSU'nda bulunmaktadır.

1. Saldırının tespit edildiği Sistemde zararlı bir yazılımın olup olmadığının anlaşılması ve önlem alınabilmesi için ilgili sistemin Ağ Bağlantısı kesilir.
2. Personelin hangi bağlantıyı tıkladığı tespit edilir.
3. Tüm personele benzer bağlantılara tıklamamaları için acilen duyuru yapılır.
4. Bağlantının kurulduğu IP adresi tespit edilerek SIEM Sisteminde arama yapılarak bu bağlantıya erişen istemciler tespit edilir. İlgili istemciler bulunarak 1. maddedeki işlemler uygulanır.
5. AntiSpam Servisi üzerinden ilgili E-Posta/IP Adresi (doğrulanarak) kapatılır. Birden fazla kaynaktan (örneğin Outlook, gmail, vb. yaygın servislerden) geliyorsa durum "abuse@domain.x" benzeri E-Posta ile bilgilendirme yapılır.
6. İstemci sistemi üzerindeki veriler, güvenli ancak diğer yedekleme alanları ile ilişkisi olmayacak şekilde depolanır.
7. Sistem "Sysinternals" Firmasının "tcpview" yazılımı ile incelenerek anormal bağlantı girişimi olup olmadığı incelenir. Şayet anormal bir bağlantı tespit edilirse "PID" alanından "Sysinternals" Firmasının "Process Explorer" yazılımı ile ilgili süreç (process) bulunur.
    a. Yazılım üzerinde bir değişiklik olduğu doğrulandığında ilgili süreç durdurularak sistemden kaldırılır.
    b. Bir değişiklik olmadığı ancak ilgili sürecin kullanıldığı düşünülüyorsa "Sysinternals" Firmasının "Process Monitor" yazılımı ile Süreç, Dosya ve Registry Kayıt Hareketleri izlenerek hangi dosyaların kullanıldığı, hangi dosyalara yazıldığı tespit edilerek ilgili dosyaların içerikleri ve ne yapıldığı kayıt edilir.
8. İlgili sistemde "tcpview" yazılımı ile tespit edilen (netstat) IP adresi, SIEM sistemi kullanılarak diğer istemciler ile ilişkisinin olup olmadığı incelenir.
9. End Point Security Rescue Disk (vb. boot bağımsız) bir medya (Live Boot) ile sistem taranır. Zararlı yazılım bulunursa temizlenir.

İLK YANIT SONRASI SİSTEMİN TEKRAR KAZANILMASI AŞAMASI

1. Sistem açılarak "Sysinternals" Firmasının "Process Explorer" yazılımı ile süreçler VirusCheck imza doğrulaması ile kontrol edilir. "Tcpview" ile kontrol edilerek bağlantılar doğrulanır. Şayet şüpheli bir uygulama bulunmaz ise Sistem ağa tekrar dahil edilir. SIEM sistemi üzerinden ağ izlenir.
2. Şayet sistem üzerindeki zararlı yazılımlar tam olarak temizlenmezse Sistem formatlanarak, Fabrika kurulumu yapılır. Geri alınması gereken dosyalar var ise Antivirüs taramasından geçirilerek kontrol edilir.

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.