1 AMAÇ

Bilgi Güvenliği Olayları Tespit ve Müdahale Prosedürü ’nün amacı bilgi güvenliği olaylarını, tespit ve raporlama süreçlerini, müdahale ekip yapısını, müdahale ve yanıt sürecini tanımlamaktır.

2 KAPSAM

Bilgi Güvenliği Olayları Tespit ve Müdahale Prosedürü ‘nün kapsamı **İYTE Bilgi İşlem Daire Başkanlığı**, bilgi varlıkları (sistemler, ağ altyapısı, basılı bilgiler... vs.) ve organizasyonunun tümüne yönelik bilgi güvenliği olayları ve bunlara karşılık verilecek müdahale tepkisidir.

İYTE Bilgi İşlem Daire Başkanlığı personeli olay tespiti, raporlama ve araştırma aşamaları açılarından ilgilidir. Olayı ele alma ve müdahale safhalarında ise öncelikli görev alacak personel ve birimler aşağıdaki gibidir:

- BİDB SOME (Siber Olaylara Müdahale) Ekibi
- Bilgi Güvenliği Birimi
- Üst Yönetim
- Ağ ve Sistem Yönetimi Birimi
- Donanım ve Teknik Destek Birimi
- Yazılım Geliştirme Birimi

3 TANIMLAR VE KISALTMALAR

Terim	Tanım/Açıklama
BGYS	Bilgi Güvenliği Yönetim Sistemi
Kurum	**İYTE Bilgi İşlem Daire Başkanlığı**
SOME	Siber Olaylara Müdahale Ekibi
USOM	Ulusal Siber Olaylara Müdahale Merkezi

4 PROSEDÜR

İYTE Bilgi İşlem Daire Başkanlığı Siber Olaylara Müdahale Ekibi aşağıdaki birimlerde çalışan kişilerden oluşur.

Bilgi Güvenliği Birimi

- Bilgi Güvenliği Birimi
- Ağ ve Sistem Yönetimi Birimi
- Donanım ve Teknik Destek Birimi
- Yazılım Geliştirme Birimi

Gerekli görülen durumlarda kurum dışı iletişimi (altyapı hizmet sağlayıcıları, Telekom otoritesi – BTK, diğer Telekom operatörleri veya itfaiye, hastane, polis gibi kamu kurumları ile) SOME başkanının bilgisi dâhilinde ilgili bölümler sağlar.

USOM ile iletişim sip.usom.gov.tr üzerinden sağlanmakta, zafiyet ve/veya siber olaylarla ilgili istihbarat alınmakta, çözüm önerileri sunulmakta ve siber olay raporlama işlemi yapılmaktadır. SOME bilgi güvenliği olayları gerçekleştiğinde olayın yayılmasını önleyici, etkisini azaltıcı ve ortadan kaldırıcı faaliyetleri hızlı, etkili ve maliyet etkin biçimde gerçekleştirmekle görevlidir. SOME, olay gerçekleştiğinde görevini yerine getirmek amacıyla aldığı kararları uygulamak için kurum içinde tam yetkilidir.

Bilgi güvenliği olayı bilgi varlıklarına yönelik tehditlerin gerçekleşmesi anlamına gelir. Bu olaylara örnek olarak aşağıdakiler verilebilir:

- Ağ iletişimi veya uygulamalara yönelik ağ (internet) üzerinden gerçekleştirilen hizmet kesinti saldırıları
- Sistemlerin (hacker saldırısı sonucu) ele geçirilmesi
- Sistemlerde virüs, spyware ve diğer kötü niyetli yazılımların belirlenmesi
- Kuruma ve müşterilerine ait bilgilerin (çeşitli şekillerde) çalınması
- Başarılı ve başarısız fiziksel ve mantıksal izinsiz giriş denemeleri
- Kurum bilgi varlıklarının (dizüstü bilgisayar, doküman, taşınabilir medya, v.d.) çalınması

Beklenmedik sistem hataları da bir bilgi güvenliği olayının yan etkisi olabilir. Bu nedenle araştırma sürecini başlatabilmek için bilgi güvenliği olayı olarak raporlanmalıdır.

SOME Ekip Başkanı önleyici tavır içinde olarak, sektörel, bölgesel, Bakanlığın kullandığı altyapıya yönelik başka şirketler ve kurumlarca maruz kalınmış olayları veya konuyla ilgili

otoritelerin duyurularını da takip ederek olay gerçekleşmeden iyileştirici faaliyet geliştirir (bakınız "Düzeltici Faaliyet Prosedürü").

4.1 Olay Tespiti

Yukarıda örnekleri verilmiş olan bilgi güvenliğini ilgilendiren tüm olaylar (gerçekleşmiş veya şüphe durumu oluşmuş olsun) Bilgi Güvenliği Birim Yöneticisine doğrudan veya BT destek personeline iletilir. Olay kayıtları "Düzeltici Faaliyet Prosedürü"ne uygun olarak (olayın aciliyetine göre hemen veya olaydan sonra) Bilgi Güvenliği Birim Yöneticisi tarafından tutulur.

SOME başkanı bilgi güvenliği olayını aşağıdaki kriterlere göre sınıflandırır:

Olay Kritiklik Sınıfı:	Yüksek	Orta	Düşük
Detaylar:	Yüksek gizlilik, bütünlük veya süreklilik ihtiyacına sahip bilgi varlığı olaydan etkilenmiş veya risk altındadır. Gizli (ör: görüşme trafik verisi) veya özel bilgi (ör: ağ konfigürasyon yedekleri) olaydan etkilenmiş veya risk altındadır. İş (iletişim hizmeti) sürekliliği etkilenmiş veya risk altındadır.	Orta gizlilik, bütünlük veya süreklilik ihtiyacına sahip bilgi varlığı olaydan etkilenmiş veya risk altındadır.	Düşük gizlilik, bütünlük veya süreklilik ihtiyacına sahip bilgi varlığı olaydan etkilenmiş veya risk altındadır.

Bilgi Güvenliği Birim Yöneticisi gerek görmesi halinde olay hakkında daha fazla bilgi toplamak için olayı raporlayan personel ile görüşür. Eğer olayı raporlayan personel düzenleyici otoritelere süreç hakkında bilgi vermek durumundaysa SOME faaliyetleri için SOME başkanından bilgi almayı gerekli periyodlarda talep edebilir. Bu talep sürecin sıra dışılığı

nedeniyle sözlü olarak yapılır ve yanıtlanır. Hukuki süreci ilgilendiren hiç bir olay yanıt faaliyeti SOME başkanı tarafından gerekli koordinasyonun gerçekleştirilmesi ve kararın alınmasından önce başlatılmaz.

4.2 Kanıt Toplama

SOME başkanı, bilgi güvenliği olayının niteliği gerektiriyorsa, Hukuk Müşavirliği ve üst yönetimin görüşlerine başvurarak adli bilişim süreci işletilip işletilmeyeceğine karar verir. Eğer disiplin süreci veya hukuki sürecin başlatılması ihtiyacı oluşabilecekse kanıt toplama süreci kanıtın geçerliliğini en yüksek seviyede tutacak biçimde işletilir.

Buna göre kanıtlar aşağıdaki esaslara göre toplanır ve incelenir:

- Kâğıt doküman halindeki kanıtlar söz konusu olduğunda dokümanı tespit eden ve gözetim altında tutan personel kanıt listesinde dokümante edilir. Dokümanların orjinalleri güvenli (kilit altında ve sadece SOME ekibinin erişimi olan) bir yerde saklanır, incelemeler mümkünse fotokopi kopyaları üzerinde yapılır.
- Elektronik formatta bir kanıt söz konusu olduğunda kanıtın bulunduğu medyanın (bilgisayar diski, yedek kartuşu, usb bellek, v.b.) tüm alanının “forensic” imajı alınır. “Forensic” imajı “write blocker” donanımı ile, yoksa yazılım tabanlı “write blocker” fonksiyonu bulunan bir forensic imaj yazılımı ile yapılır. Alınan imajın orjinalinin aynısı olduğunu kanıtlamak için kopyalama işleminden sonra hash özeti alınır ve kaydedilir (genellikle kullanılan kopyalama yazılımı vasıtasıyla yapılabilir). Orjinal kanıt’ı elde eden ve saklayan personelin isimleri tarih ve saat bilgileriyle birlikte gözetim listesine kaydedilir. Orjinal kanıt güvenli (kilit altında ve sadece SOME ekibinin erişimi olan) bir yerde saklanır. Tüm inceleme “forensic” kopyası üzerinde yapılır. İnceleme bu amaç için geliştirilmiş forensic yazılımları ile yapılır. Bu yazılımlar silinmiş dosyaları kurtarma, uzantısı ile dosya tipi uyuşmayan dosyaları tespit etme, anahtar kelime arama, benzer nitelikteki dosyaları gruplama (örneğin tüm e-posta’ları bir arada incelemeye imkân verme), yapılan işlemlerin iz kayıtlarını tutma, dosyaları kanıttan dışarı alma, raporlamayı kolaylaştırma gibi imkânlar sunar. Tüm inceleme işlemleri mutlaka sadece kopya imaj üzerinde gerçekleştirilir.

Resmi sürecin işletilebilmesi için kanıta ihtiyaç olmadığı, ancak olaya verilecek yanıtın doğru tespit edilebilmesi, verilen zararın anlaşılabilmesi için de kanıt toplama ihtiyacı olan durumlar olabilir. Bu durumlarda kanıtların kopyalarının alınması ve gözetim zinciri (chain of custody) gibi adımlar atlanabilir.

4.3 Olay Yanıt Süreci

Bilgi güvenliği olayına verilecek yanıt SOME tarafından belirlenir ve uygulanır. Yanıt sürecinde polis ve diğer otoritelerden destek isteneceğine veya sürecin tamamen bu taraflar tarafından yürütülmesine SOME başkanı, Hukuk Müşavirliği ve üst yönetimin görüşleri doğrultusunda karar verir.

Her olayın kendine has özel ve çevresel şartları bulunacağından izlenecek yanıt süreci olay bazında belirlenir.

4.4 Bilgi Güvenliği Olaylarından Öğrenme

Bilgi güvenliği olayına verilen yanıt süresince hızlı davranmak ihtiyacı olabileceğinden dokümantasyon olay kapanışına kadar gerçekleştirilmeyebilir. Ancak olay kapandıktan sonra bilgi güvenliği olay tespit ve yanıt süreçleri dokümante edilir. Olayın temel nedeni (root cause) tespit edilebilmişse dokümantasyon içeriğinde belirtilir.

Olay ardından bir uygunsuzluk veya güvenlik zayıflığı tespit edilmişse gerekli düzeltici / iyileştirici faaliyet “Düzeltici Faaliyet Prosedürü”ne uygun olarak planlanır, gerçekleştirilir ve takip edilir. Bu faaliyetlerden biri de eğer olay güvenlik farkındalık eksikliği nedeniyle gerçekleşmişse farkındalık eğitimlerinin gerekli biçimde geliştirilmesi ve gerekli personele, gerektiği sıklıkta verilmesi olabilir.

Her bir olay sonrasında USOM (Ulusal Siber Olaylara Müdahale Merkezi) tarafından belirlenmiş olan formattaki BGYS yazılımı üzerinden yapılır. Bu bilgi hem üst yönetimin bilgisine sunulur hem de USOM’a gönderilerek durumdan haberdar olmaları ve diğer SOME’lerce önlem alınması sağlanır.

5 SORUMLULUKLAR

- Bilgi Güvenliği Birim Yöneticisi: SOME'ye başkanlık, olay yönetimini koordine etme, olay kayıtlarının tutulması, olay sonrası dokümantasyon ve düzeltici / iyileştirici faaliyetlerin başlatılması
- Ağ Yönetimi Birimi; Olayın niteliğine göre olay tespiti, kanıt toplama ve olaya yanıt verme sürecinde SOME ekibi içinde kendi alanındaki görevlerin yerine getirilmesi, ilgili otorite ve diğer taraflarla ilişkilerin sağlanması
- Hukuk Müşavirliği: Bilgi güvenliği olayıyla ilgili SOME'ye hukuki süreç ve önlemler açılarından destek verilmesi

6 REFERANSLAR

- BGYS-PRO-026-02 Yedekleme Prosedürü
- BGYS-PRO-026-02 Erişim Kontrol ve Parola Yönetim Prosedürü

7 KAYITLAR

- İnternet ve Uygulamalara Erişim İz Kayıtları
- İz Kaydı Toplama Konfigürasyonları
- SOME ekibi Listesi
- Sip.usom.gov.tr raporları