KONU: OLAY İHLAL PROSEDÜRÜ

1. AMAÇ:
Erzurum Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı'nın sahibi olduğu bilgi varlıklarının bilerek veya bilmeyerek, kasten veya tesadüfen 3. şahısların eline geçmesi, kısmen veya tamamen durması/tahrip edilmesi durumunda ortaya çıkan olumsuz durumu yönetmek.
Olası zayıflıkları tespit ederek, zayıflıkları kullanacak tehditlerin sonuçlarını ortadan kaldırmak.

2. KAPSAM:
İhlalin veya zayıflığın tespiti ile başlar gerekli işlemlerin / düzenlemelerin yapılması ile son bulur.

3. TANIMLAR
Copyright: Telif hakkıdır.

IP: İnternet'te her bilgisayarın bir IP (Internet Protokol) adresi vardır. Bir IP adresi, noktalarla ayrılan dört rakam grubundan oluşur, her grupta en fazla 3 rakam olabilir; "85.102.156.141" şeklindedir. İnternete bağlanan her bilgisayara sistem tarafından verilen bir ayırt edici numara, yani bir tür "adres"tir. IP numarası sayesinde bilgisayarlar internette diğer bilgisayarlarla veri alışverişi yapar. Yani bilgisayarınızın IP numarası sayesinde, herhangi bir web sitesindeki bilgiler sizin bilgisayarınıza kadar ulaşır.

Fraud: Türkçede sahtecilik anlamına gelen fraud, elektronik ticarette sahte, çalıntı kredi kartı kullanarak veya kredi kartı bilgilerinin kopyalanarak kullanımı suretiyle yapılan online alışverişleri ifade etmektedir.

Hacker: (Bilgisayar korsanı) Şahsi bilgisayarlara veya çeşitli kurum ve kuruluşlara ait bilgisayarlara ve ağlara izinsiz olarak giriş yapan kişidir.

Hack Etmek: Elektronik veya mekanik otomat sistemlerine girilmesi gereken bilgi, jeton gibi doğru anahtarın kullanıldığını kontrol eden anahtar yuvası olan filtreyi kopya anahtarlar ile geçerek hizmet verici sistemi yanıltan kişinin yaptığı eylemdir.

Virüs: Bilgisayar ortamında birileri tarafından amaçlı olarak bir başka kişi ya da kişilere zarar vermek için yazılmış küçük yazılımlardır. Bilgisayarlara kullanıcıların istem dışı girer ve üreticinin amacı doğrultusunda çalışarak sisteme zarar verir.

Solucan: Solucan virüsü genellikle e-posta, kaynağı belirsiz programlar, forum siteleri, korsan oyun DVD ve cd leri gibi farklı yollarla bilgisayarlara bulaşır. Solucan da virüs gibi, kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır. Ancak bunu otomatik olarak yapar. İlk olarak, bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirir. Solucan bir kez sisteminize girdikten sonra kendi başına ilerleyebilir.

Spam: SPAM mailin en basit tanımı; sizin isteğiniz olmadan size gönderilen reklam içerikli maillerdir. Internet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi de genelde SPAM olarak adlandırılır.

Trojan: (Truva atı) Bilgisayar yazılımı bağlamında Truva atı zararlı program barındıran veya yükleyen programdır. Truva atlarının iki türü vardır. Birincisi, kullanışlı bir programın bir hacker tarafından tahribata uğrayıp içine zararlı kodlar yüklenip program açıldığında yayılan cinsi. Diğer türü ise bağımsız bir program olup başka bir dosya gibi görünür.

4. UYGULAMA:
Olay ihlal prosedürü üç aşamada uygulanır;

4.1. **İhlalin / Zayıflığın Ortaya Çıkması / Fark edilmesi**
İhlal olayını fark eden personel olayla ilgili olarak ivedilikle Birim/Bölüm Yöneticisini bilgilendirir. "OLAY IHLAL- ZAYIFLIK FORMU (FR.13.01)" düzenler. Bilgi İşlem Dairesi Başkanlığı'nı bilgilendirir.

Bilgi İşlem Dairesi Başkanlığı "Olay İhlal Zayıflık Formunu" "Olay İhlal Takip Çizelgesi "ne kaydeder.

FR.13.04 Olay İhlal Takip Çizelgesinde sıra no "xxxx/001" şeklinde verilir. xxxx yılı ifade eder.

4.2. **Araştırma**

İhlal olayının fark edildiği tarih ve vuku bulduğu tarihin belirlenmesi ve olayla ilişkisi olabilecek unsurların ortaya çıkarılması aşamasıdır. İhlal olayı ile ilişkisi olabilecek unsurların belirlenmesi sonucunda güvenlik olayı sınıflandırma tablosuna göre " IHLAL ARASTIRMA RAPORU (FR.13.02)" düzenlenir.

Güvenlik olayı sınıflandırma tablosu aşağıdaki gibidir.

Seviye	Tanım	ÖNEM DERECESİ
1	Olay sonucunda, organizasyonun operasyonları için çok kritik olan faaliyetlerin sürekliliği ciddi biçimde etkilenmektedir.	Kritik
2	Olay sonucunda bir uygulama veya sisteme yönelik kullanım etkilenmekte ve bu durum da organizasyonun faaliyetlerini etkilemektedir.	Majör / Yüksek
3	Olay sadece bir kullanıcı grubunu etkilemektedir. Kesintiye uğrayan faaliyetler organizasyonun operasyonlarını etkilememektedir.	Minör / Orta
4	Olay sadece bir kişiyi etkilemektedir. Kesintiye uğramış faaliyetler organizasyonun operasyonlarını etkilememektedir.	Düşük

"Olay İhlal Takip çizelgesi" en az yılda bir defa Bilgi İşlem Dairesi Başkanlığı tarafından gözden geçirilir ve ihtiyaçlar belirlenir. Yönetimin gözden geçirme toplantısında sonuçlar raporlanır.

Yönetim, rapor çerçevesinde önerilen ihtiyaçları onaylar ve onaylanan kaynakları (eğitim, araç, yazılım, donanım vs.) ayırır.

4.3. **Karar**
Bu aşamada ihlalin ortaya çıkmasında sorumlu olan unsurlar hiçbir şüpheye yer vermeyecek şekilde ortaya konur ve karar verilir. "OLAY IHLAL KARAR TUTANAĞI" (FR.13.03) üç farklı içerikte hazırlanacaktır.

4.3.1. **İhlal Personel**
İhlal Erzurum Teknik Üniversitesi personelinden kaynaklanıyorsa bu ihlalden sorumlu olan çalışanlar için durumun mahiyetine bağlı olarak amirlerinin ve Disiplin Kurulunun

değerlendirmesine göre, 3. Taraflar için de geçerli olan sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.

4.3.2. **İhlal Donanım /Yazılım**
İhlal bir yazılım veya donanımın hatasından kaynaklanıyor ise "OLAY IHLAL ARASTIRMA RAPORU" (FR.13.02) yönetime sunulur. Bilgi İşlem Dairesi Başkanlığı ekibi hatanın giderilmesi için gerekli tedbirleri alır ve sonuçlanmasını takip eder.

4.3.3. **İhlal 3. Şahıslar**
İhlal 3. şahıslardan kaynaklanıyorsa gerekli tespitler yapılarak (IP no gibi) yönetime raporlanır. Bilgi İşlem Dairesi Başkanlığı ekibi hatanın giderilmesi için gerekli tedbirleri alır ve sonuçlanmasını takip eder.

4.4. **Bilgi Güvenliği İhlal Olay Tanımları:**
Olay İhlal Takip Çizelgesin 'de olay tanımları sınıflandırılırken aşağıdaki tanımlar kullanılır.

- Yetkisiz Giriş,
- Yazılım Arızası,
- Virüs / Solucan / Trojan,
- Web sitesinin hack edilmesi,
- Tehdit / E-Posta Bombardımanı,
- Copyright Usulsüzlüğü,
- Fraud / Spam,
- Müstehcen veya çirkin mesaj gelmesi,
- Güvenlik Açıklarından Faydalanma,
- Diğer,

İLGİLİ DÖKÜMANLAR:
FR.13.01 OLAY IHLAL - ZAYIFLIK FORMU (OİZF)
FR.13.02 OLAY IHLAL ARASTIRMA RAPORU
FR.13.03 OLAY IHLAL KARAR TUTANAGİ
FR.13.04 OLAY IHLAL TAKİP CİZELGESİ

	HAZIRLAYAN	ONAYLAYAN
ÜNVANI	BGYS YÖNETİM TEMSİLCİSİ (DAİRE BAŞKANI)	GENEL SEKRETER
ADI SOYADI	Dr. Naci BAYRAK	Prof.Dr. Ahmet DUMLU
İMZA		