1. AMAÇ

Bu prosedürün amacı, T.C. Sağlık Bakanlığı Kocaeli İl Sağlık Müdürlüğü kapsamı dâhilinde, bilgi ve bilgi sistemlerini etkileyen güvenlik olaylarının tanımlanması, olayların nasıl ele alındığı ve / veya alınması gerektiğini, ihlal olaylarının sorumlularının belirlenmesi, olayların raporlanması ve işlenmesi için rehberlik sağlamaktır. Tüm çalışanlar tarafından bilgi güvenliği ihlal olaylarının rapor edilmesi; güvenlik ihlallerinin sonuçlarının hafifletilmesi ve gelecekteki güvenlik ihlallerinin azaltılması için önemli rol oynamaktadır.

2. KAPSAM

Bu prosedür, Kocaeli İl Sağlık Müdürlüğü ve bağlı tesisler bünyesindeki bilgi sistemlerini etkileyen güvenlik olaylarını kapsamaktadır.

3. TANIMLAR

3.1. Bilgi Güvenliği İhlal Olayı

Kurumun bilgilerinin gizliliğini, bütünlüğünü veya kullanılabilirliğini herhangi bir biçimde etkileme potansiyeline sahip herhangi bir olaydır. Kocaeli İl Sağlık Müdürlüğü aşağıdaki hususlardan kaynaklanacak ihlaller Bilgi Güvenliği İhlali Olarak kabul edilmiştir.

a) Kullanılan bilgi varlıklarının çalınması, kaybolması ya da kırılması

b) Bilginin Gizlilik, Bütünlük, Erişilebilirlik beklentilerindeki ihlaller

c) İnsan hatalarından kaynaklanan ihlaller

d) Genel Müdürlük ve Bakanlık tarafından yayımlanmış Bilgi Güvenliği Yönergesi, Politikalar ve Prosedürlere göre iş ve işlemlerin yürütülmemesi

e) Fiziksel Güvenlik düzenlemelerinin ihlali

f) Kontrolsüz sistem değişiklikleri

g) Yazılım ya da donanım arızaları

h) Erişim ihlalleri (yetkisiz erişim), yetkisiz bilgi kullanımına izin veren uygun olmayan erişim denetimleri

i) Siber saldırılar (Virüs, izinsiz giriş, Truva atı, casus yazılım vb. bulgular için, sistem sunucu servis problemleri için)

j) Gizli bilginin yetkisiz kişilerce ifşa edilmesi

3.2. Olay Tanımları

3.2.1 Servis Dışı Bırakma Saldırısı(Dos/Ddos)

Çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşur, bunlar genellikle bir veya birden fazla web sunucusudur. Bu sistemler saldırganlar tarafından çeşitli yöntemler kullanılarak bağdaştırılır.

3.2.2 Bilgi Sızdırma (Data Leakage)

Kurumun bilişim teknolojileri ile kullandığı, işlediği ya da ürettiği verilerin bilinçli ya da bilinçsiz bir şekilde kurum dışına taşınarak, belirlenmiş “bilgi güvenliği” politikalarının ihlali.

3.2.3 Zararlı Yazılım (Malware)

Bilgisayar sistemlerine zarar vermek, bilgi çalmak veya kullanıcıları rahatsız etmek gibi amaçlarla hazırlanmış yazılımlara genel olarak verilen ad.

3.2.4 Kimlik Taklidi

Kişilerin fiziksel, telefon ya da dijital ortamda olmadığı bir kişi gibi davranıp, onun yetkilerini bilgisi dışında kullanmasıdır.

3.2.5 Port Tarama

Sunucu üzerinde çalışan servislerin hizmet verdiği mantıksal bağlantı noktalarını ve durumlarını tespit etmek için yapılan işlemdir.

3.2.6 Veritabanı Saldırısı (Sql Injection)

Veri tabanı yazılımlarının kullanımından oluşabilecek zafiyetlerinden veri tabanının ele geçirilmesi, yönetilmesi ya da yetki yükseltilmesi şeklindeki saldırılardır.

3.2.7 Kişisel Bilgilerin Kötüye Kullanımı

Tüm kişisel nitelikteki bilgileri görüntülemek, ifşa etmek veya dağıtmak 6698 sayılı Kişisel Verilerin Korunması Kanunu (Dış Kaynaklı Doküman Listesi) usul ve esaslarına aykırıdır. Herhangi kasıtlı ya da hata ile oluşacak kişisel bilgilerin kötüye kullanımı durumların raporlanması zorunludur.

3.2.8 Oltalama (Phishing)

Dolandırıcıların kullanıcı hesaplarına rastgele e-posta göndererek bilgi sızdırmaya yönelik çevrimiçi saldırı türüdür.

3.2.9 Web Uygulamaları Güvenlik İhlalleri

ARP sızdırma, işlevselliğin kötüye kullanımı, içeriğe sızma, DNS çalınması vb. metotlar ile web sitesinin güvenliğinin tehdit edilmesi veya sağlanamaması durumlarıdır.

3.2.10 Sosyal Mühendislik

İnternette insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içerir. Gizli bilgilerin e-posta aracılığı ile iletimi, ağ üzerinden iletilen bilgilerin yetkisiz ya da yanlış alıcıya iletimi, internet üzerinden güvenli olmayan kanallar aracılığıyla veri iletimi, ortak kullanım yazıcılarından alınan çıktıların sahiplenilmemesi ya da güvenliğine önem verilmemesi, masa üstü ya da ortak alanlarda basılı kopyaların denetimsiz bırakılması vb. durumlarda tüm çalışanlar verilerin güvenliğini ve bütünlüğünü korumanın önemini göz önünde bulundurarak bilinçli hareket etmeli, ihlal durumlarını rapor etmesi gerekir.

3.2.11 Veri Kaybı / Veri İfşası

Verilerinin kaybı ya da yetkisiz kişilerce paylaşılması durumlarıdır.

3.2.12 Zararlı Elektronik Posta (Spam)

İsteğiniz olmadan, size gönderilen ticari içerikli oyada politik bir görüşün propagandasını yapmak ya da bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-posta iletileridir.

3.2.13 Parola Ele Geçirme

Depolanmaması gereken bir yerde depolanan parolaların tespiti ya da sızması durumudur. Ya da herhangi bir saldırı yöntemi ile parolaların ele geçirilmesidir.

3.2.14 Taşınır Cihaz Kaybı

CD / DVD, DAT (manyetik ses bandı), veri depolamak için USB taşınabilir veri depolama / HD sürücüler gibi taşınabilir ortamların kullanılması, kullanıcının bu tür cihazları kullanma sorumluluklarının tamamen farkında olmasını gerektirir. PC'lerin, dizüstü bilgisayarların, tabletlerin ve diğer taşınabilir aygıtların kullanılması, verilerin izinsiz erişime açık hale gelmesine neden olabilir. Kasıtlı ya da kazayla, herhangi bir taşınabilir aygıtın yetkili kullanıcısı (taşınabilir medya dahil) dışında kullanımı, kaybı veya bulunması durumunda İhlal Olay Raporlama prosedürleri aracılığıyla BGYS sorumlularına bildirilir.

3.2.15 Dolandırıcılık (Fraud)

Aldatma amacı ile yapılan kasıtlı eylemdir.

3.2.16 Diğer

Yukarıda tanımlanan ihlal olaylarının dışında bilgi güvenliğini tehdit eden diğer ihlallerdir.

4. UYGULAMA

1) İhlal bildirimleri, Olay Bildirim Formu aracılığı ile ya da **https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir** web adresi üzerinden gerçekleştirilir.

2) BGYS ekibi bilgi güvenliği ihlal olayı olup olmadığını tespit eder, analizini yapar ve yayılmasını önlemek için alınması gereken acil eylem gerekli ise süreci başlatır. Olayın ciddiyeti değerlendirilip yasal işlem öngörülmekte ise, ilgili hukuki ya da güvenlik otoriteleri sürece dâhil edilir.

3) İhlal olayının çözümü için kullanılacak bildirim yöntemi e-posta ya da telefondur.

4) BGYS ekibi tarafından yapılan değerlendirme sonucunda ihlal olayının çözümü için ilgili sorumlu tarafa (Birimin bağlı olduğu Daire Başkanına ve üst yönetime) ivedi bir şekilde iletişime geçerek olayın çözümü için harekete geçilir.

5) Kapsam dâhilinde ya da taşra teşkilatından bildirilen ihlal olayları web sitesi üzerinden sadece yetkilendirilmiş BGYS ekibi tarafından izlenmek ve rapor edilmek üzere saklanır.

6) Bildirilen ihlal olayının çözümü için atılan adımlar her bir ihlal olay kaydı için ayrı ayrı yazılarak olay kapatılır.

7) Bildirilen ihlal olayları çerçevesinde yapılan bildirimler sonucu çözümleri, herhangi bir maliyet gerektiriyor ise sorumluluk ihlalin çözümünü üretecek birime aittir. BGYS ekibi sadece olayı ilgili taraflara bildirmek suretiyle çözülmesini sağlayacaktır.

8) Bilgi Güvenliği ihlal olayları, BGYS ekibi tarafından kaydedilerek, gerekli ise Düzeltici Faaliyet planlanır ve /veya farkındalık e-postaları gönderilir. Ayrıca, yılda bir kez yapılan BGYS farkındalık eğitimleri için olay kayıtları girdi oluşturur.