BİLGİ GÜVENLİĞİ İHLAL OLAYLARI PROSEDÜRÜ

1.AMAÇ: Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumlar dâhilinde, bilgi ve bilgi sistemlerini etkileyen güvenlik olaylarının tanımlanması, olayların nasıl ele alındığı ve/veya alınması gerektiğini, ihlal olayların sorumlularının belirlenmesi, olayların raporlanması ve işlenmesini tanımlamaktır.

2.KAPSAM: Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumlar bünyesindeki bilgi ve bilgi sistemlerini etkileyen güvenlik olaylarını kapsar.

3.KISALTMALAR:

SOME: Siber Olaylara Müdahale Ekibi

4.TANIMLAR:

4.1.Bilgi Güvenliği İhlal Olayı

Kurumun bilgilerinin gizliliğini, bütünlüğünü veya kullanılabilirliğini herhangi bir biçimde etkileme potansiyeline sahip herhangi bir olaydır.

4.2. Servis Dışı Bırakma (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.

4.3.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.

4.4. Zararlı Yazılım (Malware)

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

4.5. Dolandırıcılık (Fraud)

Aldatma amacı ile yapılan kasıtlı eylemdir.

4.6. Port Tarama

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

4.7. Veri Tabanı Saldırısı

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

4.8. Web Uygulamaları Güvenlik İhlalleri

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

4.9.Sosyal Mühendislik

İnternette insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içerir.

4.10. Veri Kaybı/ İfşası

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.

4.11. Zararlı Elektronik Posta (Spam)

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

4.12. Parola Ele Geçirme

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

4.13. Taşınır Cihaz Kaybı

CD / DVD, DAT (manyetik ses bandı), veri depolamak için USB taşınabilir veri depolama / HD sürücüler gibi taşınabilir ortamların kasıtlı ya da kazayla, yetkili kullanıcısı (taşınabilir medya dahil) dışında kullanımı veya kaybı.

4.14. Kimlik Taklidi

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

4.15. Oltalama

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

4.16.Kişisel Bilgilerin Kötüye Kullanımı

Tüm kişisel nitelikteki bilgileri görüntülemek, ifşa etmek veya dağıtmak ***DKD. YN. 110 6698 sayılı Kişisel Verilerin Korunması Kanunu*** usul ve esaslarına aykırıdır. Herhangi kasıtlı ya da hata ile oluşacak kişisel bilgilerin kötüye kullanımı.

4.17.Diğer İhlal Olayları

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

5.SORUMLULAR:

Hatay İl Sağlık Müdürlüğünde faaliyet gösteren tüm personel sorumludur, bu sürecin işletilmesinden ise BGYS Komisyonu ve Hatay İl Sağlık Müdürlüğü makamı sorumludur.

6.FAALİYET AKIŞI

6.1. Bilgi Güvenliği İhlali

Hatay İl Sağlık Müdürlüğü ve bağlı tüm kurumları bünyesinde aşağıdaki hususlardan kaynaklanacak ihlaller **Bilgi Güvenliği İhlali** olarak kabul edilir;

- Kullanılan bilgi varlıklarının çalınması, kaybolması ya da kırılması,
- Bilginin gizlilik, bütünlük, erişilebilirlik beklentilerindeki ihlaller,
- İnsan hatalarından kaynaklanan ihlaller,
- Müdürlüğümüz tarafından yayınlanmış Bilgi Güvenliği Politika ve Prosedürlere göre iş ve işlemlerin yürütülmemesi,
- Fiziksel güvenlik düzenlemelerin ihlali,
- Kontrolsüz sistem değişiklikleri,
- Yazılım ya da donanım arızaları,
- Erişim ihlalleri (yetkisiz erişim), yetkisiz bilgi kullanımına izin veren uygun olmayan erişim denetimleri,
- Siber saldırılar (Virüs, izinsiz giriş, Truva atı, casus yazılım vb. bulgular için, sistem sunucu servis problemleri için),
- Gizli bilginin yetkisiz kişilerce ifşa edilmesi

6.2.Kanıt Toplama ve Olay Yönetimi

6.2.1. Olay yerinde delillerin değişmesini bozulmasını önlemek ve delilleri korumak amacıyla olay yerinin güvenliği sağlanır. Olay yeri giriş çıkışlar kontrol altına alınarak yetkisiz girişlere izin verilmez.

6.2.2. Olay yerinde gerekli görülürse tarih zaman bilgisi olan fotoğraf çekilir. Delil niteliği taşıyan materyaller etiketlenir.

6.2.3. Bilgisayar kapalı ise kesinlikle açılmaz, bağlı cihazları sökülmeden önce etiketlenir.

6.2.4. Bilgisayar açık ise ekranının fotoğrafı çekilir ve üzerinde çalışan programlar kayıt altına alınır. Bilgisayarın sistem tarih ve zaman bilgileri ve inceleme esnasındaki gerçek tarih ve zaman bilgisi kaydedilir. Yapılan işlemlerde, her aşamada ayrı ayrı kayıt tutulur. İşlemlerin kimin tarafından yapıldığı ve kullanılan yazılım ve donanım bilgileri kayıt altına alınır.

6.2.5. Değişme olasılığı yüksek olan dijital deliller, öncelikli olarak ele alınır. Bilgisayarın kapatılması veya yeniden başlatılması uçucu delillerin kaybolmasına sebep olacaktır. Bu nedenle veri kayıt işlemlerine, bellek ve ön bellekte bulunan uçucu verilerin kopyalanması ile başlanır. Bu işlem yapılmadan hiçbir şekilde bilgisayarın kapatılmaması gerekir. Delillerin zarar görmemesi için veri toplama ve kayıt işlemlerinin ilgili teknik uzmanlar tarafından "canlı analiz" şeklinde yapılması gerekir.

6.2.6. Bilgisayarın dijital imza (hash) değeri alınır. İmajların gizliliği, erişilebilirliği ve bütünlüğü sağlanır. Kopya alma (imaj) işlemi dışında kesinlikle orijinal delile dokunulmaması gerekir. Deliller toplanıp, birebir kopyası (imajı) alınmadan, delil analiz işlemlerine başlanmaz. İmaj alma işlemi de bir tutanak ile kayıt altına alınır. İmajın hangi yazılım veya araç ile alındığı mutlaka tutanağa yazılır.

6.2.7. Silinmiş verilerin yeniden kurtarılması ve şifrelenmiş verilerin şifrelerinin çözülmesi için tüm dosyalar analiz edilir. Elde edilen deliller, programlar vasıtası ile incelenir. Gerekiyorsa şifre çözme yöntemleri kullanılır.

6.2.8. Olay yerindeki dijital delillerin bütünlüğünün bozulmaması için iyi bir şekilde muhafaza edilmesi gerekir. Hassas veri depolama birimlerinin taşınmasına özen gösterilir. Taşınma esnasındaki fiziksel darbelere karşı korunur. Toplanan delillerin taşınma öncesi taşınacağı ünitelerde, mutlaka etiketlenmesi ve kayıt altına alınması gerekir. Birden fazla dijital delile müdahale edildiğinde, her birim dâhil olduğu sistem ile paketlenir (Bilgisayar-Klavye-Fare gibi) .

6.2.9. Dijital delil mutlaka tutanak ile teslim edilir. Tutanağa yazılan hash değeri kontrol edilir. Dijital delil raporu kolluk kuvvetlerine teslim edilirken raporda, delilleri kimlerin topladığı, deliller üzerinde hangi işlemlerin yapıldığı, hangi yazılım veya donanımların kullanıldığı, işlemin yapıldığı zaman, delilin üzerindeki zaman bilgisi gibi bilgiler de kayıt altına alınarak raporda açık bir şekilde belirtilir.

3/4

6.2.10. Yedeklenecek diskin hafızası şüpheli bilgisayar diskinden büyük olur. Doğruluğu ve güvenilirliği kabul edilmiş yazılım ve donanımlar kullanılır.

6.3. İhlal Bildirimi

6.3.1 Madde 2'de belirtilen Kapsam dahilinde 6.1. maddesinde belirtilen ihlal olayı ve olay türlerinden herhangi birinin gerçekleşmesi durumunda ilgili sorumlular tarafından İhlal olayının gerçekleştiği kurumun Bilgi Güvenliği Yetkilisine Bilgi Güvenliği İhlal Olayı Bildirimi yapılır.

6.3.2. Bilgi Güvenliği Yetkilisi, Bilgi Güvenliği İhlal olayını https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir adresinde bulunan Sağlık Bakanlığı merkezi ihlal bildirim sistemine girer. Ayrıca olay ile ilgili Sağlık Müdürlüğümüz web sitesi http://hatay.ism.saglik.gov.tr/TR,19888/bilgi-guvenligi.html adresinde bulunan Bİ.FR.03 ***Olay Bildirim ve Müdahale Formu 1.Bölümü (Olay Bildirimi)*** doldurularak Bilgi Güvenliği Komisyonuna sunulur ve kurumsal ihlal bildirim hafızası oluşturmak üzere bir örneği saklanır.

6.3.3. Küçük çaplı, yalnız kendi kurumunu ilgilendiren ve bilgi güvenliği yetkilisi ya da kurumsal SOME tarafında kendi imkânları ile çözülebilecek olaylara gerekli müdahale yapılarak ***Bİ.FR.03 Olay Bildirim ve Müdahale Formu 2. Bölümü (Olay Müdahale)*** doldurularak Bilgi Güvenliği Komisyonu'na sunulur ve e-posta ile bilgiguvenligi@saglik.gov.tr adresine gönderilir.

6.3.4. İhlalin oluştuğu kurum ile birlikte diğer kurum ya da kişileri etkileyecek şekilde iş sürekliliğine zarar veren veya durduran, acil müdahale gereken, kurum imajına zarar verebilecek ihlal olaylarında olay müdahale ekibi kurulur ve bu ekip gerekli müdahaleyi yapar.

Gerekli görülürse Sektörel SOME 'den görüş/destek alınır. Olayın çözümüne müteakip ***Bİ.FR.03 Olay Bildirim ve Müdahale Formu 2. Bölümü (Olay Müdahale)*** doldurularak Bilgi Güvenliği Komisyonuna sunulur ve e-posta ile bilgiguvenligi@saglik.gov.tr adresine gönderilir.

6.3.5. Olayın Sağlık Bakanlığı, diğer sağlık tesisleri ya da kamu kurum ve kuruluşları etkileyecek boyutta olması durumunda, Sektörel SOME sürece dahil olarak gerekli müdahaleyi yapar ya da yaptırır. ***Bİ.FR.03 Olay Bildirim ve Müdahale Formu 2. Bölümü (Olay Müdahale)*** Sektörel SOME tarafından doldurularak kayıt altına alınır.

7.İLGİLİ DOKÜMANLAR:

- ***DKD. YN. 110 6698 sayılı Kişisel Verilerin Korunması Kanunu***
- ***Bİ.FR.03 Olay Bildirim ve Müdahale Formu 2. Bölümü (Olay Müdahale)***