Amaç;

Bu prosedürün amacı, T.C. Sağlık Bakanlığı Giresun 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.

Kapsam;

Bu prosedür, T.C. Sağlık Bakanlığı Giresun İl Sağlık Müdürlüğü ve bağlı tesisler bünyesindeki bilgi ve bilgi sistemlerini etkileyen güvenlik olaylarını kapsamaktadır.

İhlal Bildirimi ve Olay Yönetimi

1.Bakanlık çalışanları ve vatandaşlar tarafından tespit edilen, Sağlık Bakanlığı ile ilgili her türlü bilgi güvenliği ihlal olayı, https://bilgiguvenligi.saglik.gov.tr/Home/OlayBildir adresinde yer alan merkezi ihlal bildirim sistemine girilir.

2. Merkezi ihlal birim sistemi dışında, Bakanlığının diğer birimlerince bilgi güvenliği ihlal olaylarının bildirimi için ayrı bir sistem/yazılım kurulmasına gerek yoktur.

3. Olay bildirim sistemini kullanamayacak durumda olanlar kendi kurumlarındaki bilgi güvenliği yetkililerine bildirim yapabilir. Bilgi güvenliği yetkilisine yapılan bildirimler, bilgi güvenliği yetkilisince merkezi sisteme girilir.

4. Merkezi ihlal bildirim sistemine girilen olaylar, Sağlık Bilgi Sistemleri Genel Müdürlüğü ekipleri tarafından ön değerlendirmeye tabi tutulur. Bildirim yapan kişiyle irtibat kurularak aynı zamanda ilgili kurumun bilgi güvenliği yetkilisine de bilgilendirme yapılır. İlgili bilgi güvenliği yetkilisi kendi arşivini tutmak amacıyla KLVZ-EK-17 Olay Bildirim ve Müdahale Formunun 1'nci Bölümünü (Olay Bildirimi) doldurur ve kurumsal ihlal bildirimi hafızası oluşturmak üzere saklar.

5. Küçük çaplı, yalnızca kendi kurumunu ilgilendiren ve bilgi güvenliği yetkilisi ya da kurumsal SOME tarafından kendi imkânları ile yerel olarak çözülebilecek olaylara gerekli müdahale yapılır. KLVZ-EK-17'nin 2'nci Bölümünü (Olay Müdahale) doldurularak e-posta ile bilgiguvenligi@saglik.gov.tr adresine gönderir.

6. İhlal olayı hizmet verdiği kurumla 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. İlgili ekip, gerekli müdahaleyi yapar. Destek istediği durumlarda Sektörel SOME'den görüş / destek alır. Olayın çözümünde KLVZ-EK-17'nin 2'nci Bölümünü (Olay Müdahale) doldurarak bilgiguvenligi@saglik.gov.tr adresine gönderir.

7. Yaşanılan olayın Sağlık Bakanlığı, diğer sağlık tesisleri ya da kamu kurum ve kuruluşlarını etkileyecek boyutta olması durumunda, Sektörel SOME sürece dâhil olur. Gerekli müdahaleyi yapar ya da yaptırılmasını sağlar. Sektörel SOME tarafından KLVZEK-17'nin 2'nci Bölümü (Olay Müdahale) doldurularak kayıt altına alınır.

8. Merkezi ihlal bildirimi sistemine girilen tüm ihlal olaylarının süreç ve sonuçları BGYS Birimi tarafından takip edilir.

9. Merkezi ihlal bildirim sisteminde yer alan olay türleri ve açıklamaları şu şekildedir:

9.1. Servis Dışı Bırakma Saldırısı (DoS/DDoS) : Saldırının amacı hedef alınan sistemi hizmet veremeyecek hale getiricek yöntemlerle, ilgili servisi hizmet dışı bırakmaktır. Kullanılan temel yöntem, ilgili hizmet servisine olağan dışı miktarda çok paket gönderip, engellemektir.

9.2. Bilgi Sızdırma (Data Leakage): Kurumun ürettiği, kullandığı ya da işlediği verileri bilinçli veya bilinçsiz olarak yanlış hedefe gönderilmesi, çalınması ve/veya sızdırılmasıdır.

9.3. Zararlı Yazılım (Malware): Her türlü bilgi işleme yapabilen sistemlere zarar vermek, veri çalmak ve/veya yok etmek için üretilen yazılımlardır.

9.4. Sahtecilik (Fraud): Daha çok finansal sistemlerinde karşılaşılan, aldatma amacı ile yapılan kasıtlı eylemlerdir.

9.5. Port Tarama: Herhangi bir hizmet veren sunucu bilgisayarlarında çalışan servislerin varlığını tespit etmek, bilgi toplamak ve tespit edilecek zafiyetler ile zararlı bir işlem yapma amacı ile gerçekleştirilen eylemlerdir.

9.6. Veri Tabanı Saldırısı: Veri Tabanı yazılımlarının kullanımından oluşabilecek zafiyetlerden veri tabanının ele geçirilmesi, yönetilmesi, veri sızdırılması ve/veya yetki yükseltilmesi şeklindeki saldırılardır. SQL Injection saldırısı da

buna bir örnektir.
9.7. Web Uygulamaları Güvenlik İhlalleri: Bu ihlallere örnek olarak, XXS Saldırıları, Kötü amaçlı dosya çalıştırılması, güvenli olmayan direk nesne referanslama, Sunucu taraflı çapraz kod çalıştırma (CSRF), Bilgi sızdırma ve uygun olmayan hata kontrolü, İhlal edilmiş kimlik doğrulama ve oturum yönetimi, Güvensiz İletişimler gibi ihlaller bu madde altında değerlendirilir.
9.8. Sosyal Mühendislik: Kişilerin zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye yönelik teknikler içerir.
9.9. 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, masaüstü ya da ortak alanlarda basılı kopyaların denetimsiz bırakılması vb. durumlarda yaşanan durumları ifade eder.
9.10. 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.
9.11. Parola Ele Geçirme: Depolanmaması gereken bir yerde depolanan parolaların tespiti ya da sızması durumudur. Ya da herhangi bir saldırı yöntemi ile parolaların ele geçirilmesidir.
9.12. Taşınır Cihaz Kaybı: CD / DVD, DAT (manyetik ses bandı), veri depolamak için kullanılan USB taşınabilir bellekler, Harici Sabit Disk sürücüleri gibi taşınabilir cihazlar ve her türlü bilgi işleme yapabilen cihazlar(bilgisayar, akıllı telefon, tablet v.s)'ın kaybedilmesi veya çalınması durumunu ifade eder.
9.13. Kimlik Taklidi: Kişilerin fiziksel, telefon ya da dijital ortamda olmadığı bir kişi gibi davranıp, onun yetkilerini bilgisi dışında kullanmasıdır.
9.14. Oltalama: Saldırgan kişilerin, kurumsal/bireysel kişilere e-posta göndererek, kritik bilgilerini ele geçirme ve/veya bu bilgileri paylaşmaları konusunda kandırmaya yönelik olan saldırı türüdür.
9.15. Kişisel Bilgilerin Kötüye Kullanımı: Kişisel verilerin işlenmesine ilişkin süreçlerde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yer alan usul ve esaslara uygunluk sağlanmalıdır. Kişisel verilerin işlenmesinde, 6698 sayılı Kanun'da yer alan genel ilkeler göz önünde bulundurulmalıdır. Kişisel verilerin hukuka aykırı işlenmesi ve aktarılması hâlinde; hukuki, idari ve cezai yaptırımlarla karşı karşıya kalınabilir.
2. Kanıt Toplama
2.1. Delillerin değişmesini, bozulmasını önlemek ve delilleri korumak amacıyla olay yerinin güvenliği sağlanır. Olay yerine girişler kontrol altına alınır. Yetkisiz girişlere izin verilmez. Olay yerinden çıkış yapan kişilerin üzerinde adli delil oluşturabilecek materyal olup olmadığı kontrol edilir.
2.2. Olay yerinde işleme başlamadan önce, farklı açılardan olay yerinin görüntüleri çekilir. Çekilen fotoğraflarda tarih ve zaman bilgisinin doğru olduğuna dikkat edilir.
2.3. Delil niteliği taşıyan tüm materyaller açıklayıcı bilgi içerecek şekilde etiketlenir. Bilgisayara bağlı tüm bağlantılar, bağlantı noktasını gösterecek şekilde etiketlenir ve sistem bağlı olduğu ağdan ayrılmaz.
2.4. Bilgisayara bağlı olan cihazlar tespit edilerek, sökülmeden önce etiketlenir.
2.5. Olay yerindeki bilgisayar kapalı ise kesinlikle açılmaz.
2.6. 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.
2.7. 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.
2.8. Bilgisayar kapatıldığında, sistem yapılandırma dosyaları ve geçici dosya sistemleri değişebilir. Bilgisayarın kapatılması delil bütünlüğünü bozar ve delili değiştirebilir. Olay yerindeki kapalı bir bilgisayarı açmak da yine aynı şekilde delillere zarar verebilir. Delillerin zarar görmemesi için veri toplama ve kayıt işlemlerinin ilgili teknik uzmanlar

tarafından "canlı analiz" şeklinde yapılması gerekir.
2.9. 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.
2.10. Yedeklenecek diskin hafızası şüpheli bilgisayar diskinden büyük olur.
2.11. 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.
2.12. 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)
2.13. 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.
2.14. Doğruluğu ve güvenilirliği kabul edilmiş yazılım ve donanımlar kullanılır.

OLAY BİLDİRİM / MÜDAHALE FORMU

1. Bildirimi yapan birim:

2. Bildirimi yapan personelin

Ad, Soyad :
Unvan/Birim :
Telefon :
E-posta :

3. Olay türü:

□ Servis Dışı Bırakma Saldırısı (DoS/DDoS)
□ Bilgi Sızdırma (Data Leakage)
□ Zararlı Yazılım (Malware)
□ Dolandırıcılık (Fraud)
□ Port Tarama
□ Veritabanı Saldırısı
□ Diğer (Lütfen açıklayınız):

□ Web Uygulamaları Güvenlik İhlalleri
□ Sosyal Mühendislik
□ Veri Kaybı/ Veri İfşası
□ Zararlı Elektronik Posta(Spam)
□ Parola Ele Geçirme
□ Taşınır Cihaz Kaybı
□ Kimlik Taklidi
□ Oltalama (Phishing)
□ Kişisel Bilgilerin Kötüye Kullanımı

4. Olay sistem kesintisine sebep oldu mu? □ Evet □ Hayır

5. Olayın:

Tahmini başlangıç zamanı
Tarih : …….. Saat : ……..

Tespit edildiği zaman
Tarih : …….. Saat : ……..

6. Eklemek istedikleriniz:

Dikkat: Bu kısım sadece Bilgi Güvenliği /SOME Olay Müdahale Ekibi tarafından doldurulur.

7. Siber olaylara ait iz(log) kayıtları tespit edildi mi?

□ Hayır

□ Evet

Kaynak IP : _____

Hedef IP : _____

Port : _____

Diğer : _____

8. Olayın etkisini azaltıcı ilk önlemler:

9. Olayın muhtemel sebepleri:

10. Olayın tekrarlanmaması için alınan önlemler:

11. Tahmini Olay Maliyeti

12. Eklemek istedikleriniz: