BİLGİ GÜVENLİĞİ İHLAL OLAYLARI PROSEDÜRÜ

1.AMAÇ

Hatay İl Sağlık Müdürlüğü, İl Ambulans Servisi Başhekimliği Bağlı İlçe Müdürlükleri) kapsamı dâhilinde yaşanabilecek bilgi güvenliği ihlalleri noktasında durumun nasıl yönetileceğini ifade eder.

2.KAPSAM VE SORUMLULAR

Hatay İl Sağlık Müdürlüğü, İl Ambulans Servisi Başhekimliği Bağlı İlçe Müdürlükleri Bilgi Güvenliği Politikası dokümanında kamsam maddesinde tanımlanmış alanlardır.

3.UYGULAMA

Bilgi Güvenliği İhlal Olayları (Hatay İl Sağlık Müdürlüğü, İl Ambulans Servisi Başhekimliği Bağlı İlçe Müdürlükleri) kapsamında aşağıdaki gibi yönetilmektedir. Bilgi güvenliği ile ilgili olaylar derhal rapor edilmelidir. Raporun verileceği ve bilgi sunulacak bölümler aşağıda belirtilmiştir. Kurum politikalarına uymayan her tür davranış, kurum bilgi güvenliği prensipleri ve talimatlarına aykırı her tür bilgi paylaşımı, uygunsuz PC/Laptop kullanımı, yetkisiz girişler, uygun olmayan yerde yetkisiz personelin görülmesi, bilgisayar varlıkları ile ilgili arıza, hırsızlık, kaybolma vb. olumsuzluklar bilgi güvenliği olayı kapsamına girmektedir.

Olay halinde müdahaleyi ilgili/yetkili birimler yaparlar. Olayı raporlayan kişinin müdahale etmemesi ve uzmanların müdahalesi için hiçbir şeye dokunmaması gerekmektedir.

OLAY TANIMI	YETKİLİ KİŞİ/KURUM	İLETİŞİM BİLGİLERİ
Her türlü bilgi güvenliği ihlal olayları durumunda	Sağlık Bilgi Sistemleri Şube Müdürlüğü	Cuma KOÇAK(05321205371)
Virüs, izinsiz giriş, trojan, spyware vb. bulgular için, sistem sunucu servis problemleri için	Sağlık Bilgi Sistemleri Şube Müdürlüğü	Kadir KÖSEOĞLU(5416119181)
Donanım arızaları, network problemleri için	Sağlık Bilgi Sistemleri Şube Müdürlüğü	Cuma KOÇAK (05321205371)
Veri kaybı, bilgilere yetkisiz erişim durumlarında	Sağlık Bilgi Sistemleri Şube Müdürlüğü	Cuma KOÇAK (05321205371)
Hırsızlık, kaybolma, yanma, kırılma vb. durumlar için	Sivil Savunma Birimi	Mehmet GÜRZ (05052155831)
Uygunsuz davranışlar ve politikaya uymayan kişiler için	Disiplin Birimi	Dr. Adnan ESMERLİGİL (05355155877)
Ağ üzerinden Saldırı	Sağlık Bilgi Sistemleri Şube Müdürlüğü	Kadir KÖSEOĞLU(5416119181)

3.1.Güvenlik Olayları, Temel olarak dört kategoride incelenir, bunlar;

3.1.1.Güvenlik İhlalleri (Politika veya Yönerge Uyumsuzlukları, Kontrolsüz Sistem Değişiklikleri, Erişim İhlalleri, Fiziksel Güvenlik ihlalleri, vb.)

3.1.2. Tehditler (Personelden yâda ilişkili organizasyonlardan kaynaklanacak negatif etkiler),

3.1.3. Zayıflıklar (Yetersiz Güvenlik Duvarı veya SPAM Filtresi, vb.)

3.1.4. Arızalar (Servis, Donanım, Tesis kaybı, Sistem arızaları, İnsan hataları, Yazılım veya Donanım Arızaları)

3.1.5. Zayıflıkların tespiti durumunda önlem alınması için Olay Bildirim Formu kullanılır. Olası bir tehdide meydan verecek bir zayıflığı tespit eden çalışanlar "zayıflığı test etmeden" derhal yukarıdaki yetkililere haber vermelidirler.

3.1.6. Zayıflıklar şunlardan biri olabilir, politikaya direnen kullanıcılar, işletim sistemindeki eksik yamalar, epostalardaki spamin artması, sistemin yavaşlaması, cihazların fazla ısınması, giriş ve çıkışlarda tespit edilen yetkisiz girişe uygun alanlar ve durumlar, kapatılmayan kapılar, kilitlenmeyen dolaplar, kapatılmayan oturumlar (bilgisayarı açık bırakıp gitme), dağınık ve halka açık ortamlarda duran bilgiler ve bunun gibi konularda gözlemlenen ve Bilgi Güvenliği Komisyonunun dikkatinden kaçan konular.

3.2.Olay Müdahale Sorumlulukları ve Prosedürleri

Bilgi güvenliği ihlal olayları zamanında müdahale edilip gerekli önlemler alınmadığından sonuçları çok ciddi olabilmektedir. Yanlış müdahale kararı Kurumu itibarını zedeleyecek seviyeye gelmesine neden olabilmektedir Öte yandan yarı bilgili kişilerin sisteme yapacağı müdahaleler çok önemli adli bilişim ipuçlarının kaybolmasına yol açabilecektir. Hizmet boyunca kurum için yapılan tüm güvenlik yatırımlarının (Loglama, Antivirüs, IPS, Firewall, Bilgilendirme vb.) gerçek siber saldırılarda ne kadar işe yaradığı somut bulgularla ortaya çıkaracaktır.

Bu saldırı esnasında sistem kontrol altına alınarak gerekli kontroller yapılır daha sonra bu konuyla alakalı rapor hazırlanır

"Organizasyon içerisinde gerçekleşen Bilgi Güvenliği Olaylarının mümkün olan en kısa sürede yönetime raporlayacak prosedürlerinin oluşturulması gerektiğini bildirir. Bu Prosedür, gerçekleşen olaya tepki ve olaya bağlı ek prosedürleri efektif bir şekilde uygulayacak yapıyı içermelidir.

Olay Raporlama Prosedürü, Organizasyonun Bilgi Güvenliği açısından, Her çalışanın (ve üçüncü tarafların) sorumluluklarını, işe alma ve diğer hizmet sözleşmelerinde tanımlanacak şekilde yapılandırılması ile başlanmalıdır. Organizasyonda ilk önce raporlama kültürünün bir sorumluluk olduğu sorumlular tarafından benimsenmelidir. Burada, Personel nedeni ne olursa olsun ve kendi hatası dahi olsa Güvenlik Olaylarını raporlamaya teşvik edilmelidir. Bu çok önemlidir, Çünkü Organizasyonda Kritik Güvenlik Açıklarını işaret edebilecek belirtilerin tespiti, Personelin bu durumun öneminin ve farkındalığı ile olay çapı genişlemeden önlenebilir. Güvenlik açıkları; Eğitim eksikliklerinden, Yönetimsel, Sistem tasarımdan veya herhangi bir nedenden kaynaklı olabilir (Bu durum gizli tutulursa, ele alınamayacağı unutulmamalıdır…) halinde müdahaleyi ilgili/yetkili birimler yaparlar. Olayı raporlayan kişinin müdahale etmemesi ve uzmanların müdahalesi için hiçbir şeye dokunmaması gerekmektedir.