1. BİLGİ GÜVENLİĞİ OLAY YÖNETİMİ

Olay yönetimi güvenlik olaylarının anında tespit edilerek güvenlik ihlâllerine zamanında cevaplar verilmesini sağlar. Daha önce denenen ve başarılı olan güvenlik kırılmaları, güvenlik yöneticisinin güvenlik faaliyetlerinin beklenen biçimde çalışıp çalışmadığının belirlenebilmesi, güvenlik önlemlerinin alınarak güvenlik ihlallerinin önlenmesi, bir güvenlik kırılmasını önlemek için alınan önlemlerin etkili olup olmadığına karar verilir.

1.1. BİLGİ GÜVENLİĞİ OLAYLARININ VE ZAFİYETLERİN RAPOR EDİLMESİ

Bilgi Güvenliği Olaylarının Rapor Edilmesi

- Güvenlik olaylarını mümkün olduğunca hızlı bir şekilde raporlamak için resmi bir prosedür olmalıdır.
- Raporlama prosedürü ile birlikte olaya yanıt vermek için yapılacakları belirten bir prosedür olmalıdır.
- Raporlama prosedürü ve başvuru noktası tüm personel tarafından biliniyor olmalıdır.
- Başvuru noktasındaki personel her zaman ulaşılabilir durumda ve olaya müdahale edebilecek yetkinlikte olmalıdır.
- Tüm personel ve üçüncü parti çalışanlarına karşılaştıkları bilgi güvenliği olaylarını hızla bildirme konusunda yükümlü oldukları açıklanmış olmalıdır.

Bilgi Güvenliği Zafiyetlerinin Rapor Edilmesi

- Kurum çalışanlarının sistem ve servislerdeki güvenlik zafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü olmalıdır.
- Raporlama prosedürü kolayca kullanılabilecek şekilde hazırlanmalıdır. (Personel ve üçüncü taraf çalışanları zafiyetlerin varlığını kanıtlamak için test ve girişimler yapmaktan kaçınmalıdır. Aksi halde sistemde hasar oluşabileceği gibi testi yapan personel de suçlu durumuna düşebilir).

1.2. BİLGİ GÜVENLİĞİ OLAYLARININ YÖNETİMİ VE İYİLEŞTİRMELER

Sorumluluklar ve Prosedürler

- Bilgi güvenliği olaylarına hızlı, etkili ve düzenli bir biçimde karşılık verebilmek için yönetime ait sorumluluk belirlenmiş, prosedürler oluşturulmuş olmalıdır.
- Bilgi güvenliği olaylarını ortaya çıkarmak için sistemler, sistemlerin açıklıkları ve üretilen alarmlar izleniyor olmalıdır.

- Belirtilen şu farklı olay tiplerini ele almak üzere prosedürler geliştirilmiş olmalıdır; bilgi sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilgi sisteminin kötüye kullanılması.
- Denetim sonuçları ve deliller toplanıyor ve güvenli bir biçimde saklanıyor olmalıdır.
- Açığı kapatmak ve hataları düzeltmek için gereken çalışmalar yapılırken canlı sisteme sadece yetkili personelin erişmesine, acil düzeltme çalışmalarının dokümante edilmesine, çalışmaların düzenli olarak yönetime bildirilmesi ve yönetim tarafından gözden geçirilmesine ve bilgi sistemlerinin bütünlüğünün asgari gecikme ile sağlanmasına dikkat edilmelidir.

Bilgi Güvenliği Olaylarından Deneyim Edinme

- Bilgi güvenliği olaylarını teşhis eden, bunların sınıflandırılmasını, sayılmasını ve maliyetlerinin hesaplanmasını sağlayan bir mekanizma olmalıdır.
- Geçmiş bilgi güvenliği olaylarından sağlanan tecrübe tekrarlanan veya büyük hasar meydana getiren olayların tespit edilmesinde kullanılmalıdır.

Delil Toplama

- Bilgi güvenliği olayının ardından şahıs veya kuruluşlarla ilgili yasal işlem yapılmalıdır.
- Olayla ilgili deliller toplanıyor, muhafaza ediliyor ve ilgili yargı organına sunuluyor olmalıdır.