1. İNSAN KAYNAKLARI GÜVENLİĞİ

İnsan hatalarını, hırsızlığı, sahtekârlığı ve araçların yanlış kullanılması risklerinin azaltılması, kullanıcıların bilgi güvenliği tehditlerinden ve sorunlarından haberdar olduklarının ve normal çalışma seyirleri içinde organizasyonla ilgili güvenlik politikasını desteklemek üzere donatıldıklarının garanti edilmesidir. Ayrıca güvenlik ihlallerinden meydana gelen hasarın en aza indirilmesi ve bu gibi olaylardan gerekli tecrübelerin edinilmesidir.

Bilgi güvenliği genel olarak üç bileşen üzerinde yükselir; teknoloji, süreç ve insan. İnsan bilgi güvenliğinde önemli bir unsurdur. İnsanı ilgilendiren güvenliğin sürekliliği ve gelişmesi de bu açıdan çok önemlidir.

Şirketler çoğunlukla bilgi güvenliği olgusunu salt 'teknoloji' sorunu olarak ele almaktadırlar. Genel amaçlı bilgi sistemlerinin kurulumunda bilgi güvenliği birimleri süreçlere büyük oranda dahil olurken, insan kaynakları sistemlerinin kurulumunda katılımın yarı yarıya azaldığı görülüyor.

Bilgi güvenliğini teknolojiyle özdeşleştirmek büyük bir yanılgıdır. İnsan, genelde uygulananın aksine, bilgi güvenliği alanında ilk yatırım yapılması gereken kaynaktır. Çünkü henüz (ve büyük ihtimalle daha uzun süre) otomatik ve otomatik olmayan pek çok kaynaktan gelen verileri değerlendirip otomatik olarak anlamlı bir risk analizi ve önceliklendirme yapabilecek bir teknoloji bulunmamaktadır. Bulunsa dahi bu teknolojinin uyarlanması ve ona girdi sağlayacak mekanizmaların kurulması da insan kaynağını gerektirecektir. Bu evreye gelmeden önce de insan çabasıyla pek çok çalışmanın yapılması gerekecektir. Bilgi güvenliğini yöneten olarak insana duyduğumuz ihtiyacın yanı sıra insan kaynaklı güvenlik zafiyetleri ve güvenliğin insanlar tarafından gerçekleştirilenler dahil tüm iş aktivitelerine yayılması gereği insan faktörünü bilgi güvenliği açısından önemli bir odak haline getirmektedir. Ayrıca savunma tarafında insan ne kadar önemliyse saldırı tarafında da insan o kadar önemlidir. Pek çok saldırı yaratıcı düşünceyi, otomatik, fiziksel ve insani saldırı vektörlerini birbiriyle uyumlu biçim ve sırada kullanmayı gerektirmektedir. Yani saldırgan tarafta da insan faktörü birinci öneme sahiptir. Bu açılardan insana gerekli önemi vermeyen güvenlik yönetimi önemli bir faktörü göz ardı edecektir.

1.1. İŞE ALMADAN ÖNCE

Roller ve Sorumluluklar

- Kurumun bilgi güvenliği politikası uyarınca personele düşen güvenlik rol ve sorumlulukları belgelenmiş olmalıdır.
- İşe alınacak personele yüklenecek rol ve sorumluluklar açıkça tanımlanmış ve işe alınmadan önce personel tarafından iyice anlaşılması sağlanmalıdır.

Tarama

- İş başvurularında, işe alınacak personel için doğrulama testleri yapılmalıdır.
- Doğrulama testleri iddia edilen akademik ya da profesyonel vasıfların doğruluğunu ve bağımsız kimlik doğrulama testlerini kapsıyor olmalıdır.

İşe Alınmanın Şartları

- Kurum çalışanlarının gizlilik ve açığa çıkarmama (non-disclosure) anlaşmalarını işe alınma şartının bir parçası olarak imzalamaları istenmelidir.
- Bu anlaşma işe alınan personelin ve kuruluşun bilgi güvenliği sorumluluklarını kapsıyor olmalıdır.

1.2. ÇALIŞMA SIRASINDA

Yönetimin Sorumlulukları

- Yönetim, çalışanlarından ve üçüncü parti kullanıcılarından uygulamakta olduğu politika ve prosedürler uyarınca güvenlik tedbirlerini almalarını istemelidir.

Bilgi Güvenliği Bilinci ve Eğitim

- Kurumun tüm çalışanları ve üçüncü parti kullanıcıları uygun bilgi güvenliği eğitimlerini almalıdırlar.
- Kurumsal politika ve prosedürlerdeki değişikliklerden haberdar edilmelidirler.

Disiplin Süreci

- Kurum çalışanlarının, güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin süreci olmalıdır.

1.3. GÖREV DEĞİŞİKLİĞİ VEYA İŞTEN AYRILMA

Ayrılma İle İlgili Sorumluluklar

- İşten ayrılma veya görev değişikliği sırasında yapılması gerekenler açık olarak belirlenmiş ve ilgili kişilere sorumlulukları bildirilmiş olmalıdır.

Varlıkların İade Edilmesi

- İşten ayrılma, kontratın veya anlaşmanın sona ermesi halinde kurum çalışanlarının veya üçüncü parti kullanıcılarının üstünde bulunan kuruluşa ait tüm varlıkların iade edilmesini sağlayan bir süreç mevcut olmalıdır.

Erişim Haklarının Kaldırılması

- İşten ayrılma, kontratın veya anlaşmanın sona ermesi halinde veya görev değişikliği halinde kurum çalışanlarının veya üçüncü parti kullanıcılarının kuruluşun bilgi varlıklarına veya bilgi işlem araçlarına erişim hakları kaldırılıyor veya gerektiği şekilde yeniden düzenleniyor olmalıdır.