TEMEL BİLGİ GÜVENLİĞİ-8

Veri Sızıntısı (Data Leakage)

Veri sızıntısı, bilgiye yetkili olmayan kişiler tarafından ulaşılmasıdır. Bu duruma örnek olarak, şirket çalışanların, müşterilerin ve ilişkili diğer kimselerin özel kimlik bilgilerinin üçüncü kimseler tarafından ele geçirilip halka açık internet sayfalarında yayınlanması gösterilebilir.

Veri sızıntılarını engelleme Güvenlik Bölümü çalışanlarının başlıca görevleri arasındadır. Sistem kullanıcıları dosyalarını, veri sızıntısının risklerini ve doğuracağı sonuçları tam olarak anlayamadan yollayabilir veya paylaşabilirler. Bu tip durumlara hazırlıklı olmak için; antivirüs yazılımları, şifreleme yazılımları, güvenlik duvarları DLP gibi otomatize yöntemlerle azaltacağı gibi, kişisel farkındalığın artırılması kilit öneme sahiptir.

Veri Kaybı (Data Loss)

Veri kayıpları verilerin kasıtlı olarak ele geçirilmesi dışında, verilerin yanlışlıkla kaybedilmesi ya da yok edilmesi sonucunda oluşur. Bu tip olaylar genellikle, veri taşıyan cihazların (medya ortamlarının) kaybedilmesi ile meydana gelir. Örnek olarak CD, DVD, Flash Bellekler, laptop, tablet, cep telefonu gibi bilgi depolanan araçların kaybedilmesi verilebilir.

Veri kaybı kazayla (kasıtsız) olarak gerçekleşse de kaybedilen ortam ve veri tehlike altına girecektir. Yetkisiz kişilerin erişimine açık ortamda bulunan veriler kolayca ele geçirilebilir hale gelecektir.

Veri depolama ortamının kaybolması riskine karşı şifreli diskler, uygulamalar, programlar, verilerin yetkisiz erişime karşı korunması amacıyla alınabilecek önlemler arasındadır.

Veri Çalınması/Veri Hırsızlığı (Data Theft)

Veri çalınması kasıtlı olarak yetkisiz kişilerin bilgilere ulaşma ve ele geçirmesi durumudur. Veri çalınması olayları organizasyon dışından kişiler tarafından gerçekleştirilebileceği gibi, organizasyon içinden kişiler tarafından da gerçekleştirilmesi mümkündür. Örneğin küskün çalışanların veri hırsızlığı yaptığı durumlarla organizasyonlar sıklıkla karşı karşıya gelebilmektedir.

Organizasyon içerisinde olan kişiler için veri hırsızlığı kolaylıkla gerçekleştirilebilir. Kişilerin erişim yetkileri dahilinde organizasyon için bilgi güvenliğini ihlal ederek veri hırsızlığı yapmaları için herhangi bir araç kullanmalarına gerek kalmayabilir. Özellikle verilere dışarıdan yetkisiz erişim sağlamak isteyen kişiler ise sıklıkla zararlı yazılımlar kullanırlar. Keyloggerlar da bu işlemler için tercih edilen araçlardandır. Kullanıcı aktivitelerini izlerler ve kullanıcı adları, parolalar gibi önemli bilgiler elde ederek saldırgana ulaştırırlar.

Kullanıcılara ait banka hesapları, e-posta adresleri, sosyal medya hesaplarına giriş parolaları gibi önemli bilgilerin ve verilerin çalındığı olaylara dünyada çok sayıda örnek vermek mümkündür. Veri hırsızlığı olayları ayrıca kasıtlı olarak yapılan, laptop, CD, USB Bellek gibi ortamların çalınması yoluyla da gerçekleşir.