Ramazan Canbaz

Bilgi Güvenliği

Günümüz yaşam çerçevesinde duyduğumuz ve dikkatimizi çeken en önemli kavramlardan biri ***Bilgi Güvenliği***'dir. Bu kadar telaffuz edilen ve önem derecesine vurgu yapılan ***Bilgi Güvenliği*** nedir? Bunu anlamak için ilk olarak bilginin ne olduğunu ele alalım.

Bilgi, günlük hayatımızda çok kullandığımız bir kavram olmasına rağmen tanımı yapılması oldukça zordur. Önceleri bilgi, felsefenin ilgi ve tartışma alanında yer alırken, günümüzde tüm bilim dallarının konusu haline gelmiştir. Ayrıca bilgi, sadece bilim dallarına göre değil, zamana ve değişen koşullara göre değişen bir kavramdır. Önceleri bilgi insanı şekillendiren, haber değeri taşıyan bir olgu iken günümüzde bilgi bir üretim faktörü ve alınıp satılma özelliğine sahiptir.

Bilgi Güvenliği, mevcut olan bilginin ikinci bir kişinin eline geçmemesi anlamında temel bir yaklaşım yapabiliriz. Kavramı daha da genişletmek istediğimizde bilgi güvenliği 3 ana unsurdan oluşur. "Gizlilik, Bütünlük ve Erişilebilirlik" Şimdi bu kavramları kısaca açıklayalım.

Gizlilik, bilginin yetkisiz kişilerin eline geçmemesidir.
Bütünlük, bilginin yetkisiz kişilerce değiştirilmemesidir.
Erişilebilirlik, bilginin yetkili kişilerce ulaşılabilir ve kullanılabilir olmasıdır.

Bundan 20 yıl kadar öncesinde bilişim sistemleri iş süreçlerinde çok fazla kullanılmazken günümüzde bilgi sistemleri hemen hemen her iş sürecinde yer alması açısında önemli bir noktaya gelmiş durumdadır. Bilgi Güvenliği, bu kadar önem arz eden duruma gelmiş ise, bunun sağlanmasından kimler sorumludur diye bir soru aklımıza gelebilir? Herhangi bir bilgi sisteminde aşağıdaki konumlardan birinde iseniz sorumluluğunuz var demektir.

- Bilginin sahibi,
- Bilgiyi kullanan,
- Bilgi sistemini yöneten,

Bu durum çok geniş bir kitleyi içerdiğinden *"bilgi güvenliğinin sağlanmasından herkes sorumludur"* diye genelleme yapmakta bir sakınca yoktur. Herkesin sorumlu olduğu bir durumda Bilgi Güvenliğinin seviyesi nasıl belirlenir? Bilgi güvenliğini bir zincir halkası gibi düşünürsek, bu zincir halkasının en zayıf halkası sistemin kullanıcılarıdır diyebiliriz. Unutulmamalıdır ki ***bir zincir en zayıf halkası kadar sağlamdır.*** Bilgi güvenliği seviyesi bu durumda kullanıcılara bağlı olduğundan kullanıcı bilinci bilgi güvenliği açısından son derece önem taşımaktadır. Bilinçli bir kullanıcı aşağıdaki durumlar söz konusu olduğunda bilgi işlem personellerine başvurmaları faydalı olacaktır.

- Bilgisayarınızda gereksiz bir yavaşlama durumunda,
- Sizin müdahaleniz olmadan bir bilgi kaybı veya değişikliği ile karşılaştığınızda,
- Kontrol dışı programların çalışması durumunda,
- Kontrol dışı web sayfalarının açılması durumunda,
- Virüs tespit programlarının çalışmadığını fark ettiğinizde,

Bilgi güvenliği tehditlerini ele alacak olursak, ilk sırada yer alan konu *Zararlı Programlar*'dır. Zararlı programlar{Virüs, Solucan(Worm), Truva atı(Trojan), Tuş Kaydedici(Keylogger), Casus Yazılım(Spyware)}; bilgisayarınıza zarar verebilen, bilgisayarınızı etkili bir şekilde kullanmanızı önleyen yazılımlardır. Bilgisayarınıza büyük zararlar verebilen bu programlardan korunmak için gerekli önlemler alınmaz ise oluşacak sorunların sayısı hızla artacaktır. Belki de bu sıkıntıların en başında, kişisel bilgilerin çalınması, banka hesaplarının ele geçirilmesi ve e-posta hesaplarının hacklenmesi gelmektedir.

Bilgi Güvenliği konusunu sınıflandırmak istersek 7 grupta ele alabiliriz.

1. **Ağ Güvenliği** (Network Security) : 6 başlık altında inceleyebiliriz.

    a. İçerik Güvenliği (Content Security)
        - E-Posta
        - Web
    b. Çevresel Savunma (Perimeter Defense)
        - Firewall/VPN (Güvenlik Duvarı / Sanal Özel Ağ)
        - IPS (Intrusion Prevention System / Saldırı Önleme Sistemi)
        - UTM (Unified Threat Management / Birleştirilmiş Tehdit Yönetimi)
    c. NAC (Network Access Control / Ağ Erişim Kontrolü)
    d. Wireless (Kablosuz)
    e. İzleme (Monitoring)
    f. Yönetilir Servisler (Managed Services)
        - İzleme (Monitoring)
        - Yönetim (Management)

2. **Uç/Son Nokta/Kullanıcı Güvenliği** (Endpoint Security): 5 başlık altında inceleyebiliriz.

    a. Uç/Son Nokta/Kullanıcı Savunması (Endpoint Defense)
        - Anti Malware
        - Ana Bilgisayar Güvenlik Duvarı (Host Firewall)
        - Ana Bilgisayar Tabanlı Saldırı Önleme Sistemi (HIPS)
        - Uygulamalar için Beyaz Listemele (Application Whitelisting)
    b. Disk Şifreleme (Disk Encryption)
    c. Cihaz Kontrolü (Device Kontrol)
    d. Mobil Güvenlik (Mobile Security)
    e. Uzaktan Erişim / VPN (Remote Access / VPN)

3. **Veri Güvenliği** (Data Security) : 4 başlık altında inceleyebiliriz.

    a. Veritabanı Güvenliği (Database Security)
        - Veritabanı Değerlendirme (Database Assessment)
        - Veritabanı Aktivite Kontrolü/İzleme (Database Activity Monitoring)
        - Veritabanı Şifreleme (Database Encryption)
    b. Veri Kaybı/Sızıntısı Önleme (Data Loss Prevention)
    c. Şifreleme (Encryption)
    d. Erişim Yönetimi (Access Management)

4. **Uygulama Güvenliği** (Application Security): 5 başlık altında inceleyebiliriz.

    a. Web Uygulama Güvenlik Duvarları (Web Application Firewalls)
    b. Uygulama Testi (Application Test)
    c. Güvenli Geliştirme (Secure Development)
    d. Web Uygulama Değerlendirme (Web Application Assessment)
    e. Yönetilir Servisler (Management Services)

5. **Kimlik ve Erişim Yönetimi** (Identity and Access Management): 5 başlık altında inceleyebiliriz.

    a. Dizinler (Directories)
    b. Kimlik Doğrulama (Authentication)
    c. Sağlama / Hazır Hale Getirme (Provisioning)
    d. Web Erişim Yöntemi (Web Access Management)
    e. Federation

6. **Güvenlik Yönetimi** (Security Management): 5 başlık altında inceleyebiliriz.

    a. Uyumluk / Uygunluk
    b. Güvenlik Operasyonları (Security Operations)
    c. Sistem Yönetimi (System Management)
    d. Güvenlik Açığı Yönetimi (Vulnerability Management)
    e. Olay Müdahale (Incident Response)

7. **Sanallaştırma ve bulut** (Virtualization and Cloud): 2 başlık altında inceleyebiliriz.

    a. Sanallaştırma Güvenliği (Virtualization Security)
    b. Bulut Güvenliği (Cloud Security)

Bu kategorilendirme sonucuna göre şu sıralar en popüler konular sanallaştırma, bulut bilişim, veri kaybı önleme (DLP) ve web güvenliği olarak söylenebilir. Kariyerine bilgi güvenliği alanında yön verecek olanların bu kadar konu arasından bir ya da birkaçını tercih etmeleri gerçekten zor olacak.

Türkiye'de Bilgi Güvenliği?

6 aylık dönemler halinde yayınlanan Microsoft Güvenlik İstihbarat Raporu'nun (Security Intelligence Report) son dönem sonuçlarına göre, Türkiye'deki bilgi güvenliği ile ilgili yapılan tespitler endişe uyandırıyor. Bu çalışma, dünyada bilgi güvenliği alanında en geniş örnek kümesine sahip araştırmalardan biri ve 600 milyon civarındaki bilgisayardan kullanıcıların izniyle paylaşılan sonuçlara dayalı olarak gerçekleştiriliyor.

Türkiye, son birkaç senedir dünyada 1000 bilgisayar başına düşen kötücül yazılım enfeksiyonu oranı itibarıyla en fazla enfeksiyona rastlanan ülkeler arasında yer alıyor. Son rapor sonuçlarına göre de Türkiye geçtiğimiz bir sene içerisinde 1000 bilgisayara 36.8 enfekte cihaz oranı ile lider olurken, İspanya (36.1), Kore (34.8), Tayvan (29.7) ve Brezilya (24.7) oranları ile Türkiye'yi izledi.

Ayrıca önceki dönemlere ait raporda Türkiye, SQL Enjeksiyonu olarak tabir edilen saldırı kategorisinde zafiyet taşıyan ".tr" uzantılı 88.378 sayfa adedi ile de maalesef açık ara dünya lideriydi. Tüm ".com" uzantılı alanda bile 43.144 adet bu zafiyeti taşıyan sayfa mevcutken Türkiye'de bunun iki katına denk gelen zaafiyeti taşıyan sayfa sayısının bulunması ciddi bir güvenlik tehdidini beraberinde getiriyor.

Bilgi Güvenliği için yapabileceklerimizi aşağıda sıralayabiliriz.

- Anti-Virüs (virüsten korunma) ve Anti-Spyware (casus yazılımdan korunma) programları kullanmalıyız.
- Anti-Virüs ve Anti-Spyware programlarını güncel tutmalıyız.
- İşletim sistemini güncel tutmalıyız. (İşletim sistemi yamalarını yapmalıyız)
- Güvenlik duvarı kullanmalıyız.
- İnternette girdiğimiz sitelere ve indirdiğimiz dosyalara dikkat etmeliyiz.
- Lisanslı programlar kullanmalıyız.
- E-postaları açmadan önce içeriğinin güvenilirliğini kontrol etmeliyiz.

Haziran, 2014

KAYNAKÇA;

1. **http://www.bilgimikoruyorum.org.tr/**
2. **http://www.e-siber.com/guvenlik/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir**
3. **http://blog.microsoft.com.tr/turkiyede-bilgi-guvenligi.html**