Bilgi Güvenliği Farkındalık Eğitimi

İçindekiler

BT’nin Kötüye Kullanılmasının Yaratabileceği Zararlar

- Sahip olduğunuz bilgi başkalarının eline geçebilir
- Kurumunuzun imajı zarar görebilir
- Donanım, yazılım, veri ve kurum çalışanları zarar görebilir
- Önemli veriye zamanında erişilemeyebilir
- Parasal kayıplar yaşanabilir
- Zaman kayıpları yaşanabilir

Bilgi Güvenliği Hakkında Yanlış Bilinenler

- BT Güvenliğinden Bilgi Güvenliği Birimi sorumludur.
- Antivirüs yazılımımız var olması güvende olduğumuz anlamına gelir.
- Kurumumuz güvenlik duvarı (firewall) kullanıyor, dolayısıyla güvendeyiz.
- Bir çok güvenlik saldırısı kurum dışından geliyor.

Bilgisayarınızı Kullanırken

- Bilgisayar başından kalkarken ekranınızın başkaları tarafından izlenmemesi içinekranınızı kilitlemelisiniz.

Şifrenizin Güvenliği

- En önemli kişisel bilginiz şifrenizdir.
- Şifrenizi hiç kimseyle ve herhangi bir şekilde paylaşılmamalısınız.
- ATM veya POS makinasında şifre girerken, İnternet Kafe, hava alanları, oteller ve benzeri halkın ortak kullanım alanı olan yerlerde e-postalarımıza bakarken, toplu taşıma araçları gibi kalabalık ortamlarda e-postalarımıza bakarken, Çalışma alanlarımızda bilgisayar açılış şifremizi girerken,
- Etrafımızda bizi izleyen birileri olmadığından emin olmalısınız.

Şifrenizin Güvenliği - 2

- En az sekiz karakterli olmalıdır.
- Rakam ve özel karakterler (?, !, @ vs) içermelidir.
- Büyük ve küçük harf karakteri kullanılmalıdır.
- Örnek güçlü bir şifre: AG685kt?!

Şifrenizin Güvenliği - 3

- Kişisel bilgilerle ilişkili olmamalıdır (çocuğunuzun ismi, evlenme yıldönümü, doğum günü vs.).
- Sisteme erişimde kullandığınız şifreler oyun siteleri, bilgilendirme siteleri gibi yerlerde kullandığınız şifrelerle aynı ya da benzer olmamalıdır.
- Farklı sistemler için aynı şifre kullanılmamalıdır.

Yazılım Yükleme - Güncelleme

- Kurum tarafından belirlenmiş yazılımların dışında bilgisayarlarda program bulunmamalıdır. Her bir programın açıklık oluşturma ihtimali vardır.

- Güvenilir olmayan sitelerden indirilen yazılımlar indirilmemeli ve kullanılmamalıdır.

Taşınabilir Medya Güvenliği

- USB, CD vs. gibi taşınabilir medya kullanımına özen gösterilmelidir.
- Başkaları ile paylaşıldığında bu ortamlar içerisinde gereğinden fazla bilgi bulunmamalıdır.
- Kurum dışında kullanılan bir ortam mecbur kalınmadıkla kurumda kullanılmamalı, kullanılması gerekiyorsa antivirüs taraması sonrası kullanılmalıdır.
- Taşınabilir medya, masa gibi açık alanlarda bırakılmamalıdır.

Yazıcı Kullanımı

Gizli bilgi içeren dokümanların çıktıları alınırken,

- Doküman çıktısının sayfa ve kopya sayısı olarak eksik olmadığı kontrol edilmelidir.

- Yazıcı hataları ile karşılaşıldığında gönderilen doküman iptal edilmeli ve yanlışlıkla basılmadığı kontrol edilmelidir.

- Çıktının yazıcıda basılması süresinde dokümanın başında bulunulmalıdır.

Zararlı Yazılımlar - Belirtiler

Virüs ve Spyware benzeri zararlı yazılımların belirtileri şunlardır,

- Bitmek bilmeyen pop up (reklam) pencereleri
- Tarayıcımızda istem dışında kurulan araç çubukları
- Web tarayıcımızda giriş sayfasının değişmesi
- Tab tuşu gibi bazı özel tuşların çalışmaması
- Rastgele karşımıza gelen hata mesajları
- Bilgisayarla çalışırken karşılaştığımız aşırı yavaşlık

Zararlı Yazılımlar – Korunmak İçin

Zararlı yazılımlardan korunmak için yapılması gerekenler aşağıdaki şekilde sıralanabilir.

- Karşınıza çıkan pop-up pencerelerindeki bağlantılara tıklanmamalıdır.
- Pop-up pencerelerini kapatırken, pencere içindeki kapat tuşunu kullanmak yerine, pencerenin sağ üst köşesinde bulunan “X” işareti kullanılmalıdır.
- Karşınıza çıkan pencerelerde beklemediğiniz bir soru çıktığında, doğrudan “Evet” seçeneği seçilmemelidir.
- Spyware ile mücadele için kullanılan bir çok yazılım da aslında başlı başına casus yazılımdır. Sistem yöneticisine danışmadan bu tip yazılımlar kurulmamalıdır.
- Antivirüs programı kapatılmamalıdır.
- Uzantısı exe, scr, zip, rar olan dosyalara özel dikkat göstermelidir.

Zararlı Yazılımlar – Şüpheli Durumlarda

Bilgisayarınıza zararlı yazılım bulaştığından şüphelendiğiniz durumlarda bulent.eryilmaz@desmerguvenlik.com.tr adresine e-posta adresine haber vermekte tereddüt etmeyiniz.

E-posta Güvenliği

- Spam e – postalar nedeni ile kişisel ve kurumsal bilgileriniz 3. kişiler tarafından öğrenilebilir. Kullanıcı adı/şifreniz ve diğer kişisel ve kurumsal bilgilerin güvenliği, zamanın verimli kullanılması için gelen e – postaların Spam olmadıklarından emin olunuz.
- Gönderen e – posta adresi bilmediğiniz ya da şüpheli olabilir. Bildiğiniz bir kurumun adının benzeri olabilir.
- Kaynağı tanınmayan e-postalar kesinlikle açılmamalıdır.
- Güvenilmeyen eklentiler açılmamalıdır.
- Gelen e – postadaki linkleri, **buraya tıklayın** yazılarını tıklanmamalıdır.
- Spam olduğu düşünülen e-postalara cevap verilmemelidir.
- Linki sağ tıklayıp kopyaladıktan sonra gidilecek adresi inceleyerek, emin olduktan sonra ziyaret ediniz.
- Şifrenizi başkasının öğrenmesi durumunda sizin e-postalarınızı okuyabileceğini, sizin adınıza kurum içindeki ve dışındaki kişilere e-posta gönderebileceğini unutmayınız.
- İnternet kafe ve diğer genel yerlerden yapacağınız bağlantılarda sistemden çıkmayı unutmayınız.

Sosyal Mühendislik

Sosyal Mühendislik: Günümüzde yaygın olarak kullanılan aldatma yöntemi olan Sosyal Mühendislik saldırısından aşağıdaki durumlarda şüphelenilmesi gerekir.

- Telefon ile arandıysanız, karşı tarafın telefon numarasını istediğinizde
- Yüz yüze görüşme ise, adres ya da telefon bilgisi istendiğinde
- İsteğin yerine getirilmemesi durumunda kötü sonuçlar doğacağının vurgulanması ,
- Sıra dışı taleplerde bulunulması ,
- Soru sorduğunuzda rahatsız olunması ,
- Yetkili olduğunun öne sürülmesi ,
- Bildiğiniz konu ile ilgili isimlerin ardada sıralanması ,
- Konunun acil olduğunun üzerine vurgu yapılması ve baskı kurulmaya çalışılması,
- İltifat edilmesi veya kur yapılması,

Sosyal Mühendislik – Şüpheli Durumlarda

Kurumunuz içerisinde böyle bir durumla karşılaşılması halinde

1. **Karşı tarafa hiçbir bilgi vermeden telefon görüşmesinin veya e-posta yazışmasının sonlandırılması,**
2. **bulent.eryilmaz@desmerguvenlik.com.tr adresine ivedi olarak bilgi verilmesi gerekir.**

Dosya Paylaşımları

- Paylaşılması gereken bir dosyaya erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.
- Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.

Güvenlik Olayı Bildirilmesi

- Aşağıdaki durumlarla karşılaştığınızda bilgi sistem personeline(Bülent Eryılmaz) başvurunuz.
  - 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,
  - Antivirüs ajanının çalışmadığını fark ettiğinizde.