BİLGİ GÜVENLİĞİ EL KİTABI

1. PAROLA (ŞİFRE) GÜVENLİĞİ

1.1. Parola Güvenliğinde Dikkat Edilecek Hususlar

- Parolanızı ele geçirmek isteyenler, özel programlar kullanarak sık kullanılan yüzlerce parola örneğini ya da sözlüklerdeki binlerce kelimeyi hızlıca deneyerek parolanızı ele geçirebilirler.
- İyi korunmayan, yazılı ya da sözlü olarak paylaşılan parolalar, yazılı bulunduğu ortama ulaşılarak ya da kulak misafiri olunarak ele geçirilebilir.
- Bilgisayar virüsleri gibi zararlı programlar bilgisayardaki işlemlerinizi izleyerek parolanızı ele geçirebilirler.
- Parolanız, bir başkası tarafından ele geçirilirse veya böyle bir şüphe varsa, yapılacak ilk iş *parolanın değiştirilmesi* olmalıdır.
- Eğer aynı parola ya da çok benzerleri başka sistemlerde de kullanılıyorsa, *diğer parolaların da* değiştirilmesi önem arz eder.

1.2. Güçlü Parola Oluşturmada Dikkat Edilecek Hususlar

- Oluşturulan bir parolanın "güçlü" kabul edilebilmesi için aşağıdaki özellikleri göstermelidir.
  - En az *8 karakter*den oluşur.
  - *Harf*lerin yanı sıra, *rakam* ve "?, @, !, #, %, +, -, *, %" gibi *özel karakterler* içerir.
  - *Büyük* ve *küçük* harfler bir arada kullanılır.
- Parola oluştururken aşağıdaki önerileri de dikkate almak gerekir.
  - *Kişisel bilgiler* gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin doğum tarihiniz, çocuğunuzun adı, soyadınız vb.)
  - *Sözlükte bulunabilen kelimeler* parola olarak kullanılmamalıdır.
  - Çoğu kişinin kullanabildiği *aynı veya çok benzer yöntem ile geliştirilmiş* parolalar kullanılmamalıdır.

2. E-POSTA GÜVENLİĞİ

2.1. E-Posta Saldırı Tipleri

2.1.1. Spam (İstenmeyen E-Posta)

Bir e-posta, talepte bulunmayan birçok kişiye birden gönderilmişse, buna istenmeyen e-posta denir. Bu e-postaların içeriği genelde ticari (“UCE”) oluyorsa da, ticari olmayanları (“UBE”) da vardır.

2.1.2. Taklit (Oltalama) E-Postası (Phishing)

Taklit (oltalama) e-postası, *kimlik bilgilerini çalmak* amacıyla, istenmeyen e-posta veya açılır pencere yoluyla yapılan bir *aldatma yöntemidir*.

Saldırgan, önceden tasarlanan bir hikâye üzerinden, kullanıcıyı e-postanın güvenilir bir kaynaktan geldiğine inandırıp özel bilgilerini (kredi kartı, şifre vs.) ele geçirmeye çalışır.

Korunmak İçin:

- *Kişisel ve mali bilgileri,* tanış olunan kişiler dâhil hiç kimseyle, *e-posta yoluyla paylaşmamak.*
- *E-posta mesajlarındaki internet bağlantılarına tıklamamak.*
- *"http" yerine "https" ile başlayan adreslerin daha güvenli olduğunu bilmek.*
- Kredi kart hesap özeti, banka bildirimleri gibi *bilgilendirme dökümanlarını sık sık gözden geçirmek.*
- *Zararlı yazılımlara karşı korunma programları (Anti-virus, anti-spyware, güvenlik duvarı) gibi güvenlik yazılımları kullanmak ve bu programları sık sık güncellemek.*

2.1.3. Aldatma E-Postası (Hoax)

Gelen e-postayı *başkalarına göndermeyi* ya da herhangi *başka bir eylemde bulunmayı* sağlamak amacı ile, içinde aldatmaya ve kandırmaya yönelik ilginç bir konu (ölümcül hastalık, hediye, acil haber, uyarı, komplo teorisi) geçen e-postalardır.

Aldatma E-Postası nasıl anlaşılır?

- Mesajın sonunda *ad soyad* belirtilmez veya belirtilen isim *araştırıldığında* anlatılanlara uyan *somut bilgiye ulaşılamaz.*
- İçerisinde aşağıdaki gibi ifadeler geçer.
  - *'Bu e-postayı bütün tanıdıklarına gönder'*
  - *'Anlatılanlar aldatmaca değildir'* veya *'bu bir şehir efsanesi değildir'*
- Sıklıkla *büyük harfle* yazılmış kelimeler ve *birden çok ünlem işareti* (!!!) birlikte kullanılır.
- Anlatılanlarda *mantıksal olarak çelişen* noktalar vardır.
- Öncesinde veya eş zamanlı olarak *başkalarına da iletilmiştir.*

2.2. E-Posta Yoluyla Yapılan Saldırılardan Korunma Yolları

- Taklit (yemleme) veya aldatmaca e-postası olduğundan şüphelenilen bir e-posta alındığında, sistem yöneticisi ile görüşülüp kurum genelinde gerekli uyarının yapılması sağlanmalıdır.

- Bilinmeyen göndericilerden gelen e-postada içeriğindeki linke kesinlikle tıklanmamalıdır.

- Tanıdık göndericilerden gelen linklere de mesafeli ve şüpheci yaklaşılmalıdır. Zira, hesap bir başkası tarafından ele geçirilmiş veya taklit edilmiş olabilir.

- Kurum içerisinde komik resimler, ilginç olaylar ve bilgilendirici yazılar toplu olarak gönderilmemeli veya gönderilecekse "gizli karbon kopya" (bcc) olarak gönderilmelidir. Aksi takdirde, bir kişi bu e-postayı kurum dışı bir hesaba gönderdiğinde, birçok kurumsal e-posta adresine ulaşılabilir.

3. SOSYAL MÜHENDİSLİK

Sosyal mühendislik, internet ortamında, insanların zaafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içerir.

3.1. Sosyal Mühendislik Yöntemleri

3.1.1. Telefon yolu ile

En etkili sosyal mühendislik ataklarından biridir. Hedef kişi, bir dolandırıcı tarafından aranır ve arayan kişi yetkili biri gibi davranarak yavaş yavaş kişisel belgilere ulaşır veya istediği eylemleri yaptırır.

3.1.2. Çöpleri Boşaltma (Dumpster Diving)

Önemli ve kötü niyetli kullanıma uygun birçok bilginin, kurumun veya şirketin çöplerinden derlenerek elde edilmesidir. Kısa notlar, şirket/kurum idari politika bilgileri, olaylar ve tatil izinleri, sistem işleyiş şekilleri, hassas veriler ya da giriş/çıkış isim ve şifreleri, organizasyon grafikleri, kaynak kod çıktıları, taşınabilir dijital ortamlar, mektuplar, kısa formlar, eskimiş donanımlar vs. gibi.

Bu kaynaklar, kötü niyetli kişiler için zengin bilgi damarlarıdır. Organizasyon grafikleri, organizasyondaki yetkili pozisyondaki kişiler hakkında bilgiler içerir. Küçük notlar, giriş oluşturmak için cazip ve ilginç küçük bilgiler içerir. Takvimler çok önemlidir. Hangi işçinin, ne zaman iş yeri dışında olacağını belirtir. Sistem el kitapları, hassas bilgiler ve diğer teknik bilgi kaynakları, ağa izinsiz girebilmek için gerekli bilgileri verebilir. Son olarak, eski donanımlar, özellikle sabit diskler yeniden onarılıp tüm kullanışlı bilgiler elde edilebilir.

3.1.3. İkna Etme

Dolandırıcılar, ataklarda, psikolojik bir etki kurabilmek için sosyal mühendislik ile mükemmel bir psikolojik etki oluşturma üzerinde çalışırlar. Taklit etme, kendini sevdirme, riayet etme, sorumluluk yayma ve sade bir arkadaş olarak görünme yöntemlerini denerler. Bu metotların kullanımında ana hedef gizli bilgileri öğrenebilmek için inandırıcı olmaktır.

3.1.4. On-Line Sosyal Mühendislik

Sosyal ağları (Twitter, İnstagram, Facebook vb.) çok etkin kullanarak sizi arkadaşınız kadar iyi tanıyabilirler. Facebook aracılığıyla anne kızlık soyadını öğrenmek dakikalar almakta ve bu basit bilgi ile birçok işlem yapılabilmektedir. İnternet, hedeflenen şifreleri sosyal mühendislik ile elde etmek için önemli bir alandır. Birçok kullanıcının yaptığı başlıca hata, aynı şifreyi birçok hesapta kullanmaktır. Bir kullanıcının şifresi elde edildiği zaman birçok hesapta denenir.

3.2. Sosyal Mühendislikten Korunma Yöntemleri

- Kullanıcılar eğitilmelidir. Sosyal Mühendisliğe karşı alınacak en iyi tedbir, kullanıcıları eğitmekten geçer. Bu eğitime en alt kademedeki kullanıcıdan, en üst kademedeki kullanıcıya kadar herkes katılmalıdır.
- Eğitimde, kullanılan yöntemler her yönüyle anlatılmalı, örnekler verilmeli ve kullanıcılar bilinçlendirilmelidir.
- Telefonda arayan hiç kimseye şifreler ve önemli bilgiler verilmemelidir.

- Büyük şirketlerde veya kurumlarda "yardım masası" denilen bölümler vardır. Bu bölümleri arayıp sözde yardım isteyen kişilerle bilgi paylaşımı yapılmamalıdır. Kimlik doğrulaması tam olarak yapılmalıdır.
- Uygun olmayan yöntem ve kanallardan kurumsal bilgiler paylaşılmamalıdır.
- Parola gizliliği prensibi, kurum genelinde uygulanmalıdır.
- Gerektiğinde, "Ben kurumsal hattan sizi arayayım" denilmelidir.
- Kurumsal gizlilik taşıyan evraklar, uygun yöntemlerle imha edilmelidir.
- E-Posta, posta ile gelen CD, yardımcı yazılımlar vs. kullanımında dikkatli olunmalıdır.

4. BİLİŞİM CİHAZLARI FİZİKSEL GÜVENLİĞİ

Fiziksel güvenlik göz ardı edilse de en önemli unsur olarak karşımıza çıkmaktadır. Bizim için önemli olan cüzdanımızı veya sırt çantamızı nasıl ulu orta, açıkta bırakmıyorsak, bilgi işlem materyallerini de ulu orta ve korunmasız olarak bırakmamamız gerekmektedir. Bilinçsiz veya kötü amaçlı saldırılara maruz kalmamak için fiziksel olarak alınabilecek önlemlere gelince:

- Bilgisayar oturumuna mutlaka şifre konulmalıdır. Şifre, yazarken gizlenmelidir.
- Kişisel şifreler herhangi bir dokümana yazılmamalıdır. Yazılması durumunda da iyi muhafaza edilmelidir.
- Taşınabilir veri ortamları (CD/DVD, Taşınabilir Disk, taşınabilir PC, Cep telefonu vb.) açık ortamlarda bırakılmamalıdır.
- Arızalı Bilgi İşlem Cihazlarını mutlaka Bilgi İşlem Daire Başkanlığına ulaştırılmalı, yetkisiz müdahalelere izin verilmemelidir.
- Arızalanan taşınabilir veri ortamları çöpe atılmadan önce imha edilmelidir.
- Bilgisayarın mutlaka BIOS şifresi olmalı ve BOOT seçeneklerinde en önde Harddisk olmalıdır.

5. SOSYAL MEDYA GÜVENLİĞİ

Sosyal Medya, yeni nesil web teknolojilerinin getirdiği kullanıcı kolaylığı ve iletişim hızıyla yakalanan eş zamanlı bilgi paylaşımının yapılarak takip edildiği dijital platformdur.

Sosyal medya üzerinden yapılacak bilgi, haber ve video paylaşımı konusunda çok dikkatli olunması gerekmektedir. Ayrıca bu işlemler nedeniyle yargılanılmakta veya hakaret veya tehdit unsuru paylaşımlar yargı önünde suçlu duruma düşürebilmektedir. Bunun yanında, sosyal medya mağduru olmamak için yapılması gerekenler de var.

5.1. Sosyal Medya Kullanımında Dikkat Edilmesi Gerekenler

- Resmi olmayan hiçbir sayfa ve profile itibar edilmemelidir.
- Kişisel bilgilerin herkese açık görünür şekilde yer almasına izin verilmemelidir.
- Yapılan paylaşımların içeriğine ve suç unsuru taşıyıp taşımadığına dikkat edilmelidir.
- Sosyal medya üzerinden maruz kalınan söz ve davranışlar hakkında suç duyurusunda bulunma hakkı vardır.
- Hiçbir yerde özel bilgiler paylaşılmamalı ve tanınmayan kişiler arkadaş listesinde yer almamalıdır.

- Fotoğraf veya videolar paylaşılmadan önce fotoğrafta yer alan diğer kişilerden mutlaka izin alınmalıdır.
- Yer bildiriminde bulunurken, aslında bulunulan adres ve konumun da paylaşıldığı unutulmamalıdır.
- Ekranlarda karşılaşılan her bilginin doğruluğu mutlaka sorgulanmalı ona göre hareket edilmelidir.
- Twitter ve Facebook gibi sosyal ağlarda gezinirken kaynağı belirtilmeyen aldatıcı linkler tıklanmamalıdır.
- Sizin, ailenizin, çocuklarınızın, yakınlarınızın stratejik önem taşıyan bilgilerini, toplantılarını ve seyahatlerini vb. kamuya açık olmayan bilgileri paylaşmaktan kaçının.

6. ZARARLI YAZILIMLAR

Zararlı yazımlar kullanıcı tarafından izin verilmeyen işlemler gerçekleştiren kötü amaçlı programlardır.

Zararlı yazılımlar kullanıcı verisi silme, engelleme, kopyalama, değiştirme, çalma, bilgisayar ve bilgisayar ağlarının performansını düşürme gibi zararlı amaçlar için programlanmaktadırlar. Zararlı yazılımlar kullanıcı sistemlerine internet üzerinden bulaşabildiği gibi, harici diskler, USB cihazları gibi harici medya üzerinden de bulaşabilir.

6.1. Zararlı Yazılım Çeşitleri:

6.1.1. Bilgisayar Virüsleri: Virüsler, uygulamalara zarar vermek, dosyaları silmek ve sabit diski yeniden formatlamak gibi çeşitli şekillerde bilgisayarlara zarar verir. Bazıları ise zarar vermektense, sadece sistem içinde çoğalmak, sistemi yavaşlatmak için programlanmışlardır.

6.1.2. Solucan: Sistemde bir açık oluşturup kötü amaçlı kişilere sistemi kontrol etme yetkisi verebilmektedirler.

6.1.3. Casus Yazılım: Sadece kişisel bilgileri ele geçirmek için tasarlanmışlardır. Bilgisayarlarda yer alan bilgileri karşı tarafa gönderen bu casus yazılımlar, keylogger gibi klavye hareketlerini takip edebilirler.

6.1.4. Reklam Yazılımı (Adware): Hakkınızdaki pazarlama verilerini toplamak amacıyla tasarlanmış programlara verilen genel adıdır.

6.1.5. Truva Atı (Trojan): Sistemi diğer bilgisayarlarca internet ya da ağ üzerinden kontrol edebilmeye açık hale getiren yazılımlardır.

6.1.6. Botnetler: Bilgisayarı bir bot'a (zombi olarak da bilinir) çeviren kötü amaçlı yazılımlardır. Böyle bir durumda bilgisayarlar, kullanıcıların bilgisi dışında internet üzerinden otomatik görevleri gerçekleştirebilir.

6.1.7. Fidye Yazılımı: Fidye yazılımı saldırılarında çoğunlukla aynı rutin yöntem kullanılır. Önce bilgisayar korsanları tarafından kullanıcının ilgisini çekecek bir bağlantı veya dosya içeren e-posta gönderilir. Merak edip bu bağlantıya tıklayan ya da dosyayı indiren kullanıcının bilgisayarına zararlı yazılımlar bulaşır. Çoğu zaman kullanıcı, bilgisayarı ya da dosyaları kilitlenene kadar zararlı yazılımların bulaştığını anlayamaz.

6.2. Zararlı Yazılımlardan Korunma Yöntemleri.

- Lisanslı yazılımlar kullanılmalı, korsan yazılımlar kullanılmamalıdır.
- Tüm yazılımlar güncel tutulmalıdır.
- Güçlü parolalar kullanılmalı ve gizlilik sağlanmalıdır.
- Güvenilir olmayan, özellikle halka açık kullanımı olan bilgisayarlarda kişisel parolalar girilmemelidir.

- Güvenlik duvarı, geçici olarak bile olsa asla kapatılmamalıdır. Güvenlik duvarı, bilgisayar ile internet arasına koruyucu bir engel koyar.
- Bilinmeyen kişilerden gelen postaların ekleri açılmamalı veya antivirüs taramasından geçirilmelidir.
- Dosya indirilmesini isteyen pencerelere itibar edilmemelidir.
- Bilgisayarda oturum açmak için kullanılacak hesap, yönetici ayrıcalıklarına sahip olmamalıdır.
- E-devlet gibi uygulama ve portalları kullanılırken bağlantı adreslerinde bulunan güvenlik simgeleri kontrol edilmelidir. Adres satırı incelenerek doğru siteye bağlanıldığından emin olunmalıdır.