

YMH321 Bilgi Sistemleri ve Güvenliđi

Güvenlik ve Hacking Kavramları

Bölüm - 3

Prof.Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliđi Bölümü

Konu Başlıkları

- Bilişim güvenliği
- Bilişim güvenliği niçin önemlidir ?
- Hacker,
- Hacker çeşitleri,
- Hacker'lerden korunma yolları,
- Sosyal Mühendislik kavramı,
- Sosyal Mühendislik çeşitleri,
- Sosyal Mühendislerin kullandığı yöntemler,
- Sosyal Mühendislerinden korunma yolları

BİLİŞİM GÜVENLİĞİ NEDİR VE NİÇİN ÖNEMLİDİR?

- Bilişim suçları ve Güvenlik araştırması nın her yıl hazırladığı rapora göre bilişim suçları neredeyse her yıl 2 katına arttığı gözlenmiştir.
- Bilişim teknolojilerinin hayatımızın her alanında girmiş olmasıyla birlikte faydaları kadar bize dokunan zararları da ortaya çıkmıştır. Bilişim teknolojileri geliştikçe sistemlere yapılan saldırılar artmakta ve saldırı teknolojileri gelişmektedir.

BİLGİ GÜVENLİĞİMİZ İÇİN NELER YAPABİLİRİZ ?

- Şifre güvenliği
- Güvenilmeyen adreslerden gelen e-posta'ları okumak için dahi olsa açmamak (Resimli E-posta eklentileri)
- Geliştiricisi bilinmeyen Facebook Application 'lara katılmamak
- Tanımadığımız kişilerden gelen isteklere, aktivitelere katılmamak (Facebook, MSN vs.)
- Gerçek bilgilerimizi her yerde paylaşmamak (e-posta, TC kimlik No vs.)
- İnternette verdiğimiz tüm bilgilere birilerinin ulaştığını düşünerek her düşündüğümüzü, yaptığımızı vs. ulu orta paylaşmamak ☺
- Bilgi güvenliğimiz için birden fazla adres (e-posta vs.) kullanmaya özen göstermeliyiz.

Bunları biliyor muydunuz ?

- MSN'de hotmail ve windowslive.com gibi uzantılarda tek bir şifre ile korunurken, gmail vs. gibi Microsoft haricindeki diğer uzantılarda MSN ve mailin aynı şifre olması zorunlu değil.
- Facebook 'da hangi bilgisayardan (hatta browser'dan) giriş yaptıysan o bilgisayarın bilgilerini kayıt edip, eğer bilmediğin bir ortamdan adresine giriş yapılmış ise oturumu sonlandırabiliriz.
- WLM 2011 ile birlikte bir bilgisayarı güvenilen bir bilgisayar olarak gösterip, şifreni unuttuğunda direk güvenilen bilgisayar üzerinden hiçbir soru sorulmaksızın yeni şifre oluşturabiliriz.

HACK – HACKER KAVRAMLARI ?

- Hacker: Bilişim teknolojilerindeki bilgisini İYİ veya KÖTÜ olmak üzere bir sistemi ele geçirmek üzere kullanan kişi
- Hack: Kısaca bir hacker'ın yaptığı saldırıya verilen genel ad

DÜNYADAKİ BİLİŞİM SUÇLARI EN ÇOK HANGİ ÜLKELERDE İŞLENİYOR ?

- Türkiye, Rusya ve Brezilya
- Sebep: Bilişim suçlarına olan cezaların yetersiz kalması ve yeterince uygulanamaması

HACKER ÇEŞİTLERİ

- Yaptığı saldırı düzeyine göre Beyaz ve siyah şapkalı olmak üzere ikiye ayrılır.
- Ayrıca, siyah şapkalı hackerlar kendi içinde ayrılabilir.
- -Script Kiddies (Lamer): Kendini bir şey zanneden hacker 😊
- -Phreakers: Santral ve telefon hatlarının açıklarını kullanan hacker
- -Crackers: PC yazılımlarını kıran ve yayınlayan hacker
- -Grey Hat Hackers: Hem savunma hemde saldırı amaçlı çalışan hacker. Amacı sadece kazanmaktır

DÜNYANIN EN ÜNLÜ HACKER'I KİMDİR ? YAPTIĞI SALDIRILAR

- **Kevin David Mitnick** (**Condor** olarak da bilinir) (d. 6 Ağustos, 1963), ilk bilgisayar korsanlarından olup en meşhurdur. 15 Şubat 1995'te FBI tarafından yakalanmıştır. Fujitsu, Motorola, Nokia ve Sun Microsystems gibi şirketlerin bilgisayar ağlarına izinsiz girmekten suçlu bulunarak 5 yıl hapis cezası almıştır. Cezası 21 Ocak 2000'de, bilgisayarlara yaklaşma yasağı 21 Ocak 2003'te bitmiştir. Günümüzde, beyaz şapkalı bir bilgisayar korsanı olarak güvenlik danışmanlığı yapmakta ve dünya çapında kongrelere katılmaktadır.
- Mitnick, fotoğrafı FBI'in "En Çok Aranılanlar" listesinde yer alan ilk hacker olarak kayıtlara geçti ve neredeyse listeden hiç eksik olmadı. "İflah olmaz bir suçlu" olan çocuk ruhlu Mitnick "Sanal Dünya'nın Kayıp Çocuğu" olarak da tanındı.

DENNIS RITCHIE VEYA KEN THOMPSON'I TANIYOR MUSUNUZ ?

- İlk başlar siyah şapkalı hacker olup sonradan beyaz şapkalılara katılan ünlü hacker'lardan.
- Esas ünleri C ve C++ Dillerini yazıp, Unix işletim sisteminin baş mimarı olmalarıdır.
- C programlama dili bugün hâlâ yazılım dünyasında aktif olarak kullanılmaktadır ve C++, Java, C# gibi modern programlama dillerini de etkilemiş konumdadır.

DENNIS RITCHIE VEYA KEN THOMPSON'I TANIYOR MUSUNUZ ?

- Ünlü Linux işletim sistemi ve onun araçları Dennis Ritchie'nin yaptıklarına dayanmaktadır. Windows işletim sistemi de Unix uyumlu araçlar ve geliştiriciler için C derleyicileri içermektedir.



Ken Thompson (solda) ile Dennis Ritchie (sağda)

SOSYAL MÜHENDİSLİK KAVRAMI =?

- Akıllı insan kendi aklını kullanır. Daha akıllı insan ise hem kendi aklını hem de başkalarının aklını kullanır.
- BT alanında yeterli teknik bilgiye sahip olup açık aramaktansa insanların zayıf ve bilgisiz noktalarını kötü niyetli kullanan yaratıktır

SOS. MÜH. ÇEŞİTLERİ ?

- İnsan tabanlı ve PC Tabanlı olmak üzere ikiye ayırabiliriz.
- PC tabanlı Sos. Müh. hem aklını hem de PC bilgilerini kullanan kişidir desek herhalde yanlış olmaz.

SOS. MÜH. ÖRNEKLERİ?

- Sahte mail (Bir kişi ya da kurum adına mail göndererek kandırma)
- Bir web sitesinin tasarım olarak benzerini yapıp, domain olarakta çok benzer bir domain alıp, bilgilerimize erişmek
- Reklam'lara tıkla para kazan vs. sahte siteler.
- Kendisini bir firmanın yetkili kişisi gibi tanıtıp bilgilerine erişmek.

Sonuç

Sorular

