



Güvenlik ve Virüsler

ODTÜ BİDB

İbrahim Çalışır, Ozan Tuğluk, Cengiz Acartürk

04.04.2005



Bilgi güvenliği neden gerekli?

- Kişisel bilgi kaybı
- Üniversiteye ait bilgilerin kaybı
- Bilgiye izinsiz erişim ve kötüye kullanım
- Prestij kaybı
- Maddi kayıplar
- Serviste aksama



Sunucu Bilgisayar

- ODTÜ ağında dağıtık servis
- Birimlerdeki sunucular
 - E-posta
 - FTP
 - Web
 - DNS



Sunucu Bilgisayar

- Sorunlar
 - Güncelleme
 - İşletim sistemi
 - Sunucu yazılımlar
 - Gereksiz kullanıcılar, güvensiz erişim
 - Zayıf parolalar
 - Belgeleme



Sunucu Bilgisayar

- Önlemler
 - Gerekmedikçe servis vermemek
 - Sunucu bilgisayar kurulması zorunlu durumlarda
 - İşletim sisteminin güvenilir olması
 - Sunucu yazılımların güvenilir olması
 - Zayıflık taraması testleri (Nmap, Nessus vb.)
 - Kritik dosyalarının hash verisinin ayrı bir ortamda depolanması



Sunucu Bilgisayar

- Önlemler
 - Yedekleme
 - Belgeleme
 - Yazan insanın yanı sıra okuyan insanın anlayabileceği dilde yazılmalı
 - Depolandığı yer belli olmalı
 - Paylaşılmalı



Masaüstü Bilgisayar

- İlk kurulumda yaşanan problemler
 - Windows XP yaşam süresi: 30 dakika
 - Güncelleme
 - Kullanılmayan servisler
 - Windows Dosya ve Yazıcı paylaşımı
- Öneri
 - Ağ bağlantısız kurulum/güncelleme
 - Güvenli Kurulum CD'si



Masaüstü Bilgisayar

- Kurulumdan sonra yaşanan problemler
 - Güncelleme (işletim sistemi ve yazılımlar)
 - Virüs, rootkit, spyware vb. problemler
- Öneri
 - Otomatik güncelleme
 - Zayıflık taramaları (Nmap, Nessus vb.)
 - Yedekleme



Güvenlik Tehditleri

- Virüs ve solucanlar
 - Masaüstü ve sunucu Windows işletim sistemleri
 - Microsoft SQL Server, Microsoft IIS Web Server vb. Windows sunucu yazılımları
 - E-posta, web sayfaları ve P2P dosya paylaşım programları ile ve ağ üzerinden yayılma



Güvenlik Tehditleri

- Virüs ve solucanlar
 - Nasıl farkedilir?
 - Korunma ve temizleme
 - İşletim sistemi kurulumu
 - Otomatik güncellemeler
 - Virüs taramasını güvenli kipte yapmak
 - Kullanıcıların bilgilendirilmesi
 - ODTÜ'ye lisanslı antivirüs yazılımları: Mcafee 8.0i, Symantec Norton 9.0



Güvenlik Tehditleri

- Gereksiz servisler
 - Windows işletim sistemlerinde
 - Telephony
 - Telnet Server
 - Alert
 - Windows Time Server...



Güvenlik Tehditleri

- Güvensiz erişim ve öneriler
 - Telnet yerine SSH kullanılmalı
 - FTP yerine SFTP kullanılmalı
 - Zayıf parola kullanılmamalı
 - Aynı parola uzun süre kullanılmamalı
 - E-posta okuma programlarında SSL'li erişim
 - <https://webmail.metu.edu.tr>
 - Outlook, Thunderbird vb. e-posta okuma programlarında SSL ayarları



Güvenlik Tehditleri

- Rootkit
 - Nedir?
 - Nasıl farkedilir?
 - Korunma ve temizleme yöntemleri
 - İşletim sisteminin yeniden kurulması
 - Araçlar (Rootkit Revealer, Rootkit Hunter)



Güvenlik Tehditleri

- Spyware
 - Nedir?
 - Nasıl farkedilir?
 - Korunma ve temizleme yöntemleri
 - Araçlar (Adaware, Mcafee 8.0, Spyware Sweeper vb.)



Güvenlik Tehditleri

- Phishing & Pharming saldırıları
 - Nedir?
 - Yöntemler?
 - Nasıl farkedilir?
 - Korunma yöntemleri
 - Bilgilenme (<http://www.antiphishing.org>)



Web Siteleri

- Koordinatörler web sitesi: <http://coordinators.metu.edu.tr/>
- Güvenlik web sitesi: <http://guvenlik.metu.edu.tr>
- Antivirüs web sitesi: <http://antivirus.metu.edu.tr>
- BİDB web sitesi: <http://www.bidb.odtu.edu.tr>
- Kısıtlanan IP'ler: <http://affected.metu.edu.tr>



TEŞEKKÜRLER