



Mehmet Fatih Zeyveli

CISSP

fatih@beyaz.net

Kullanıcı Tarafı Güvenliđi

Giriş

Güvenlik Kuralı : “Client Side Security does not Work”



Neden?

- Bilgisayarların kullanıcıların kontrolünde olması,
- Çok sayıda kullanıcı bilgisayarı bulunması,
- Farklı kullanıcıların farklı taleplerinin olması,
- Kullanıcı, Bilgi İşlem, yönetim uyumsuzluğu,
- Tehditlerin artmış olması,
- Uygulamaların artması ve karmaşıklaşması,
- Uygulamaların ticari kaygı ile yeterli test yapılmadan piyasaya sürülmesi.
- Server tarafındaki zayıflıklar,
- Şifre zayıflıkları,
- Hukuki sıkıntılar.
- Kullanıcıların bilgisizliği,



Kullanıcıların bilgisizliđi

- Sistemlerin karmaşıklığı,
- Kullanıcıların yeterli bilgi ve eğitiminin olmaması,
- Programları güvenlik için ayarlamanın zorluğu,
- Teknolojilerin hızlı gelişmesi,
- Her türlü program ve bilgiye kolayca erişebilme.

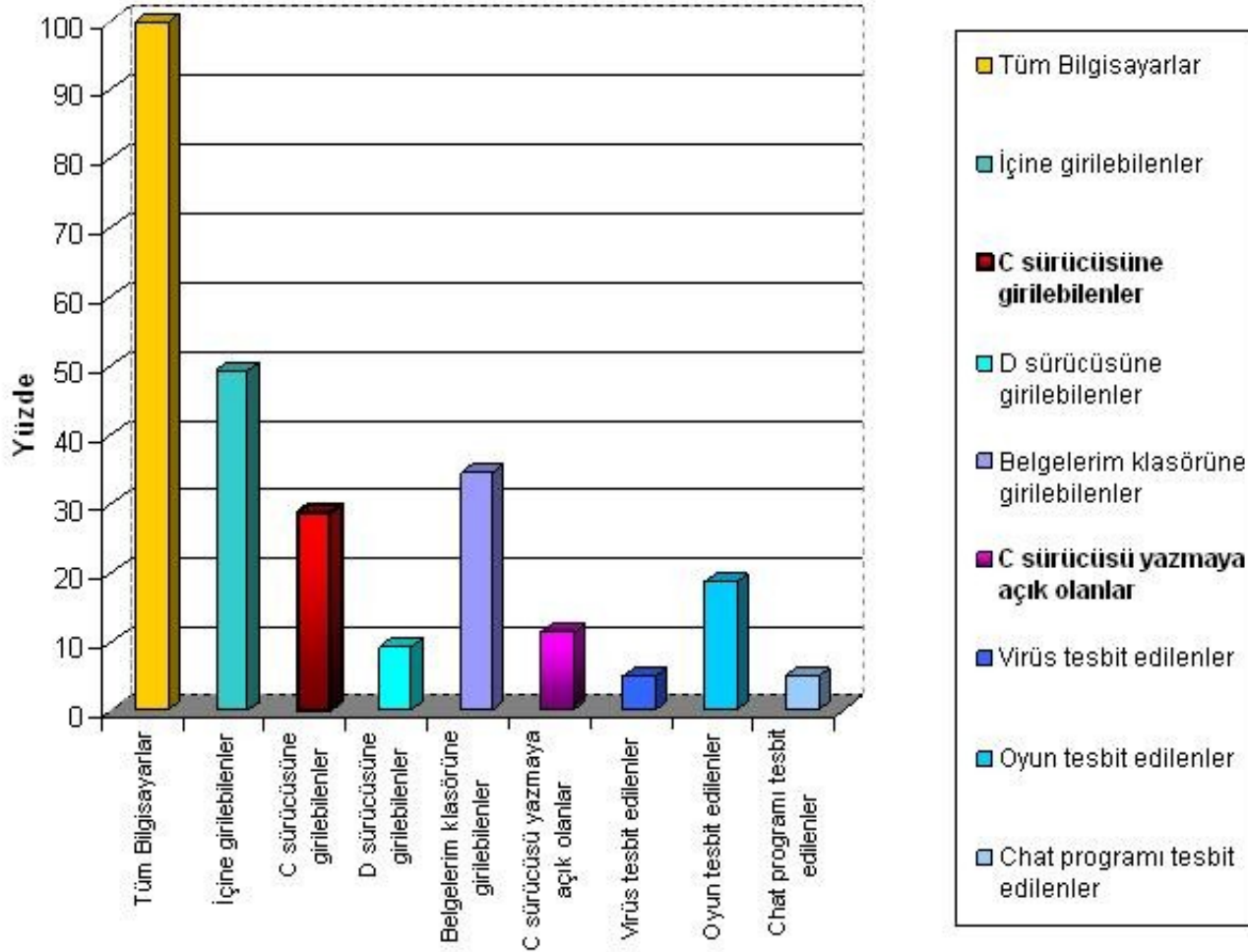


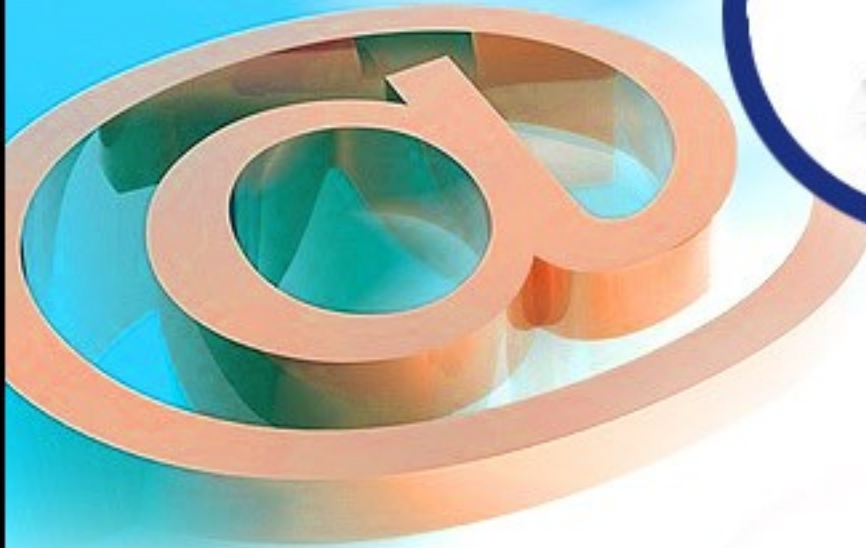
Istatistikler

- **92% of IT managers report that spyware has infected their organizations -2004 Harris Poll**
- **Dell estimates that spyware now triggers more than 20% of their support calls**
- **Forrester survey found that 17% of systems are infected with spyware, and 7% of help desk calls are due to spyware Protects**
- **Approximately \$11.5 million in proprietary information was reported stolen in 2004.**
- **By first-half 2004, 90% of Global 1000 enterprises will have experienced an internal network disruption.**
- **Over the first six months of 2004, there were over four-and-a-half times the number of viruses and worms as the same period in 2003.**



İstatistikler





Tehditler

Zararlı uygulamalar

- **Virus**
- **Trojan**
- **Worm**



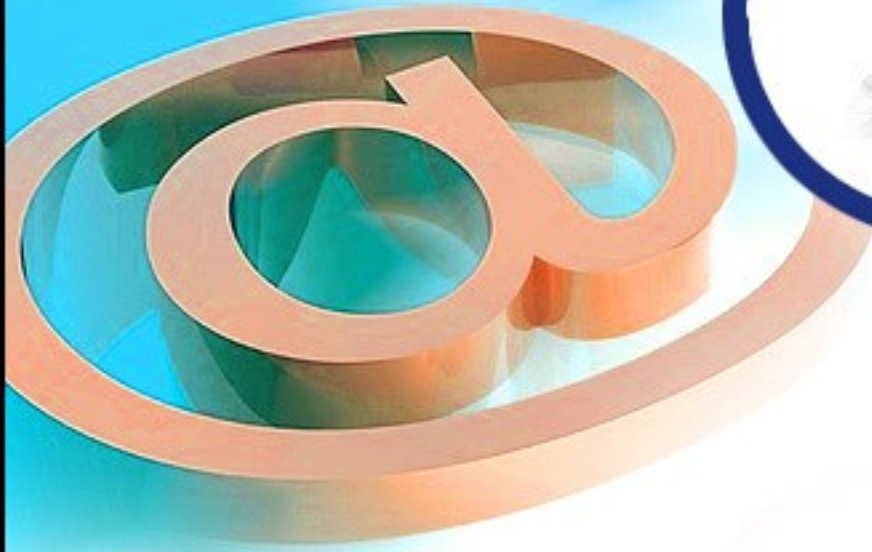
45

WWW

Diğer Tehditler

- **Saldırılar**
 - Exploitler
 - Ağı dinleme
 - Spoofing
- **Kandırma (Social Engineering)**
- **Kimlik Hırsızlığı (Fraud)**
- **Keylog**
- **Spam**



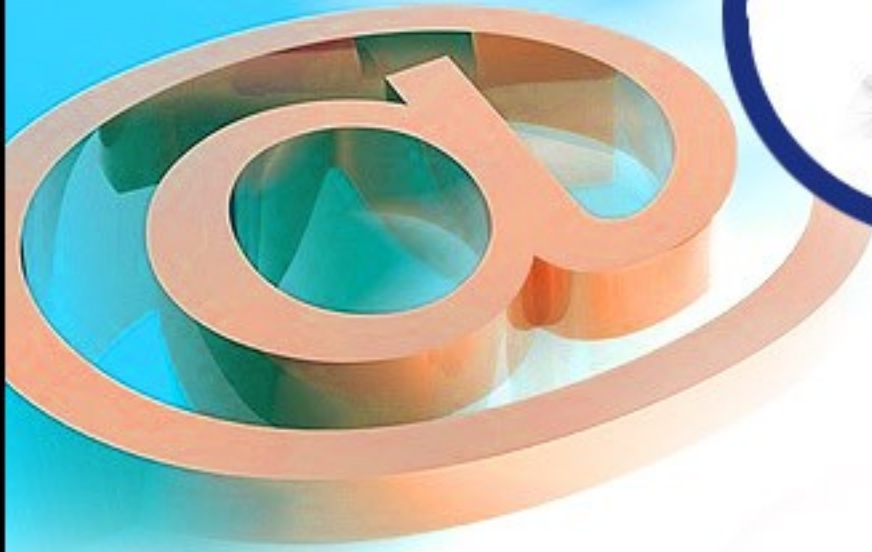


Sonuçlar

Getirdiđi Sorunlar

- Veri Kaybı
- Veri alınması
- Maddi Kayıp
- Süre Kaybı (bilgisayarların kapalı olması)
- Bakım Maliyetinin artması





Çözümler

“Clien Security” uygulamaları

- Anti-Virus
- Anti-Spyware
- Personel Firewall
- Dijital Sertifika
- Server Tarafı teknolojileri
 - Firewall
 - Antivirus gateway
 - IDS/IPS
 - Content Filtering
 - Port Filtering

Avantajları

- Yetenekli uygulamalar

Dezavantajları

- Maliyet
- Düzenli güncelleme gerektirmesi
- Yeni çıkan saldırıları tanımama
- Farklı saldırılara karşı zayıf.



Thin Client

Dummy Terminal : Tüm işlemler sunucuda, sadece ekranlar aktarılıyor.

Avantajları

- Tek noktada güvenlik
- Merkezi kontrol

Dezavantajları

- Pahalı
- Network bağımlı
- Çok uygulamalı ortamlarda sıkıntılı
- Ses ve görüntü uygulamalarında sıkıntılı



Merkezi Kullanıcı ve kısıtlama

Active Directory, Group Policy : Neye İzin verilir, neye izin verilmediğinin belirlenmesi.

Avantajları

- Merkezi Kontrol

Dezavantajları

- Active Directory gerektirmesi,
- Ayarlama zorluğu,
- Tanımlanmamış tehditleri engelleyemez,
- Düzenli takip ve güncelleme gerekir,
- Microsoft uygulamalarında yetenekli, diğer uygulamalarda zayıf
- Admin, local admin kullanıcısı tehlikeli,
- Fazla sınırlandırma, kullanımı engelleyebiliyor.



Açık Kaynak sistem ve uygulama kullanımı

Avantajları

- Güvenilir
- Ucuz

Dezavantajları

- Zor
- Alışkanlık yok
- Görsellik zayıf
- Tanıtım zayıf



Restore on Boot (AçılıŖta Bilgisayarı yenileme)

Avantajları

- Bilgisayara yüklenen zararlı, zararsız tüm uygulamalar silinir. (virus, trojan vb)
- Her türlü ayar ilk haline alınır,
- Bakım maliyetleri minimuma iner,
- Bilgisayarlar daha çok aktif olurlar,
- Kullanıcıya sınırlandırma getirmez

Dezavantajları,

- Zararlı uygulamalar bilgisayar kapatılana kadar devrede olabilir,
- Yeni uygulama kurulumu zordur,
- Kullanıcıya sınırlandırma getirmez,
- Lüzumlu bilgiler silinebilir,
- Güncelleme zordur.



White List

Sadece izin verilen uygulamaların çalışması,

Avantajları

- Bilinmeyen ve gelecek tehditlere karşı koruma sağlar,
- White-List otomatik oluşturulur,
- Güncelleme ihtiyacı yoktur,
- Kullanıcıları yeni uygulama çalıştırma haricinde sınırlandırmaz,
- Bakım maliyetlerini düşürür,
- Network bağımlı değildir

Dezavantajları

- Yeni uygulama çalıştırılmak istenirse white-list e eklenmesi gerekir,
- Kullanıcılar sevmez,



Deep Freeze

Her açılıŖta diski ilk haline getirir.

Klasör silinse

Format atılsa

Masaüstü ayarları deęiŖtirilse

Yeni program yüklense

Virus bulaŖsa

İŖletim sistemi bozulmalarını engeller.

Zararlı programların buluşmasını engeller. (virus, trojan, worm vb.)

Yönetimi kolaylaŖtırır.

Kullanıcıya sınırlandırma getirmez.

(Bilgisayarın Disket ve CD'den açılıŖ özellięi BIOS'dan kapatılmalıdır)



Deep Freeze Özellikler

Garantili bir teknolojisi vardır. (kopyalama yapmaz)

5.000.000 dan fazla lisanslı kullanıcısı vardır.

Windows'un çekirdek seviye sürücülerini değiştirerek sağlar.

Açılışda zaman kaybı yoktur,

Diske ek bir yük getirmez, (hatta disk yükünü azaltır),

Windows ve Mac %100 uyumludur.

Disklerin bir kısmı dondurulmuş (frozen), bir kısmı açık (thawed) bırakılabilir.

Uzaktan yönetilebilir,

Güncelleme Yapılabilir,

Silinmeyen disk oluşturulabilir,



Deep Freeze Özellikler

Ağ ortamında merkezden yönetilebilir,
Ağ ortamında merkezden yüklenebilir,
Deep Freeze ayarları merkezden değiştirilebilir,

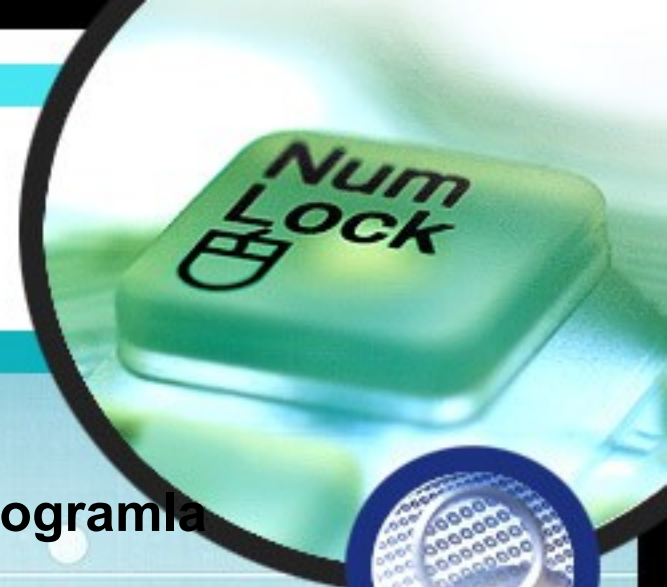
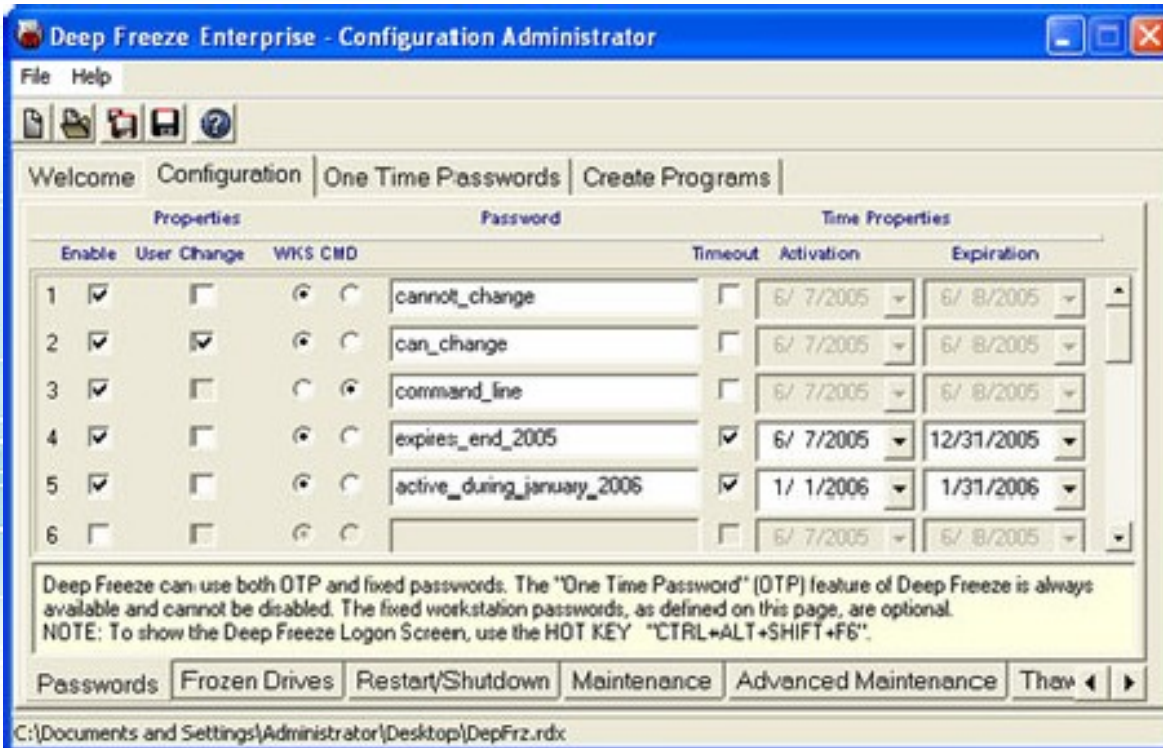
Güncelleme Yapılabilir,
Silinmeyen disk oluşturulabilir,



Deep Freeze Configuration Admin

Farklı yükleme dosyaları oluşturabilir.

Yükleme dosyaları ile ilgili her türlü ayar bu programla yapılır.



Deep Freeze Configuration Admin

Farklı Deep Freeze konfigürasyon dosyaları oluşturulabilir.

Deep Freeze kurulumları için farklı yetkilerde kullanıcılar oluşturulabilir.

Tek kullanımlık şifre oluşturulabilir.

Hangi sürücülerin dondurulacağı belirlenbilir.

Bilgisayarların otomatik kapanma veya yeniden açılma saatleri belirlenebilir.

Windows ve Anti-virus güncelleme ayarları belirlenebilir,
Silinmeyen disk oluşturulabilir,



Deep Freeze Server Console



The screenshot displays the 'Deep Freeze Enterprise Server Console' application window. The interface is divided into several sections:

- Menu Bar:** File, View, Select, Help
- Toolbar:** Contains various icons for navigation and management, including a search icon, a refresh icon, and a 'ALL' button.
- Network and Groups:** A tree view on the left showing the network structure. It includes 'Entire Network', 'DEEFPREZE', 'User Defined Groups', and '[History]'. Under 'Remote Consoles', it shows a specific IP address '[192.168.1.150:1971]' with its own sub-tree.
- Workstations:** A list on the right showing four workstations: 'WORKSTATION-1', 'WORKSTATION-2', 'WORKSTATION-3', and 'WORKSTATION-4'. 'WORKSTATION-1' is currently selected.
- Status Panel:** Located at the bottom left, it provides a summary of workstation states:

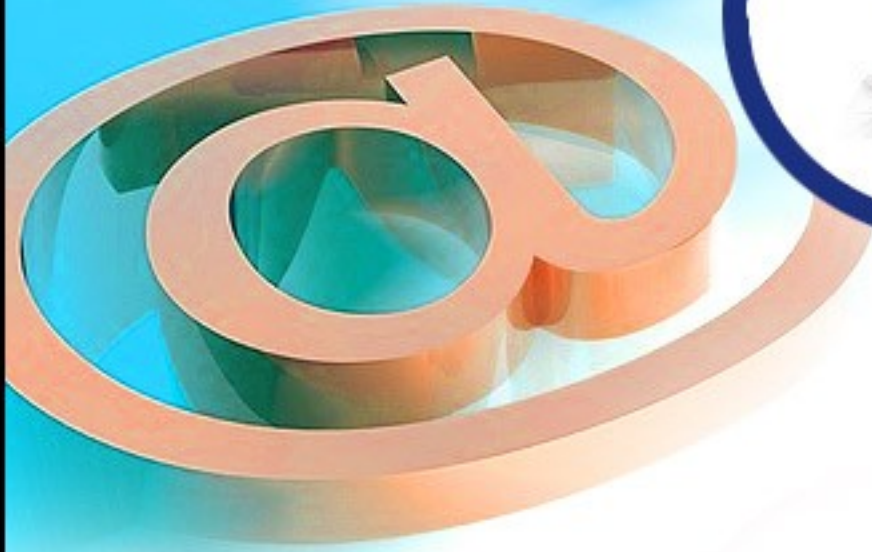
Frozen	4
Thawed	0
Target	0
History	0
Total	4
- Footer:** Displays 'Port :1971' and 'Remote Control Disabled'.



Deep Freeze Server Console

- Merkezden tüm Deep Freeze yüklü bilgisayarları görür ve kontrol eder,
- Gruplar oluşturulabilir,
- Deep Freeze ayarları merkezden tek tek veya topluca değiştirilebilir,
- Bilgisayarlar merkezden açılıp kapatılabilir,





Teşekkürler
