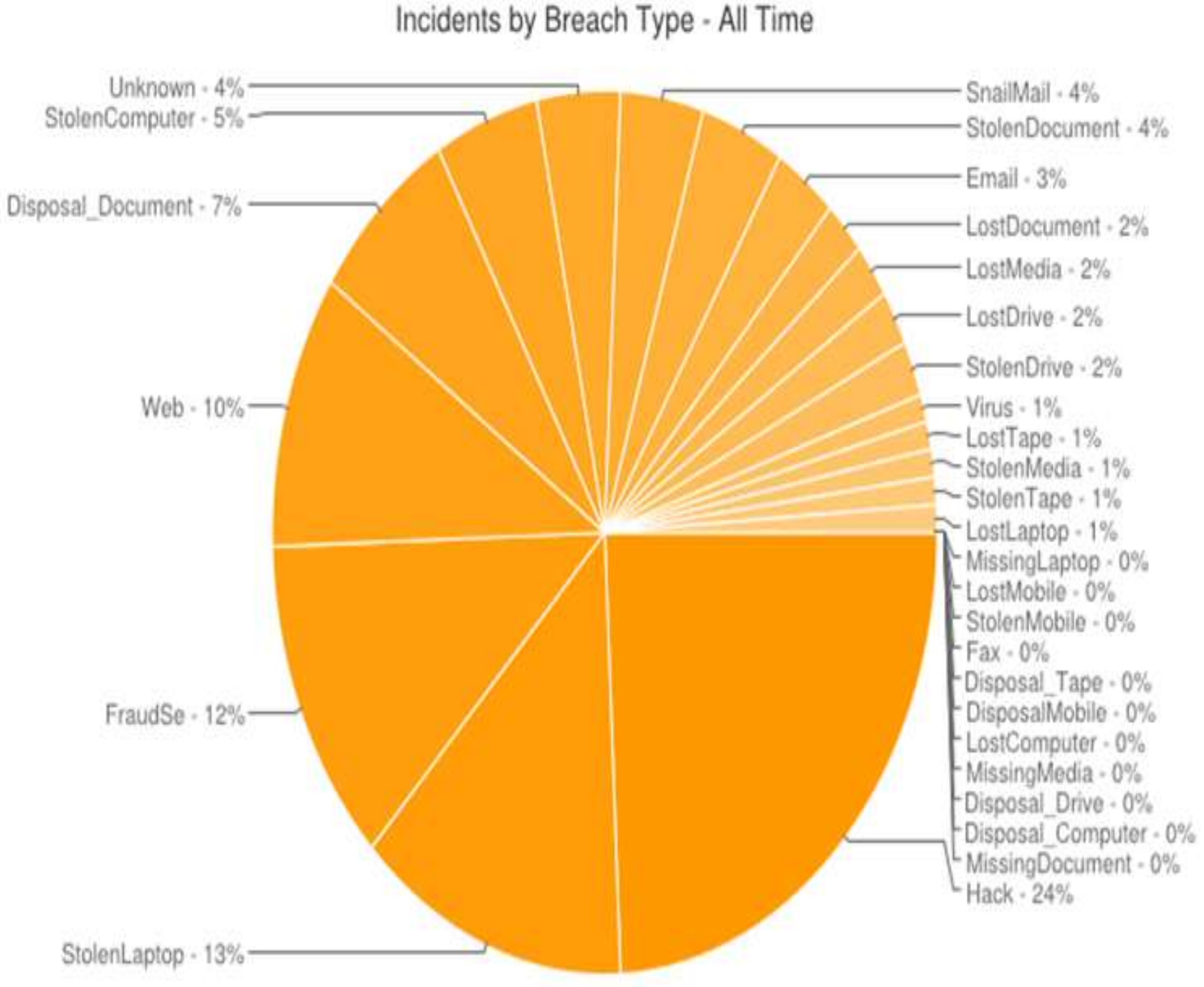
BİLGİSAYAR VE ERİŞİM GÜVENLİĞİ

Güvenliğin sadece küçük bir yüzdesi teknik güvenlik önlemleri ile sağlanıyor. Büyük yüzde ise kullanıcıya bağlı.


Incidents by Breach Type - All Time
Unknown - 4%
StolenComputer - 5%
Disposal_Document - 7%
Web - 10%
FraudSe - 12%
StolenLaptop - 13%
SnailMail - 4%
StolenDocument - 4%
Email - 3%
LostDocument - 2%
LostMedia - 2%
LostDrive - 2%
StolenDrive - 2%
Virus - 1%
LostTape - 1%
StolenMedia - 1%
StolenTape - 1%
LostLaptop - 1%
MissingLaptop - 0%
LostMobile - 0%
StolenMobile - 0%
Fax - 0%
Disposal_Tape - 0%
DisposalMobile - 0%
LostComputer - 0%
MissingMedia - 0%
Disposal_Drive - 0%
Disposal_Computer - 0%
MissingDocument - 0%
Hack - 24%

YOU?

SORUMLU KİM PEKİ ?

- **Sorumlu herkes:**
  - *–Bilginin sahibi*
  - *–Kullanıcılar*
  - *–Bilgi sistemini yönetenler*

- **En zayıf halka bilgi güvenliğinin seviyesini belirlemektedir.**
- **Çoğunlukla en zayıf halka insandır.**

Kötüye Kullanımı Sonucu Oluşan Zararlar

Romeo ve Juliet bir chat odasında buluşmuşlar

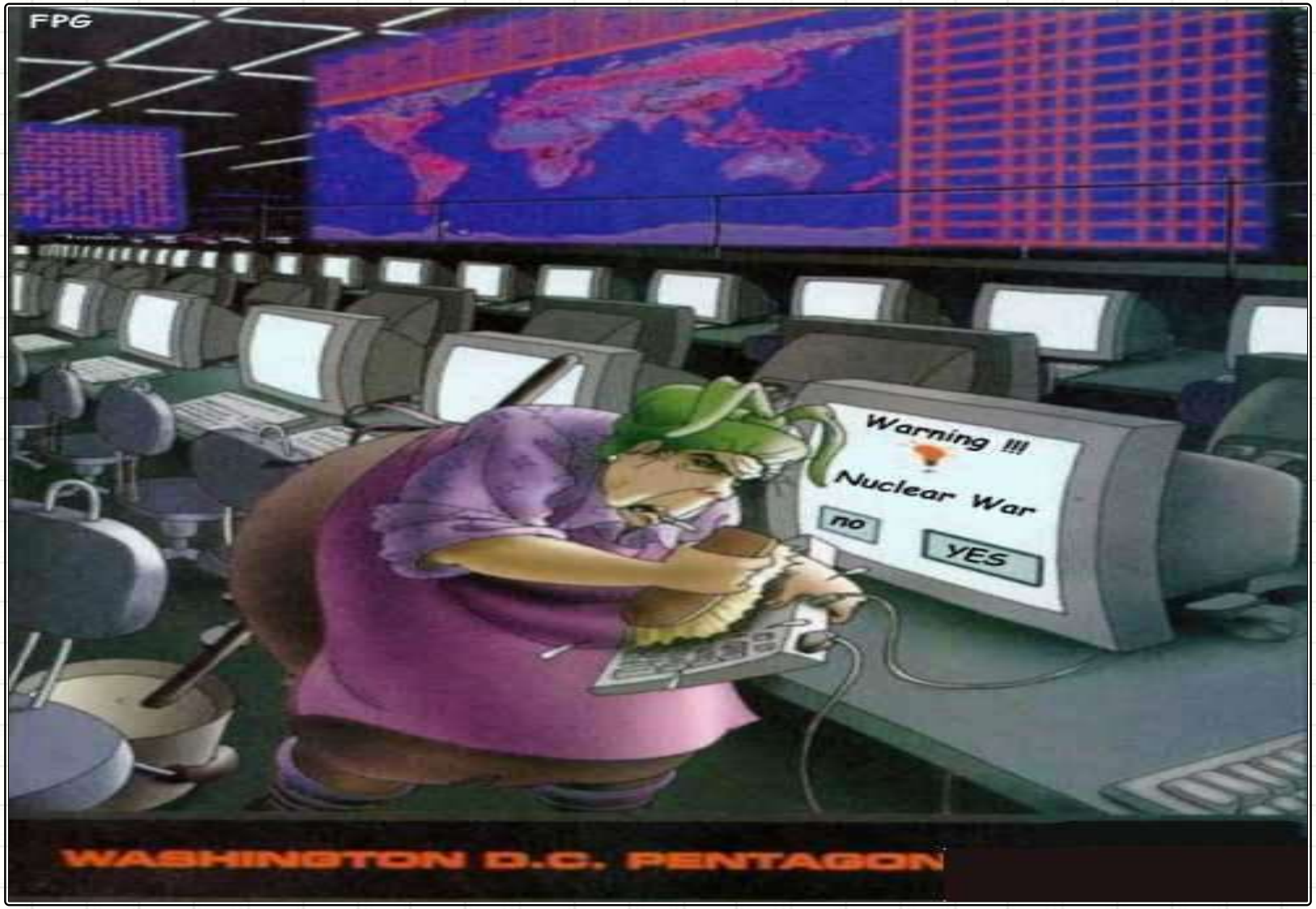
ama beraberlikleri trajik bir sonla noktalanmış.

KULLANICI BİLİNCİ !!!!

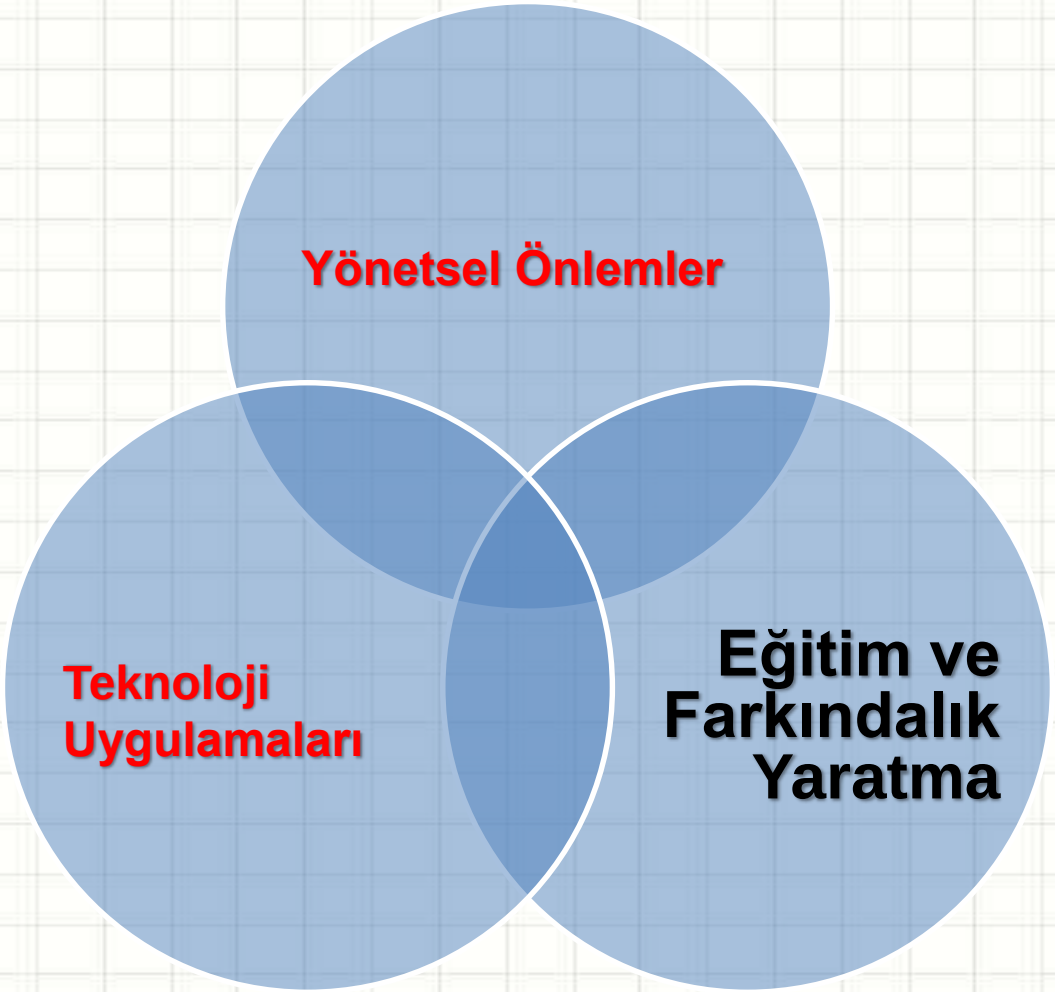
BİTMEDİ!!!!

- Bir kullanıcının güvenlik ihlali tüm sistemi etkileyebilir.
- Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır.
- Kullanıcılar tarafından dikkat edilebilecek bazı kurallar sistemlerin güvenliğinin sağlanmasında kritik bir öneme sahiptir.

YANLIŞLAR, YALNIŞLAR !!!



Bilgi-Bilişim Güvenliği Nasıl Sağlanır?



FİZİKSEL ERİŞİM GÜVENLİĞİ

Bilgisayara giriş güvenliği, bilgisayarın içinde sakladığımız bilgilerin güvenliği anlamına geldiğini biliyoruz.

En Kolay Giriş Prensibi

Herhangi bir saldırgan, bir bilgisayar sistemine girmek için kullanılabilecek en kolay yolu deneyecektir.

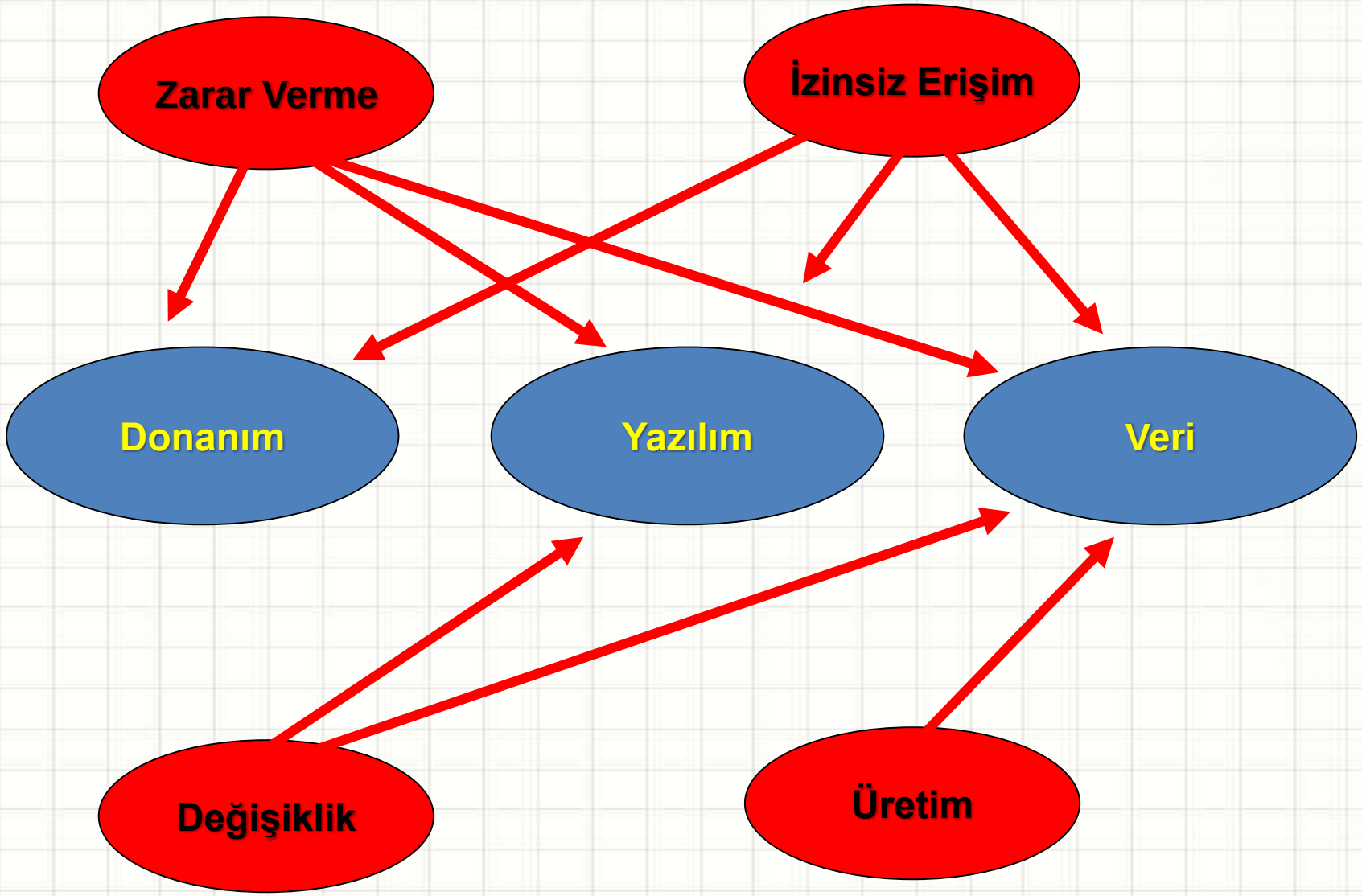
En Kolay Giriş Prensibi

En kolay yol demek, en belirgin, en çok beklenen, veya saldırılara karşı en çok önlemi alınmış olan yol demek değildir.

Sizce Nasıl?

Peki, bilgisayarınıza fiziksel olarak erişebilen bir kişinin bilgisayarınızdaki tüm bilgilere ulaşması normal mi?

Güvenlik Açıkları



Güvenlik Açıkları (Donanım)

- **Kasıtsız Zarar**
  - *Yiyecek-içecek*
  - *Hayvanlar*
  - *Toz*
  - *Yıldırım*
  - *Kaba kullanım*
- **Kasıtlı Zarar**
  - *Hırsızlık*
  - *Fiziksel zararlar (kırma, bozma, parçalama)*

Güvenlik Açıkları (Yazılım)

- **Silinme**
  - *Kasıtsız*
  - *Kasıtlı*
- **Değiştirilme**
  - *Truva Atları*
  - *Virüsler*
  - *Arka kapılar*
  - *Bilgi sızdırma*
- **Hırsızlık**
  - *Lisanssız kullanım*
  - *İzinsiz kopyalama*

Güvenlik Açıkları (Veri)

- **Gizliliğin ihlali**
  - *Dinleme (dinleyiciler, alıcılar, sniffer)*
  - *Bilgi sızdırma (insanlar yoluyla)*
- **Engelleme**
  - *Silme*
  - *Ulaşılamaz, ya da kullanılamaz hale getirme*
- **Bütünlüğün bozulması**
  - *Veri değişikliği*
  - *Sahte veri*

Gerektiği Kadar Koruma Prensibi

Değerli şeyler (yazılım, donanım, veri) sadece **değerleri geçerli olduğu sürece** korunmalı.

Gerektiği Kadar Koruma Prensibi

Korumak için harcanan süre, çaba ve para, korunan şeyin değeriyle orantılı olmalı.

Saldırgan Grupları

- **Amatörler**
  - ***Kişiler:*** Olağan bilgisayar kullanıcıları
  - ***Saldırı şekli:*** Çoğunlukla bir açığı farketme ve yararlanma şeklinde

Saldırgan Grupları

- **Kırıcılar (Crackers)**
  - *Kişiler:* Lise veya üniversite öğrencileri
  - *Saldırı şekli:* Sadece yapmış olmak için, veya yapılabildiğini görme / gösterme için, açık bulmaya çalışma şeklinde

Saldırgan Grupları

- **Profesyonel Suçlular**
  - *Kişiler:* Para karşılığı bilgisayar suçları işleyenler
  - *Saldırı şekli:* Saldırının hedefleri önceden belirli, planlı ve organize şekilde

ilk adım fiziksel güvenliktir

En çok karşılaşılan problemlerden birisinin dizüstü bilgisayarların çalınması olduğunu biliyor musunuz?

Kritik alanlarda bilgisayar sistemlerine ulaşmak için yetkili kişilerin bir çok kimlik doğrulama mekanizmasından geçmesi gerekir.

KULLANICI ……

Neden Giriş Güvenliği?

Fiziksel erişimi kontrol ettikten sonra ***bilgisayara giriş güvenliği***nden bahsetmek de doğru olacaktır.

Neden Giriş Güvenliği?

Bilgisayara giriş aşamasında alınan güvenlik tedbirleri sayesinde yetkisi olmayan kişiler…

Neden Giriş Güvenliği?

Fiziksel olarak bilgisayarınıza erişebilseler de bilgilerinize erişemeyeceklerdir.

Neden Giriş Güvenliği?

Bilgisayarınız bir bilgisayar ağına veya internete bağlı olsa da, ağ üzerinden bilgilerinize erişemeyebilirler.

Yöntem !

*Bilgisayarınız açılırken **kullanıcı adı ve parola sormuyorsa** bilgisayarınızı bilgisayarınıza fiziksel olarak ulaşabilen herkes açabilir ve kişisel bilgilerinize erişebilir.*

Yöntem !

Bu nedenle ilk olarak ***bilgisayarınızın “kullanıcı adı” ve “parola” ile açılmasını sağlayın!***

Temel Hatalar …

Bilgisayarlarında giriş parolası kullanmamayı nasıl açıklıyorlar?

Temel Hatalar ...

"Çevremdekilere, arkadaşlarıma güveniyorum, bilgisayarıma girmezler."

Temel Hatalar …

"Bilgisayarımda ki bilgiler zaten çok kritik değil."

Temel Hatalar ...

"Ekran koruyucu her çalıştığında tekrar şifre girmek çok sıkıcı."

Temel Hatalar …

"İsteyen zaten bilgisayarımdaki bilgilere farklı yerlerden de ulaşabilir, benim bilgisayarımı korumam bir şeyi değiştirmez."

PAROLA GÜVENLİĞİ

Parolalar genel olarak iki şekilde ele geçirilebilir.

PAROLA GÜVENLİĞİ

Tahmin ederek *ya da deneme yanılma yolu ile ele geçirilebilir.*

Örnek ...

123
1234
12345
123456
1234567
12345678
123456789
1234567890
123123
12321
123321
123abc
123qwe
123asd
1234abcd
1234qwer
1q2w3e
a1b2c3
admin
Admin
administrator

qwewq
qweewq
qwerty
qweasd
asdsa
asddsa
asdzxc
asdfgh
qweasdzxc
q1w2e3
qazwsx
qazwsxedc
zxcxz
zxccxz
zxcvb
zxcvbn
passwd
password
Password
login
Login
pass

mypass
mypassword
adminadmin
root
rootroot
test
testtest
12
21
321
4321
54321
654321
7654321
87654321
987654321
0987654321
0
00
000
0000
00000

00000
0000000
00000000

1
11
111
1111
11111
111111
1111111
11111111
2
22
222
2222
22222
222222
2222222
22222222
-

3
33
333
3333
33333
333333
3333333
33333333
4
44
444
4444
44444
444444
4444444

Conficker solucanının yayılırken denediği şifrelerden örnekler

PAROLA GÜVENLİĞİ

Parolanızın çalınması *ile yani hırsızlık yaparak ele geçirilebilir.*

Olası senaryolar …

*Tanıdığın bir kişi **senin hakkında bildikleriyle** parolanı tahmin edebilir.*

Olası senaryolar …

Tanımadığın bir kişi ise ***herkesin sık kullandığı*** *bilinen, basit parolaları deneyerek şifreni bulabilir.*

Çoğu kişinin aynı anahtarı var

300,000 Kişi Bu Şifreyi Kullanıyor

32 milyon şifresini bir hacker saldırısında kaybeden sosyal ağ uygulamaları satan RockYou Inc.sitesinde çalınan şifrelerin büyük bölümünün "123456"dan oluştuğu ortaya çıktı.

Geçtiğimiz haftalarda gerçekleşen hacker saldırısının ardından sosyal ağ uygulamaları satan RockYou Inc., 32 milyon kayıtlı kullanıcının isim ve şifrelerini çaldırdı.

Çalınan şifrelerle ilgili bir araştırma yapan güvenlik yazılımı şirketi Imperva, çalınan şifrelerin bir dökümünü yayınladı. Sitede en çok kullanılan şifreler ise şaşkınlık yarattı; zira neredeyse 300 bin kişinin "123456" şifresini kullandığı ortaya çıktı.

Çokkk basitler…..

celik	Kullanıcının soyismi. 8 karakterden az. Sadece harfler kullanılmış. Özel karakterler, rakamlar kullanılmamış.
alicelik	Kullanıcının adı ve soyadı
Ali_celik1234	İçerisinde kullanıcı ismi ve soyismi geçiyor.
ali123	Kullanıcı isminin türevi de zayıf bir şifredir. 8 karakterden az.
antalya	Özel isim. Kullanıcının doğum yeri ise daha zayıf bir şifredir.
34bg356	Araç plakası.
13nisan1967	Doğum tarihi ya da önemli bir tarih.
Qwerty123	Çok kullanılan karakter sıraları.
Mercedes	Özel isim
Kalem	Sözlüklerde bulunan bir kelime. Bunun yanında 8 karakterden az.
Kalem111	Kelimenin türevi

Güncel örnekler….

No.	Kullanıcı Adı	Şifre	No.	Kullanıcı Adı	Şifre
1	[redacted]	aaaaaa	26	[redacted]	22222
2	[redacted]	12345	27	[redacted]	77777
3	[redacted]	ebru4	28	[redacted]	99999
4	[redacted]	neslihan1	29	[redacted]	102008
5	[redacted]	55555	30	[redacted]	22222
6	[redacted]	12345	31	[redacted]	123456
7	[redacted]	478912	32	[redacted]	beyza
8	[redacted]	qweasd	33	[redacted]	11111
9	[redacted]	99999	34	[redacted]	sinancan1265
10	[redacted]	ihsan	35	[redacted]	tanun
11	[redacted]	44444	36	[redacted]	nihat4
12	[redacted]	aliizci	37	[redacted]	66666
13	[redacted]	atice	38	[redacted]	kartanesi
14	[redacted]	12345	39	[redacted]	asuman
15	[redacted]	sem70	40	[redacted]	ankara
16	[redacted]	ahmet	41	[redacted]	qazqaz
17	[redacted]	yurda	42	[redacted]	ikmal
18	[redacted]	raman	43	[redacted]	ikmal4
19	[redacted]	12345	44	[redacted]	sepya
20	[redacted]	asdfg	45	[redacted]	muafi
21	[redacted]	iha14	46	[redacted]	12345
22	[redacted]	Oca.09	47	[redacted]	19200
23	[redacted]	Nazli	48	[redacted]	12345
24	[redacted]	122008	49	[redacted]	444111
25	[redacted]	fer462	50	[redacted]	12345

Olası senaryolar …

Parolanı bulmak isteyen kişi ***özel programlar*** *kullanarak sık kullanılan yüzlerce parola örneğini ya da sözlüklerdeki binlerce kelimeyi hızlıca deneyerek parolanı belirleyebilir.*

Olası senaryolar …

İyi korunmayan, yazılı ya da sözlü olarak paylaşılan *parolalar, yazılı bulunduğu ortama ulaşılarak ya da kulak misafiri olunarak ele geçirilebilir.*

Adamlar çalışıyor ...

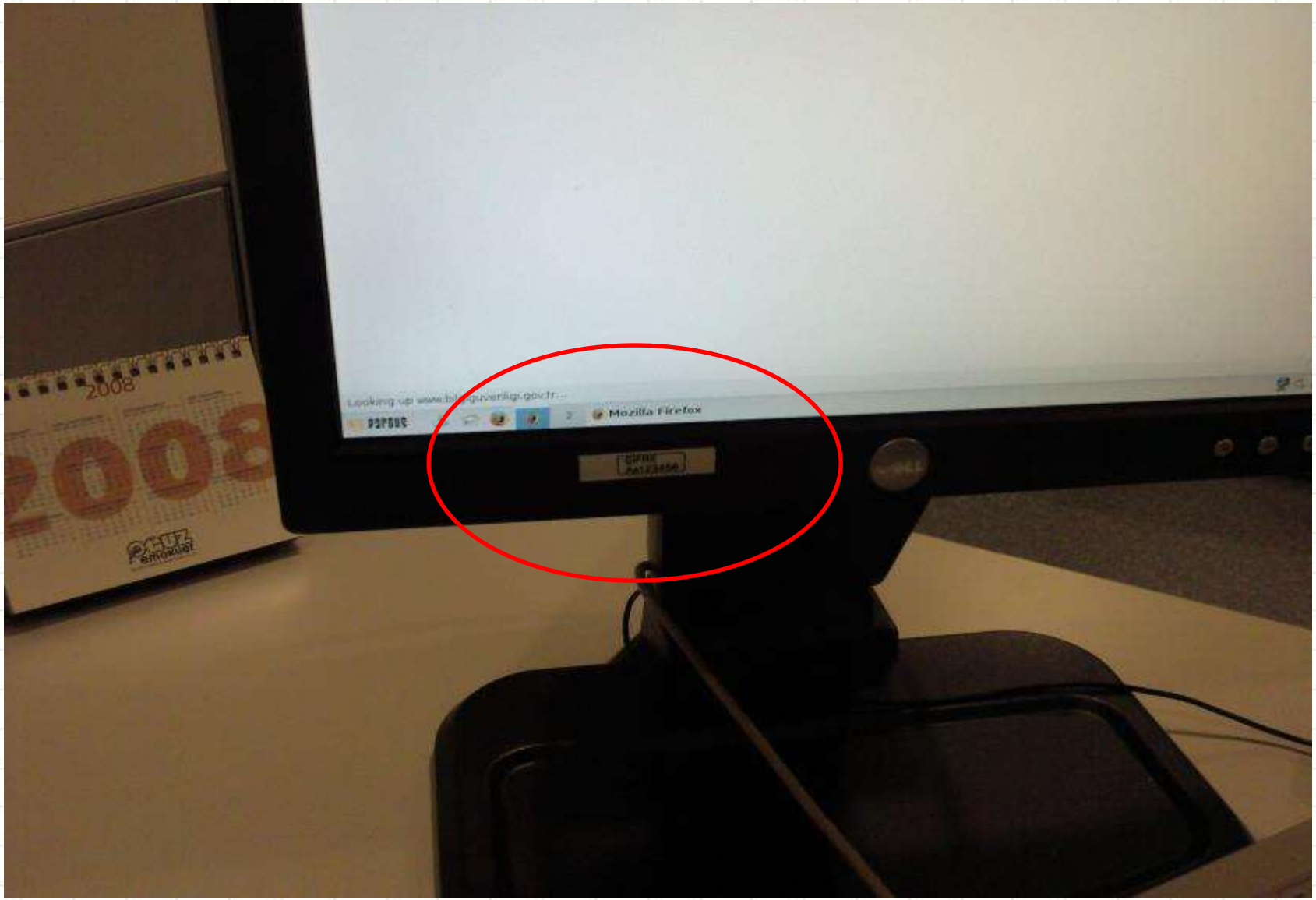
AKŞAM
TÜRKİYE'NİN GAZETESİ
14 ŞUBAT 2007 ÇARŞAMBA
30 YENİ KURUŞ

1 milyon hesap Rus mafyasında

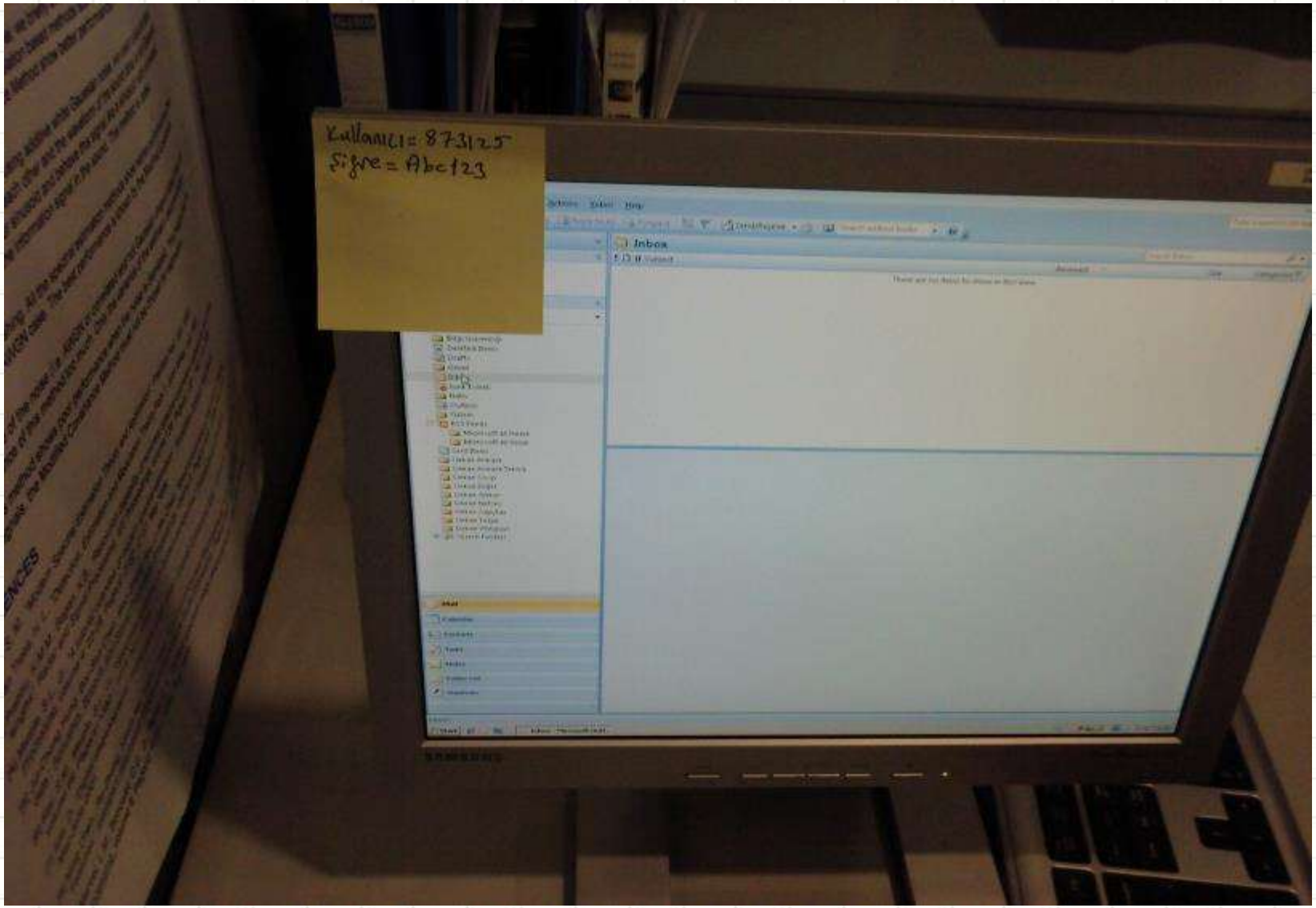
Hollywood filmi gibi siber soygun...Türk ve Rus hackerlar, 1 milyon kişinin banka hesabına ulaştı. Şimdilik 500 bin YTL vurgun ortaya çıkarıldı. Rus bağlantısına Interpol el koydu

EN büyük sanal soygun 3 aylık takiple çözüldü. İzmir merkezli çete, Rusya'dan 3 usta hackerla anlaştı. Bu kişiler, Türkiye'deki banka hesaplarına sızdı. Virüslü maillerle

Bazen ona da ihtiyaç duymaz..



Başka söze gerek …



Bu da var ….

Olası senaryolar …

Bilgisayar virüsleri gibi zararlı programlar *bilgisayardaki işlemlerini izleyerek parolanı ele geçirebilir.*

Parolamızı ele geçirildi ne …

Eğer aynı parolayı ya da çok benzerlerini başka sistemlerde de kullanıyorsak, ***diğer parolaları da*** *değiştirmeyi öneririm.*

Güçlü Parola ?

Tahmin edilmesi kolay olmayan ya da deneme yanılma yolu ile ***ele geçirilmesi oldukça zor olan*** *parolalara* ***güçlü parola*** *denir.*

DEVLETİN favori şifresi 1111-1234-0000

CUMHURBAŞ-
KANI Abdullah

kişinin kimlik ve adres
bilgisinin herhangi

operatörlerinde bulunduğu
anlaşılmaktadır.

En az **8 karakter**den oluşur.

Oluşturulan bir parolanın "*güçlü*" kabul edilebilmesi için aşağıdaki özellikleri göstermelidir.

- ***Harf**lerin yanı sıra, **rakam** ve "?, @, !, #, %, +, -, *, %" gibi **özel karakterler** içerir.*
- ***Büyük** ve **küçük** harfler bir arada kullanılır.*

Kusursuz Parola yoktur

Kurallara uygun parola oluştururken genelde yapılan hatalardan dolayı saldırganların ilk olarak denedikleri parolalar vardır.

- ***Kişisel bilgiler*** *gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin doğum tarihiniz, çocuğunuzun adı, soyadınız, ... gibi)*
- ***Sözlükte bulunabilen kelimeler*** *parola olarak kullanılmamalıdır.*
- *Çoğu kişinin kullanabildiği* ***aynı veya çok benzer yöntem ile geliştirilmiş*** *parolalar kullanılmamalıdır.*

Parola Politikası ?

Kurumlarda *parola güvenliğini sağlamak amacı ile parola oluşturma ve değiştirme politikaları geliştirilir. Bu politikalara uygun hareket etmek tüm kurum çalışanlarının sorumluluğudur.*

Hatırlaması kolay güçlü parola

Hem güçlü parola oluşturmak hem de bunları yazılı ortamda saklamadan hepsini hatırlamak zor olabilir. İşte size bu durumu kolaylaştıracak bir kaç ipucu:

- *1Env,2Esv - Bir elin nesi var, iki elin sesi var.*
- *10Y15mgyhy her yaştan.*
- *B1990y7.amo*
- *Mt98y4.a - Mez*

Dikkat !

Güçlü gibi görünse de çok kullanılan ve çok kolay tahmin edilebilen parolalardan kaçınmak gerekmektedir.

Bu parolalar klavyedeki harf sırası, alfabedeki harf sırası gibi popüler kurallardan oluşturulmaktadır.

Örneğin:

- *"123qwe", "qwe123", "123qweasd", "qwer1234", ...*
- *"qweasd", "123QweAsd", "asd12345", "Asd123", ...*
- *"qwerty", "qwerty123", "qazwsx123", ...*
- *"abc123", "123abc", "1234abcd", ...*
- *"123456", "987654321", "1234qqqQ", ...*

Güçlü parolalar vermek gerekli ama

*Verdiğiniz parolanın **korunması ve paylaşılmaması** da bir o kadar önemlidir.*

Peki, parolalarımızı nasıl koruyabiliriz?

Parolanızı korumak için

- *Kağıt ya da elektronik, herhangi bir ortamda **açıkça yazılmış olarak bulundurulmamalıdır**. Yazılı bulundurulması gerektiğinde saklanan ortamın güvenliği sağlanmalı ve parolalar kilit altında saklanmalıdır.*
- ***Farklı sistemlerde farklı parola** kullanılması olası riskleri azaltacaktır.*
- *Parolalar belirli aralıklarla **değiştirilmelidir**.*
- ***Antivirüs** yazılımları güncel tutulmalıdır.*

Sakızlar ve parolalar birbirine benzer

Yazılı parola bulunur (ve alınır)

- *Ezberlememek için ya da unutma kaygısı ile çoğu kişi parolalarını bir yerlere yazarlar. Peki onları ne kadar koruyabilirler? "**Anahtar paspasın altında**" yazan bir tabelayı kapıya asmak, hırsıza davet çıkarmak demektir. Peki, bilgisayarının üstünde kullanıcı adını ve parolayı yazmak ne kadar anlamlı?*
- *Masa üstünde duran "**parola.txt**" isimli bir dosya ne kadar güvenli olabilir?*

Kapılar farklı. Peki ya anahtarlar?

- *Evinizin anahtarını, arabanızın anahtarını, dükkanınızın anahtarını, hatta varsa kasanızın anahtarını aynı yaptırmak ister misiniz? Böylece tek bir anahtarla istediğiniz kapıyı açabilirsiniz.* ***Peki bu süper anahtar kaybolursa ya da çalınırsa neler olabilir?*** *Farklı sistemlerde farklı parolalar kullanmak güvenlik açısından son derece önemlidir.*
- *Evdeki ve işyerindeki bilgisayarlarımızda, ya da aynı mekanda da olsa farklı amaçlarla kullanılan sistemlerde farklı parolalar kullanmak önemli bir alışkanlıktır.*

SONUÇ

Fatih Sultan Mehmet demiş ki

"Sırrıma sakalımın bir tek telinin vakıf olduğunu bilsem, sakalımı kökünden keserim."

Birazda Sektörden

- *Turistik ürünün yapısı gereği tüketiciler tarafından somut olarak algılanamamasından dolayı tüketiciler turistik ürün ya da destinasyon hakkında önceden ayrıntılı bilgiye gereksinim duymaktadırlar.*
- *Günümüzde tüketiciye bu bilgi, bilgi iletişim teknolojilerinin sağladığı olanaklarla iletilmektedir.*
- *Turistik ürünün soyut yapısı, turizm ve bilgi teknolojileri endüstrilerini bir araya getirerek turistik ürünün daha yaratıcı şekilde pazarlanmasını ve somut hale gelmesini sağlamaktadır.*
- *Bilgi, turistik tüketicilerin soyut bir ürün satın almalarından kaynaklanan riskleri azaltmaktadır.*

Sektörde Bilgi Nerede?

- *Fiziksel ortamlar; kağıt, tahta, pano, faks, çöp/atık kağıt kutuları, dolaplar vb.*
- *Elektronik ortamlar; bilgisayarlar, mobil iletişim cihazları, e-posta, USB, CD, disk, disket vb. manyetik ortamlar.*
- *Sosyal ortamlar; telefon görüşmeleri, muhabbetler, yemek araları, toplu taşıma araçları, sosyal aktiviteler.*
- *Tanıtım platformları; internet siteleri, broşürler, reklamlar, sunular, eğitimler, video ya da görsel ortamlar.*

Bilgi Güvenliği Gerektiren

Donanım, yazılım ve ağ yazılımları
Bilgisayar ve ağ sistemleri
Büro otomasyon, rezervasyon, muhasebe, ücret ve üretim işlevlerine yönelik yönetim uygulamaları
Taşınabilir / kablosuz iletişim aygıtları,
Yönetim destek sistemleri, karar destek sistemleri ve yönetim bilgi sistemleri gibi yönetsel araçlar,
İşletmeye özel yönetim uygulama sistemleri,
Veri tabanları ve bilgi yönetim sistemleri
İnternet, extranet ve intranet,
İşletme çevresi ile yürütülen işlemler için ağ bağlantıları (Elektronik veri aktarımı – EDI ya da extranet)
Ürünlerin internet üzerinden ya da elektronik ortamda dağıtımı,
Bilgisayarlı rezervasyon sistemleri,
Global dağıtım sistemleri (Galileo / Amadeus, SABRE, Worldspan gibi),
Bilgisayarlı rezervasyon sistemleri ile global dağıtım sistemlerindeki aracılar (THISCO ve WIZCOM gibi),
Destinasyon yönetim sistemleri,
İnternet tabanlı seyahat aracıları (Expedia.com, Travelocity.com, Preview Travel, Priceline gibi),
Cep telefonu/WAP üzerinden rezervasyon sistemleri
Gelişmiş teknolojiye dayalı sistemler ile desteklenen geleneksel dağıtım teknolojileri (videotekst gibi),
Çağrı merkezleri,

Kaynak: Buhalis, 2003: 88

Bilgi Kullanıcıları?

- *Kurum çalışanları*
- *Yüklenici firma personeli*
- *Yarı zamanlı personel*
- *Stajyerler*
- *Ziyaretçiler*
- *İş ortaklarının çalışanları*
- *Destek alınan firmaların personeli*
- *Müşteriler*
- *Kurumun bilgi varlıklarına erişim gereksinimi olan / bilgiyi kullanan herkes…*

Ne Sağlayacağız?

Turistik Tüketiciye ait …

Özel hayatın gizliliğini mi?

Kişisel verinin korunması mı?

Yazılım Yükleme ve Güncelleme

Güvenli Olmayan Yazılımlar

Günümüzde bilgisayar sistemleri üzerinde ciddi boyutlarda hasara neden olan zararlı programlar vardır.

Virüs, casus yazılım ve solucan gibi isimler alan bu tip zararlı yazılımlara karşı önlem almak zorunludur.

Nedir bunlar?

Bu yazılımların bilgisayarınıza bulaşma yollarından birisi bilgisayarınıza kurduğunuz güvenli olmayan bir yazılım olabilir. Güvenli olmayan yazılımlar denilince akla gelenler şunlardır;

- *korsan yazılımlar,*
- *korsan müzik ve film dosyaları,*
- *kırılmış (crack) programlar ve yazılımlar ile*
- *kaynağını bilmediğiniz yerden edindiğiniz herhangi bir program.*

Güvenli olmayan (tehlikeli) yazılım kaynakları nelerdir?

Bu yazılımların nereden geldiklerini, kaynaklarını bilmek korunmak açısından kritik olmaktadır. Tehlikeli yazılımları bilgisayarınıza bilerek veya bilmeyerek kendiniz kurmuş olabilirsiniz.

- *e-Posta mesajlarınızda dikkatsiz davranarak;*
  - *e-Posta mesajınızdaki bir dosya ekini kontrol etmeden açtığınızda, ya da*
  - *e-Posta içerisindeki kaynağı şüpheli bir bağlantıyı kontrol etmeden tıkladığınızda,*
- *Güvenli olmayan web sitelerinden yazılım indirdiğinizde,*
- *Yoldan geçerken aldığınız bir CD ile*
- *Farklı bilgisayarlara taktığınız USB belleği, güncel anti-virüs programlar ile kontrol etmeden kullanmaya devam ettiğinizde,*
- *fark etmeden bilgisayarınıza tehlikeli yazılımların yüklenmesine sebep olabilirsiniz.*

korunmak için …

- *Kırılmış (crack) program siteleri, oyun siteleri, sohbet siteleri, porno siteler gibi **riskli web sitelerine** girmekten kaçının*
- *İnternet sayfalarında gezinti yaparken çıkan mesajları **okumadan** "evet" veya "tamam" gibi seçenekleri tıklamayın*
- *E-posta ile gelen bir eklentiyi açmadan önce **kaynağını kontrol edin** ve eklentiyi **virüs taramasından** geçirin.*
- *E-posta içinde gelen **bağlantıları açmadan önce** hedef web sayfasını **kontrol edin**.*
- ***Kaynağından emin olamadığınız** veya korsan yazılım içerebilen **USB bellek veya cd'leri** bilgisayarınızdan uzak tutun.*

Güncelleme ! ?

Saldırılar en çok ne zaman gerçekleşir biliyor musunuz?

- *Bir güvenlik açıklığının yayınlanması ile ilgili güncellemenin yayınlanıp uygulanması arasında geçen kısa sürede*
- *Bu nedenle yazılımlarımızı **düzenli** **ve** **sürekli** olarak güncellemek önemlidir.*

Açıklar ne olur…

Yazılımlarda zaman zaman hatalar veya eksiklikler keşfedilir. Bilgisayar sistemlerini dışarıdan gelecek saldırılara (virüs ya da hacker) açık hale getiren bu zaaflara ***güvenlik açıklığı*** *denir ve ancak yazılımlar* ***güncellenerek*** *kapatılabilir.*

Bilgisayarınıza kurduğunuz ve kullandığınız tüm yazılımlarda bazı hatalar ve güvenlik açıklıkları keşfedilebilir.

Tabii saldırganlar için işletim sistemi ve popüler programlardaki açıklıklar daha cazip olabilmektedir.

Paylaşımlarımı Neden Korumalıyım?

*“Bazı kullanıcılar, **zaten paylaştığım** dosyalarımı neden koruma ihtiyacı duyayım ki” diye düşünebilir. Fakat basit bir dosya erişimi ve paylaşımı nedeni ile çok farklı problemlerle karşılaşmak mümkündür.*

Tehlike nerede ?

*"**Paylaştırılmış klasörler**" başkasının erişimine izin verdiğiniz ve çoğu zaman dosya paylaşmak amacıyla kullandığımız klasörlerdir.*

*Paylaştığınız bir klasöre ya da dosyaya **herkesin, bütün haklarla** ve kullanıcı sınırı olmadan erişmesine izin vermeniz, bu paylaşımdan gelebilecek tüm tehlikelere imkan vermeniz anlamına gelir.*

Paylaştırılmış klasörlerden gelebilecek zararlar

- *Sizin haberiniz olmadan aynı ağdaki bir kişi paylaştığınız dosyalara **erişebilir, değiştirebilir hatta silebilir**. Sizin istemediğiniz ya da bilmediğiniz kimseler tarafından da elde edilerek size ve bilgisayarınıza çeşitli zararlar verilebilir.*
- *Yine bu gibi paylaşımlar çoğu zaman **virüslerin ve zararlı yazılımların** yayılmak için kullandıkları alanlardır. Başka birinin bilgisayarına bulaşmış bir virüs, sizin paylaşım alanınızdan bilgisayarınıza kolaylıkla bulaşabilir.*

Dosya paylaşım yazılımlarıyla gelen tehlikeler

Film, müzik veya yazılımlarınızı paylaşmak amacıyla bilgisayarınıza kurduğunuz "Dosya paylaşım yazılımları" aracılığı ile zararlı yazılımların yayılmasına olanak sağlıyor olabilirsiniz.

Örneğin: *Kaza, eMule, Bittorent, LimeWire gibi yazılımlar kullanıyor iseniz bilgisayarınızı zararlı yazılımlara karşı korunmanız gerekir. Çünkü*

- *Bu yazılımları kullanarak indirmiş olduğunuz bir ofis programı, veya eğlenceli bir uygulama aslında bir truva atı olabilir.*
- *Aynı zamanda bu yazılımlar ile tanımadığınız kötü niyetli kişilerin de bilgisayarınıza erişimini ve hatta kişisel bilgi ve dosyalarınızı görebilmesini sağlıyor olabilirsiniz.*

Telif haklarının ihlali problem olabilir

"Paylaştırılmış klasörler" veya "Dosya paylaşım yazılımları" kullandığınızda karşınıza çıkabilecek bir diğer sorun telif haklarının gözardı edilmesi meselesidir.

- *Paylaşım yazılımıyla elde ettiğiniz veya paylaştığınız bir dosyanın telif haklarını **isteyerek veya istemeyerek** ihlal etmiş olabilir ve yasaları çiğnemiş olabilirsiniz.*
- *Bu durum, sizi yasal açıdan zor durumda bırakabilecek sonuçlar doğurabilir.*

Nasıl Korunulur ?

Dosyalarınızı korumanın en iyi yolu dosya paylaşım yazılımı kullandığınız veya herhangi bir şekilde internet ortamında paylaşıma izin verdiğiniz bir bilgisayarda, kişisel bilgi ve dosyalarınızı bulundurmamaktır.

Dosya ve Veri Kaybı

Farklı nedenlerle farklı zamanlarda veri kaybı yaşayan ne çok kişi var biliyor musunuz?

Kullanıcılar her ne kadar dosyalarını veya verilerini kaybetme olasılıklarının düşük olduğunu düşünse de bilişim dünyasında bu durum "olağan bir şekilde" karşılanacak kadar sık yaşanabiliyor.

En kritik zamanlarda, örneğin;

- *yıllık bir projeyi tamamlayıp teslim edeceğiniz bir günde,*
- *hazırladığınız dokümanı son başvuru zamanı bitmeden yollamaya çalışırken,*
- *teslim zamanı yaklaşan bir ödev ile uğraşırken,*

*kısacası bir dosyaya en ihtiyacınızın olduğu bir zamanda veri ve dosya kaybı yaşamamak için **tedbirli olmak** gerekir.*

Yedekleme

Alınan çeşitli tedbirlere rağmen aksilikler yaşanabilir. Bu gibi durumlarda kaybedilen dosya veya verinin yerine tekrar konulması ile dosya veya veri kayıplarının önüne geçmek mümkün.

*Tabii, öngörülü davranıp dosya ve verilerin **düzenli olarak yedeklenmesi** şartı ile.*

3 önemli husus

- *Yedek dosya isimleri*
- *Yedekleme zamanları*
- *Yedek dosyaların yeri*

Turizm İşletmeleri için…

Turizm işletmeleri gibi kurumsal yapılarda çalışan kişiler için yedekleme işlemi sadece kurum çalışanı için değil tüm kuruluş için önemlidir.

Bu sebeple kurum politikalarına uygun hareket etmek ve kurumun yedekleme politikası hakkında bilgi sahibi olmak önemlidir.

Özel notlar

Bir çok bilgisayarda birden tüm bilgilerin yedeğini almak verimli olmayacağından, genellikle, kurumlarda belirli klasörlerin yedeği otomatik olarak alınır, personelin, kurumsal bilgileri otomatik olarak yedeklenen klasörlere kaydetmesi istenir.

Bir kurum çalışanı nelere dikkat etmeli?

- *Kurumun yedekten geri dönme prosedürlerini öğrenmek.*
- *Kurumun yedekleme dönem ve zamanlarını bilmek.*
- *Kurumsal olarak otomatik yedeklenen klasörleri bilmek.*
- *Kurumsal bilgileri veya yedeklenmesi gereken tüm dokümanları yedeği alınan klasör altına kaydetmek.*

Tehditler ve Korunma

Zararlı Programlar

Sosyal Mühendislik

Zararlı programlar

Zararlı programlar; bilgisayarınıza zarar verebilen, bilgisayarınızı etkili bir şekilde kullanmanızı önleyen yazılımlardır. Bilgisayarınıza büyük zararlar verebilen bu programlardan korunmak için gerekli önlemler alınmaz ise oluşacak sorunların sayısı hızla artacaktır.

Zararlı Program Çeşitleri

Ne yazık ki bilgisayarınıza zarar verebilecek programların sayısı çok fazladır ve dikkat edilmediği takdirde bilgisayarınız kötü amaçlı kişilere karşı savunmasız hale gelir.

*Bu programlar **karakteristik özelliklerine** göre farklı kategorilerde toplanır.*

Zararlılar…

- *Virüs*
- *Solucan (Worm)*
- *Truva atı (Trojan)*
- *Tuş Kaydedici (Keylogger)*
- *Casus yazılım (Spyware)*

Zararlı Programlar Nasıl Bulaşır ve Anlaşılır?

Nasıl bulaşır?

- E-posta ekleri ile
- İnternetten indirilen ya da paylaşılan program ve dosyalar ile
- Usb (taşınabilir) bellekler ile
- Anlık mesajlaşma yolları ile (ICQ gibi).

Nasıl anlaşılır?

- Programların çalışmasında bozukluklar olması
- İsteğimiz dışında dosyaların silinmesi veya eklenmesi
- Bilgisayarda belirli bir yavaşlık olması virüs belirtisi olabilir.

Zararlı Program Bulaştıysa Ne Yapmalı?

Bilgisayarınıza zararlı program bulaştığından şüphelendiğinizde, ***hiç zaman kaybetmeden*** *harekete geçilmelidir.*

İlgili kişilere, bir kurumda iseniz bilgi işlem birimine ***haber vermek*** *çok önemlidir.*

Yardımcı programlarla durumu ***tespit etmek*** *ve zararlı programlardan* ***acilen kurtulmak*** *gerekir.*

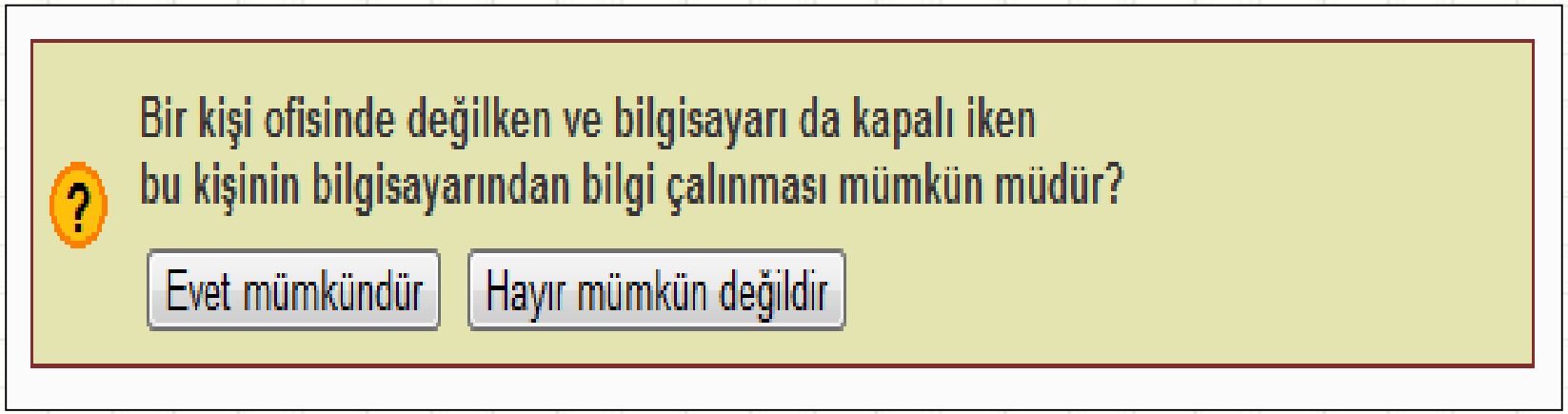
Ayrıntıları ile …

- *Varsa, ilgili kişileri **bilgilendirin**.*
  Bu kişiler, var olan duruma müdahale edebilecek kişiler olduğu gibi bu durumdan etkilenebilecek kişiler de olabilir.
- *Güncel bir **antivirüs programı** ile bilgisayarınızı taratın,*
  - *bulunan virüslerin temizlenmesini,*
  - *temizlenemiyorsa silinmesini,*
  - *silinemiyorsa karantinaya alınmasını sağlayın.*
- ***Güvenlik duvarı** aktif değilse aktif hale getirin, güncel değilse güncelleyin.*
- *İşletim sisteminizin **güncellemeler**ini yapın ve ihtiyaç duyulan işletim sistemi yamalarını uygulayın.*

Sosyal Mühendislik

Tehlike hiç ummadığınız bir anda hiç ummadığınız bir yerden gelebilir.

Olağan dışı durumlarla karşılaştığınız zaman harekete geçmeden önce bir kez daha düşünün. ***Kendinizi büyük bir tuzağın içine düşmek üzere iken bulabilirsiniz.***



Yine insan faktörü

Çoğu kişi, kandırılma olasılığının çok düşük olduğunu düşünür ve genellikle güvenlik gündeme geldiğinde teknik tedbirlerden bahseder. Oysa, bilgi güvenliği sağlanırken ***insan faktörünün*** *payı teknik önlemlerden çok daha büyüktür!*

Bu yanlış inancın farkında olan saldırganlar, isteklerini o kadar akıllıca sunar ki hiç kuşku uyandırmadan, kurbanın güvenini kazanıp, kolaylıkla istedikleri bilgiye ulaşabilirler.

Yöntem & donanım

*Bir sosyal mühendisin temel özelliği, **basit** fakat genelde amacına ulaşan **donanım**lar ve **teknik**ler kullanarak saldırı yapmasıdır.*

İyi & Kötü amaçlılar

*Sosyal mühendislerden sahip oldukları bu yetenekleri ve teknikleri iyi yönde kullananlar **beyaz şapkalılar**; kötü niyetle kullanmak isteyenler ise **siyah şapkalılar** olarak adlandırılır.*

Favori araçlar

Bir sosyal mühendisin favori araçları

- Telefon, e-Posta gibi iletişim araçları
- Google gibi arama motorları
- Facebook gibi sosyal ağlar
- Sosyal mühendislik donanımları

DİKKAT!! Bu yöntemleri kullanan kişiler

- kurum içi terimleri kullanabilir,
- kurum çalışanı gibi davranabilir,
- kendisini ortak iş yürütülen bir şirketin çalışanı gibi tanıtabilir
- yetkili biri gibi davranış gösterebilir,
- yardıma ihtiyacı olan, işe yeni girmiş biri rolüne girebilir,
- bir sistem yaması yükletmek için çalışan bir sistem üreticisi gibi arıyor olabilir,
- önce kendisi sorun yaratmış olup, sonra bu sorunu çözmeye çalışan bir kişi gibi karşınıza çıkabilir,
- masum görünen bir e-posta ekinde zararlı bir yazılım göndermiş olabilir

Daha çok örnek …

Çoğu kişi sosyal mühendislik saldırıları ile karşı karşıya kalıyor. Çevrenizde benzer olaylar gerçekleştiği halde fark etmiyor olabilir misiniz?

Ne yazık ki bilinçsiz bireyler bu saldırılara daha çok maruz kalıyor ve çeşitli zararlar görebiliyor.

E-posta örneği

Tarih: 10 Kasım 2010, Çarşamba, 11:41
Gönderen: ahmetzen@golfgrup.com
Alıcı: sensin@postaci.com
Konu: yakın akraba

Saldırganın kullandığı bazı noktalar

- Kurbanın bir şekilde dahil olmasını sağlayan sahte bir senaryo uydurmak
- Kurbanı para kazanacağına inandırmak
- Kendisi hakkında güven kazanmak amacıyla çeşitli sahte kimlikler hazırlamak
- E-posta, sms ve telefon açma yöntemlerinin üçünü bir arada kullanmak

Saygılarımla,
Ahmet Akın,
mhyakin@safim.com

Banka örneği …

Bir bilgi güvenliği danışmanlık firması, bir bankanın bilgi güvenliğinden sorumlu müdürünü ziyaret eder ve bankaya bilgi güvenliği testi yapmayı teklif eder. Müdür itiraz eder. Güvenlik firması danışmanı ile arasında şöyle bir konuşma geçer;

- Bizim böyle bir teste ihtiyacımız yok. Yeterince güvenliyiz. En iyi yazılım ve donanımları satın aldık ve piyasadaki en iyi personel bizde.

- O zaman biz size bir test yapalım, eğer bir açıklık bulursak ücretimizi alırız, eğer herhangi bir açıklık bulamazsak ücret talep etmeyiz.

Bu arada danışmanlık firmasından bir personel lavaboya gitmek üzere toplantıdan ayrılır ve o sırada sekreterin, bilgisayarında film sitelerini incelediğini görür. Hemen yanına yaklaşır ve filmlerle ilgili konuşmaya başlar:

- Bu aktörün son filmini seyrettiniz mi? Eğer seyretmediyseniz sizin için DVD'ye çekip gönderebilirim.

- Çok memnun olurum. Tabii sizin için zahmet olmayacaksa.

O günkü toplantıdan sonra danışman ofise döner. Zararlı bir yazılım ile birlikte filmi DVD'ye çeker ve kargoyla sekretere gönderir. Zararlı yazılımın sekreterin evdeki değil de ofisteki bilgisayarında çalışmasının garanti etmek için telefon eder.

- Size kargoyla gönderdiğim DVD'yi bir bilgisayarınızda dener misiniz? Bazen kaydederken hata olabiliyor.

Sekreter de denemek amacı ile DVD'yi çalıştırır ve filmin çalıştığını söyler, teşekkür eder ve telefonu kapatır. Zararlı yazılım ofiste etkin hale gelmiştir ve yaptığı iş bilgi güvenliği müdürünün bilgisayarında, masaüstüne **"Sisteminizi ele geçirdik, geçmiş olsun :)"** yazan bir not bırakmaktır.

Sıfırıncı Gün Açıklıkları - Zeroday

Zeroday (Sıfırıncı gün açıklıkları) daha önceden bilinmeyen veya tespit edilmemiş ancak ciddi saldırılara yol açacak zafiyetler barındıran yazılım veya donanım kusurlarıdır. Zeroday açıklıkları çoğunlukla saldırı gerçekleşene kadar tespit edilmesi zor olan zafiyetlerdir.

Zeroday saldırısı ise geliştiricilerin bir yama veya düzeltme yayınlamaya fırsat bulamadan saldırganın zafiyeti istismar etmesi ve zararlı yazılımı yaymasıyla gerçekleşir. Bu nedenle bu zafiyet sıfırıncı gün açıklığı (zeroday) olarak isimlendirilmiştir.

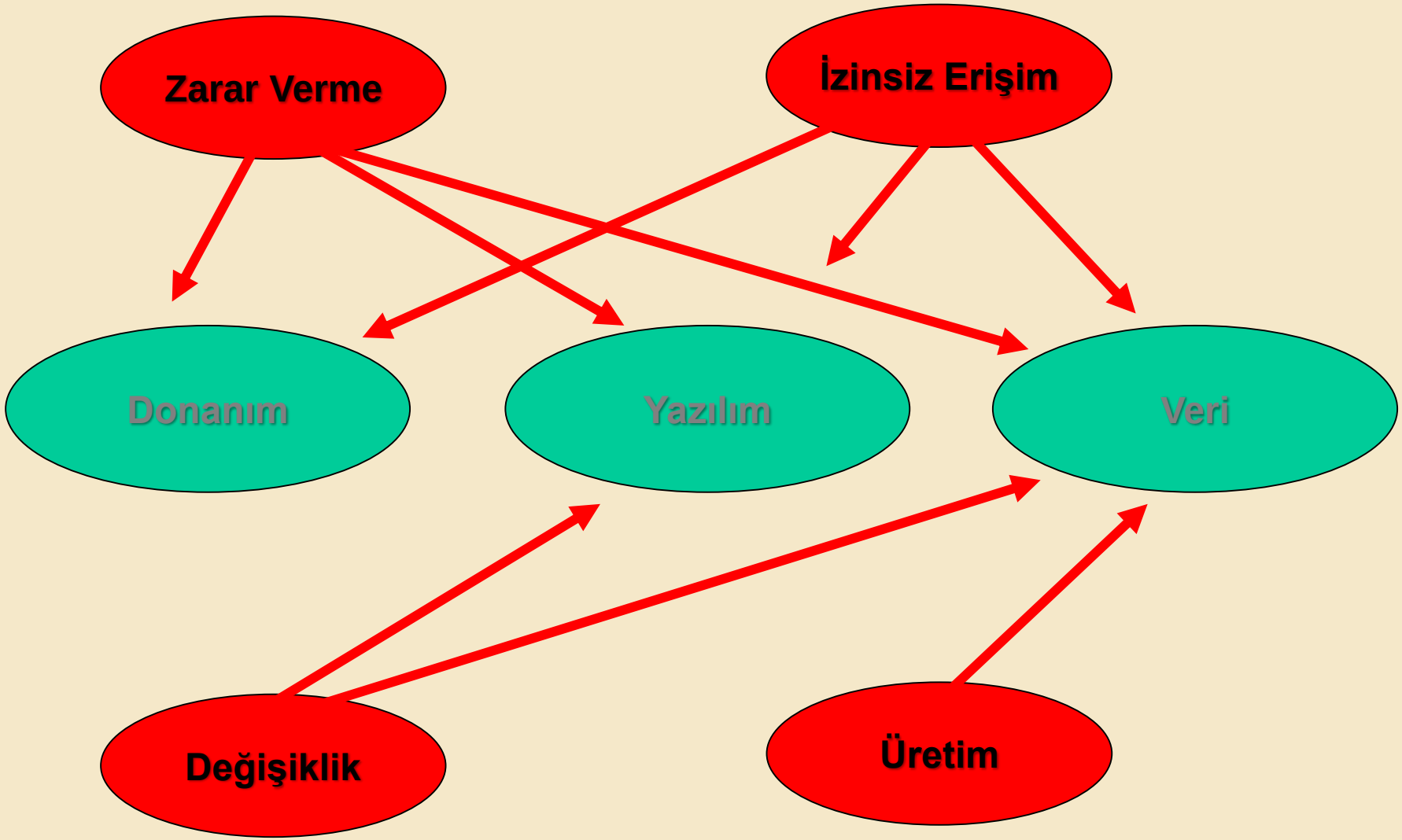
Zeroday saldırısına neden olan etmenler:

- Yazılımcıların geliştirdikleri uygulamanın bir zafiyet barındırdığının farkında olmadan uygulamayı kullanıma geçirmeleri
- Saldırganın zafiyeti geliştiriciden önce saptaması veya geliştiricinin bir düzeltme üretmesine fırsat vermeden istismar etmesi
- Zafiyet hala istismar edilmeye açık ve ulaşılabilir iken saldırganın istismar kodunu yazıp uygulaması

Yama yazılıp kullanıma alındıktan sonra açıklık artık zeroday olarak adlandırılmaktan çıkmaktadır. Zeroday açıklıklarının tespit edilme süreci bazen aylar hatta yıllar almaktadır.

ÖZETLERSEK

Bilgi Güvenliği Açıkları



Bilgi Güvenliği İçin On Altın Kural

- Gizli olduğu düşünülen bilgiler mutlaka güvenli ortamlarda tutulmalıdır.
- Önemli bilgilerin kaybedilme olasılığına karşılık, o bilgilere harcanılan
- zaman ve maliyeti de göz önünde bulundurarak belli aralıklarla bilgiler
- yedeklenmeli
- Şifreler korunmalıdır.
- Bilgisayarda mutlaka antivirüs, antispam, anticasus yazılımları kullanılmalıdır.
- Mutlaka orjinal ekipmanlar kullanmaya özen gösterilmelidir.
- Bilgisayar kullanılmadığı zamanlarda erişimi sınırlandırılmalıdır.
- İnternet ortamından indirilen ve içeriği belli olmayan dosyalar açılmamalıdır.
- Bilgi internet ortamında kolayca takip edilebilir. Bu nedenle yasalarca yasaklanmış sitelerden uzak durulması gerekir.
- Kurumlar bilgi güvenliği konusunda bilgisini artırmalı, güvenlik açıklarını sürekli takip ederek mutlaka gidermeye çalışmalıdır.

Veri/Bilgi hangi nitelikleri korunacaktır?

Bilgi güvenliği, bilgilerin izinsiz erişimlerinden ve kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden korunacaktır.

Sonuç Olarak

Güvenlik, bir varlığı çeşitli zararlı etkenlerden korumaktır.
Söz konusu bilgi güvenliği olunca korunmak istenen varlık, bilginin kendisidir.

Geçmiş Olsun …