BEZMİÂLEM
VAKIF ÜNİVERSİTESİ

Bilgi İşlem Direktörlüğü
Eğitim Birimi

BİLGİ GÜVENLİĞİ

Sunum İçeriği

- **BİLGİ GÜVENLİĞİ NEDİR?**
- Sağlık Bakanlığının Bilgi Güvenliğine Verdiği Önem
- *Hangi Bilgiler Gizlidir?*
- Kişisel Veri – Hasta bilgisi
- **Bilgi güvenliği neden önemli. Başımıza neler gelebilir? Kendinize hiç sordunuz mu?**
- **Bilgi Güvenliğinden Kim Sorumludur?**
- **Sağlık Bakanlığının Bilgi Güvenliğine Verdiği Önem**
- **Bilgi İşlem Direktörlüğü Faaliyetleri**
- Güvenliğin Önemi
- **Herkes sorumlu ise bilgi güvenliğinin seviyesi nasıl belirlenir?**
- **Bilgisayara giriş güvenliği nedir, neden önemlidir?**

Sunum İçeriği

- **Güçlü Parola**
- **Parolaların Korunması**
- En Kötü Şifreler
- Şifre Güvenliği Neden Önemli?
- **Güvenli Olmayan Yazılımlar Nelerdir?**
- **Gazete Manşetleri**
- **Güvenli olmayan (tehlikeli) yazılım kaynakları nelerdir?**
- **Yazılımları Güncellemek Neden Önemli?**
- **Dosya ve Veri Kaybı**
- **Veri Kaybı ve Olası Nedenleri**
- E-Posta Güvenliği
- Cazip bir teklif mi yoksa bir tehdit mi?

BİLGİ GÜVENLİĞİ NEDİR?

- **Bilgi güvenliği,** bilgileri izinsiz erişimlerden ve kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden koruma işlemidir.

- **Bilgi güvenliği;** kendimizi geliştirmekle, öğrendiklerimizi uygulamakla ve öğrendiklerimizi yakınlarımızla paylaşmakla sorumlu olduğumuz bir konu. **Güvenlik tedbirleri almadan bilişim teknolojilerini kullanmak** günümüzde "*inanılmaz bir risk alıyorsunuz*" anlamına geldi. Kısacası bu konudan uzak durmak mümkün değildir.

Kişisel Veri – Hasta bilgisi

- Belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgilerdir.
- Sağlıkla ilgili kişisel veri;
- Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyebileceği için hassas verilerdir.
- Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumu hakkında bilgi edinilmesine neden olur.

Bilgi güvenliği neden önemli. Başımıza neler gelebilir? Kendinize hiç sordunuz mu?

Bilgi Güvenliğinden Kim Sorumludur?

- Herhangi bir bilgi sisteminde aşağıdaki konumlardan **herhangi birisinde iseniz sorumluluğunuz var** demektir.
- Bilginin sahibi
- Bilgiyi kullanan
- Bilgi sistemini yöneten
- Bu durum çok geniş bir kitleyi içerdiğinden *"bilgi güvenliğinin sağlanmasından **herkes sorumludur**"* diye genelleme yapmakta bir sakınca yoktur.

Bilgi Güvenliğinden Kim Sorumludur?

- Bu durumda Bilgi güvenliğinin sağlanmasından **herkes sorumludur**.
- Bu sorumluluklar yasal olarak da ifade edilmiş ve **5651 sayılı kanun** *"İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi"* amacı ile düzenlenmiştir.
- **5651 sayılı kanun** gereği Ortak paylaşım ağlarında internet gezintileriniz yasal zorunluluk olarak kayıt altına alınıyor.

Sağlık Bakanlığının Bilgi Güvenliğine Verdiği Önem

- Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığının 2005/153 sayılı Genelgesinde bahsettiği gibi; **‘Özellikle hasta ve hastalık kayıtlarının gizlilik ve mahremiyeti önem arz etmektedir’** şeklinde belirtmiştir.
- Hasta kaydı bilgisi kapsamına, hasta ile ilgili sözlü bilgi, yazılı bilgi, tıbbı müdahaleler, ön tanı, teşhisler, grafik imajları, fatura gibi konular girmektedir. Aynı genelgede bu bilgilerin öneminden ve ilgisiz kişilerin bilgiye erişiminin yasak olması gerektiğinden bahsedilmiştir.
- Türk Ceza Kanununa Göre;
- Kişilerin özel hayatının gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis cezası ile veya adli para cezası ile cezalandırılır.

Sağlıkta mahremiyet dönemi!

Sağlık Bakanlığı, son günlerde sıkça tartışılan hasta-doktor arasındaki fişleme iddialarını ortadan kaldırmak amacıyla hasta bilgilerinin mahremiyeti için yeni bir yönetmelik hazırladı.

Bu haberin mail olarak size ulaşmasını mı istiyorsunuz? Sağlık Aktüel Mail Grubu'na dahil olmak için tıklayın!..

Sağlık Bakanlığı, hasta bilgilerinin işlenmesi ve mahremiyetinin sağlanması için yeni bir yönetmelik taslağı hazırladı. Taslağa göre, kişi isterse sağlık sisteminde kayıtlı olan bazı sağlık bilgilerini sistemden sildirebilecek. Ancak şahıs, kamunun sağlığını ilgilendiren bir hastalığa sahipse, istese bile bu özel bilgileri sistemden silinmeyecek.

Tüm kişisel sağlık verilerinin kayıt altına alınabilmesi için yapılacak uygulamada, veri mahremiyetinin sağlanması, işlenmesi ve işleyecek gerçek ve tüzel kişilerin uyacakları esas ve usulleri belirlendi. Yönetmelik, tüm kurum, kuruluş ve şahısların görüş ve önerilerine açıldı. Taslağa göre, kişisel sağlık verileri, mevzuatla belirlenen görev alanına ve toplanma amacına uygun olarak işlenecek. Sağlık verilerinin işlenmesinde vatandaşın açık rızası aranacak. İlgili kişinin rıza veremeyecek durumda olması durumunda yasal temsilcisinin, çocuklarda kendi rızasının yanı sıra ana ve babasının veya yasal temsilcisinin rızası alınacak. Kişinin sağlık durumunun

Hastaneler, siber saldırı özel birimi kuracak

Salı, 27 Eylül 2011

Sağlık Bakanlığı, hastanelerdeki kalite standartlarını belirledi. Hastanelerin internet sitelerinde güvenlik en üst seviyeye çıkarılacak. Hastanelerin bilgi sistemlerine dışarıdan gelecek olası siber saldırılar için özel birimler oluşturulacak.

Hizmet Kalite Standartları (HKS) kapsamında hastaneler, son zamanlarda artan hacker saldırılarına karşı internet ve bilgisayar konusunda uzman kişileri bünyesinde istihdam edecek.Sağlık Bakanlığı'nın üzerinde uzun süredir çalıştığı HKS'nin kriterleri belirlendi. HKS devlet, özel ve üniversite hastanelerini yakından ilgilendiriyor. HKS'de hastanelerin güvenliğine geniş yer veriliyor. Buna göre 24 saat güvenlik görevlisinin yanı sıra hastane kullanım alanlarına en az 6 ay kadar kayıt saklama süresi olan kameralar konulacak.

Bilgi İşlem Direktörlüğü Faaliyetleri

- Hasta kaydı bilgisine yetkiniz dahilinde Hastane Otomasyon yazılımı üzerinden rahatlıkla ulaşabilirsiniz.
- Sizin şifrenizin güvenliği, hasta bilgilerinin güvenliğini de kapsar.
- Bu yüzden HBYS şifrenizin güvenliği ve gizliliği önemlidir.
- Bezmialem Vakıf Üniversitesi Bilgi İşlem Direktörlüğü olarak, Bilgi güvenliğinin öneminin farkındayız ve olası risklere karşı sizleri korumak adına gerekli önlemleri alıyoruz.
- Tüm bu önlemlere rağmen, yaşanabilecek olası olaylar karşısında, hukuksal süreçte teknik olarak size yardımcı olabilmek için, sizlerin desteğine ihtiyacımız var.

Bilgi İşlem Direktörlüğü Faaliyetleri

- Peki nelere dikkat etmelisiniz?
- Bizmed HBYS şifrenizi kimseyle paylaşmayın.
- Bilgisayar oturum şifrenizi kimseyle paylaşmayın.
- Kurumsal mail adresinizin şifresini kimseyle paylaşmayın.
- Şifrelerinizi düzenli periyodlarda mutlaka değiştirin.
- Güçlü şifreler edinin.
- Bilgisayarınızla işlem yapmadığınız zamanlarda bilgisayarınızı mutlaka şifre moduna geçirin. (ctrl+alt+delete)

Güvenliğin Önemi

- Bundan 20 yıl kadar önce, bilgi işlem servisleri günümüzdeki kadar yaygın kullanılmadığından, bilişim sistemleri günümüzdeki kadar önemli bir yere sahip değildi.
- Daha iyi açıklamak gerekirse, eskiden hastaya ait bilgilerin hepsi kağıt üzerinde işlenip, saklanırken, günümüzde dijital hastane ortamlarına geçiş hızlanarak devam etmekte ve hemen hemen her bilgi elektronik ortamda saklanmaktadır.
- İşte bu sebeple bilişim sistemlerinin güvenliği iş süreçlerimizin ve faaliyetlerimizin yürütülebilirliği açısından çok önemlidir.

Güvenlik Bir Bütündür

Ayaklardan birisi olmasa ne olur?
Ayaklardan birisi kırık olsa ne olur?

Bilgi Güvenliğinin Seviyesi

- Bilgi sistemlerini bir zincir gibi düşündüğümüzde bu zincirin en zayıf halkası çoğunlukla sistemin kullanıcılarıdır. Unutulmamalıdır ki ***bir zincir en zayıf halkası kadar sağlamdır.***

- Bilgi güvenliğinin seviyesi de bu durumda kullanıcılara bağlı olduğundan, **kullanıcı bilinci** bilgi güvenliğinin sağlanması için son derece hayati bir öneme sahiptir ve bilgi güvenliği seviyesini belirler.

En zayıf halka = Bilgi güvenliğinin seviyesi

Çoğunlukla en zayıf halka insandır.

Güvenlik Bilincinin Önemi

- Bilgi güvenliğinin en önemli parçası **kullanıcı güvenlik bilincidir.**
- Oluşan güvenlik açıklıklarının önemli bir kısmı **kullanıcı hatasından** kaynaklanmaktadır.
- Saldırganlar (Hacker) çoğunlukla kullanıcı hatalarını kullanmaktadır.
- Bilgi güvenliğinin en zayıf halkası kullanıcılardır.
- 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.

Bilgisayara giriş güvenliği nedir?

- Bilgisayara giriş güvenliği, bilgisayarın içinde sakladığınız bilgilerin de güvenliği anlamına gelmektedir. Bu nedenle son derece önemlidir.
- **Bilgisayarınıza fiziksel olarak erişebilen bir kişinin bilgisayarınızdaki tüm bilgilere ulaşması normal mi?**

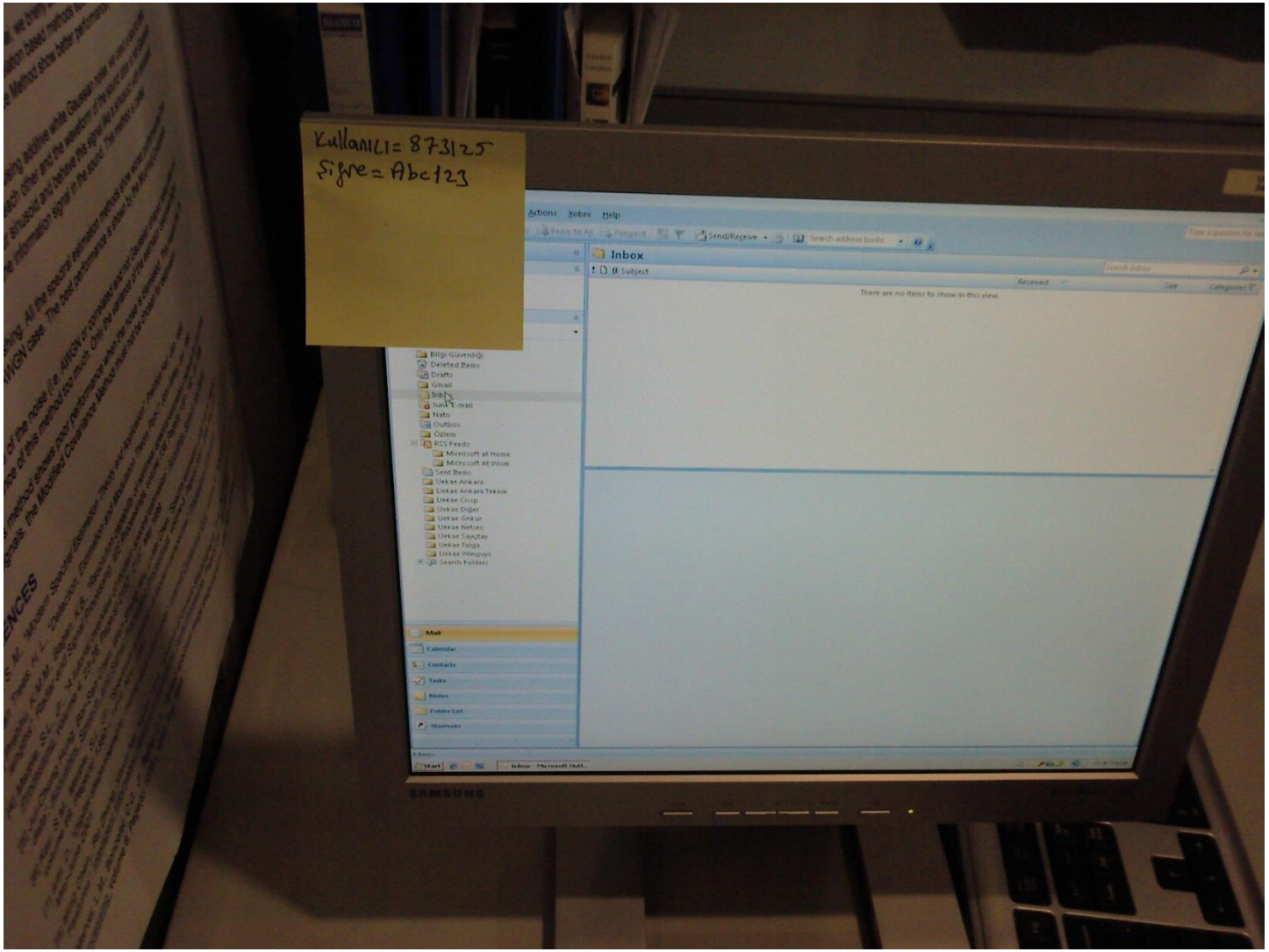
Güçlü Parola

- Bilgisayarımıza fiziksel olarak erişilse bile, bilgi güvenliğimiz için ve bilgilerimize kolaylıkla erişilememesi için güçlü ve erişilemeyen parolalar kullanmamız gerekmektedir.
- Tahmin edilmesi kolay olmayan ya da deneme yanılma yolu ile **ele geçirilmesi oldukça zor olan** parolalara **güçlü parola** denir.
- Oluşturulan bir parolanın "güçlü" kabul edilebilmesi için aşağıdaki özellikleri göstermelidir. En az **6 karakter**den oluşur.
- **Harf**lerin yanı sıra, **rakam** ve "?, @, !, #, %, +, -, *, %" gibi **özel karakterler** içerir.
- **Büyük** ve **küçük** harfler bir arada kullanılır.

Parolaların Korunması

- Güçlü parolalar vermek gerekli ama yeterli değildir. Verdiğiniz parolanın **korunması ve paylaşılmaması** da bir o kadar önemlidir.
- Peki, parolalarımızı nasıl koruyabiliriz?
- 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.

Şifrelerinizi İyi Muhafaza Edin



Sakızlar ve parolalar birbirine benzer. *Nasıl mı?*

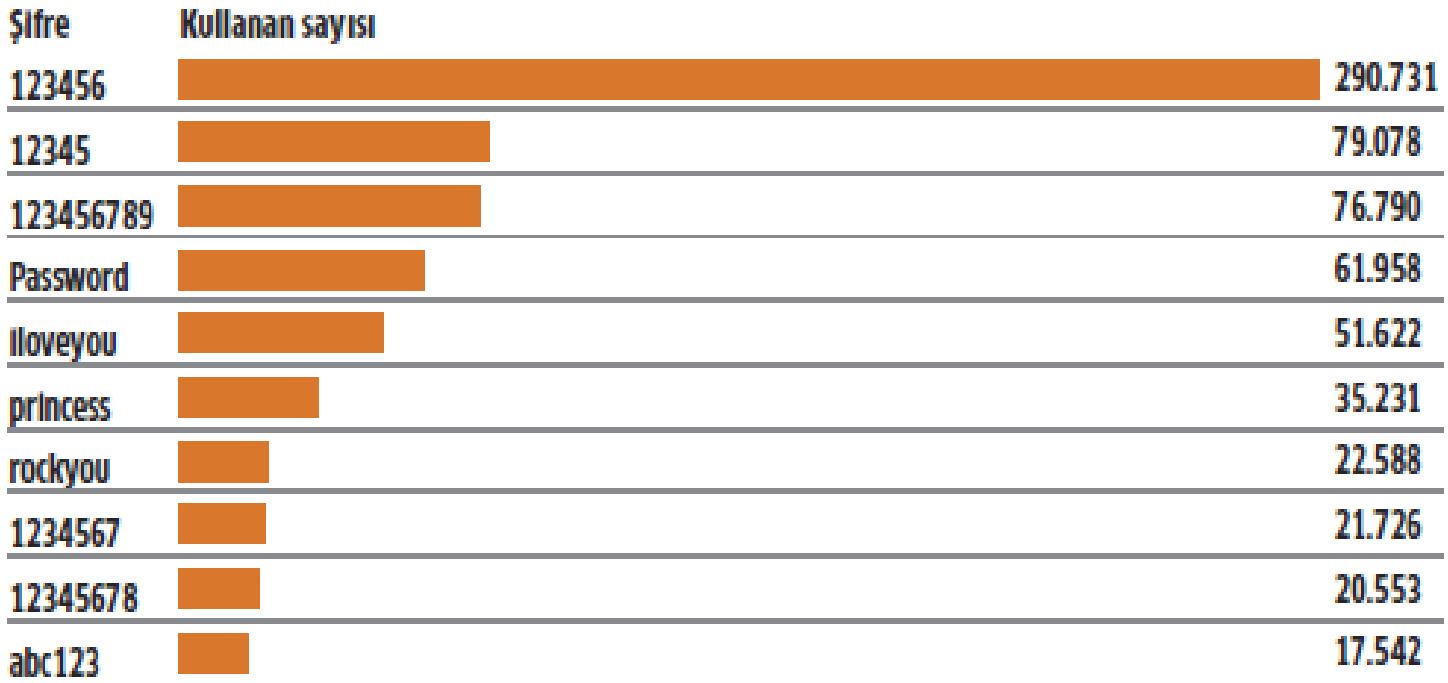
- Parolalar kişiye özeldir, herkesin farklı bir sakız çiğnemesi gibi.
- başkalarıyla **paylaşılmaz**, herkesin sakızı/parolası farklıdır.
- ara sıra **yenilemek** gerekir, bayat bir sakız güzel değildir ve zor çiğnenir
- **ortalıkta bırakılmaz**, yoksa ciddi sorunlar yaratır çiğnenmiş bir sakız sokağa atıldığında olduğu gibi



En Kötü Şifreler

EN KÖTÜ ŞİFRELER

Çevrimiçi oyun sitelerinden Rockyou'daki hacker'lar internette kullanılan 32 milyon anahtarı yayınladı. Çoğu kullanıcının ne kadar basit şifreler kullandığı ortaya çıktı.



KAYNAK: IMPERVA

Hacklendi; şifresi: 12345

Batı dünyasının görevini terk etmesi için ağır baskı uyguladığı Suriye Devlet Başkanı Beşar Esad, küresel hacker grubu Anonymous'un da hedefi oldu.

Güncelleme:09 Şubat 2012 12:35

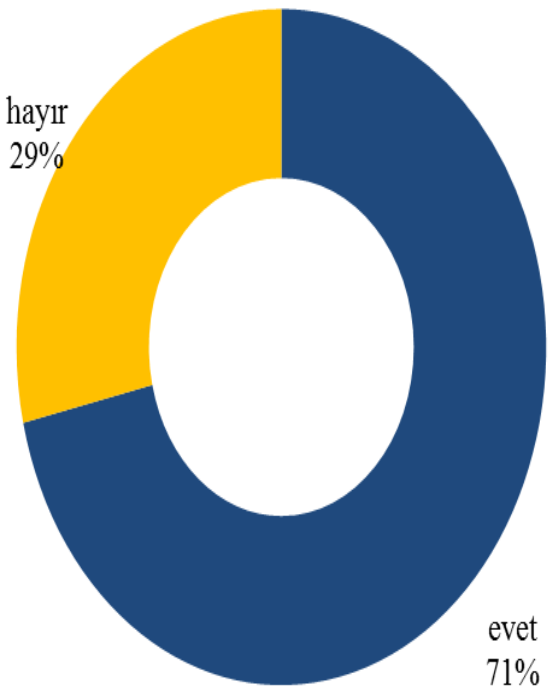
Anonymous, Başbakanlık bürosunun e-**mail** hesabına girerek yüzlerce yazışmayı internete sızdırdı.

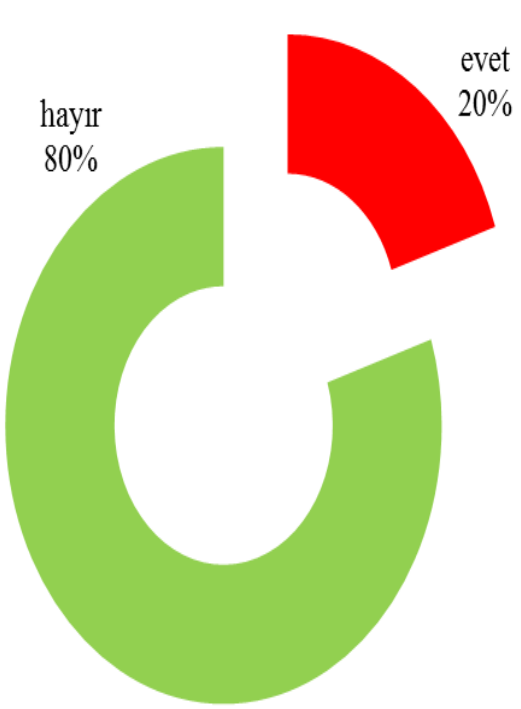
Haaretz gazetesinin haberine göre, Anonymous, Başbakanlık bürosunun 78 çalışanının e-mail hesaplarına girdi. **Hacker**ların kolaylıkla erişim sağladığı hesapların çoğu için kullanılan **şifre**nin "12345" olduğu ortaya çıktı. Bu şifre, 2011'de internetin en kolay kırılan 25 şifresi sıralamasında ikinci sırada yer almıştı.

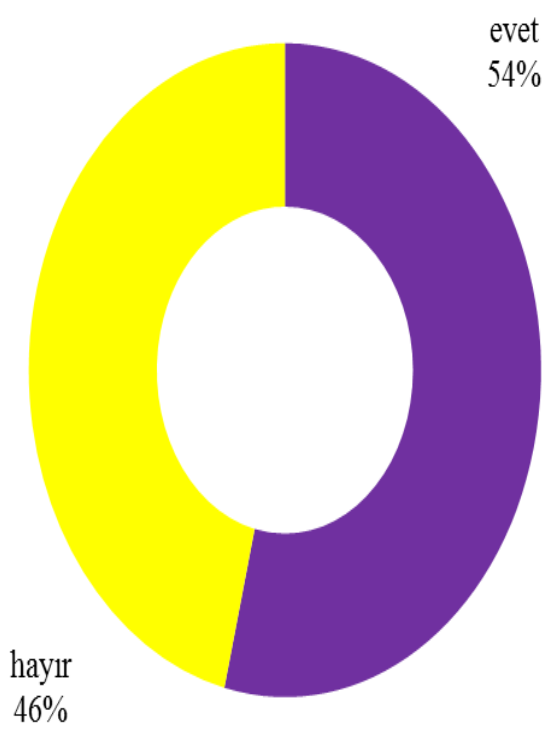
E-mail hesabına girilen isimler arasında devlet bakanı Mansur Fadlallah Azzam ve Esad'ın basın danışmanı Bouthina Şaban'da bulunuyor. İnternete sızdırılan e-maillerden birinde, Esad'ın Aralık 2011'de ABD'li gazeteci Barbara Walters'a verdiği röportaj için hazırlanan belgeler de yer alıyor.

ABD'Lİ YÖNLENDİRMEK İÇİN YAPILMASI GEREKENLER

- Sağlık Bakanlığının yaptığı anket sonuçları;







Olası Örnekler

- Hasta dosyasına her türlü müdahale sizin bilginiz dışında, sizin şifrenizle yapılabilir. En basit düzeydeki örnek;
- **E-reçete** yazılabilir,
- **İlaç raporu** yazılabilir,

- Hastaya yıllık maliyeti çok yüksek olan ilaç raporu sizin şifrenizle yazılıyor. Ancak bu durumdan sizin haberiniz yok. Herhangi bir hukuki süreçte işlem sizin şifrenizle yapıldığı için tek sorumlu sizsinizdir.

Yaşanmış Olay

- Hastaya yazılan yanlış epikriz de veya yapılan yanlış işlemde hukuki sonuçlar yine size yansıyacaktır. Örneğin;
- Uzman Doktor Ali Veli'nin sekreteri deneme amaçlı, Ali Veli'nin kimlik bilgilerini kullanarak, Ali Veli adına ameliyat işlemi girişi yapmış ve ameliyat rapor kartını oluşturmuş.
- Sekreter deneme amaçlı yaptığı işlemi sistemden silmeyi unutuyor.
- Böyle bir deneme yapıldığından doktorun haberi bile yok ancak, bu deneme kendi kullanıcı adıyla yapılıyor.
- Faturalama döneminde bilgileri SGK'ya ulaşıyor. Kendi kendini ameliyat etmiş gibi görünen doktorun davası hala sonuçlanmadı.

Güvenli Olmayan Yazılımlar Nelerdir?

- 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.
- 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.

Gazete Manşetleri

BEZMİÂLEM VAKIF ÜNİVERSİTESİ

Türk'ün Facebook cinayeti ABD'de yasa çıkarttırdı

ABD'de, geçen ocak ayında Facebook'ta "İlişkim yok" yazdığı için Şengül Vatansever'i iki çocuklarının gözü önünde öldürüp intihar eden Selami Özdemir olayı, ABD'de yeni yasa çıkarılmasını sağladı. Dehşet gecesinin ses kayıtları medyada yayınlanırken, yeni yasa ile aile içi şiddet uygulayanlar GPS ile takip edilecek.

■ Razi CANİKLİGİL / NEW YORK

- "YARDIM edin, babam anneme vurdu".
- "Üzgünüm, İngilizcem çok iyi değil. Eşim 'bom bom' diye kapıyı vuruyor. Anlıyorsunuz değil mi".
- "Yardım edin, kocam çok öfkeli. Kapıda".

Silah sesleri, çığlıklar ve ağlayan bebek sesleri.

İşte bunlar, 19 Ocak Cumartesi günü ABD'nin Connecticut eyaletinin West Haven kentinde, kıskançlık krizine giren Selami Özdemir'in iki çocuğuyla birlikte Şengül Vatansever'e yaşattığı dehşet gecesinden '911 acil servisi'nin kayıtlarına düşen sesler. Amerikan kamuoyunun "Facebook cinayeti" olarak bildiği olayın yaşandığı gecenin 6 dakikalık "911 polis acil yardım" ses kayıtları, savcılık kararıyla medyada yayınlandı.

Şengül Vatansever ve çocuklarının bozuk İngilizcesi ile polisten çaresizce yardım isteyişi, silah ve çığlık sesleri dinleyenlerin kanını dondururken, şikayet edildiği halde Özdemir'in serbestçe dolaşmasına izin veren Amerikan polisinin ihmalini de gözler önüne serdi.

24 saat aktif sığınak

Olayı soruşturan eyalet savcısı raporunda polisin ihmalleri ve alınacak önlemler sıralanınca, Connecticut valisi M. Jodi Rell, bu konuda yeni bir yasa imzaladı. Yasa, bundan böyle aile içi şiddet uygulayanların polis tarafından GPS (Küresel Yer Belirleme Sistemi) ile takip edilmelerini öngörüyor. Yeni yasa ile ayrıca aile içi şiddet ile mücadele için yeni bir fon oluşturuldu. Böylece şiddet mağdurları ile ilgilenmek için daha fazla kişi işe alınacak ve 24 saat aktif sığınaklar oluşturulacak.

Göz göre göre cinayet

ŞENGÜL Vatansever, geçen 19 Ocak'ta Selami Özdemir tarafından öldürülmeden önce polisi arayıp yardım istemiş, ancak önce gözaltına alınan Selami Özdemir daha sonra arkadaşlarının ödediği 25 bin dolar kefaletle kurtulmuştu.

Mahkemenin Vatansever'den uzak durması ve eve yaklaşmaması konusunda karar vermesine rağmen Özdemir yine eve gelmiş, polisin uzaklaşınca biri 7 aylık, diğeri 6 yaşında iki çocuğunun gözleri önünde Şengül Vatansever'i tabancayla öldürüp intihar etmişti.

Olayın ardından koruma altına alınan iki çocuk ise, henüz Türk vatandaşlığına sahip olmadıkları için, çiftin Türkiye'deki akrabalarına teslim edilmedi. Şengül Vatansever ve Selami Özdemir'in cenazeleri, Giresun'da birlikte kılınan cenaze namazından sonra aynı mezarlıkta yan yana defnedilmişti.

Sahte kredi kartlarıyla alışveriş

Muğla'da vatandaşların ve turistlerin kredi kartı bilgilerini kopyaladıkları ve hazırladıkları "sahte kredi" kartları ile alışveriş yaptıkları iddia edilen 3 kişi gözaltına alındı. Edinilen bilgiye göre, Muğla Emniyet Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Şube Müdürlüğü ekipleri, vatandaşların ve turistlerin kredikartı bilgilerini kopyaladıkları ve hazırladıkları "sahte kredi" kartları ile alışveriş yaptıkları belirlenen kişilerin yakalanması için çalışma başlattı.

122 BOŞ KART ELE GEÇİRİLDİ

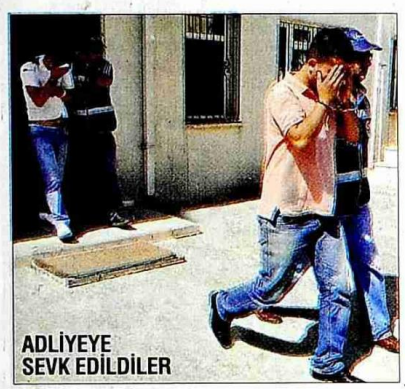
Çalışma kapsamında, Fethiye ve Köyceğiz ilçelerinde eş zamanlı operasyonlar düzenlendi. Düzenlenen operasyonlarda şüpheliler S.K, S.Z. ve H.G.gözaltına alındı.Gözaltına alınan zanlılarla birlikte, "kredi kartı kopyalama cihazı, 122 boş kredi kartı, 18 kopyalanmış kredi kartı, 3 dizüstü bilgisayar, bir banka şubesine ait 200 TL'lik nakit çekim fişi" ele geçirildi. Zanlıların, ifade işlemlerinin tamamlanmasının ardından adliyeye sevkedileceği öğrenildi.

---

2 MİLYON TL HAKSIZ KAZANÇ SAĞLADIKLARI İLERİ SÜRÜLEN 3 KİŞİ ELE GEÇTİ

KREDİ KARTI VURGUNU

Çok sayıda kişiye ait kredi kartı bilgilerini ele geçirerek vurgun yapan zanlılar, teknik takibe takıldı



Gözaltına alınan zanlılar, sorgulanmak üzere adliyeye sevk edildi (solda). Zanlılarla birlikte kredi kartı kopyalama cihazı, 122 boş kredi kartı, 3 dizüstü bilgisayar ve banka nakit fişleri ele geçirildi.

Muğla Fethiye'de, çok sayıda kişiye ait kredi kartı bilgilerini ele geçirerek yaklaşık 2 milyon TL vurgun yaptığı ileri sürülen üç kişi Muğla'da yakalandı. Polise başvuran 50 mağdur vatandaş, kendilerinden izinsiz başkaları tarafından adlarına kredi kartı çıkarıldığını bildirdi. Kaçakçılık Şube Müdürlüğü ekipleri, yaptıkları tahkikat sonrası Fethiye'de ikamet eden S.K. (30) isimli zanlı tarafından mağdur vatandaşlara ait kredi kartı bilgilerinin alınarak boş kredi kartına, kredi kartı kopyalama cihazı ile sahte kredi kartı çıkarıldığı bilgisine ulaştı. S.K. isimli zanlı gözaltına alındı.

Köyceğiz ilçesinde de sahte kredi kartını kullandığı ileri sürülen S.Z. (24) ve H.G. (26) isimli zanlılar yakalandı. Zanlıların gösterdikleri yerlerde yapılan aramada, bir kredi kartı kopyalama cihazı, 3 adet kart yazıcı, bir kart okuyucu cihaz, 64 adet manyetik şeritli, 58 adet şeritsiz boş kredi kartı, 18 adet kopyalanmış kredi kartı, 16 adet PVC tanıtma kartı, 3 dizüstü bilgisayar, 2 hafıza kartı, 4 adet CD ele geçirildi. Kredi kartlarının ait olduğu bankaların çoğunun Türkiye'de şubesi bulunmayan yabancı banka olduğu açıklandı.

KARTLARLA ALTIN SATIN ALDILAR

Zanlıların başkaları adına düzenledikleri sahte kredi kartları ile daha çok elden çıkarılabilecek altın, bilgisayar ve cep telefonu gibi eşyalar aldıkları ve satışta zorlanmadıkları ileri sürüldü. Piyasayı 2 milyon TL dolandırdıkları ileri sürülen 3 zanlı adliyeye sevk edildi. Zanlıların dolandırıcılık, emniyeti suistimal ve sahtecilik suçlamasıyla yargılanacakları öğrenildi. İHA

Doktor önlüklü, teğmen kimlikli hacker yakalandı

Salı, 26 Nisan 2011

'Sosyal mühendislik' yöntemiyle dolandırıcılık yapan 10 kişilik dolandırıcılık çetesi çökertildi. Nüfus müdürlüklerini arayan ve çete üyelerinin "Doktoruz. Bu kişi hastanemizde ameliyat edildi. Üzerinden kimlik çıkmadı. Kayıt yapmamız lazım" veya "Polisiz. Gözaltına aldığımız kişinin kimlik bilgileri lazım" diyerek çok sayıda kişinin kimlik bilgisine ulaştığı, bu kişiler adına yüksek limitli kredi kartları çıkartarak 500 bin liralık vurgun yaptığı tespit edildi.

Liderliğini sahte üsteğmen kimliği ile dolaşan 'Komutan' lakaplı Cemalettin Y.'nin yaptığı belirlenen çete, özellikle doktorlardan gelen şikayetler üzerine ortaya çıkarıldı.

Kurbanlarını internetten tespit ediyorlardı

Şikayetler üzerine harekete geçen İstanbul Emniyet Müdürlüğü Bilişim Suçları ve Sistemleri Şube Müdürlüğü ekipleri, 10 kişiden oluşan kredi kartı çetesini tespit etti. Teknik ve fiziki takipte, çetenin internetteki çeşitli sitelerden maddi durumu iyi olan kişileri tespit ettikleri anlaşıldı.

İnternet korsanları ele geçirdikleri bilgileri, kişi ve kurumlara, hatta devletlere karşı şantaj amacıyla kullanıyor.

E-posta adresine yeni bir haber geliyor. Uluslararası adresli gönderici de konu da tanıdık. Alıcıya, ertelenen bir konferansla ilgili haber gönderiliyor. E-posta tabii merak içinde açılıyor ve metinde, ekte gönderilen belgede konferansa ilişkin yeni tarih ve planın yer aldığı belirtiliyor. E-postayı alan kamu görevlisi de hiç tereddüt etmeden ekteki dosyayı açıyor.

İşte internet korsanları, bu yöntemle Alman hükümet kaynaklarından hassas verilere ulaşabiliyor. İlk başta zararsız gibi görünen e-posta, aslında bilgisayardaki verileri tarayan "truva atı" ya da kısaca "truva" denilen virüsü içeriyor.

Federal Enformasyon Teknolojileri Güvenliği Dairesi ise bu saldırılara engel olmaya çalışıyor. Kurumun verilerine göre 2012 yılında hükümet organlarına yaklaşık bin yüz hacker saldırısı düzenlendi, ancak bunlardan hiçbirinde büyük bir veri hırsızlığı yapılamadı. Sadece bir saldırıda kopyalanmak istenen dosyanın yüzde 15'i indirilebildi.

Kızıl Hackerlar polis sistemini hackledi

Ankara Emniyet Müdürlüğü'nün sistemine giren internet korsanları polise gönderilen ihbarları ele geçirdi.

Güncelleme:27 Şubat 2012 20:52

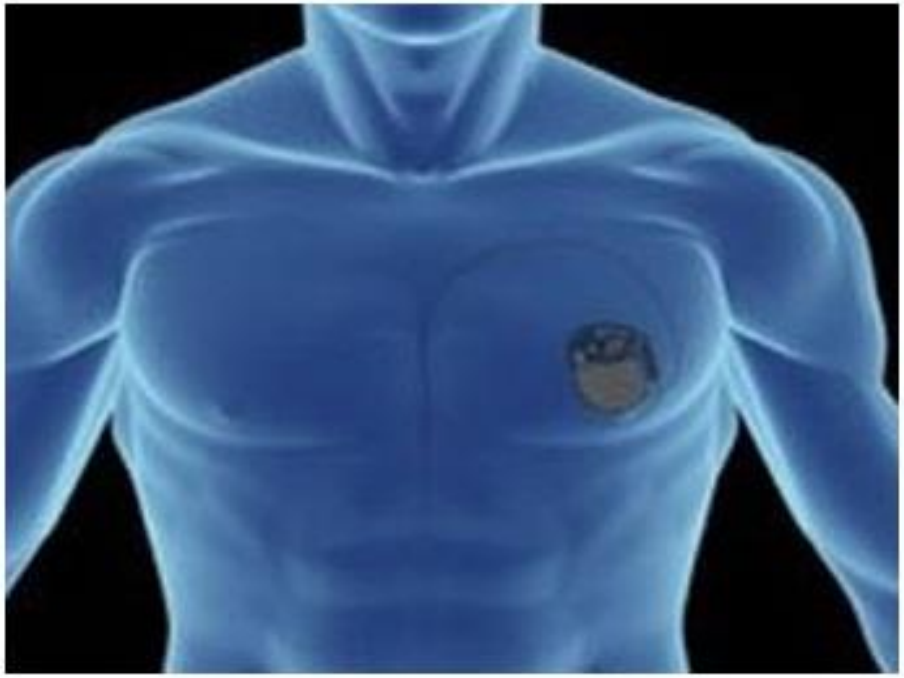
Ankara Emniyet Müdürlüğü'nün bilgisayar sistemini **hack**leyen internet korsanları, güvenlik şubesine yönlendirilen bazı belgeleri ele geçirmeyi başardı.

Kendilerine 'Kızıl **Hacker**lar' adını veren korsanlar, şifresini kırarak girdikleri Ankara Emniyet Müdürlüğü bilgisayar sisteminden çaldıkları belgeleri internet sitelerinden "**Polis**in Gizli Belgelerini ve Muhbirlerini Açıklıyoruz!" başlığıyla yayınladı.

Belgelerde bazı vatandaşların polise gönderdiği ihbarlara ilişkin yazışmaların olduğu görülüyor.

"SİTE KAPATILSIN"

Olayı doğrulayan Ankara Emniyet Müdürlüğü yetkilileri, şifresi kırılan sistemin tıpkı 155 Polis İmdat hattı gibi internet üzerinde kurulan bir



İmplantlara hacker uyarısı

İnternet korsanlarının, tıbbi implantlara erişim sağlayıp hastaların sağlığını tehlikeye atabileceği hatta ölümlerine neden olabileceği öne sürüldü.

Güncelleme:11 Nisan 2012 09:45

Bu iddia her ne kadar modern bir korku filminden alınma bir komplo gibi görünse de güvenlik uzmanları, böyle bir senaryonun gerçekleşmesinin aslında gayet mümkün olduğunu belirtti.

Bir siber güvenlik uzmanının bildirdiğine göre, **hacker**lar için, insan bedeninin içinde bulunan elektronik aygıtların uzaktan kumanda sisteminin ele geçirilmesi oldukça kolay. Çünkü bu sistemlerin güncellenmesi, tamamen korumasız kablosuz ağlarla sağlanıyor.

Ağa ulaşan sanal suçlunun, aygıtı kapatmak ya da **hasta**ya aşırı doz ilaç enjekte edilmesi komutu vermek gibi ölümle sonuçlanabilecek işlemler yapabileceği ifade ediliyor.

Yazılımları Güncellemek Neden Önemli?

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

Yazılımları Güncellemek Neden Önemli?

- Bu açıklıkları giderme amacı ile yazılım ve işletim sistemleri geliştiricileri
- yeni sürümler,
- yazılım yamaları, ya da
- hizmet paketleri yayınlar.

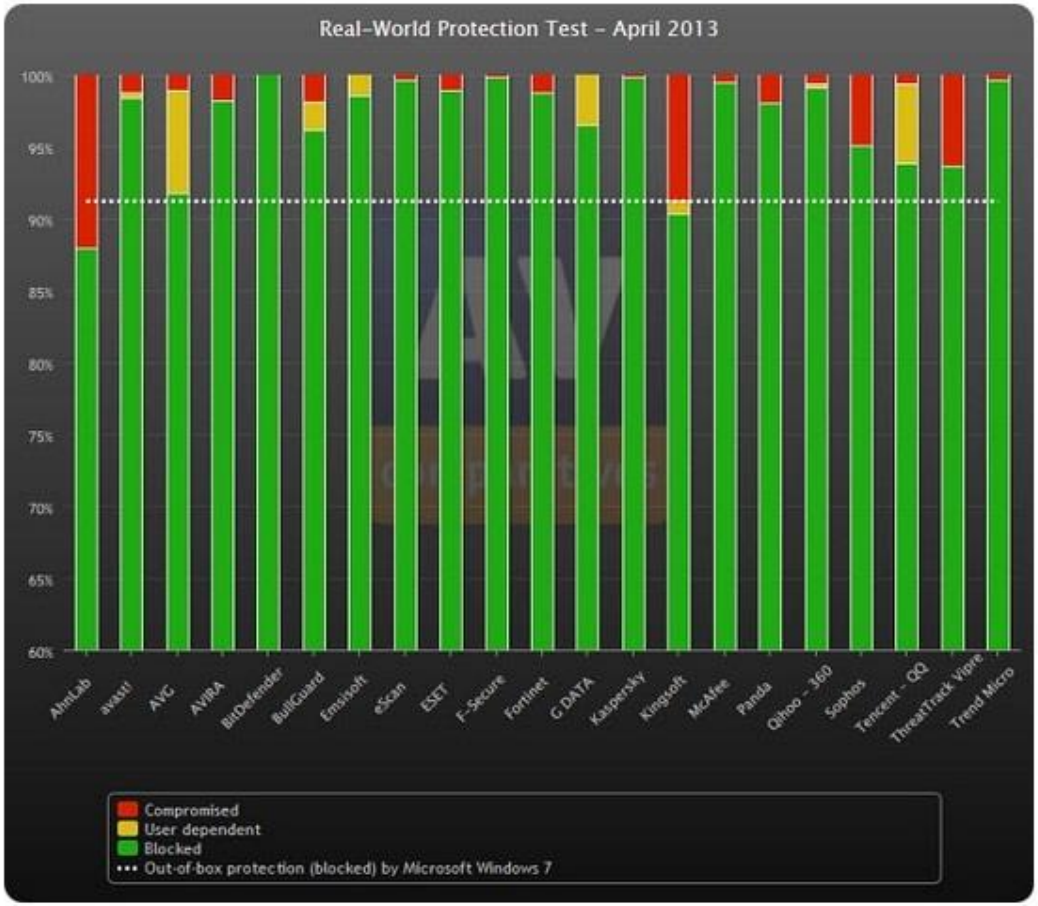
- Yayınlanan güncellemelerin **sürekli takip edilmesi** ve bilgisayarlarınıza **gerekli kurulumların hızla yapılması** gerekir.

Antivirüs Yazılımınızı Güncel Tutun

BEZMİÂLEM VAKIF ÜNİVERSİTESİ

Antivirüsler, Nisan 2013'te böyle sıralandı!

Antivirüs laboratuvarı AV-Comparatives'in "gerçek dünya" testinin sonuçları ortaya çıktı!



Dosya ve Veri Kaybı

BEZMİÂLEM VAKIF ÜNİVERSİTESİ

- 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 raporu tamamlayıp teslim edeceğiniz bir günde,
- hazırladığınız dökümanı son başvuru zamanı bitmeden yollamaya çalışırken,
- kısacası bir dosyaya en ihtiyacınızın olduğu bir zamanda veri ve dosya kaybı yaşamamak için **tedbirli olmak** gerekir.

Veri Kaybı ve Olası Nedenleri

- Bilgisayar dünyasında verilerin kayıtlı oldukları ortamda yerine konamayacak şekilde tahrip olması ya da silinmesi ile **veri kaybı** gündeme gelir. Aşağıdaki örneklerde açıklandığı gibi veri kaybının farklı nedenleri olabilir; Örneğin;
- İşletim sisteminde ortaya çıkabilecek bir problem
- Donanım hatalarından dolayı
- Kullanıcı hatası (yanlışlıkla dosya/klasör silinmesi gibi)
- Zararlı programların veya saldırgan kişilerin müdahalesi

E-Posta Güvenliği

- E-posta yaşamınızın ne kadar içinde? Gün içerisinde kaç e-posta mesajı alıyorsunuz? Her gün kaç tane e-posta mesajı yolluyorsunuz?
- Kaç farklı e-posta adresi kullanıyorsunuz?
- Binlerce kişiye ulaşabilme ihtimali, elektronik posta haberleşmesini cazip bir saldırı ortamına da dönüştürüyor.
- Sizin için iletişim anlamına gelen e-posta, saldırganlar için **size ve yakınlarınıza erişim**,
- Reklam ve zararlı program yayma fırsatı demektir.
- Toplu eposta gönderme işleminin kolaylığı ve teknolojik gelişmeler düşünülürse saldırganların **tek ihtiyaçları** eposta adresiniz ve bir an için dikkatsiz davranmanız.
- Bu kadar çok kullanılan bir aracın kurumsal olarak da kullanılması saldırganların kurum içi bilgilere ulaşmasına fırsat verdiğinden e-posta saldırıları ile kurumsal olarak da mücadele etmek gerekir.

- İstenmeyen e-posta (spam), oltalama, yemleme ya da taklit e-posta (phishing), veya aldatmaca e-posta (hoax);
- Bu terimler size yabancı geliyorsa, bir an önce öğrenmekte fayda var. Unutmayın tuzaklara düşmemek için önce onları farkedebilmeliyiz.
- Sakıncalı epostalar konusunda her zaman dikkatli olmak gerekir.
- Kurum içerisinde eposta kaynaklı problemlere hızlı müdahale etmek, problemleri çok büyümeden, kurumdaki tüm kullanıcıları etkilemeden çözmek için hem bireysel olarak hem de kurumsal olarak üstümüze düşen görevler vardır.

Cazip bir teklif mi yoksa bir tehdit mi?

Bunlara her an dikkat etmeli:

- Kimden geldiğini bilmediğiniz epostalara
- Nereye gideceği belli olmayan bağlantılara
- Ne yapacağı belli olmayan eklentilere

Uzmanlardan Bilgi Güvenliği Tavsiyeleri

BEZMİÂLEM VAKIF ÜNİVERSİTESİ

EUGENE KASPERSKY, İş adamı ve anti virüs şirketi Kaspersky'nin kurucusu

"Sosyal ağlarda bir şey paylaşmadan önce iki kez düşünüyorum"

PROF. DR. THORSTEN HOLZ, Bochum'daki Ruhr Üniversitesi'nde sistem güvenliği araştırmacısı

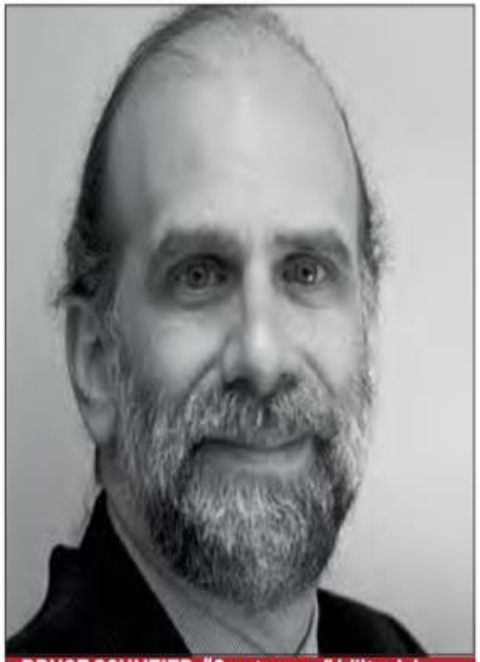
"Facebook ve Google'ı sadece cep telefonundan aldığım güvenlik koduyla kullanıyorum"

JOANNA RUTKOWSKA, Güvenlik araştırmacısı ve QubesOS'un geliştiricisi

"İki bilgisayarım var, biri internet diğeri iş için"

Uzmanlardan Bilgi Güvenliği Tavsiyeleri

BEZMİÂLEM VAKIF ÜNİVERSİTESİ



BRUCE SCHNEIER, "Crpytogram" bülteninin yazarı, kriptografi uzmanı

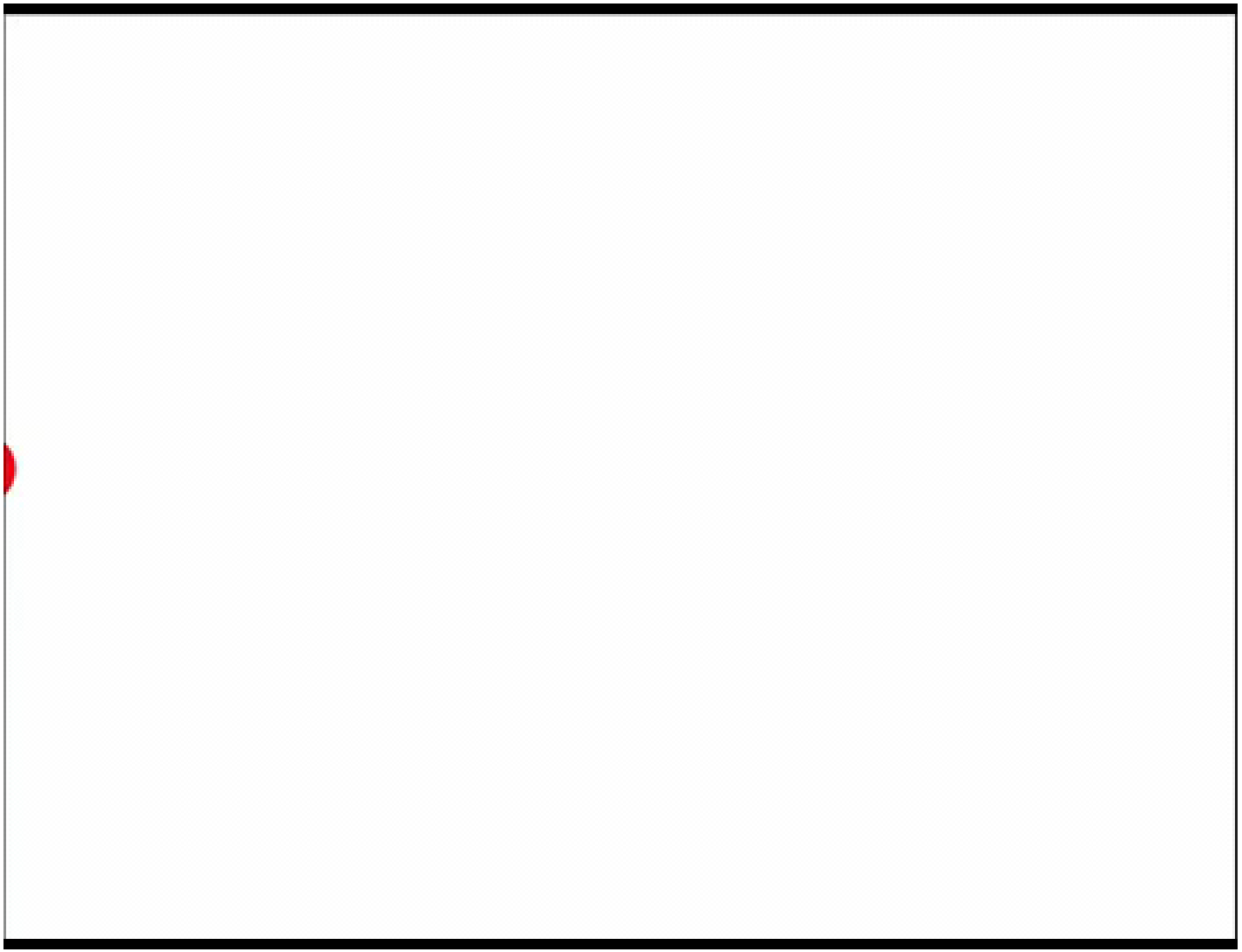
"Her iki üç günde bir tüm kişisel verilerimi yedeklerim"

BRIAN KREBS, Hacker ve kara borsa forumlarında güvenlik uzmanı

"Sadece bildiğim programları kurar, işim bitince de silerim"

STEPHEN PAO, Güvenlik şirketi Barracuda Networks'ün başkan yardımcısı

"Mümkünse her durumda, özellikle de Facebook'ta HTTPS kullanırım"



Son Söz

- Tehlike hiç ummadığınız bir anda, hiç ummadığınız bir yerden gelebilir.
- Tanımadığınız kişilerden gelen isteklere karşı temkinli davranılmalıdır.
- Size özel bilginizi (örneğin parolanızı) kimseyle paylaşmamalıdır.
- Sistem yöneticisi
- Yan masada oturan mesai arkadaşınız


Eğitimden sonra bilinçlenen kullanıcılar hayatlarının sonuna kadar güvenli bir şekilde bilgisayar kullanmışlar...
DATA DICTIONARY
RECYCLE BIN
© Bülent Oktay
bulentoktay.com

Kaynakça

- http://www.icisleri.gov.tr/
- http://www.bilgiguvenligi.gov.tr/kilavuz-dokumanlar/index.php
- http://www.bilgimikoruyorum.org.tr
- www.**saglik**.gov.tr
- www.**bilgiguvenligi**.org.tr
- http://www.youtube.com/watch?v=fYmVSLn5o0w
- http://www.medimagazin.com.tr
- http://www.saglikaktuel.com/