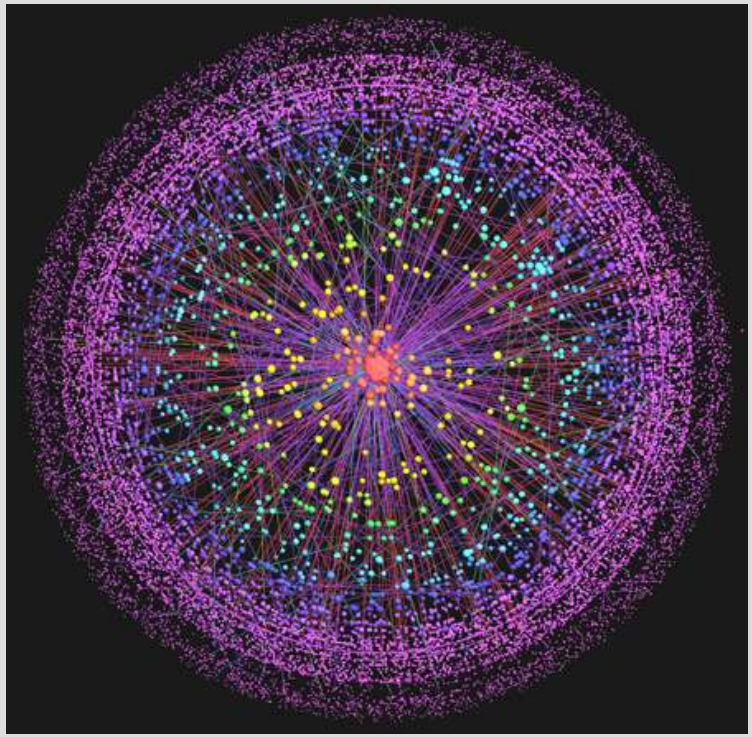
TÜBİTAK

UEKAE



Bilgisayar Güvenliği ve Internet

Temmuz 2009

TASNİF DIŞI

İçindekiler

- TÜBİTAK-UEKAE: Bilgi güvenliği konusunda yapılanlar
- Siber savaş ve “botnet” nedir?
- Türkiye için riskler
- Dünya’da ve Türkiye’de yapılan ve yapılması gereken çalışmalar
- Sonuç: Internet güvenliği için TÜBİTAK-UEKAE’nin önerileri

TÜBİTAK-UEKAE'nin Yaptığı Çalışmalar

E-Dönüşüm Eylem Planı 88. Madde:

Ulusal Bilgi Sistemleri Güvenliği Programı (UBGP)

Proje süresi: 4 yıl (Ocak 2007 – Aralık 2010)

- KOORDİNASYON: Ulusal Bilgisayar Olayları Müdahale Koordinasyon Merkezi'nin (BOME) kurulması
- EĞİTİM: Kamu kurumları bilgi işlem personeline bilgi sistemleri güvenliği eğitimleri verilmesi
- DOKÜMANTASYON: Kamu kurumları için bilgi sistemleri güvenliği ile ilgili kılavuz dokümanların hazırlanması ve portal aracılığı ile paylaşılması
- YÖNETİM: Pilot kurumlara Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulması
- İZLEME: Sanal Ortam Savunma Sistemi'nin kurulması

Ulusal Bilgi Sistemleri Güvenliği Programı

Ulusal Bilgi Sistemleri Güvenliği portalının kurulması:
http://www.bilgiguvenligi.gov.tr

Siber Savaş Nedir?

- Siber Savaş, ekonomik, politik veya askeri nedenlerle hedef seçilen ülkeye bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırılardır.

- Siber Savaş'ta yapılabilecek saldırılar:
  - Web sayfalarının ele geçirilmesi
  - Hizmet dışı bırakma (DoS/DDoS) saldırıları,
  - İnternet üzerinden karşı propaganda,
  - Gizlilik dereceli bilgilerin ele geçirilmesi,
  - Kritik sistemlere yönelik saldırılar (enerji, iletişim, finans, güvenlik altyapısı vb.)
- Bu saldırıların çoğu "botnet" adı verilen bilgisayar ağları aracılığı ile yapılmaktadır.

Siber Savaş

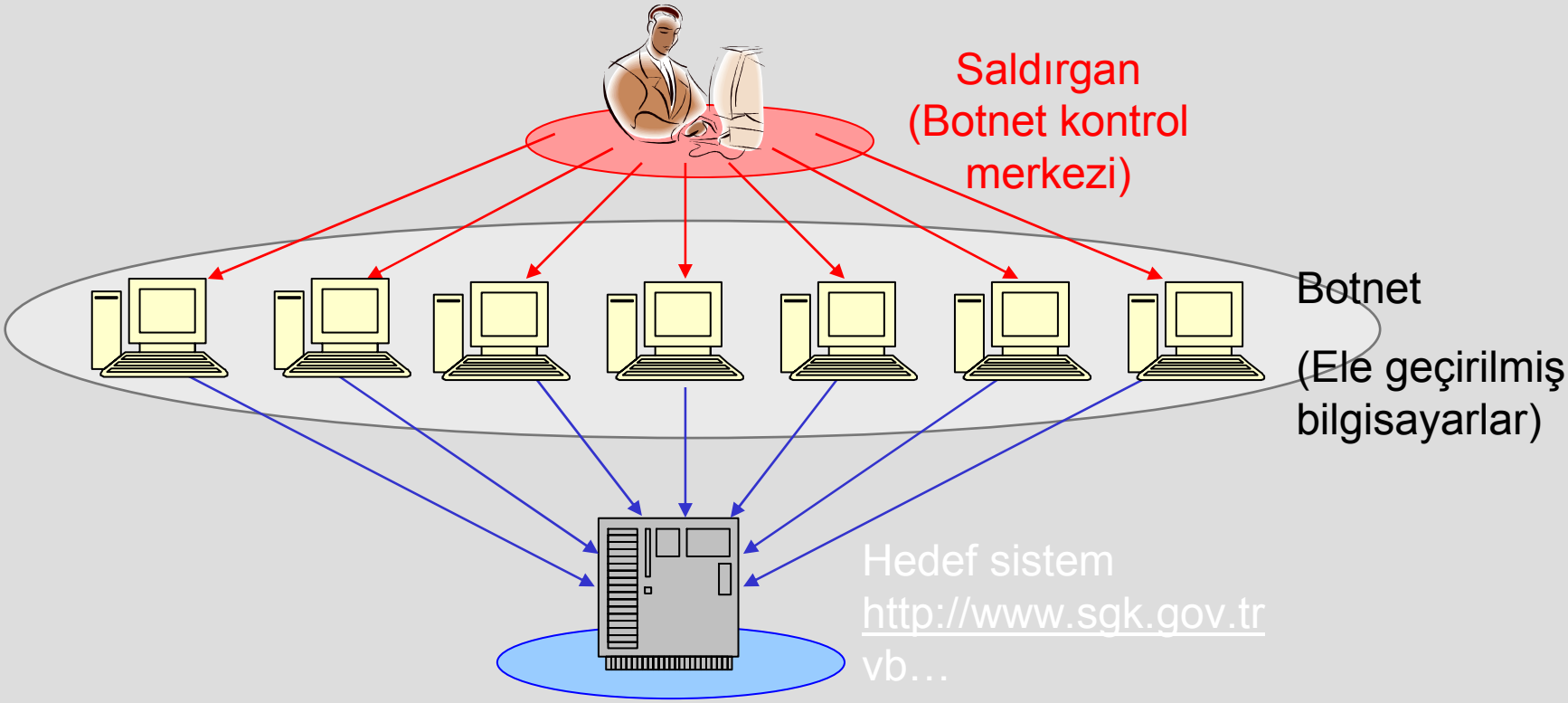
26 Nisan 2007 tarihinde Estonya'nın "Bronz Asker Heykeli"ni kaldırması ile ilk siber savaş başladı.

- Rusya Federasyonu – Estonya (Mayıs 2007)
- Rusya Federasyonu – Gürcistan (Temmuz 2008)
- İran'da yaşanan olaylar (2009 Haziran)

Sonuç:

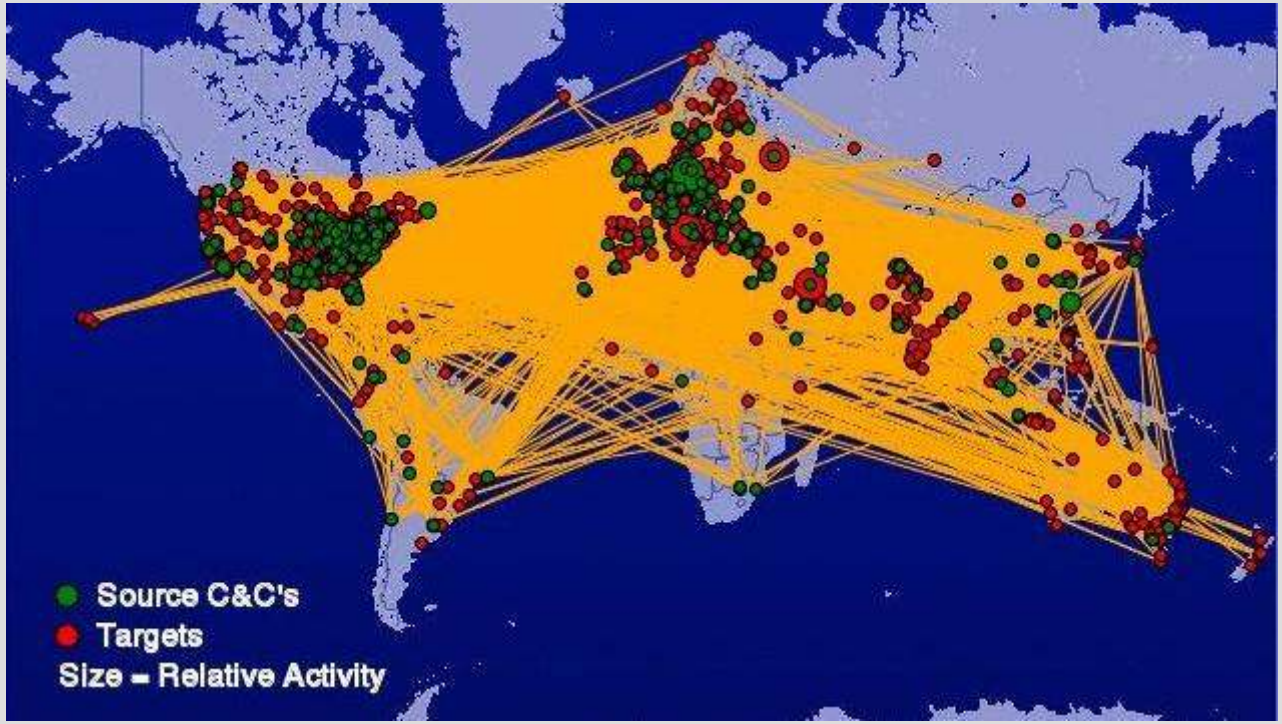
- Siber savaş artık bir kavram değil gerçektir.

“Botnet” nedir?



- Internet’e bağlı durumda bulunan bilgisayarlar güvenlik önlemleri alınmadığı takdirde kötü niyetli kişi/kurumlar tarafından ele geçirilebilmektedir.
- Ele geçirilmiş bilgisayarlardan oluşan ağa “Botnet” adı verilmektedir.

Dağıtık Hizmet Dışı Bırakma Saldırıları (DDoS)



Shadowserver Foundation
www.shadowserver.org

- Bir Botnet'in bilinçli olarak Internet'te bulunan bir sisteme yönlendirilmesi ve bu sistemin devre dışı bırakılması mümkündür (DDoS).
- Saldırgan, Botnet'e bağlı bilgisayarlar ve hedef sistem Dünya'nın herhangi bir ülkesinde veya farklı ülkelere dağılmış durumda bulunabilir.

“Botnet”ler ve Türkiye

- Türkiye, 2008 verilerine göre Dünya’da*
  - “Botnet”lere ev sahipliği yapan ülkeler sıralamasında 8.
  - Spam e-posta üretiminde 5. (2008’in son beş ayında 2.)
  - 2007’de 15. sıradan 2008’de 9. sıraya çıkarak kötü niyetli faaliyetlerin toplamının %3’ünün kaynağı durumundadır. (En hızlı yükselen ülke)
  - Yükselen diğer iki ülke, Brezilya ve Polonya’dır.
- Internet’te yer alan kiralık Botnet ilanlarında Türkiye 40 USD / 1000 bilgisayar ile “ucuz botnet” ligindedir.
- NATO’nun siber savunmadan sorumlu biriminden Türkiye’nin DDoS faaliyetlerine karıştığına dair bilgi alınmaktadır.
- Türkiye’nin elindeki bilgisayar parkı, kendi takdiri dışında kullanılabilecek kuvvetli bir silaha dönüşmüştür.

(*) “Symantec Global Internet Security Threat Report. Trends for 2008. Vol. XIV”, 2009/4

Türkiye'de Kamu Kurumlarının Bilgi Sistemleri

Kamu kurumlarının bilgi sistemleri ile ilgili olarak aşağıdaki tespitleri yapmak mümkündür:

- Kamu kurumları hizmetlerini Internet üstünden vermek için çalışmalarını sürdürmektedir.
- Kritik sistemlerin bir kısmı Internet'e bağlıdır.
- Teknoloji hızla değişmektedir.
- Bilgi ve iletişim sistemleri güvenliği sadece bilgi işlem - bilgi sistemleri sorumluluğuna verilmektedir.
- Donanım ve yazılımda büyük oranda yurtdışı bağımlılığı, ve
- Kamunun bilgi işlem birimlerinde yetersiz yapılanma mevcuttur.

Türkiye ve Bilgi Güvenliği Riski

- Türkiye içinde ciddi düzeyde “botnet” konuşlanması söz konusudur.
- Kamu bilgi sistemleri hızla Internet’e açılmaktadır.
- Kamu bilgi sistemleri için “kabul edilemez risk” söz konusudur!!!

Dünya'da Siber Suçlar ve Ülkelerin Reaksiyonları

TASNİF DIŞI

TÜBİTAK UEKAE

SABAH

Sanal casusluk endüstriye dönüşüyor

'Çin, bizi savaşta değil sanal alemde vuracak'

Amerika, siber savaşı başlattı

Dünya çapında teröre karşı savaş ilan eden ABD, savaşı sanal aleme de taşıdı. Savunma Bakanlığı (Pentagon), teröristlerle internette de savaşmak için yeni stratejiler geliştirdiğini açıkladı. El Kaide ve diğer örgütlerin internet sayesinde militan yetiştirip para topladığına dikkat çeken Pentagon, bu sitelere saldırarak yok edeceklerini belirtti. ABD Hava Kuvvetleri bünyesinde gerçekleştirilecek 4 yıllık proje için 40 milyon dolardan fazla bütçe ayrıldığı belirtildi. Bu alanda stratejiler geliştiren "sanal cephenin komutanı" General John Davis, "Bugüne kadar terörist siteleri sadece istihbarat için takip ediyorduk. Artık aktif bir stratejiye geçerek yok etme yoluna gideceğiz. Çünkü teröristler bu sitelerden çok fazla yarar sağlıyor. ABD askerlerinin görüntülerini yayımlayarak propaganda amacıyla da kullanıyorlar" dedi.

Radikal

Siber çete çökertildi

Binlerce hesaptan milyonlarca liralık vurgun yapan 17 kişi gözaltında

DHA - İZMİR - Bilgisayarınızı açtınız. Karşınıza bankanızdan geldiği belirtilen bir e-mail çıktı. Sizden bilgilerinizi güncellemenizi istedi. Sorulan yanıtladınız. Tebrikler siz de avlandınız! 'Fishing' (balıkavı) adı verilen yöntemle artık

İlk siber savaşın galibi 'Kızıl Ordu'

Geçtiğimiz ay sessiz sedasız ve yöntem olarak benzersiz bir savaş yaşandı. Rusya, Estonya'ya organize bir saldırı düzenledi ve ülkenin ticaret ve kamu düzenini dize getirmeyi başardı

Taktikler eşliğinde yeni çağlı insanlık bir ülkeyi dize getirmek kâlâ mümkün. Ama artık kapa yollar da var.

1918 yılında Alman ordularına yenilen Rusya'dan bağımsızlığını ilan eden Estonya, aynı Almanya'nın Rusya ile yaptığı gizli bir anlaşmanın ardından 1940 yılında Rus askerlerinin işgaliyle başlayan süreçte Sovyet Sosyalist Cumhuriyetler Birliği'nin bir üyesi olmak zorunda kalmıştı. 1989'da şarkılarla başlayan kıpırdanmanın ardından 1991 yılında sonunda Estonya yeniden bağımsızlığını kazandı. Ancak bu yeni süreçte Rusya'nın Estonya üstündeki hâkimiyet arzusunun söndüğü de söylenemez. Bunun son örneklerinden biri de geçtiğimiz günlerde internette yaşandı.

Sebep bir savaş anıtı

İnternetin yoğun olarak kullanıldığı ve büyük bir siber ekonomiye sahip Estonya geçtiğimiz ayın hemen her gününde web sunucularında ciddi bir savaşlamaya, hatta devre dışı kalmaya sahne oldu. Sistem yöneticilerinin yaptığı araştırmanın sonucunda bütün bu saldırının Rusya'dan yönetildiği ve çıkış noktasının 27 Nisan'da Rusya'nın bir savaş anıtının kaldırılması olduğu ortaya çıktı

Hürriyet

Pentagon'u çökerten hacker'lar konuştu

Hurriyet.com.tr

Geçen hafta ABD'li yetkililerin sistemlerinde çok ciddi hasarlara yol açan saldırılarla karşılaştıklarını açıklaması gözleri yine hacker'lara çevirdi. CNN'in konuştuğu ABD'nin belalısı Çinli hackerlar ise Pentagon'un bilgisayarlarına girdiklerini iddia ediyor.

Siber-şantajın hedefi ofis çalışanları

"Eğer xxx no'lu hesaba 30 euro yatırmazsan bilgisayarına çocuk pornosu resimleri yükleriz". Son bir yıldır, özellikle Avrupa ülkelerinde bazı ofis çalışanlarına gönderilen bu tür e-mail'ler internet üzerinde yeni bir suç işleme tarzının ortaya çıktığını gösteriyor. Polisin "siber şantaj" ifadesiyle tanımladığı olayda, çok sayıda ofis çalışanına e-mail gönderen hacker'lar, belirtilen hesaba para yatırılmazsa o kişinin bilgisayarındaki dosyaları silmek ya da çocuk pornosu fotoğrafları yüklemekle tehdit ediyor.

İnternette PKK virüsüne dikkat!

KAYSERİ DHA

Milliyet

PKK'lı bir grup "hacker"in geliştirdiği bir virüs internet kullanıcılarını tehdit ediyor. Uzmanlar, "Terörü lanetliyoruz. Herkesi Birlik olmaya çağırıyoruz" mesajı ve lanettheteror@hotmail.com adresine karşı dikkatli olunmasını istedi.

Çünkü mesaj açıldığında sözde terör karşıtı resimler ve yazılar çıkıyor. Ancak en sonunda ise bunun PKK tarafından yapıldığını ve tamamen aldatmaca olduğunu içeren Türkiye karşıtı Kürdistan yanlısı bir resimle bütün sisteminizin çöktüğünü, bilgisayarınızdan bütün verilerin silindiğini söylüyor. Ve gerçekten verileriniz siliniyor. Silinmeden önce de msn listenizdeki tüm arkadaşlarınıza e-postayı yolluyor.

Dünya'da Siber Suçlar ve Ülkelerin Reaksiyonları

Obama 'internet komutanı' atayacak

29 Mayıs 2009

Artık 'Sanal Savaş' çağındayız. Barack Obama, ABD'nin hem devlet kurumlarının hem de özel sektörün bilgisayar sistemlerini yabancı sanal ajanlara karşı koruyacak bir güvenlik birimi oluşturuyor.

Obama'nın başına bir generali ataması beklenen "siber çar" makamının, ulusal güvenlik danışmanı statüsünde olacağı belirtiliyor. Resmi ve özel bilgisyar sistemlerini sanal ajanların yanı sıra hacker'lar, kriminal çeteler ve teröristere karşı da koruyacak "askeri sanal alem komutanlığının" bugün açıklanması bekleniyor. Ayrıca Obama yönetimi, halkı da internet üzerinden oluşabilecek güvenlik tehditleri konusunda bilinçlendirmek için yeni bir eğitim kampanyası başlatmayı da planlıyor. Yeni 'siber çar', Başkana bağlı olacak ve hem Ulusal Güvenlik Konseyine hem de Ulusal Ekonomik Konseye sürekli rapor hazırlayacak.

Güvenlik Çözümlerinde Uyulması Gereken İlkeler

1) Kullanılabilirlik X Güvenlik dengesi

(Faydalı ancak güvenlik seviyesi düşük sistemler kullanılmalı mı?)

2) Bilgi ve iletişim sistemleri güvenlik mekanizmalarında milli çözüm ihtiyacı

3) Koordinasyon

İyilerin de (kamu bilgi sistemi personeli) en az kötüler kadar işbirliği yapması (kamu kurumları-özel sektör-sivil toplum örgütleri koordinasyonu)

Güvenlik Çözümlerinde Uyulması Gereken İlkeler

4) Uluslararası İşbirliği

- TÜBİTAK-UEKAE bünyesinde kurulmuş olan TR-CERT, NATO-CIRC (Computer Incident Response Capability) ile işbirliği protokolü imzalamıştır. (2006)
- TÜBİTAK-UEKAE, NATO Cyber Defence Management Authority'ye ulusal temas noktasıdır. (2008)
- NATO, TÜBİTAK-UEKAE'den, Afganistan'daki NATO birlikleri için CERT kurmasını ve eğitim vermesini talep etmiştir. (Temmuz 2009)
- TÜBİTAK-UEKAE, 21 kamu kurumunun katıldığı Ulusal Elektronik Ortam Savunma Stratejisi belgesinin taslağının hazırlanmasında koordinatörlük yapmış ve taslak belgeyi Başbakanlığa göndermiştir. (Ocak 2009)

Yapılması Gerekenler

- Ulusal Sanal Ortam Güvenlik Stratejisi'nin yayınlanması
- Bilgi Güvenliği konusunda gerekli olan yasal düzenlemelerin yapılması
- Ülke yeteneklerinin geliştirilmesi
- Bilgilendirme ve bilinçlendirme çalışmaları
- Ulusal kritik bilgi ve iletişim sistem altyapılarının güvenliği
- Ulusal Bilgisayar Olaylarına Müdahale Organizasyonunun kurulması
- Uluslararası eşgüdüm

Yapılması Gerekenler

- BİLGİ GÜVENLİĞİNDE EN ÖNEMLİ ETKEN EĞİTİMDİR.
- Kamuoyunun bilinçlendirilmesi gerekmektedir.
- Basit önlemlerin alınması ile güvenlik düzeyinde ciddi iyileşme sağlanabilir.
- Kurumsal bilgi sistemleri ile kişisel kullanıcıların (ev bilgisayarları) ayrı ayrı değerlendirilmesi gerekir.

Kişisel Bilgisayarlar için Önlemler

Ev bilgisayarlarında alınabilecek basit fakat etkili önlemler:

1. Bilgisayarlara işletim sistemi güncellemelerinin yüklenmesi.
2. Bilgisayarlarda anti-virüs uygulamalarının çalıştırılması.
3. Şüpheli içeriğe sahip Internet sitelerine bağlanılmaması.
4. Yabancı adreslerden gelen elektronik posta iletilerinin açılmaması.
5. Kullanılmadığı durumlarda bilgisayarların kapalı tutulması.

Kamu Kurumları Güvenliği için Sonuç (1/2)

1. Ulusal Sanal Ortam Güvenlik Stratejisi'nin yayınlanması
2. Bilgi Güvenliği konusunda gerekli olan yasal düzenlemelerin yapılması
   - Ulusal kritik bilgi ve iletişim sistem altyapılarının (finans, enerji, haberleşme, güvenlik...) güvenliği sağlanması ve garanti edilmesi Bilgilendirme ve bilinçlendirme çalışmaları
   - Ulusal Bilgisayar Olaylarına Müdahale Organizasyonunun ve Sanal Ortam Savunma Sisteminin kurulması
   - Bilgi Güvenliği Rehberliği
   - ...
3. Uluslararası eşgüdüm

Kişisel Bilgisayarlar için Sonuç (2/2)

Kişisel bilgisayar kullanıcıları, yeni bilgisayarlara eklenecek bir bilgi güvenliği notu ile

- Basit ve etkili önlemleri almaya davet edilmeli,
- Internet'teki (www.bilgiguvenligi.gov.tr ve benzeri) ulusal bilgi güvenliği kaynaklarına yönlendirilmelidir.

Sorular

Mert Üneri

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Md. Yrd.

uneri@uekae.tubitak.gov.tr

Tel: 0312 468 23 16

EK-1: Internet'te gerçekleşen kötü niyetli faaliyetler

Kötü niyetli faaliyetlerin ülkelere göre dağılımı*

2008 sıra no.	2007 sıra no.	Ulke	2008 faaliyet yüzdesi	2007 faaliyet yüzdesi	Kötü niyetli yazılım sıralaması	Spam zombi sıralaması	"Phishing" sitesi sıralaması	Bot (DDos zombi) sıralaması	Saldırı kaynağı sıralaması
1	1	A.B.D.	%23	%26	1	3	1	2	1
2	2	Çin	%9	%11	2	4	6	1	2
3	3	Almanya	%6	%7	12	2	2	4	4
4	4	Birleşik Krallık	%5	%4	4	10	5	9	3
5	8	Brezilya	%4	%3	16	1	16	5	9
6	6	İspanya	%4	%3	10	8	13	3	6
7	7	İtalya	%3	%3	11	6	14	6	8
8	5	Fransa	%3	%4	8	14	9	10	5
9	15	Türkiye	%3	%2	15	5	24	8	12
10	12	Polonya	%3	%2	23	9	8	7	17

(*) "Symantec Global Internet Security Threat Report. Trends for 2008. Vol. XIV", 2009/4

EK-2: Bilgi Güvenliği Notu

Bilgisayar Güvenliği ve Internet

İstatistikler günümüzde Dünya'da yaklaşık 1.600.000.000 Internet kullanıcısı bulunduğunu bildirmektedir. Bu sayı hızla artmaktadır.

Kötü niyetli kişi ve organizasyonların da faaliyet gösterdiği bu ortamda, Internet'e bağlı bilgisayarlar çeşitli tekniklerle ele geçirilebilmekte ve bilgisayarın asıl sahibinin bilgisi dışında kullanılabilmektedir.

Bu durum ulusal düzeyde bilgi işlem ve iletişim altyapısında hasara neden olabileceği gibi kişisel bilgisayarınızın kullanılamaz hale gelmesi sonucunu da doğurabilir.

Bilgisayar kullanıcıları tarafından alınması tavsiye edilen önlemler aşağıda belirtilmiş olup, bu önlemler istenmeyen durumların ortaya çıkma olasılığını tamamen ortadan kaldırmasa da azaltacaktır:

1. Bilgisayarınıza işletim sistemi güncellemelerinin yüklenmesi.
2. Bilgisayarınızda Anti-virüs uygulamalarının çalıştırılması.
3. Şüpheli içeriğe sahip Internet sitelerine bağlanılmaması.
4. Yabancı adreslerden gelen elektronik posta iletilerinin açılmaması.
5. Kullanılmadığı durumlarda bilgisayarın kapalı tutulması.

http://www.bilgiguvenligi.gov.tr/... adresinden daha fazla bilgi alabilirsiniz.

TÜBİTAK UEKAE
Bilişim Sistemleri Güvenliği Grubu