E-DEVLET VE SİBER GÜVENLİK

6 ŞUBAT 2013

Gülce UZUN	Bil. Müh. 4. Sınıf Öğrencisi

Akış

- Siber Güvenlik Nedir?
- Neden Siber Güvenlik Stratejilerine İhtiyaç Duyulur?
- Genel Olarak Neler Yapılabilir?
- Siber Güvenlik Taslakları, Standartları
- Siber Güvenlikle İlgili Uluslararası Değerlendirme
- Ülkelerin Siber Güvenlik Çalışmaları
- Uluslararası Saldırılar

SİBER GÜVENLİK NEDİR?

SİBER GÜVENLİK

Günümüzde, pek çok bölgesel ve uluslararası kuruluş, siber güvenlik konusunda;

- Ülkeler arasında bilgi paylaşımı,
- Yasal ve teknik boyutta ulusal kapasitelerin geliştirilmesi,
- Farkındalığın arttırılması,
- Uluslararası işbirliğinin sağlanması

gibi hedefleri sağlamaya yönelik faaliyetler yürütmektedir.

NEDEN SİBER GÜVENLİK STRATEJİLERİNE İHTİYAÇ DUYULUR?

1. Ülke siber güvenlik ihtiyaçlarının ortaya konulması
2. Kavramların ve adımların tarif edilmesi
3. Hedeflerin doğru belirlenebilmesi
4. Hedeflere uygun sistematik ve beklenen amaca yönelik adımların atılabilmesi
5. Atılmış adımların denetimi, izlenmesi ve iyileştirilmesi gibi nedenlerle siber güvenliğe ihtiyaç duyuyoruz.

GENEL OLARAK NELER YAPILABİLİR?

1. Bu programların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması,
2. Bilgisayarda şifre korumalı ekran koruyucu kullanılması,
3. Kurmuş olduğunuz programların paylaşıma açık olup olmadığını kontrol ediniz,
4. Bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkılması,
5. Kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi,

GENEL OLARAK NELER YAPILABİLİR?

6. Bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi,

7. Disk paylaşımlarında dikkatli olunması,

8. İnternet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi,

9. Önemli belgelerin parola ile korunması veya şifreli olarak saklanması,

10. Gizli veya önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi,

GENEL OLARAK NELER YAPILABİLİR?

11. Kullanılmadığı zaman İnternet erişiminin kapatılması,

12. Önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması

13. Eğer Windows kullanıyorsanız güncellemeleri yapmanız,
gibi önlemler, basit gibi gözükebilecek ama hayat kurtaracak önlemlerden bazılarıdır.

Siber Güvenlik Taslakları, Standartları

- Siber güvenlikle ilgili alınacak önlemleri belirlemek ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında Siber Güvenlik Kurulu kuruldu.

TASLAK

2 SAYFALIK TASLAK:

- amaç-kapsam,
- tanımlar-kısaltmalar,
- ilkeler,
- görev ve yetkiler,
- isbirliği-koordinasyon,
- çalışma grupları,
- geçici kurullar ile
- yürütme bölümlerinden oluşuyor.

STANDARTLAR

- Common Criteria (CC), Türkçeye genel veya yaygın kriter olarak çevrilebilir.

- Amaç Uluslararası Standartlara dayanan Enformasyon tekniğinin güvenliğini sağlamak ve değerlendirmektir. (ing. Common Criteria for Information Technology Security Evaluation, kısaca CC.) Temeli Avrupa'nin geliştirdiği ITSEC, "Orange-Book" TCSEC, ABD'nin ve Kanada'nin CTCPEC kriterlerine dayanıyor.

STANDARTLAR

- ISO27001 Bilgi Güvenliği Yönetim Sistemi – Gereksinimler,
- ISO27002 Bilgi Güvenliği Yönetim Sistemi için Uygulama Kodları,
- ISO27003 Bilgi Güvenliği Yönetim Sistemi için Uyarlama, Gerçekleştirme Kılavuzu,
- ISO27004 Bilgi Güvenliği Yönetim Sistemi – Ölçekler, Raporlar,
- ISO27005 Bilgi Güvenliği Yönetim Sistemi – Risk Yönetim,
- ISO27006 Bilgi Güvenliği Yönetim Sistemi – Denetim ve Belgelendirilmesi için Şartlar.

Siber Güvenlik ile İlgili Uluslararası Değerlendirme

- Ülkemizin üyesi olduğu Birleşmiş Milletler ve bünyesinde yer alan Uluslararası Telekomünikasyon Birliği, Ekonomik İşbirliği ve Kalkınma Teşkilatı ve Avrupa Konseyi'nin yanı sıra, hâlihazırda tam üyelik müzakere sürecini sürdürdüğü Avrupa Birliği tarafından siber güvenlik konusunda yürütülmekte olan faaliyetleri şöyledir:

Birleşmiş Milletler Çalışmaları:

- Farkındalık,
- Sorumluluk,
- Güvenlik ihlallerine tepki verebilme,
- Etik,
- Demokrasi,
- Risk değerlendirme,
- Güvenlik tasarımı ve uygulaması,
- Güvenlik yönetimi ve
- Yeniden derlendirme olarak ortaya koymaktadır.

ULUSLARARASI TELEKOMÜNKASYON BİRLİĞİ'NİN ÇALIŞMALARI

- Radyo spektrumunun küresel çapta ortak kullanımını koordine etmek,
- Uydu yörüngelerinin tahsisinde uluslararası işbirliğini sağlamak,
- Gelişmekte olan dünyada elektronik haberleşme altyapısının da geliştirilmesini sağlamak,
- Farklı haberleşme sistemleri arasında sorunsuz bağlantılar kurulmasına imkân verecek, dünya çapında kabul gören standartlar oluşturmak ve
- Siber güvenliğin sağlanması gibi güncel konularda çalışmalar yapmaktır.

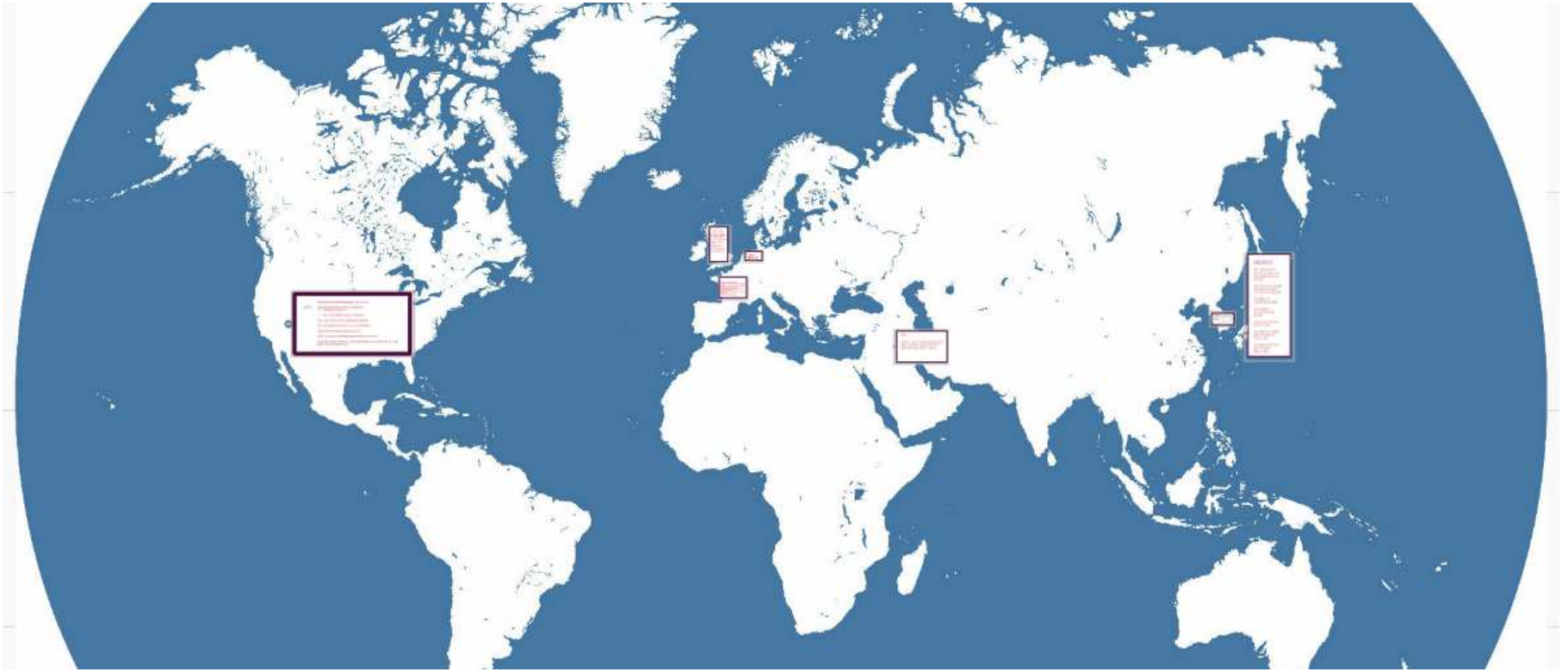
EKONOMİK İŞBİRLİGİ VE KALKINMA TEŞKİLATI'NIN ÇALIŞMALARI

- 1960 yılında kurulan, tüm gelişmiş ülkeler ve ülkemiz dâhil 30 üyesi bulunan Ekonomik isbirliği ve Kalkınma Teşkilat (Organization for Economic Cooperation and Development -
- OECD), ekonomiden çevreye, tarımdan teknolojiye kadar çok geniş bir alanda faaliyetler yürüten uluslararası bir kuruluştur. Siber güvenlik konusuna büyük önem veren OECD, bu konudaki çalışmalarını 1980'den bu yana sürdürmektedir.

AVRUPA BİRLİĞİ'NİN ÇALIŞMALARI

- AB, siber güvenliğin sağlanması ve kritik bilgi ve altyapıların korunması için alınabilecek olası yasal, teknik ve idari tedbirleri belirlemek amacıyla;
- Bilgi Toplumu Teknolojileri ve Avrupa Güvenlik Aratırma Program Kritik Bilgi Altyapıları Aratırma Koordinasyon Projesi Avrupa Kritik Altyapıların Korunması Program (European Programme for Critical Infrastructure Protection - EPCIP) gibi projeler ve programlar yürütmekte ve AB üyesi veya aday ülkelerin yürütmekte olduğu pek çok projeyi desteklemektedir.

ÜLKELERİN SİBER GÜVENLİK STRATEJİLERİ



ABD

- Kamu kurumları genelinde saldırı önleme sistemleri kurma
- Kamu kurumlarının ağlarını tek bir ağ altında güvenli
- internet bağlantıları ile yönetme
- ARGE faaliyetlerinin koordine edilmesi ve yönetilmesi
- Mevcut siber operasyon merkezlerinin birbirine bağlanması
- Karşı siber casusluk planlarının geliştirilmesi ve uygulanması
- Siber güvenlik eğitim çalışmalarının genişletilmesi
- Caydırıcılık stratejileri ve programlarının tanımlaması ve geliştirilmesi
- Kritik altyapı alanlarını içine alan ve devletin sorumluluklarını tanımlayan genişletilmiş siber güvenlik çalışmalarının yürütülmesi

ALMANYA

- Kritik bilgi ve altyapıların korunması
- (Kişi ve kurumların) Haklarının güvence altına alınması
- ‘Ulusal Siber Güvenlik Kurulu’ oluşturulması
- Devlet tarafından onaylanan servislerin kullanılmasının teşvik edilmesi (elektronik kimlik, De-Mail vb.)
- Önleyici tedbirlerin ve Kamu/Özel sektör işbirliğinin koordinasyonu, bilgi ve tecrübe değişiminin artırılması
- AB ve BM düzeyinde yürütülen çalışmalara katkı ve komşu ülkelere destek verilmesi
- Sürekli olarak güvenilir ve sağlam BT sistem ve ürünlerinin kullanılmasının sağlanması
- Tehdit ve uygun savunma ölçüt ve araçlarının sürekli olarak gözden geçirilmesi

İNGİLTERE

- Tehdit motivasyon ve kabiliyetlerini azaltarak siber altyapı ve hizmetlere yönelik tehditlerin azaltılması
- Tehdit aktörleri hakkında bilgi toplaması
- Bilgi, kabiliyet ve karar vermenin geliştirilmesi
- Teknik ve insan kabiliyetlerinin geliştirilmesi
- Kamu bilgi ve farkındalığının artırılması
- Doktrin ve politika geliştirilmesi

FRANSA

- Kritik ulusal altyapıların siber savunmalarının güçlendirilmesi
- Siber güvenlik alanında en son teknolojik gelişmelerin izlenmesi, araştırma yeteneklerinin geliştirilmesi,
- Bilimsel araştırma faaliyetleri ile birlikte uzmanlık ve eğitim faaliyetlerinin yürütülmesi
- Kamu ağları içerisinde, akıllı kart teknolojisine (Fransız
- mükemmeliyet alanı) dayalı yeni bir kimlik doğrulama sisteminin oluşturulması
- Daha güvenli bir kamu intranetine sahip olma
- Kritik altyapı işletmecilerine ait bilişim sistemlerinin güvenliği konusunda, kamu-özel ortaklığı oluşturma
- Kişi ve kurumların farkındalık ve motivasyonlarını artırma

JAPONYA

- Olası büyük bir siber saldırıya karı hazırlık ve karşı koyma planlarının yapılması
- Siber saldırı bilgi toplama ve paylama sisteminin kurulması ve kullanılması
- Bilgi güvenliği kampanyası yapılması
- Kişisel bilginin korunmasının teşvik edilmesi
- Uluslararası ittifakların güçlendirilmesi
- Bilgi güvenliği alanında insan kaynaklarının geliştirilmesi
- Bilgi güvenliğine ilişkin yasal altyapının düzenlenmesi

GÜNEY KORE

DEĞERLENDİRME BAŞLIĞI	MERKEZİLEŞME ÖNCESİ DURUM	MERKEZİLEŞME SONRASI DURUM
VERİ MERKEZİNİN ORTALAMA DEVRE DIŞI KALMA SÜRESİ (MAKİNE/AY)	67 DAKİKA	4,8 SANİYE
DDOS SALDIRISI HAFİFLETME SÜRESİ	-	20 SANİYE
FELAKET KURTARMA SİSTEMİ	YÜZDE 45	YÜZDE 61
MALİYET TASARRUFU (SATIN ALMA VE İŞLEME)	-	YÜZDE 30
YILLIK ENERJİ TASARRUFU (KARBONDİOKSİT VE ELEKTRİK)	-	YÜZDE 30 3 TON CO_2 3,75 Mw / SAAT ELEKTRİK
BIT ÜRÜN SATINALMALARI TASARRUFU (2009 - 2010)	-	112 MİYON DOLAR
HİZMET MÜŞTERİ MEMNUNİYETİ	YÜZDE 64	YÜZDE 89
NCIA PROJELERİNE KOBİ KATILIMI	YÜZDE 26,7 (2010)	YÜZDE 51 (2012)

Güney Kore Kamu Entegre Veri Merkezi Kazanımları

İRAN

İran son 3 yıldır siber dünyada savunma ve saldırı teknolojilerini geliştirmek için var gücüyle çalışıyor, yatırımlar yapıyor.

KARŞILAŞTIRMALAR

KARŞILAŞTIRMALAR

- ABD: Somut uygulama adımlarına ağırlık vermektedir.
- İngiltere: Karşı koyma esaslıdır ve proaktif tutumlara öncelik vermektedir.
- Fransa: Kamu BT altyapıları ve servislere ilişkin somut öneriler getirmektedir.
- Almanya ve Japonya: Yeni kurumsal yapılar ve yasal düzenlemelere vurgu yapmaktadır.

ULUSLARARARASI DEĞERLENDİRME

ULUSLARARASI DEĞERLENDİRME

- ZARARLI YAZILIMLAR:

1 - Morris Solucanı,

2 - Back Orifice,

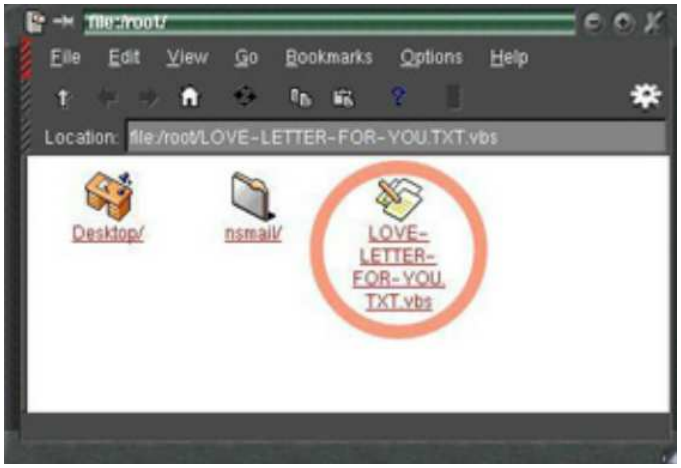
3 - Melissa,

4 - I.love.You,

5 - Code Red,

6 - Nimda,

7- Blaster,



ULUSLARARASI DEĞERLENDİRME

- ZARARLI YAZILIMLAR:

8 - Slammer,

9 - Sasser,

10- Zeus,

11- Conficker,

12- stuxnet,

13- duqu,

14- flame

ULUSLARARASI DEĞERLENDİRME

- SİBER SUÇ/CASUSLUK OLAYLARI:

15 - Titan Yağmuru

16- GhostNET

17- Aurora Operasyonu

18- Wikileaks

ULUSLARARASI DEĞERLENDİRME

- SİBER SAVAŞLAR:

20- Çöl Fırtınası Operasyonu

21- Ay Işığı Labirenti

22- NATO Kosava Krizi

23- Estonya Siber Savaşı

24- Gürcistan Siber Savaşı

REFERANSLAR

- http://www.siberguvenlik.org.tr/
- http://www.cyberhub.com/cyberpowerindex
- http://www.bilgimikoruyorum.org.tr/
- http://www.mmg.org.tr/dergi-indir/0e69eca71f.pdf
- http://www.cybersecurity.gov.tr/publications/uksgf.pdf
- http://www.futuregov.asia/articles/2011/aug/13/south-korea-outlines-cyber-security-strategy/?goback=%2Egde_3776184_member_66068559
- http://www.bilgiguvenligi.org.tr/index_files/sunumlar/ulusal_siber_guvenlik_strateji_taslak_belgesi.pdf
- http://tr.wikipedia.org/wiki/Bilgisayar_g%C3%BCvenli%C4%9Fi
- http://t24.com.tr/haber/suleyman-anil-siber-komutanlik-bolumunuz-yoksa-eksiksiniz/106479
- http://tr.wikipedia.org/wiki/Common_Criteria
- http://www.commoncriteriaportal.org/

TEŞEKKÜRLER