BİLİŞİM SUÇLARI

SUNU PLANI

- Teknoloji ve Oluşturduğu Tehditler
- Bilişim Suçu Nedir?
- Bilişim Suçları Kategorileri ve Suç Tiplerine Örnekler
- Bilişim Suçlarının Hukuki Durumu
- Türkiye'de Bilişim Suçları ile Mücadele
- Mücadelede Karşılaşılan Problemler
- Son Sözler

Teknoloji ve Oluşturduğu Tehditler

Özellikle internet'in icadı ile:

- Küreselleşme, sınırlar ortadan kalkmıştır
- Kolay ve hızlı iletişim imkanı
- Bilgiye hızlı ulaşma ve bilginin hızlı yayılımı
  - Suç gruplarının internet üzerinden propaganda yapması
  - Dünya çapında, yandaşlarıyla çok kolay ve hızlı bir şekilde iletişime geçebilmeleri
  - Özellikle organize suçlarda suç gruplarının birleşimi
- İnsanların, Nesnelerin ve Paranın Hızlı hareketi
- Bir çok kritik bilginin elektronik ortamda iletilmesi ve işlenmesi
- Askeri ve tıb alanı gibi çok önemli alanlarda otomasyona geçilmesiyle birlikte bir çok sistemin bilgisayar ile yönetilmesi

Bilişim Suçları

Değişik şekillerde telaffuz edilmektedir:

- Yüksek Teknoloji Suçları (Hi-Tech Crime)
- Bilgisayar Suçları (Computer Crime)
- İnternet Suçları (Internet Crime)
- Bilgi Teknolojisi Suçları (IT Crime)

Bilişim Suçu Nedir ?

- Ceza kanununu ihlal eden, işlenmesinde, veya araştırılmasında bilgisayar teknolojisi bilgilerini içeren her suç bilişim suçu olarak tanımlanmaktadır . (Amerikan Adalet Departmanı,2004)

Bilişim Suçlarında Katogoriler

- Şiddet İçeren Suçlar
- Şiddet İçermeyen Suçlar

Şiddet İçeren Suçlar

Bir veya birden fazla kişiye karşı fiziksel tehlike barındıran suçlardır.

- **Siber Terorizm (Cyberterrorism):** Bilişim sistemleri kullanılarak terör suçunu işleme, planlama ve kordine etmek
  Ör: Hava Trafiğini kontrol eden bilgisayar sistemindeki verileri değiştirme ve uçakların çarpışmasını sağlama, Hasta kayıtlarını değiştirerek yanlış doz ilaç alınmasını sağlama v.b.

- **Tehditle saldırı (Assault by threat) :** Bir kişiyi veya sevdikleri kişileri terör içerikli olarak bilişim sistemleri kullanarak tehdit etme.

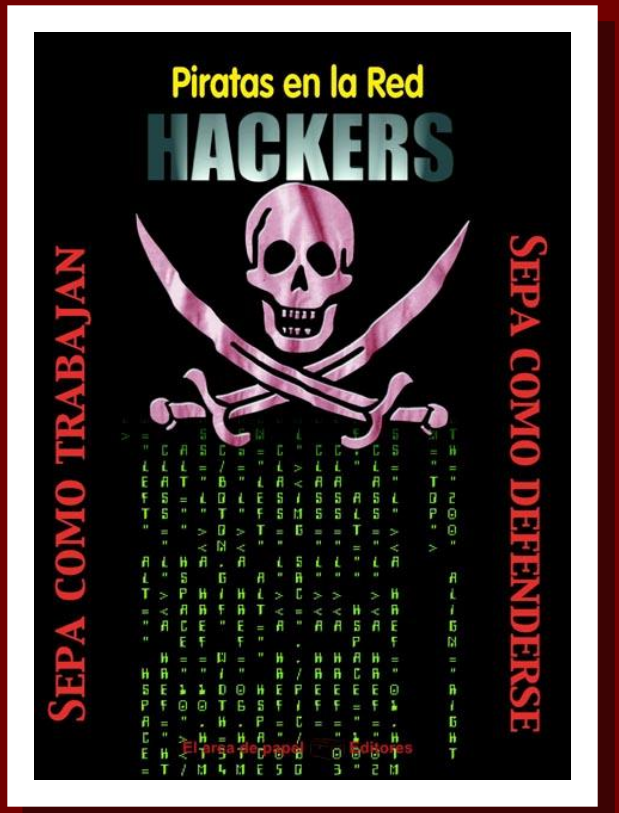
- **İnternet Üzerinden Taciz, Hakaret (Cyberstalking)**

- **Çocuk Pornografisi (Child Pornography):**
  - Küçük çocukları kullanarak pornografik materyal oluşturanlar
  - Bu materyallerin dağıtımını sağlayanlar
  - Bu materyallere erişenler

Şiddet İçermeyen Suçlar

Sanal dünyanın fiziksel teması pek içermeyen anonim yapısı itibariyle bilişim suçlarının geneli şiddet içermeyen suçlar kategorisinde değerlendirilir:

- Siber İhlal
- Siber Hırsızlık
- Siber Dolandırıcılık
- Yıkıcı Siber Suçlar
- Diğer şiddet içermeyen suçlar



Siber İhlal

- Bir bilişim sistemine yetkisi olmadığı halde giriş gerçekleştiren, fakat söz konusu sisteme veya sistem üzerindeki herhangi bir nesneye zarar vermeyen ve kötüye kullanmayan suçları içermektedir.
- Genellikle yetkisiz erişim olarak teleffuz edilmektedir.
  - Bir kişinin bilgisayarına girip, maillerini okuma
  - Hangi programları kullandığı not etme
  - Hangi web sitelerini ziyaret ettiğini öğrenme

Siber Hırsızlık

- Bilişim sistemlerini kullanarak bilgi, para ve benzeri değerleri çalarak işlenen suç tipidir.
- Bir çok farklı tipte karşımıza çıkmaktadır:
  - Zimmete Geçirme
    - Yetkili, güvenilen birisi tarafından
  - Kanunsuz Ödenek
    - Yetkisi olmayan, güvenilmeyen birisi tarafından
  - Endüstri Casusluğu
    - Ticari Sırları, finans bilgilerini, müşteri bilgilerini, pazarlama stratejisi v.b bilgileri çalma
  - Eser Hırsızlığı
    - Bir kişiye ait yazıları, refer etmeden kullanmak.
  - Korsancılık
    - Telif hakkı bulunan yazılım, müzik, film, kitap v.b yetkisiz olarak kopyalama
  - Kimlik Hırsızlığı

Kimlik Hırsızlığı

- Kimlik hırsızlığı, dolandırıcının kişisel bilgilerin, doğum tarihi, bankadaki ayrıntıları ya da sürücü belgesi numaraları gibi temel parçalarını elde ederek, başkasının kimliğine bürünmesi suçudur.

- Keşfedilen kişisel bilgiler daha sonra yasadışı olarak kredi başvurusunda bulunmak, mal ve hizmet satın almak ya da banka hesaplarına erişim sağlamak için kullanılır.

http://www.hsbc.com.tr/OnlineServisler/Guvenlik/OnlineTerimler.asp

Siber Dolandırıcılık

- Bilişim sistemlerini kullanmak suretiyle kendine çıkar sağlama maksatlı yanlış yönlendirme yapılarak işlenen suçlardır.
- Siber Hırsızlıktan farklı olarak siber dolandırıcılıkta kişi kendi rızasıyla, gönüllü olarak eylemi gerçekleştirir.
- Ör: Fakir birine yardım etmek için bir hesap numarasına para yatırmanızı isteyen bir e-mail, internet üzerinden alışveriş yapan bir sitenin parayı aldıktan sonra hizmeti vermemesi, "Get Rich Quick" v.b

E-Banka Dolandırıcılığı

Genellikle şu teknikler kullanılmaktadır:

- Kullanıcının e-banka sistemine giriş için kullandığı kullanıcı adı şifre ve benzeri bilgileri ele geçirme
  - Phishing
  - Sosyal Mühendislik
  - Zararlı Kodlar:
    - KeyLogger
    - Screen Logger
    - Virüs, Truva atı v.b.
- Yönlendirmeler
  - DNS Saldırıları

Phishing

- İngilizce "Balık tutma" anlamına gelen "Fishing" sözcüğünün 'f' harfinin yerine 'ph' harflerinin konulmasıyla gelen terim, oltayı attığınız zaman en azından bir balık yakalayabileceğiniz düşüncesinden esinlenerek oluşturulmuştur.
- Kullanıcıya tuzak mailler gönderip, bir şekilde sahte bir linke (Örneğin Sahte E-banka sitesinin) tıklaması ve açılan siteye bir takım özel bilgileri vermesi şeklinde tanımlanabilir.
- Phishing ile ilgili Türkçe makale:

"Sanal Dolandırıcılıkta Son Nokta Phishing" http://www.iem.gov.tr/iem/?idno=147

Phishing Örnekleri - Garanti

Kimden: "garanti@garanti.com.tr" <java@wongfaye.com>
To: Yuzunay <yuzunay@ankara.pol.tr>
Subject: Saygili Musterimiz Garanti Bankasi

Saygili Musterimiz,

Farkli IP-adreslerden banka hesabiniza girmeye calisildigini tespit ettik. Seyahatteyken hesabiniza girmeye calistiysaniz bunun gibi hesap acma tesebbusleri buna bagli olabilir. Ancak hesabinizi acmak girisiminde bulunmadiysaniz hesabinizla ilgili bilgilerin kontrol edilmesi icin en acil sekilde bankaniza basvurmanizi teklif ederiz.

http://www.garantlbank.com

Sabiriniz icin tesekkur ederiz.

Saygilarimizla,

Garanti Bankasi

Phishing Örnekleri - Garanti

Yıkıcı Siber Suçlar

- Ağ sistemlerini etkisiz kılma, veriye zarar verme veya yoketme gibi maksatlarla işlenen siber suçlardır.
  - Zararlı Kodlar
    - Virüsler
    - Truva Atları
    - Kurtçuklar
  - DoS saldırıları
  - Crack ve Hack saldırıları

Diğer Şiddet İçermeyen Siber Suçlar

- İnternet üzerinden fahişelik servisi verme veya fahişelik reklamı yapma
- İnternet Üzerinden Kumar
- İnternet Üzerinden ilaç, uyuşturucu madde satımı
- Siber Kara Para Aklama
- Siber Kaçak Mal

Türkiye'de
En Sık Karşılaşılan Suçlar

- Çocuk pornografisi (175 dosya, 2005 yılı ilk 8 ay)
- E-Banka Dolandırıcılığı
- Sitelere Yetkisiz Erişim
- İnternet Üzerinden Hakaret, Konuşma
- Kredi Kartı Dolandırıcılığı
- Yasadışı Yayınlar

Çocuk Pornografisinin Hacmi

- Son yıllarda Çocuk Pornografisi Sanayisinin, uluslar arası ve ticari yönden oldukça büyük bir sanayi olduğunu söyleyebiliriz. Amerika'da çocuk pornografisinin, yıllık yaklaşık 2-3 milyar dolar hacme sahip büyük pazarlardan biri olduğu belirtilmektedir

  (John Carr, "Theme Paper on Child Pornography for the 2nd World Congress against the commercial sexual exploitation of Children)

- John Hopkins Üniversitesinin Koruma Projesine göre, bazı toplumlarda çocuk trafiği çok yüksek seviyelerde seyretmektedir. Elde edilen verilere göre,
  - Indiana'da 14 yaşındaki 200.000 Nepali kızının seks kölesi olarak çalıştırıldığı,
  - Sri Lanka'da yaşları 6 ila 14 arasında değişen 10.000 çocuğun geneleve düştüğü,
  - 600.000 Taylandlı çocuğun fahişelik için satıldığı ve
  - 1991-97 arasında Komboçyalı 15.000 kızın cinsel kölelik için satıldığı tespit edilmiştir

5237 sayılı Yeni Türk Ceza Kanunu

- *Madde 226: Müstehcenlik*
  - *Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır*

  - Detaylı Bilgi ->

"İnternet Üzerinden Çocuk Pornografisi ve Mücadelede Yaşanan Sıkıntılar"
Y. Uzunay, M. Koçak, Polis Bilimler Dergisi, Cilt 7 Sayı 1, ss.97-116, ANKARA , 2005
www.ankara.pol.tr/html/bilisim/belgeler
www.ankara.pol.tr/yusufuzunay

Bilişim Suçlarının Türk Ceza Kanunundaki yeri

Bilişim Suçları ile ilgili maddeleri Türk Ceza Kanunu açısında iki grupta toplayabiliriz:

- Salt bilişim suçu olarak nitelendirilenler
- Salt bilişim suçu olarak nitelendirilemeyenler

Salt bilişim suçu olarak nitelendirilenler

- Salt bilişim suçu olarak nitelendirebileceğimiz suçlar 5237 sayılı yeni Türk ceza kanununun "Bilişim Alanında Suçlar" başlıklı bölümünde yer almıştır:
  - Madde 243: Bilişim Sistemine Girme
  - Madde 244: Sistemi engelleme, bozma, verileri yok etme veya değiştirme
  - Madde 245: Banka veya kredi kartlarının kötüye kullanılması

Madde 243: Bilişim Sistemine Girme

- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.
- (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.
- (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Madde 244: Sistemi engelleme, bozma, verileri yok etme veya değiştirme

- (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.
- (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.
- (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.
- (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.

Madde 245: Banka veya kredi kartlarının kötüye kullanılması

- (1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adli para cezası ile cezalandırılır.
- (2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

Türkiye'de Bilişim Suçları ile Mücadele

- Genellikle kolluk kuvvetleri tarafından yürütülmektedir.
  - İl Emniyet Müdürlükleri Bilişim Suçları Büro Amirlikleri
  - Kaçakcılık Daire Başkanlığı Yüksek Teknoloji Suçları Birimi
  - Kriminal Daire Başkanlığı Bilişim Suçları Birimi

Mücadelede Karşılaşılan Uluslar arası Problemler

- Uluslar arası alanda ilgili birimler arası işbirliği eksikliği
- Ülkelerde değişiklik gösteren kanunlar ve uluslar arası ortak kanunların yetersizliği
- Birçok farklı sınıflandırma ve tanımın olması
- Zaman senkronizasyonu problemi

Tanım Farklılıkları

- Çocuk Pornografisi alanında:
- Tanımlamalara bakıldığında çoğunda, temel olarak "çocukları veya küçükleri içeren cinsel eylemi temsil eden görüntü veya figürler" ifadesine benzer ifadelere rastlanılmaktadır.
- Fakat özellikle bazı noktalarda belirgin farklar olduğu da göze çarpmaktadır. Örneğin; çocuk pornografisi kapsamında bazı tanımlar, çocuğu temsil eden her türlü görsel ve sesli materyali içerirken, bazı tanımlara göre resimler, çizimler ve çizgi filmler çocuk pornografisi kapsamına alınmamaktadır. Bu da çocuk pornografisi suçunun sınırlarının, tam olarak belirlenememesi anlamına gelmektedir.

Türkiye'de Bilişim Suçları ile Mücadelede Karşılaşılan Problemler

- Servis sağlayıcıların belirli bir süre log tutma zorunluluğunun olmaması
- İnternet Kafeler, Kablosuz erişim noktaları gibi ortak kullanım alanlarından internete girişlerde herhangi bir kimlik denetim mekanizmasının olmaması
- Bilişim suçları ile mücadelede kanunların yetersiz kalması
- Hukukçuların konu hakkında yeterli teknik düzeyde bilgiye sahip olmaması
- Dijital Deliller ve delillendirme ile ilgili sıkıntılar ve hukuki problemler
- Bilişim suçları boyutunda kolluk kuvvetleri dışında özellikle üniversitelerimizde yeterli oranda bilimsel çalışma yapılamaması
- Bilişim suçları ile ilgili merkezi bir birimin olmayışı ve çalışmaların dağınık bir şekilde yürümesi
- Vatandaşımızın konu hakkında yeterli düzeyde bilgiye sahip olmayışı
- Teknik altyapı yetersizliği ve Güvenlik & Mahremiyet çelişkisi

SON SÖZLER

- Bilişim Suçlarıyla mücadelede sadece polisin yaptığı çalışmalar değil diğer unsurlar da oldukça önemlidir.
- Kanun Koyucular uygun kanunlar oluşturmalıdır.
- Bilişim Camiası ve Toplum hem kendilerini bu tip suçlara karşı koruyacak önlemler almalı hem de bilişim suçları ile ilgili konulara çok dikkatli olup, şüphelenecek bir durum söz konusu olduğunda yetkililere haber vermelidir.
- Bilişim Uzmanları suçların teknik boyutunda daha çok çalışmalar yapmalı ve özellikle dijital delillerin toplanması, korunması, kurtarılması, analiz edilmesi, doğrulanması ve sunulmasında kullanılabilecek programlar üretmeli ve konu ile ilgili birimlere teknik destek sağlamalıdır.

DOLANDIRICILIK VAKA ANALİZLERİ

- MSN
- Cep Telefonu
- Para Aklama
- Sahte SMS
- Sahte E-mail
- Kredi Kartı
- Online Bankacılık

SON SÖZLER

- Üniversitelerde bilişim suçları, adli bilişim gibi konularda merkezler, çalışma grupları, bölümler, uzmanlık eğitimleri açılmalı ve bilimsel alandaki son gelişmeler takip edilip, ülke içindeki bilişim suçları ile ilgili çözülemeyen ve sıkıntılı olan konular üzerine çalışmalar başlatmalı ve standart prosedürler belirlemelidir.
- Devlet yapılan bütün çalışmaları organize etmeli, ülke genelinde konu ile ilgili çalışanları maddi ve manevi desteklemeli ve uygun kanunların çıkarılması için komisyonlar oluşturmalıdır. Ayrıca Suçların koordinasyonunun sağlanması açısından merkezi bir birim oluşturulmalıdır.

SON SÖZLER

- Kanun adamları kendilerini bilişim suçları ve özellikle dijital delilller konusunda eğitmeli, bu suçlara karşı dava kazanabilecek yeterliliğe sahip olmalıdır. Örneğin hukuk fakültelerine bilişim suçları ile ilgili dersler getirilmelidir.
- Mahkemeler bilişim suçlarına karşı adil ve etkili cezalar verebilmelidir.
- Sivil Toplum örgütleri bilişim suçları ve bu suçlar içerisinde özellikle çocuk pornografisi gibi kritik öneme sahip konularda çalışmalı, halkımızı daha çok bilgilendirmelidir.
- Medya, bilişim suçları, bu suçlardan korunma yolları ve suç esnasında yapılabilecek şeyler konusunda programlar yapmak suretiyle vatandaşımızı eğitebilir. Aynı zamanda konu hakkında daha fazla çalışılması gerektiğini vurgulayabilir.

SORU-CEVAP

Teşekkürler

Derleyen

Serkan KAMBER

Trabzon | 2008

Kaynak: Yusuf Uzunay yuzunay@ii.metu.edu.tr