Yasalar ve Bilişim Etiği

Ahmet Haşim Yurttakal

İçerik

- Etik
- İnternet Mimarisi Yönetim Kurulu
- Bilgisayar Korsanları
- Bilişim Suçları
- Kanun Türleri

Kurumsal Bilgi Güvenliği ve Bilişim Hukuku kitabından hazırlanmıştır.

ETİK

Etik

- Etik, ahlak felsefesidir. Etik, insanın bütün davranış ve eylemlerinin temelini araştırır.
- Etik → iş hayatı
- Ahlak → sosyal yaşam

Etik Yaklaşımlar

Meta Etik

- Etiğin doğasını, neden etiğe ihtiyaç duyduğumuzu araştırır.
- Eleştireldir.
- İyilik nedir? Bir şeyin iyi veya kötü olduğunu nasıl söyleyebiliriz?

Normatif Etik

- Pratik ahlak kuralları, ahlaklı bir hayatın nasıl yaşanacağı ile ilgilenir
- Kuralcıdır.
- Şu gibi durumlarda ne yapmalıyız? Doğru olması gereken şeyler nelerdir?

Uygulamalı Etik

- Normatif etik kurallarını spesifik meselelere uygular . Bilişim Etiği, Mühendislik Etiği gibi
- Betimleyicidir.
- Bir eylem gerçekleştirirken doğru yol nedir?

Etik Kuramlar

Teolojik

- Sonuçsalcıdır, Geniş bakış açısına sahiptir
- Sonuçların araçları meşrulaştırdığını öne sürer. Eylem sonuçta faydalı ise süreç içindeki bazı kötü şeyler göz ardı edilebilir.
- En bilinen kuram faydacılık.

Deontolojik

- Eylemlerin sonuçları değil, eylemin kendisi üzerinde durur
- "Sana nasıl davranmasını istiyorsan sen de öyle davran" "Eğer herkes böyle yaparsa ne olur?"
- İnsan hakları evrensel beyannamesi bu etik anlayışın somut bir göstergesidir.
- En bilinen kuram Kantçılık.

Yasa ve Etik

- Çoğunlukla yasalar etik kurallardan çıkarılır fakat etik olan her şeyi yasalara yansıtmak mümkün değildir.
- Bazı şeyler yasalara uygun olmasına rağmen etik olmayabilir.
- Bilişim konusunda bilgisayar korsanlığı, dosya paylaşımı, internetin demokratik olup olmaması, lisanslamalar sıklıkla tartışılan konulardır.

Bilgisayar Etikleri Enstitüsü (Computer Ethics Institute)

1. Bilgisayar başka insanlara zarar vermek için kullanılamaz.
2. Başka insanların bilgisayar çalışmaları karıştırılamaz.
3. Bilgisayar ortamında başka insanların dosyaları karıştırılamaz.
4. Bilgisayar hırsızlık yapmak için kullanılamaz.
5. Bilgisayar yalan bilgiyi yaymak için kullanılamaz.
6. Bedeli ödenmeyen yazılım kopyalanamaz ve kullanılamaz.
7. Başka insanların bilgisayar kaynakları izin almadan kullanılamaz.
8. Başka insanların entelektüel bilgileri başkasına mal edilemez.
9. Kişi yazdığı programın sosyal hayata etkilerini dikkate almalıdır.
10. Kişi, bilgisayarı, diğer insanları dikkate alarak ve saygı göstererek kullanmalıdır.

İNTERNET MİMARİSİ YÖNETİM KURULU (IAB)

İnternet Mimarisi Yönetim Kurulu

- İnternet Mimarisi Yönetim Kurulu (Internet Architecture Board-IAB) İnternet'in tasarımı, yönetimi, ve mühendisliğinin koordinasyonunu sağlar.
- İnternet'in geliştirilmesi varlığını sürdürmesi için oluşturulmuş bağımsız teknik bir komitedir.
- IETF (Internet Engineering Task Force) ve IRTF (Internet Research Task Force) olmak üzere 2 alt komisyonu vardır.
- Bu birimler İnternet'in etik kullanımıyla da ilgilenirler.
- İnternet'in korunması için federal birimlerle çalışır
- Yeni teknolojiler, metotlar, prosedürler geliştirir.

IAB Belirlediği Etik Kurallar

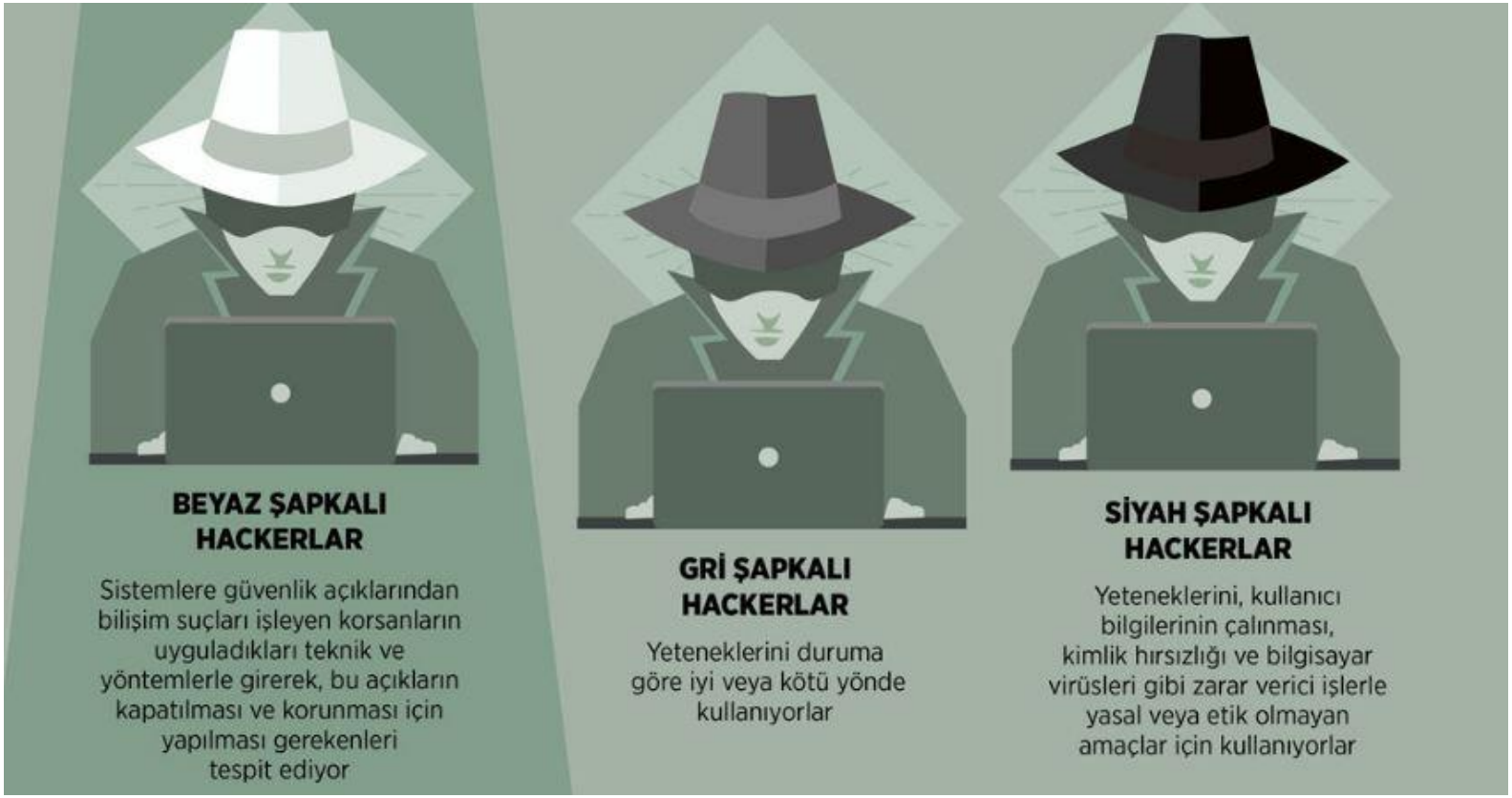
- Bilerek İnternet üzerinde yetkisi olmayan kaynaklara erişilmeye çalışılması
- İnternet'in kullanımını kesintiye uğratmak
- İnsan, bilgisayar veya kapasite kaynaklarını bilerek boşa harcamak
- Bilgisayar kaynaklı bilginin bütünlüğünün bozulması
- Başkalarının gizliliğinin ihlal edilmesi

KORSANLAR

Motivasyon, Fırsat, Suç İşleme

- Motivasyon: Suçun kim tarafından ve neden işlendiği ile ilgilenir. Şöhret, heyecan, ekonomik, ailesinin hastalığı veya diğer sıkıntılar
- Fırsat: Suçun nerede ve ne zaman olduğu ile ilgilenir. Bazı açıklıklar ortaya çıktığında olur. Güvenlik duvarının etkin olmaması gibi. Erişim Kontrolü, yetkilendirme, izleme mekanizması
- Suç İşleme: Suçun başarılı olması için gerekli yeteneğe bağlıdır.

Bilgisayar Korsanları, Saldırganlar



Organize Hackerlar - siber suçlular, hacktivistler, teröristler ve devlet destekli hackerlar örgütleri, script kiddies

İç ve Dış Tehditler

- İç Güvenlik Tehditleri
  - Çalışan veya sözleşme ortağı olabilir
    - Gizli verileri yanlış ele alma
    - İç sunucuların veya ağ altyapısı aygıtlarının işlemlerini tehdit etme
    - Virüs bulaşmış USB ortamını kurumsal bilgisayar sistemine bağlayarak dış saldırıları kolaylaştırın
    - Kötü amaçlı e-posta veya web siteleri aracılığıyla kötü amaçlı yazılımları ağa yanlışlıkla davet edin
    - Doğrudan erişim nedeniyle büyük hasara neden olabilir
- Dış Güvenlik Tehditleri
  - Ağ veya bilgi işlem aygıtlarındaki güvenlik açıklarından yararlanma
  - Sosyal mühendisliği kullanarak erişim elde edebilme

Siber Savaş

- Düşmanlara, uluslara veya rakiplere karşı avantaj elde etmek için kullanılır
  - Diğer ulusların altyapısını sabote edebilir
  - Saldırganlara devlet personeline şantaj yapma olanağı verir
  - Vatandaşlar hükümetin onları koruma yeteneğine olan güvenini kaybedebilir.
  - Hedeflenen ulusu fiziksel olarak işgal etmeden vatandaşların hükümetlerine olan inancını etkiler.

Örnekler

- 2010 yılında İran'ın Buşehr ve Natanz'daki nükleer tesislerine Stuxnet zararlı yazılımı ile saldırı yapılmıştır.
  - İnternete kapalı bir ağa, o şehirde ücretsiz dağıtılan USB Bellek ile bulaştırılmıştır.
  - Windows İşletim Sistemi'nde o güne dek bilinmeyen 4 açık kullanılmıştır (Zero Day)
  - Birkaç kişilik grubun 1-2 yıllık çalışması sonucu olduğu tespit ediliyor
  - Elektrik motorunun sınır değerlerinin çok üstünde çalıştırılması sağlanarak fiziksel zarar veriliyor

Örnekler

- 2014 yılında Mandiant firmasının yayınladığı rapora göre ABD'nin 20 sektöründeki 141 şirketin terabaytlarca bilgi çalındı.
- 2015 yılından itibaren fidyecilik ataklarında artış görülmüştür.
- 2007 yılında Estonya'ya yapılan siber saldırı ile ülkenin e-devlet,e-bankacılık,e-ticaret siteleri çökertilmiş. 30Mbps olan dışarıya çıkış İnternet hattı DOS ile devre dışı bırakılmıştır. AB ve NATO'dan yardım istemiştir.
- Talinn'de NATO Siber Güvenlik Mükemmeliyet Merkezi kurulmuştur.
- 2008'de Gürcistan'nın Güney Osetya'yı işgali üzerine siber saldırı olmuştur.

Örnekler

- Duqu, Flame gibi kritik yapılar
- 2016'da Brexit ve ABD Başkanlık seçimleri, Cambridge Analytica
- Yapay Zeka kötü niyetli kişiler tarafından kullanılırsa, suç işlerse?
  - Cihaza mı, Kontrol Eden Kişiye mi, Geliştiricisine mi ceza verilmeli

BİLİŞİM SUÇLARI

Bilişim Suçları-İşlem Güvenliği

- Küsüratlar Tekniği
  - Küçük suçlar farkedilmeden büyük kazanç sağlayabilir. Banka örneği
- Script Kiddies
  - Hazır programlar kullanır, derinlemesine bilgisi yoktur. Sonuçları öngöremez. Sistemde bıraktığı izlerle yakalanır.
- Veri Değiştirme
  - Sisteme yanlış bilgi girme. 1997'de Taco bell işçicisi kasiyer programını 2.99$'lık girişi 2.98$ gösterdi. Yakalanıncaya dek 3600$ biriktirdi.

Bilişim Suçları-İşlem Güvenliği

- Fazla verilen haklar
  - Sadece okuma hakkı yerine tüm hakların verilmesi
- Parola yakalama
  - Parolanın başka bilgisayara gönderilirken yakalanması . Brute force
- Ortam dinlemesi
  - Tüm elektrik cihazları çalışırken dışarıya bir elektromanyetik sinyaller yayar. Bu sinyaller cihaz hakkında bilgi verir.

Bilişim Suçlarının Hukuki Takibi

- Bilişim alanında suçlar giderek artmakta
  - Suçun tanımı, takibi, yasalara uygun cezası verilmeli. Güvenlik zincirinde bazı eksiklikler nedeniyle mekanizma etkin değil.
- Sahte adres, botnet, izlerin sürülmez hale gelmesi, kurumdaki yetersiz güvenlik önlemleri, kayıtların tutulmaması, bilgi uzmanı olmaması, Yasalardaki belirsizlikler..

USOM

- NATO’nun kara, hava deniz, uzaydan sonra 5. operasyonel alanı siber alan
- BTK bünyesinde Ulusal Siber olaylara Müdahale Merkezi (USOM) kritik altyapıları anlık izleyerek saldırıları önlemeye çalışır.
- Siber Olaylara Müdahale Ekibi (SOME)

KANUN TÜRLERİ VE ANAYASA

Kanun Türleri

- Bilgisayar hukuku, medeni, ceza ve idari hukuk olmak üzere 3 kısma ayrılır.
- Medeni hukuk: Vatandaşların şahsi durumları, ailevi ilişkiler, miras gibi kuralları düzenleyen hukuk dalıdır. Cezalandırma para ödeme veya kamu hizmeti şeklinde olur.
- Ceza hukuku: Suç kapsamına giren eylemleri inceler. Genel ve özel ceza hukuku olarak ikiye ayrılır. Genel ceza bütün suçlar için geçerli ilkeler, özel ceza hukuku ülkenin kanunlarına göre suç görülen eylemler. Ceza hukukunda hapis cezası da verilebilir.
- İdari hukuk:idarenin kuruluşuna yapısına, işleyişine, idarenin yerine getirdiği işlevin düzenlenmesine yöneliktir.
- Korsanlar suç işlerken yasaların zayıf olduğu ülkeleri seçerler.

Fikri Mülkiyet Yasaları

- Diğerlerinden farklı olarak kimin suçlu veya suçsuz olduğuna bakmaz.
- Firmaların yada kişilerin fikri mülkiyet haklarını nasıl koruyacaklarını ve bu haklar ihlal edilirse neler yapılabileceğini belirler.
- Ana konu verilerin korunmasıdır. Verinin sahibi verileri korumak için önlem almak ihlali durumunda mahkemede göstermek durumundadır.
- Bir çalışanın firmasının şifreli özel bir dosya paylaşması durumunda, firma çalışanın bu konuda bilinçlendirildiğini ispat etmesi gerekir.

Ticari Sır

- Ticari işletmelerin ve firmaların rekabet etmesinde ve piyasadaki gücünü belirlemesinde önemlidir.
- Şirkete ait ürünün formülü, matematiksel model, programın kaynak kodu
- Kamuya açık olmayan, herkes tarafından erişilmeyen bilgilerdir.
- Şirket çalışanlarıyla veya firmalarıyla gizlilik anlaşması imzalar.

Telif Hakları

- Bir fikir veya eser üzerindeki mülkiyet hakkıdır.
- Kullanma, satışını yapma, kiralama, izinsiz kullanmasını, çoğaltılmasını mahkeme kararı ile önleme gibi haklardır.
- © Copyright, Her hakkı mahfuzdur
- Bilgisayar programları, arayüzler de telif hakları ile korunabilir.

Ticari Marka

- Bir marka bir ülkede ünlenirse kısa zamanda benzer isimde başka markalar çıkabilir.
- Bu durumda haksız rekabet marka tescili ile önlenebilir.

Patent

- Buluşu yapan kişi ile devlet arasında yapılan sözleşmedir.
- Patentin temelini oluşturan bilginin açıklanması karşılığında patentteki fikirlerin (14-17 yıl)kullanım hakkını buluşu yapan kişiye sunar.
- Patent gerçek bir mülkiyet gibi satılabilir, değiş-tokuş edilebilir.
  - Fikir kullanılabilir olmalı
  - Fikir basit bir formül, kural, teori, bilimsel ilke, doğa kanunu olmamalı
  - Mevcut durumun önemsiz bir uzantısı olmamalı
  - Yeniliğe sahip olmalı, yayınlanmamış olmalı

Yazılım Korsanlığı

- Yazılıma ait fikri mülkiyet hakkının ihlali yazılım korsanlığına girer.
- Yazılımların çoğu İnternetten lisansı kontrol ediyor. Güncellemede lisansı kontrol ediyor.
- Büyük yazılım şirketleri Software Protection Agency (SPA) kurdular.
- BSA (The Software Alliance) yazılım lisanslarını ve haklarını koruyan ABD merkezli bir şirket.

Türkiye'de Kişisel Verileri Koruma

- Türkiye gerek bireysel, gerek kurumsal, gerekse yönetimsel düzeyde veri işleyen teknolojilerin oldukça yaygın kullanıldığı bir ülkedir. Nitekim Türkiye'de yalnızca cep telefonu abonesi, İnternet ve Facebook kullanıcısı sayılarının incelenmesi bile bireysel düzeyde kullanım yaygınlığına kavrayabilmek için yeterlidir.
- Türkiye'de kişisel verileri dijital ortamda toplayan, kayıt eden, birbirleri ile ilişkilendiren ve üçüncü kişilere aktaran sistemler yaygın bir biçimde kullanılırken bu kullanımdan kaynaklı önemli "yan etkileri" ortadan kaldırmaya yönelik olan kişisel verilerin korunması alanında hukuksal düzenlemelerin yetersiz olduğu belirtilmelidir

Türkiye’de Kişisel Verileri Koruma

- 2013 yılında Türkiye Cumhuriyeti Devlet Denetleme Kurulunun (DDK) yayınladığı bir raporda, kişisel verilerin korunması ve veri güvenliğinin sağlanmasında önemli eksiklikler bulunduğu çarpıcı bir biçimde ortaya konmuştur.
- DDK'ya göre : Seçmen niteliğine sahip 50 milyonun üzerindeki vatandaşın, adı, soyadı, ana ve baba adı, doğum yılı, doğum yeri, adres bilgisi seçimlere girme yeterliliğini taşıyan onlarca partiyle paylaşılmaktadır.
- Paylaşılan elektronik ortamdaki verilerin çoğaltılmasını ve başkalarıyla paylaşılmasını engelleyecek hiçbir mekanizma öngörülmemiştir. Bu verileri alan partilerin bu verileri koruma yeterlilikleri ve almaları gereken önlemler konusunda da herhangi bir belirleme yapılmamıştır

Türkiye'de Kişisel Verileri Koruma

- Denetim çalışmaları sırasında ayrıca hassas veri içeren sistemlere erişimde kullanıcılara iki haneli sayısal şifre verilebildiği, 1111, 0000, 1234 gibi kolay tahmin edilebilir şifrelerin kullanıldığı; bazı kurumların çağrı merkezinden sadece ad, soyad ve T.C. kimlik numarası beyan edilerek maaş tutarları, gidilen sağlık kurumu, muayene olunan doktor, alınan ilacın adı, ödenen katılım payı miktarı gibi birçok kişisel bilgiye ulaşılabildiği saptanmıştır

Türkiye Cumhuriyeti Anayasası

- Devletin temel amaç ve görevleri arasında insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak (5. madde)
- Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir (20. madde)

Milletlerarası antlaşmalar

- “**Usulüne göre yürürlüğe konulmuş Milletlerarası antlaşmalar kanun hükmündedir**”.(90. madde) dolayısıyla Türk hukuk sisteminde uluslararası antlaşmalar iç hukuk sisteminin bir parçasıdır.
- “Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda **milletlerarası antlaşma hükümleri** esas alınır.
- Kişisel verilerin korunması anayasal temelini 20. maddedeki doğrudan düzenleme yanında, dolaylı olarak Anayasanın 90. maddesinde de bulmaktadır.
- Bu hükümler Avrupa İnsan Hakları Mahkemesi (AİHM) tarafından belirlenir.

TCK’nin 135. maddesi

- Hukuka aykırı olarak kayıt eden kimseye **bir** yıldan **üç** yıla kadar **hapis cezasının** verilmesi öngörülmüştür.
- Kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına ve sendikal bağlantılarına ilişkin bilgileri hukuka aykırı olarak kaydeden kimse de aynı yaptırım ile cezalandırılacaktır.

TCK’nin 136. maddesi

- Kişisel verileri, hukuka aykırı olarak **bir başkasına veren**, **yayan** veya **ele geçiren kişi**, **iki** yıldan **dört** yıla kadar hapis cezası ile cezalandırılır.

TCK’nin 138. maddesinde

- Kanunların belirlediği **sürenin geçmiş olmasına karşın** verileri sistem içinde **yok etmek**le yükümlü olanlara görevlerini yerine getirmediklerinde **bir** yıldan **iki** yıla kadar hapis cezası verilir.

SON