Bilişim Hukuku

3 – Bilişim Suçları

Bilişim Suçu Nedir?

- Bilişim alanındaki gelişmelere paralel artış gösteren ve teknolojinin yardımı ile genellikle sanal bir ortamda kişi veya kurumlara maddi veya manevi zarar verecek davranışlarda bulunmaktır.

- Bilişim suçu, bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suçtur.

Bilişim Suçu Nedir?

- Bir bilgisayarda ya da bilgisayar olarak nitelendirilememesine rağmen veri-iletişimi sağladığı için bilişim alanının unsurlarından olduğu kabul edilmesi gereken diğer elektronik, manyetik, mekanik araçlar üzerinde
- örneğin,
  - cep telefonları,
  - üzerindeki web paneli sayesinde ağa bağlanıp bilgi aktarımı yapabilen elektronik ev aletleri,
  - üzerinde yüklü programlar aracılığıyla şifreli yayınları alan, bunları işleyen ve bunlardan sonuç çıkaran dekoderler

- veya bunları veri-iletişimi için birbirine irtibatlayan soyut veya somut bir ağ üzerinde gerçekleştirilebilir eylemler

Siber Suç Nedir?

- Siber uzay ortamında işlenen suç
- Bilgisayarlar aleyhine veya bilgisayarlar aracılığıyla işlenen suç
- Bilgisayarın amaç veya araç veya her ikisi olarak kullanıldığı hukuka aykırı eylem

Siber Suç Nedir?

- Herhangi bir suçun elektronik ortam içerisinde işlenebilme imkânı bulunuyor ve bu ortam içerisinde gerçekleştirilen fiil, genel olarak hukuka aykırı veya suç olarak tanımlanabiliyorsa bu suçları siber suçlar olarak değerlendirebiliriz.

- Siber suç, bilgisayar veya ağ sistemleri yolu ile bilgisayar veya ağ sistemleri içerisinde ya da bilgisayar ve ağ sistemlerine karşı işlenebilir.

Siber Suç Nedir?

- Siber suç kavramıyla bilişim suçları ifade edilmekle birlikte, bilişim suçlarının tek bir bilişim sisteminde işlenen şekli değil, bilişim sistem ağları vasıtasıyla (özellikle internet) işlenen suçlar kastedilmektedir.

Klasik Suçlardan Farkları

- Bilişim suçlarını ve siber suçları klasik suçlardan ayıran en önemli etken işlenme şekilleridir.

- Klasik suç tiplerinde suçun maddi unsurunu oluşturan eylemler faillerin fiziki hareketleriyle meydana gelmektedir.

- Bilişim suçlarında (siber suç veya internet ortamında işlenen suçlar) ise, genellikle failin bilgisayarın klavyesine dokunması veya mouse tıklaması dışında fiziki hareket olmamakta ancak fiziki hareketlerle meydana getirilebilecek zararlardan çok daha fazlası bu şekilde oluşabilmektedir.

Klasik Suçlardan Farkları

- Bilişim alanındaki suçlar, bilinen, klasik usullerin dışında çok daha hızlı, kolay ve dikkatlerden uzak işlenebilmekte, tespit edilebilmesi ise daha zor olmaktadır.

- Bu tür suçlar, sadece çıkar amaçlı yapılmamakta; kimi zaman da toplumda aradığını bulamayan insanların, kendilerini ispat için başvurdukları bir yol olabilmektedir.

Klasik Suçlardan Farkları

- Bu gün bilişim suçlarının büyük bir kısmı internet ortamı aracılığıyla gerçekleştirildiğinden, fiiller de daha ziyade amaçlanan işi yerine getirmeye yönelik olarak yapılmış "yıkıcı yazılımlar" adı verilen programlar üzerinden yapılmaktadır.

- Bu yazılım ya da tekniklere her gün yenileri eklenmekle birlikte, şu ana kadar sık rastlananlardan hareketle, örnek olarak
  - sistem güvenliğinin kırılıp içeri girilmesi (hacking),
  - salam tekniği,
  - Truva atı (trojan horse),
  - ağ solucanları (Network worm),
  - tavşanlar (rabbits),
  - bukalemunlar (chamelon),
  - mantık bombaları (logic bombs),
  - virüsler,
  - çöpe dalma,
  - gizli dinleme,
  - veri aldatmacası v.s. verilebilir

Truva Atı

- Bilişim alanında en sıklıkla rastlanan suç işleme yöntemi olan **Truva atı yazılımı**, Truva savaşında kullanılan tahta atın hediye olarak Truvalılara gönderilip, tahta at kalenin içine girdikten sonra atın içine gizlenen düşman askerlerinin kaleyi ele geçirmelerindeki mantık ile çalışmaktadır.

- Bunlar internet üzerinden veya e-posta yoluyla bilgisayarlara sızan ve kullanıcı farkına varmadan kendi kendilerine internete bağlı olunduğu anlarda dışarıya veri gönderen programlardır.

Truva Atı

- Çoğunlukla internet üzerinden ücretsiz indirilen yazılımlardaki sistem dosyaları içine, Truva atı yazılımı eklenerek kullanıcılara ulaştırılmaktadır.

- Bu yazılımı bilgisayarına yükleyen kullanıcı, görünüşte yararlı olan yazılımı bilgisayarına kurduğunda Truva atı yazılımı da kendisini fark ettirmeden çalışmaya başlamaktadır.

Mantık Bombaları

- Truva atı metodunun bir türüdür.
- Bunlar, bilgisayar sistemini şaşırtmak, bozmak veya felç etmek için programlanmaktadır ve bunu gerçekleştirmek için, bilgisayara ya mantık dışı ya da yapılan işlemin aksine sürekli bilgi göndermektedir.
- Mantık bombaları, bilişim sistemlerinde veya ağlarında, daha önceden belirlenmiş özel durumların gerçekleşmesi durumunda zarar verici sonuçlar oluşturur.
- Bir mantık bombası, belirlenmiş özel durum gerçekleşene kadar ‘Truva atı’ programı gibi davranır.
- Ancak özel durumun gerçekleşmesinden sonra bilişim sisteminde zararlı etkisini meydana getirir ve bu noktada her zaman kendisini gizli tutmaya çalışan Truva atı programından ayrılır.

Ağ Solucanları

- Virüs gibi kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır.
- Bunu otomatik olarak yaparlar.
- Bellek veya ağ bant genişliğini tüketirler.
- Kullanıcının etkisi olmadan kendi kendine çalışabilen ve aynen kendisi gibi bir kopyasını, veri iletim ağına bağlantısı olan diğer bilişim sistemlerine kopyalayabilen yazılım türlerine verilen genel addır.
- Bir iletişim ağındaki sistemler arasında herhangi bir donanım veya yazılıma zarar verme zorunluluğu olmaksızın dolaşırlar.

Ağ Solucanları

- Ağ üzerinden bir bilişim sistemine gelen bir ağ solucanı, ya bir virüs gibi davranarak yazılıma zarar verir ya da sisteme bir Truva atı bırakır.
- Çoğu zaman ise iletişim ağında çalışan sistem operatörlerine yakalanmamak için bıraktıkları tüm izleri silerler.
- Solucanlar, bilgisayarın hafızasına yerleşen ve hafıza kısmı yokmuş gibi davranarak sürekli olarak kendilerini buraya yazan yazılımlardır.

Tavşanlar

- Çok hızlı üreyen, kısa zamanda kolonileşerek bilişim sisteminin bilgi işleme gücünü azaltan, bilgisayara veya bilişim sitemine durmaksızın gereksiz işler yapması için komut veren bir yazılımdır.

- Bunlar, işlemciye sürekli anlamsız komutlar vererek işlemcinin bilişim sisteminin normal işleyişini sağlayan komutlarını vermesini engellemekte ve giderek sistemin yavaş çalışmasına ve en sonunda da sistemi çalışamaz hale gelmesine sebep olurlar.

Tavşanlar

- Tavşanlara örnek olarak şu olay verilebilir.
- Büyük bir şirketten atıldığı için sinirlenen bir programcı, giderken şirketin bilgisayarına 400 byte'lık, tek işlevi kendinin tam bir kopyasını yapmak olan *"Sarmaşık"* adında bir program bırakır.
- Program işten çıkarılan programcının ayrılmasından 24 saat sonra uyanır, kendini kopyaladıktan sonra tekrar uyur.
- Bir gün sonra *Sarmaşık'ın* iki kopyası kendilerini tekrar kopyalar ve bu işlem her gün katlanarak sürüp gider.
- İki hafta sonunda şirket bilgisayarının yan işlevlerinde gecikmeler ve bariz hatalar olmaya başlar.

Tavşanlar

- Artık belleği *sarmaşık'ın* tıpatıp aynı kopyasını barındırmaktadır, (yani 6,5 milyon byte'lık bir çöplük)
- 2 gün sonra ise bilgisayar hiçbir şey yapamaz hale gelir.
- Çünkü belleğini *sarmaşık'ın* yarım milyondan fazla kopyası kaplamıştır.
- Görüldüğü gibi çok küçük ve basit işlevli bir program, çok kısa bir sürede kendisini fark ettirmeden büyük bir şirketin bütün sistemini çalışamaz hale getirmiştir.

Bukalemun

- Sistem için normal çalışan ve zararsız bir yazılım gibi duran ve onun niteliklerine sahipmiş gibi görünen yazılımlar, Truva atlarının yakın akrabalarıdır.

- Bir bukalemun her defasında çok kullanıcılı bir sistemde kullanıcı adları ve şifreleri için giriş iletilerini taklit edecek şekilde dâhiyane bir şekilde programlanır.

- Sisteme giren bütün kullanıcıların adlarını ve şifrelerini gizli dosyaya kaydeder, daha sonra sistemin bakım için geçici süre kapatılacağına ilişkin bir mesaj verir.

Salam Tekniği

- Çok fazla sayıda kaynaktan, çok az sayıda değerin transferini esas alır.

- Bu yöntem özellikle bankaların bilişim sistemlerinde gerçekleştirilen hukuka aykırı yarar sağlama suçları için kullanılan etkin bir tekniktir.

- Sistemin esası çok fazla kaynaktan (örneğin çok sayıda banka hesabından) kaynak bağışına çok az miktarda hukuka aykırı yarar sağlanması esasına dayanır.

Salam Tekniği

- Bu yöntemde, hesaplardaki rakamların virgülden sonraki küsuratlarının ya son rakamı ya da son iki rakamı yani kuruşlar failin belirlediği bir hesaba aktarılarak orada biriktirilmektedir.

- Böylelikle banka ya da hesap sahipleri hesaplarda meydana gelen yetkisiz hareketi fark edememekte, ancak küçük miktarların çok sayıda kaynaktan toplanmış olması fail açısından büyük miktarda bir hukuka aykırı yarar sağlamaktadır.

Gizli Kapılar

- İşletim sistemleri veya çok işlevli kullanıcı sistemleri hazırlayan bilgisayar programcılarının bunları meydana getirirken ileride ortaya çıkabilecek durumlara göre, sistem şifrelerinde değişiklik yapabilmeyi veya yeni şifreler girebilmeyi sağlamak üzere sisteme bıraktıkları çeşitli giriş yollarına denmektedir.

- Bu mekanizmaların, program veya işletim sistemi tamamlandığında ortadan kaldırılması gerekir, ancak bazen ya hata sonucu veya ileride kullanılmak amacıyla bu mekanizmalar ortadan kaldırılmaz.

- Bu gibi durumlarda, bu kapılar kötü niyetli kişilerin yasadışı faaliyetlerine hizmet etmesi amacıyla kullanılır.

Hacking

- Hedefle ilgili keşif yapan korsanlar önemli bilgilere ulaşmakta ve bu verileri kullanarak internet üzerinden eylem gerçekleştirecekleri bilişim sistemine girmektedirler.

- Bilişim korsanları, ulaştıkları hedef sistemi tarayarak açık portları, işletim sistemini, çalışan servisleri, paylaşılan kaynakları ve kullanıcı isimlerini belirlemektedirler.

- Bu giriş genellikle bilişim sisteminin işletim yazılımını yazan kişilerin gerektiğinde yazılımı ve dolayısıyla sistemi korumak amacıyla bıraktıkları arka kapıları bularak buradan sızmak yoluyla gerçekleştirirler.

- Bu yolla sisteme sızan sanal korsanlar, bu andan itibaren sistemi çökertmektedirler.

- Sisteme sızmak için '*hacker'*ların kullandığı pek çok yöntem vardır.

- Şifre kurmak, ağı gözetlemek, oturum çalmak, tampon belleği taşırmak, DOS saldırıları yapmak bu yöntemlerden sadece bazılarıdır.

Bilgi Aldatmacası

- Bilgisayara yanlış veri girilmesi veya bazı verilerin kasten bırakılmasıdır.
- Böylece fail, bilgisayara girdiği veya bilgisayarda bıraktığı veriler ile mevcut veriler üzerinde istediği yönde değişiklik yapma veya cihazı istediği yönde kullanma imkânına kavuşmaktadır.
- Bu yöntem, bilişim sistemlerine yetkisiz veya yetkili müdahale imkânı olan kişilerce işlenebilir.
- Bunlar; verileri yaratan, kaydeden, işlenme esnasında nezaret eden, nakleden, kontrol eden, şifreleyen kişiler olabilir.

Çöpe Dalma veya Artık Toplama

- Herhangi bir bilgisayar sisteminin çalışmasından geriye kalan veri ve bulguların toplanması işlemidir.

- Bu bilgilerin elde edilme yöntemlerinden ilki, çıktı birimlerince kullanılan ve daha sonra çöpe atılan kâğıt, yazıcı şeridi vb. malzemeler üzerinde kalan bilgilerin toplanması yöntemidir.

- İkincisi ise bilişim sisteminin belleğinde bulunan ve artık ihtiyaç kalmayan silinmiş bilgilerin gelişmiş tekniklerle yeniden elde edilmesidir.

Gizlice Dinleme

- Bilişim sistemlerinin veri naklinde kullandığı ağlara girilerek veya bilişim sistemlerinin az da olsa yaydığı elektromanyetik dalgalar yakalanarak verilerin tekrar elde edilmesi tekniğidir.

- Bu teknik bilgisayar ekranlarının yaydığı elektromanyetik dalgaların yakalanması ve tekrar ekran görüntüsüne çevrilmesi suretiyle işlenebileceği gibi bilgisayarlar arasında veri naklinde kullanılan ağlara yapılan fiziksel müdahaleler sonucu, ağda nakledilen verilerin ele geçirilmesi şeklinde de işlenmektedir.

Süper Darbe

- IBM uyumlu yazılımlarda uygulanan ve disketten diskete programın kopyalanmasını önleyen “kopya koruma” programlarını atlatan bir program olarak ortaya çıkmıştır.
- Daha sonraları, bütün kontrolleri geçerek, sisteme müdahale eden programlar olarak tanınmıştır.
- İş dünyasında kullanılan bilgisayarların çoğunda hırsızlığa karşı bir koruyucu güvenlik sistemi vardır.
- Sistemin kilitlendiği durumlarda, en kısa zaman içinde yeniden çalışıp işlevsel olabilmeleri için “süper zap” programları kullanılmaktadır: bu programlar bir yandan sistemdeki çeşitli emniyet tedbirlerini aşarken, diğer yandan da meydana gelen sorunları süratli bir şekilde düzeltmektedir.
- Tüm güvenlik kontrollerini aşarak, sistemde değişiklikler yapabilmesi bu programın kötüye kullanılmasına neden olmakta ve program kullanıcısına hiçbir güvenlik kontrolüne uğramadan istediği değişiklikleri gerçekleştirme imkânı tanımaktadır.

Eşzamansız Saldırılar

- İşletim sistemlerinin eşzamansız olan çalışmasından yararlanır.
- Birçok sistemin, programları eşzamanlı yani aynı anda kullanamamasından hareket eden bazı failler, geliştirdikleri saldırı teknikleri ile, bilgisayar işletim sistemlerinde, daha doğrusu programdaki veriler üzerinde çeşitli ihlaller meydana getirmektedirler.
- Birçok işletim sistemi, uygulanan değişik bilgisayar programlarının fonksiyonlarını ifa etmek için eşzamansız olarak çalışırlar.
- Örneğin bir çıktı alınması sırasında bu işlem için çeşitli görevlerin sırayla çağrılması gerekir.
- İşletim sistemi bu istekleri bekletir ve kaynaklar ulaşılabilir hale gelince isteğe uygun olarak istek sırasına göre veya bir öncelik düzenine göre yerine getirir.
- İşte, bu bekleme sırasında iyi bir programlama bilgisine sahip bazı kimseler çeşitli rutin işlemler yardımıyla veriler üzerinde istedikleri doğrultuda değişiklik gerçekleştirebilmektedir.

İstem Dışı Alınan Elektronik Postalar - spam

- Pek çok kullanıcının bilişim sorunudur.
- İngilizce anlamı, *“baharatlı domuz yollamak”* olan “spamming”, bir kişiye ya da bir siteye gereksiz veya kaba çok fazla sayıda mektup göndermenin internet dilindeki karşılığıdır.
- Burada, aynı mesajın çok sayıdaki kopyasının bu tip bir mesajı alma talebinde bulunmamış kişilere, bir nevi zorlayıcı nitelikte gönderilmesi söz konusudur.
- Bu sözcük, ürünlerinin reklâmlarını internet aracılığı ile binlerce kişiye yollayan bazı firmaların kullandığı tekniği tanımlamak için de kullanılır.
- Spam, genellikle bir ürünün reklâmı, pazarlanması ve pornografik içerikli reklâm ve mesajların dünya çapında kitlelere ulaştırılması amacını taşımaktadır.

Kimlik Hırsızlığı

- Bir başkasının üçüncü şahısları ve bilgi işlem sistemlerini kendisinin söz konusu kişi olduğuna ikna ederek yanıltmasına, o şahsın çıkarlarına zarar verip kendisine çıkar sağlamasına, ya da bu dolandırıcılığa olanak verecek bilgilere ulaşmasına **“kimlik hırsızlığı”** veya **“kimlik avı”** denilmektedir.

- Birçok kişi bu suçluların nasıl evine bile girmeden bu bilgilere ulaştığına inanamaz.

Kimlik Hırsızlığı

- **Kimlik hırsızlarının başlıca yöntemleri:**
  - kimlik kartı, kredi kartı veya banka kartı çalmak,
  - posta kutusundan ya da çöp kutusundan belge çalmak,
  - cep telefonundan ya da bilgisayardan dosya kopyalamak,
  - acil bir telefonmuş gibi arayarak, **“annen kaza geçirdi”**, **“arabanız çalınmış”**, **“polis sizi arıyor”**, vb. şeyler söyleyerek karşıdaki kişinin paniğe kapılmasını sağlayıp kişisel bilgilerini istemek,
  - tam temizlenmemiş eski bilgisayar, eski disk, eski USB bellek ele geçirmek,
  - güvenilir bir web sayfasının (örneğin çalıştığınız bankanın) benzerini kurbana sunup kimlik bilgilerini o yolla vermesini sağlamak,

Kimlik Hırsızlığı

- bilgi işlem sistemlerinde korsanlık (hacker) yapmak,
- kimlik hırsızlığı amaçlı virüs yazıp bulaştırmak,
- internette kişisel bilgiler aramak ve toplamak,
- kimlik belge ve bilgilerini başkalarına çaldırtmak,
- kişisel şifre ve parolaları gizlice izlemek,
- yüz yüze veya telefonda kişileri kandırıp bilgi almak,
- namına adres değişikliği kaydettirip belgelerin korunmasız bir yere gönderilmesini sağlamak,
- kişinin bilinen bilgilerinden bilinmeyen bilgilerini tahmin etmek,
- gasp ya da zor kullanarak kimlik bilgilerine ulaşmak

Kimlik Hırsızlığı

- Kimlik hırsızlarına av olmaktan korunmanın yolları :
  - hassas kişisel bilgilerin neler olduğunu ve nerelerde bulunduğunu bilmek
  - bilgilere kimlerin normalde ulaşabildiğini bilmek
  - bilgileri kilit altında tutmak, şifrelemek
  - bellek malzemesini elden çıkarmadan önce tam silmek, yayınlamamak
  - yazarken elini gizlemek, gerekmiyorsa yazmamak, silmek, bulundurmamak, taşımamak
  - TC kimlik numarası, adresi, anne kızlık soyadı, vb. bilgileri almaya çalışacak kimlik hırsızlarına karşı tüm aile bireylerini bilinçlendirmek
  - bilgi taleplerine karşı temkinli olmak
  - kişisel bilgileri sadece güvenilir ve ilişkiler dolayısıyla ihtiyacı olan kişilere ve ihtiyaç olduğu kadar bilgi vermek
  - kişisel bilgilerin açık edilme riskinin fark edildiğinde önüne geçmek
  - açık edilmiş gizli bilgileri/kaybolan belgeleri bir an önce gerekli mercilere haber vermek ve değiştir(t)mek
  - emniyete giderek durumu belgeler ile birlikte anlatmak
  - dava açılmasını sağlamak