BİLİŞİM SUÇLARI

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.

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.

Bilişim Suçu Çeşitleri

- **Bilgisayar Virüsleri (Computer Viruses):**

- Bilgisayar virüsleri işletim sisteminin ve makine dilinin verdiği olanaklar kullanılarak yazılan, kendi kendisini çoğaltabilen, kopyalarını çeşitli yöntemlerle başka bilişim sistemlerine ulaştırarak bu sistemleri de etkileyebilen yazılımlardır.

Bilişim Suçu Çeşitleri

- **Reklam Yazılımı (Adware):**
- Bu programlar ana bilgisayarlara otomatik olarak reklam gönderir.
- Bilindik reklam yazılımı türleri arasında web sayfalarındaki açılır reklamlar ve genellikle "ücretsiz" yazılımlara eşlik eden program içi reklamlar yer alır.
- Bazı reklam yazılımları ise nispeten zararsızdır.
- Reklam yazılımları kişilerin bilgisi ve onayı dahilinde yüklendiğinden bu tür programlara genellikle kötü amaçlı yazılım denmez.
- Bunlar genellikle "olası istenmeyen programlar" olarak tanımlanır.

Bilişim Suçu Çeşitleri

- **Casus Yazılım (Spyware):**

- Casus yazılım, adından anlaşıldığı gibi bilgisayarınızda yaptıklarınızı takip eder.
- Tuş vuruşları, göz atma alışkanlıkları ve hatta oturum açma bilgileri gibi verileri toplar ve ardından genellikle siber suçlular olmak üzere üçüncü taraflara gönderir.
- Bilgisayarınızdaki belirli güvenlik ayarlarını da değiştirebilir veya ağ bağlantılarını kesintiye uğratabilir.

Bilişim Suçu Çeşitleri

- **Fidye Yazılımı (Ransomware):**

- Fidye yazılımları bilgisayarınıza virüs bulaştırır, ardından kişisel belgeler veya fotoğraflar gibi hassas verileri şifreleyip bunlar karşılığında fidye talep eder.

- Ödemeyi reddederseniz veriler silinir.

- Bazı fidye yazılımı varyantları bilgisayarınıza erişimi tamamen kilitler.

Bilişim Suçu Çeşitleri

- **Truva Atı (Trojan):**

- Genellikle meşru yazılım kılığındaki bir tür kötü amaçlı yazılımdır.
- Kullanıcılar genellikle kandırılarak Truva Atlarını sistemlerine yükler ve çalıştırırlar.
- Truva Atları etkinleştirildikten sonra siber suçluların sizi takip etmelerine, hassas verilerinizi çalmalarına ve sisteminize arka kapı erişimi elde etmelerine sebep olur.

    - Veri silme
    - Veri engelleme
    - Veri değiştirme
    - Veri kopyalama
    - Bilgisayarların veya bilgisayar ağlarının performansını düşürme

- Truva atları, diğer bilgisayar virüsleri ve solucanlarının aksine kendi kendilerine çoğalamaz.

Bilişim Suçu Çeşitleri

- **Truva Atı (Trojan):**

- Truva atlarının, verdiği zarara göre birçok çeşidi mevcuttur.

- **Arka kapı**

- Arka kapı Truva atı, kötü amaçlı kullanıcıların bilgisayarın kontrolünü ele geçirmesini sağlar. Yazarın virüslü bilgisayarda, dosya gönderme, alma, başlatma ve silme, veri görüntüleme ve bilgisayarı yeniden başlatma dahil olmak üzere istediği her işlemi yapmasına olanak tanır.
- Arka kapı Truva atları, genellikle bir grup kurban bilgisayarı bir araya getirerek suç işleme amacıyla yararlanılabilecek bir botnet veya zombi ağı kurmak için kullanılır.

Bilişim Suçu Çeşitleri

- **Truva Atı (Trojan):**

- **Girişim**
- Girişimler, bilgisayarınızda çalışan uygulama yazılımının barındırdığı güvenlik açığından faydalanan veriler veya kodlar içeren programlardır.

- **Rootkit**
- Rootkit'ler, sisteminizdeki belirli nesneleri veya etkinlikleri gizlemek üzere tasarlanmıştır. Bunların başlıca amacı, genellikle kötü amaçlı programların algılanmasını önleyerek programların virüslü bir bilgisayarda çalışacağı süreyi uzatmaktır.

- **Trojan-Banker**
- Trojan-Banker programları; online bankacılık sistemleri, e-ödeme sistemleri ve kredi veya banka kartı ile ilgili hesap bilgilerinizi çalmak için tasarlanır.

Bilişim Suçu Çeşitleri

- **Truva Atı (Trojan):**

- **Trojan-DDoS**

- Bu programlar, hedeflenen bir web adresine Hizmet Reddi (DoS) saldırıları düzenler. Bilgisayarınızdan ve diğer birçok virüslü bilgisayardan birden çok istek göndererek gerçekleştirilen saldırı, hedef adrese aşırı yüklenilmesine yol açarak hizmet reddine neden olur.

- **Trojan-Downloader**

- Trojan-Downloader'lar bilgisayarınıza Trojanlar ve reklam yazılımı gibi yeni kötü amaçlı yazılım programı sürümleri indirip yükler.

Bilişim Suçu Çeşitleri

- **Truva Atı (Trojan):**

- **Trojan-Dropper**
- Bu programlar, bilgisayar korsanları tarafından Trojanları ve/veya virüsleri yüklemek ya da kötü amaçlı programların algılanmasını engellemek için kullanılır. Tüm antivirüs programları, bu tür Truva atlarında bulunan tüm bileşenleri tarayamaz.

- **Trojan-FakeAV**
- Trojan-FakeAV programları, antivirüs yazılımının etkinliğini taklit eder. Bu programlar, bildirdikleri tehditler aslında var olmadığı halde, tehditlerin algılanması ve kaldırılması karşılığında kullanıcıdan para sızdıracak şekilde tasarlanmıştır.

- **Trojan-GameThief**
- Bu tür programlar, online oyuncuların kullanıcı hesap bilgilerini çalar.

Bilişim Suçu Çeşitleri

- **Truva Atı (Trojan):**

- **Trojan-IM**
- Trojan-IM programları; ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype ve benzeri anlık mesajlaşma programlarında kullandığınız oturum açma bilgilerini ve parolaları çalar.

- **Trojan-Ransom**
- Bu tür Truva atları, bilgisayarınızdaki verileri değiştirerek bilgisayarın doğru çalışmamasına veya belirli verilerin kullanılamamasına yol açar. Suçlu, fidye isteğinde bulunur ve ancak bu paranın ödenmesi karşılığında bilgisayar performansını eski haline getirir veya verilerinizin üzerindeki engeli kaldırır.

Bilişim Suçu Çeşitleri

- **Truva Atı (Trojan):**

- **Trojan-SMS**
- Bu programlar, cep telefonunuzdan özel ücretli telefon numaralarına kısa mesajlar göndererek para harcamanıza neden olabilir.

- **Trojan-Spy**
- Trojan-Spy programları, örneğin klavyeyi kullanarak girdiğiniz verileri izleyerek, ekran görüntüleri alarak veya çalışan uygulamaların listesini edinerek bilgisayarı nasıl kullandığınızla ilgili casus bilgiler toplayabilir.

- **Trojan-Mailfinder**
- Bu programlar, bilgisayarınızdaki e-posta adreslerini toplayabilir.

Bilişim Suçu Çeşitleri

- **Salam Tekniği (Salami Techniques):**

- Bu teknik çok fazla sayıda kaynaktan, çok az sayıda değerlerin transferini esas alır. Genel olarak, tekniğin uygulanmasında Truva atı programları kullanılır. Bu yöntem özellikle bankacılık alanında kullanılmaktadır.

Bilişim Suçu Çeşitleri

- **Tavşan (Rabbit):**

- 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.

Bilişim Suçu Çeşitleri

- **Gizli Kapılar (Trap Doors):**

- İşletim sistemleri normal şartlar altında yetkisiz şekilde girişe veya herhangi bir program ya da kod çalıştırmasına ve değiştirilmesine izin vermeyecek şekilde tasarlanmaktadır.

- İşletim sistemlerini ve programları hazırlayan programcılar, ilerde ortaya çıkabilecek durumlara karşı hatta bulma amacıyla kod ekleyebilmek veya ara program çıktısı alabilmek amacıyla programa istediğinde “trap doors” adı verilen durma mekanizmaları eklerler.

- Bu gizli kapıların program ve işletim sistemi tamamlandığında temizlenmesi gerekir. Ancak bazı durumlarda hata sonucu olarak ya da ileride kullanılmak amacıyla gizli kapılar kapatılmaz. Bu durumlarda gizli kötü niyetli kişiler tarafından kullanılabilmektedir.

Bilişim Suçu Çeşitleri

- **Bukalemun (Chameleon):**

- 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.

Bilişim Suçu Çeşitleri

- **Mantık Bombası (Logic Bomb):**

- Mantık bombaları, bilişim sistemlerinde veya ağlarında, daha önceden belirlenmiş özel durumların gerçekleşmesi durumunda zarar verici sonuçlar yaratan programlardır.

- 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.

Bilişim Suçu Çeşitleri

- **Ağ Solucanları:**

- Ağ solucanları, herhangi bir kullanıcı müdahalesine ihtiyaç duymadan kendi kendini çalıştırabilen ve kendisi bir kopyasını ağa bağlı olan diğer bilişim sistemlerine de kopyalayabilen bir programdır.

- Ağ solucanları çoğunlukla bilgisayar virüsleri ile karıştırılmaktadır.

- Fakat ağ solucanları, bilgisayar virüsleri gibi sisteme zarar verme zorunluluğu olmadan da sistemin içinde dolaşabilmektedir.

Bilişim Suçu Çeşitleri

- **Eşzamansız Saldırılar (Asynchronous Attacks):**

- Bilgisayarın aynı anda birden fazla işlemi yürütmesine eşzamanlı çalışma denmektedir. Bilgisayar belirli durumlarda eşzamanlı çalışma yerine işlemleri belirli sırada yürüterek, bir işlemin başlamasını diğer bir işlemin sonucuna göre belirlemesine ise eşzamansız çalışma adı verilmektedir.

Bilişim Suçu Çeşitleri

- **Süper Darbe (Super Zapping):**

- Süper Darbe yazılımları, bütün güvenlik kontrollerini atlatarak sisteme müdahale eden programlardır.

Bilişim Suçu Çeşitleri

- **Veri Aldatmacası (Data Diddling):**

- Veri sistemlerine veri girilirken yanlış veriler girilmesi veya girildikten sonra değiştirilmesidir. Bilişim suçları alanında uygulanan basit, güvenli ve yaygın bir suç tekniğidir.

- Veri aldatmacası, bilişim sistemlerine verilerin girilmesi sırasında müdahaleler, verilerin değiştirilmesi sırasında yapılan müdahaleler, bilginin alınması sırasında yapılan müdahaleler olarak gruplandırılabilir.

Bilişim Suçu Çeşitleri

- **Gizlice Dinleme (Eavesdropping):**

- Bilişim sistemlerinin veri taşımada kullandığı ağlara girilerek veya bilişim sistemlerinin yaydığı elektromanyetik dalgaların yakalanarak verilerin elde edilmesi yöntemidir.

Bilişim Suçu Çeşitleri

- **Çöpe Dalma (Scavenging):**

- Çöplenme veya atık toplama olarak adlandırılan yöntem, bilişim sisteminde gerçekleştirilen veri-işlem sonunda kalan bilgilerin depolanmasıdır. Bu bilgiler öncelikle, çıktı birimlerince üretilen ve daha sonra çöpe atılan kâğıt, mürekkep şeridi gibi malzemeler üzerinde kalan bilgilerin toplanmasıyla elde edilmektedir. Diğer bir teknik ise bilişim sisteminin belleğinde bulunan ve artık ihtiyaç duyulmayan silinmiş bilgileri, gelişmiş yöntemlerle tekrar geri getirmektedir.

Bilişim Suçu Çeşitleri

- **Yerine Geçme (Masquerading):**

- Yetkisi olmayan veya sınırlı erişim yetkisi olan bir kişinin, parola veya erişim kodunun yazılması veya ona özgü niteliklerin taklit edilmesi şeklinde yapılmasına denmektedir.

Bilişim Suçu Çeşitleri

- **İstem Dışı Alınan Elektronik İletiler (Spam):**

- Spam teknik olarak, internet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi olarak ifade edilebilmektedir.

Bilişim Suçu Çeşitleri

- **Ağ Solucanları (Network Worms):**

- Ağ solucanları, herhangi bir kullanıcı müdahalesine ihtiyaç duymadan kendi kendini çalıştırabilen ve kendisi bir kopyasını ağa bağlı olan diğer bilişim sistemlerine de kopyalayabilen bir programdır.

- Ağ solucanları çoğunlukla bilgisayar virüsleri ile karıştırılmaktadır. Fakat ağ solucanları, bilgisayar virüsleri gibi sisteme zarar verme zorunluluğu olmadan da sistemin içinde dolaşabilmektedir.

Bilişim Suçu Çeşitleri

- **Sırtlama (Piggybacking):**

- Fiziksel ya da elektronik yollarla kullanılmasıyla bilişim sistemlerine yetkisiz olarak girme tekniğidir.

Bilişim Suçu Çeşitleri

- **Bot'lar:**

- Bot'lar belirli eylemleri otomatik olarak gerçekleştirmek için tasarlanan programlardır.

- Bunlar pek çok meşru amaç için kullanışlı olsa da aynı zamanda kötü amaçlı bir yazılımdır.

- Bot'lar bir bilgisayara girdikten sonra makinenin kullanıcı onayı veya bilgisi olmadan belirli komutları yürütmesine neden olabilir.

- Korsanlar daha sonra ele geçirilen bilgisayarları uzaktan yönetmek, hassas verileri çalmak, kurbanların etkinliklerini takip etmek, otomatik olarak spam yaymak veya bilgisayar ağlarında yıkıcı DDoS saldırıları başlatmak için kullanılabilecek bir "botnet" (robot ve ağ anlamına gelen robot ve network kelimelerinin kısaltılmışı) oluşturmak amacıyla aynı bot ile birden fazla bilgisayara virüs bulaştırmaya da çalışabilir.

Bilişim Suçu Çeşitleri

- **Oltalama (Phishing):**

- Phishing, genel olarak bir kişinin parolasını, banka hesabını veya kredi kartı bilgilerini öğrenmek amacıyla kullanılır
- Saldırgan tarafından özel olarak hazırlanan phishing e-postası resmi bir kurumdan geliyormuş gibi ya da gerçek bir e-posta şeklinde görülür. Hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilerek parolalarını vermeleri sağlanır. Diğer bir yandan bu e-postalara eklenen dosyaların çalıştırılması ile kurbanların bilgisayarları ele geçirilerek saldırganın kontrolü altına girebilir.
- Phishing saldırılarında saldırgan kişi bir “yem” hazırlar ve bu yeme kurbanların takılmasını amaçlar. Yem genelde maaş zammı, hediye, ücretsiz tatil, para ödülü şeklinde cezbedici senaryolardan oluşturulur. Kurumlar için büyük riskler oluşturan bu saldırı türüne karşı büyük kayıplar yaşanmaması için kurum çalışanlarının bilgilendirilmesi gerekmektedir.

Bilişim Suçu Çeşitleri

- **Kredi Kartı Sahtekârlıkları**

- Elektronik ortamda kredi kartı sahtekarlığında; sahte müracaat, sahte kart, hacking, fishing, web link, wireless network hırsızlığı gibi yöntemler kullanılmaktadır.

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
  - emniyet'e giderek durumu belgeler ile birlikte anlatmak
  - dava açılmasını sağlamak