D.E.Ü. İ.İ.B.F. Dergisi
Cilt: 10, Sayı: I, 1995, ss.141-165

BİLGİSAYAR SUÇLARI VE İÇ DENETİM YÖNTEMLERİ

Seha SELEK (*)

ÖZET

Bilgisayar suçu ifadesi genel bir terim olarak kullanılmakta ve işlenmesi için bilgisayardan dolaylı ve/veya dolaysız yararlanmayı gerektiren her türlü suçu ifade etmektedir. Konunun anlaşılabilirliğini kolaylaştırabilmek için bilgisayar suçları;

- Bilgisayar hilesi ve
- Bilgisayar bağlantılı suç olarak iki başlık altında incelenecektir.
- Bilgisayar Hilesi Suçun işlenmesine katılan bir veya daha fazla insanın fayda sağladığı veya sağlıyabileceği ve bir veya daha fazla sayıda kurbanın zarara uğradığı veya uğrayabileceği ve gerçekleştirilmesinde bilgisayardan yararlanıldığı istemli hareketlerdir. Bilgisayar bağlantılı suç gerçekleştirilmesi için bilgisayar teknolojisinin gerekli veya bilgisayarın suçun temel hedefi olduğu yasadışı bir eylemdir, biçiminde tanımlanabilir.

Bilgisayar ve/veya bilgisayar suç olarak tanımlanabilen suçlar veya bu suçların işlenmesinde kullanılan yöntemler on ki ana grupta toplanabilmektedir. Bu yöntemler Veri Hileciliği, Truva Atı Dilimleme Teknikleri, Superzapping, Tuzak Kapıları, Mantık Bombaları, Zaman Uyumu Sağlanmayan Hareketler (Asnkorone Hareketleri), Çöpçülük, Veri Sızıntısı, Sırtta Taşıma ve Başkasının Yerine Geçme, Hatlara Giriş, Benzetişim ve Modelleme'dir.

Bilgisayar suçlarını işlenmeden önleyici tedbirler ise;

1) Sistem dizaynı
2) İç denetim ve
3) Kullanılması gereken güvenlik cihazları olmak üzere üç ana başlık altında incelenmiştir.

GİRİŞ

Son yıllarda işlenen bilgisayar suçlarının sayısı hızla artmaktadır.Bunun, yani bilgisayarların suç işlemede yaygın olarak kullanılmaya başlanılmasının başlıca nedenleri şöylece özetlenebilir: (Wilson vd. 1989: s. 25/2, 3).

1) Günümüzde gerek özel ve gerekse iş yaşantısında bilgisayarlar; iş hayatında özellikle tesadüfi girişli açık devre -on-line- sistemler; yaygın olarak kullanılmaktadır. On line- açık devre bilgisayar sistemi; merkezi işlem birimine zaman ayırım esasına göre giriş hakkı kazanan bilgisayar kullanıcısının, merkezi işlem birimindeki işletimcinin araya girmesine ve yardımına gerek kalmaksızın sistemi çalıştırarak veri yükleyebildigi ve/veya istediği yeri ve/

(*) Doç.Dr. D.E.Ü.İ.İ.B.F. İşletme Bölümü.

veya çıktıları elde edebildigi bir sistemdir (Hicks vd. 1981: s. 566). On-line; deyimi aynı zamanda işlemlere ilişkin verilerin kaynaklandıkları noktalardan önceden sınıflandırılmalarına gerek kalmadan sisteme girilebildigi yöntemi ifade etmek için de kullanılmaktadır (Selek, 1990, s. 109). Günlük hayatta bu yaygın kullanım toplumun bilgisayarlara ilgisini ve kullanıcıların sayısını her geçen gün artırmaktadır.

Bilgisayar suçları yargı, polis tarafından ve iş dünyasında yeterince anlaşılamamıştır. Polis örgütünün ve savcılığın bu konudaki bilgi ve deneyimi sınırlıdır.Genellikle de bilgisayar suçunun bilgisayarın içinde işlendiğini düşünmektedir.

2) Bilgisayar eğitimi yaygınlaşmıştır.Günümüzde ülkemizde de gerekli olanaklara sahip ilkokullarda çocuklarımız bilgisayar eğitimine ve kullanmaya başlamaktadırlar.Bu eğitim ortaokul, lise ve yüksek öğrenimde daha da yaygınlaşmakta ve kalitesi yükselmektedir.Kabiliyetli ve meraklı öğrenciler, öğrenim ve öğretim dönemlerinde bilgisayar konusunda ileri düzeyde bilgi ve deneyim kazanabilmektedirler.

3) Evlerde ve işyerlerinde kullanılan tek kullanıcılı bilgisayarların günümüzde kolaylıkla elde edilen modemler ve telefon kanalları ile çok kullanıcılı açık devre -on line- sistemlere ve diğer kişisel bilgisayarlara bağlama olanakları artmıştır.

Bu olanaklar coğrafik engellerin aşılmasına yardımcı olmaktadır. Örneğin; bir terminalden telefon hatları ile bu terminalin kurulu bulunduğu yere çok uzak bir bölgede kurulu bir diğer terminal ile bağlantı kurarak bir suçun işlenebilmekte veya bir suçun işlenmesine katılınabilmektedir.

4) Bilgisayarlardan aşırı derecede yararlanma isteği veya kullanımı dikkatleri bu konuda yoğunlaştırmada ve güvenlik ile hileciliğe karşı korunma önlemlerine verilen önemi azaltmaktadır.Bu nedenle de donanım ve yazılım alanlarında yararlanılan güvenlik sistemlerinden istenilen teknolojik fayda sağlanamamaktadır.

5) İşletme bilgi işlem görevlileri ve diğer bilgisayar kullanıcılara genellikle güvenlik bilincine ve güvenlik önlemlerinin alınabilmesi için gerekli olan iç kontrol bilgisine sahip değildirler. Onların temel amacı hızlı, ekonomik ve engellenmemiş bir veri işleme sürecinin yürütülmesidir.

6) Bir çok firmada bilgi işlem birimi görevlilerine karşı yönetim çok hoşgörülüdür.

Bu personelin çalışmalarına getirilen sınırlamalar az ve üzerlerindeki gözetim zayıftır.

2) Bilgisayar Bağlantılı Suç: Bılgisayar bağlantılı suç ıse; daha geniş kapsamlıdır. Bir beyaz-yakalı suç, bir işletme suçu-muhasebe hilesi- veya herhangi bir diğer ekonomik suç olabileceği gibi, bir şiddet eylemi olabilir. Örneğin suç eylemi ile bir bilgisayar donanımı ve onun bünyesinde saklanan veri/bilgiler tahrip edilebilir (Porter, v.d, s. 431). Bu tahribat, donanım ve bilgilerin sahiplerinin uğrayacakları maddesel zararlara ek olarak bilgisayar teknolojisinden yararlanılarak yürütülen hassas işlemlerin aksamasına neden olarak, toplum yaşantısının düzenini bozabilir. Örneğin elektronik vezne sistemi ve on-line sistem kullanarak müşterilerine hizmet veren bir bankanın bilgisayar sisteminin merkezi işlem birimi - central processing unit - tahrip edilerek hem bankaya ve/veya bu sistemi sigortalayan sigorta şirketine maddesel kayıp verdirilebilir.Aynı zamanda sistem yeniden kurulup, yedeğe alınan veri/bilgilerin yeniden sisteme yükleninceye kadar geçen süre içinde bankanın müşterilerine hizmet vermesi engellenir.

Bu açıklamalar ışığında bilgisayar bağlantılı suç; gerçekleştirilmesi için bilgisayar teknolojisinin gerekli veya bilgisayarın suçun temel hedefi olduğu bir eylemdir, biçiminde tanımlanabilir. Bilgisayarlarla ilişkili her suçun bir bilgisayar suçu olarak tanımlanıp, tanımlanamayacağı bazı durumlarda sorun olmaktadır. Örneğin, bilgisayar satıcısı bir firmadan, demostrasyondaki bir sistemin çalınması bir bilgisayar suçu değil, adi bir hırsızlıktır. Çünkü malı çalınan firmanın aynı değerde başka bir varlığın çalınması ile o bilgisayarın çalınması arasında uğrayacağı zarar arasında bir ayrım yapma imkanı yoktur. Ayrıca suçu işleyenin o bilgisayarı çalarak bilgisayarlarla ilişkili özel bir yarar sağlayacağı da açık değildir.

Bir suçun bilgisayar suçu olması için;

1) Bir elektronik bilgi işlem sistemine başkalarına zarar verecek hileli kayıt ve/veya verilerin girilmesi,

2) Bilgisayar imkanlarının kötü amaçlara ulaşmak için kullanılması,

3) Bilgisayara önceden yüklenmiş bilgilerin değiştirilmesi ve/veya tahribi,

4) Para veya işletmenin diğer varlıklarının, hizmetlerin ve/veya değerli verilerin bilgisayar teknolojisinden yararlanarak çalınmasıdır.

Bilgisayar donanımının bilgisayar suçunda oynadığı rol ise, 1. Suçun Hedefi, 2. Suç Konusu, 3. Suç Aracı, 4. Suç sembolü olarak dört noktada toplanabilir (Wilson v.d, s. 25/5).

1. Suçun Hedefi

Donanımın, sistemlere yüklenmiş program ve/veya verilerin veya

düzenli çalışabilmesi için sistemi destekleyen klima, kesintisiz güç kaynağı gibi ünitelerin çalınıp veya tahrip edildigi eylemlerde; bilgisayar suç konusunu oluşturmaktadır.

2. Suç Konusu

Bir suçun işlendiği yer veya çevre bilgisayar ise; bilgisayar suç konusunu oluşturmaktadır.

3. Suç Aracı

Bazı suç türleri veya suç işleme yöntemleri bilgisayar teknolojisinden yararlanmayı gerektirecek ölçüde karmaşık olabilir. Örneğin; bilgisayar, telefon sistemini yasal olmayan bir şekilde kullanabilmek için gerekli kotları-şifreleri elde etmek için kullanılabilir. Ya da bir zimmet suçunun planlanmasında ve yapılacak denetimlerde tespitini önlemek için muhasebe kayıtlarının ayarlanmasında kullanılabilir.

4. Suç Sembolü

Zaman zaman bilgisayar kişileri aldatmak veya korkutmak için kullanıldığında suçun sembolünü oluşturmaktadır. Örneğin, bir hizmetin yapılmasında ve/veya ürünün üretilmesinde bilgisayar teknolojisinden söz edilerek toplumun aldatılmasının hedeflenmesi durumunda bilgisayar; suçun sembolü olmaktadır.

Dünyadaki gelişmelere paralel olarak ülkemizde de bilgisayar kullanımının ve bilgisayar suçlarının yaygınlaşmasının sonucunda yasal düzenlemeye gerek duyulmuş, 3756 sayılı Kanun'un 20-24. maddeleri ile 765 sayılı Türk ceza kanunun 525. maddesine eklenen a-d bendleri ile " Bilişim Alanında Suçlar " olarak tanımlanan eylemler açıklanarak, bunları yapanlara verilecek cezalar belirtilmiştir (Resmi Gazete, 1991, s. 5-6). Bu Kanunun 21. maddesinde bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirme eylemini yapana bir yıldan üç yıla kadar hapis, 1 milyon TL.' sından 15 milyon TL.' sına kadar para cezası verileceği belirtilmiştir.

Aynı Kanun'un 22. maddesinde ise; başkasına zarar vermek veya kendisine veya bir başkasına yarar sağlamak amacı ile bilgileri otomatik olarak işleme tabi tutmuş bir sistemi veya verileri diğer herhangi bir unsuru kısmen veya tamamen tahrip eden, değiştiren, silen, sistemin işlemesine neden olanlara iki yıldan altı yıla kadar hapis ve 5 milyon TL. sından 50 milyon Tl.sına kadar ağır para cezasının verileceği belirtilmiştir. Dolayısıyla bu maddede belirtilen eylemler suç olarak kabul edilmiştir.

Ayrıca bu maddenin ikinci parağrafında bilgileri otomatik işleme tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayana 1 yıldan 5 yıla kadar hapıs ve 2 milyon TL. sından 20 milyon TL. sına kadar para cezası verileceği belirtilmiştir.

Aynı Kanun'un 23. maddesinde ise; hukuk alanında kanıt olarak kullanılmak üzere sahte belge düzenlemek ile sisteme verileri giren veya önceden girilmiş verileri değiştirenlerin bir yıldan üç yıla kadar hapis cezası ile cezalandırılabileceği belirtilmektedir.

Yukarıda açıklanan üç madde hükmü incelendiginde bilgisayar suçlarının üç grupta ele alındığı ve eksikleri olmakla beraber daha önce belirtilen kriterlere uygun olarak tanımlandığı söylenebilir.

21. madde hükmü proğram, veri ve benzerlerinin sistemden hukuka aykırı olarak alınmasının cezalandırılması gereken bir eylem olrak ifade etmekte, buna karşın bu program ve verilerin sistemin dışında bulunan bir bilgi işlem ortamından alınmasına, örneğin; bilgi işlem kitaplığında saklanan program ve/veya veri yüklü disketlerin alınmasına, değinilmemektedir. Bu durumda program ve/veya verilerin sistemden alınması bilgisayar suçu olarak, kitaplıktan alınması ise adi bir hırsızlık olarak kabul edilmektedir. Halbuki disketlere yüklenmiş program ve verilerin yararlanabılmek için elektronik bilgi işlem sisteminin kullanılması gereklidir.Bu nedenle de bu eylem de kanımızca bir bilgisayar suçudur.

II. BİLGİSAYAR SUÇLARINI ONLEYİCİ TEDBİRLER

Bu çalışmanın önceki kesitlerinde genel olarak tanıtılmaya çalışılan ve bundan sonraki bölümlerde türler itibarıyle işleniş bıçimleri ve soruşturma yöntemleri ayrıntılı olarak incelenecek bilgisayar suçlarını işlenmeden önleyici tedbirler ise bu kesitte özlü olarak tartışılacaktır.

Bu önlemler:

1) Sistem dizaynı

2) İç denetim ve

3)Kullanılması gereken güvenlik cıhazları olmak üzere üç ana başlık altında incelenebilir.

1. Sistem Dizaynı

Bir firmada elektronok bılgi işlem sistemi dizayn edilirken sadece verilerın işlenmesi amaçlanmamalı, etkili bir ıç denetım sisteminin kurulmasınıda önem verilmelidir.İç denetim sisteminin, işletme sisteminin dizaynı

sırasında kurulması, sonradan eklemekten daha ucuza mal olmaktadır. Eğer bir örgütte iç denetim mekanizması etkili değilse bu eksiklik giderilmedikçe dış denetimde başarılı olması beklenilmelidir.Sistem dizayn edilirken iç ve dış denetçiler ile bilgisayar uzmanlarının görüşleri muhakkak alınmalı, işbirliği yapmaları sağanmalıdır.

En geniş anlamı ile denetim ekonomik faaliyetler ve olaylara ilişkin bilgilerin önceden belirlenmiş kriterlere uygunluk derecesini araştırmak amacı ile bu faaliyetler ve olaylara ilişkin kanıtların sistematik ve tarafsız olarak elde edlimesi, değerlenmesive sonucun ilgili taraflarca iletilmesi sürecidir. (Roberson vd. 1988: s. 169: Porter vd. 1984 s. 8: Selek, vd, 1987: s. 86: Güredin: s.5). Kanıt: doğruluğu test edilecek bilgi ve işlemlerdir.Bir konuda doğru değerleme yapabilmek için o alanda yeterli ölçüde kanıt toplanmalıdır. Önemlilik, risk güvenlirlik ile maliyet ve fayda analizi kanıtın yeterliligine etkin eden başlıca faktörlerdır (Bkz. Robertson vd. 1988: s. 163, 164; Çömlekçi 1980: s. 5).

Dış denetim ise: örgüt amaçlarına en etkin ve verimli şekilde ulaşılıp ulaşılmadıgının . faaliyetlerinin hukuk düzenine uygun yürütülüp yürütülmediginin veya raporlanan bilgilerin doğru ve güvenilir olup olmadıgının örgütle çıkar ilişkisi bulunan kişiler ve\veya devlet adına örgüt dışındaki kişiler tarafından araştırılması ve incelenmesi faalıyetleridir (Kepekçi 1988: s. 31).

2. İç Denetim:

Elektronik bilgi işlem birimi etkinliklerinde iç denetim ilkelerine titizlikle uyulmalıdır. Bu birimde: görev ayrımı ilkesine uyulmalı, herhangi bir görevlinin verinin işlenmesi ve raporlanması sürecinin tümüne tek başına hakim olmasına izin verilmememelidir (Wilson vd. 1984: s. 26/23/24; Hiçks vd. 1981: 286-289; Wallace 1984: s. 283, 286).

Sistem dizaynı ve analizi, sistem ve uygulama programlarının hazırlanması-yazılımı-elektronik bilgi işlem sisteminin işletimi ile verinin işlenmesi görevleri özellike değişik kişilere verilmelidir. Bu birimin her görevlisinin düzenli olarak tatil yapması zorunlu tutulmalı, tatilde olduğu sürede yerine bir başkası görevlendirilmelidır.Hassas konularda özel önlemler alınmalıdır. Yani işe alınanların, görev yeri değiştirilenlerin dürüstlük ve güvenirliği test edilmelidir.

Hile ve kaçamaklara karşı daıma uyanık bulunulmalıdır. Çalışanarın görevlerinin değiştirildigi gibi, güvenlik için kullanılan gizli şifre ve kotlar da uygun aralıklarla değiştirilmelidir.

Elektronik bilgi işlem sistemlerinin ve bu sistemlere geniş imkanı veren terminallerin etkin bir şekilde denetimi ve olası bilgisayar suçlarının önlenmesinde önemli bir işlemdır (Wilson vd. 1989: 25/18).

Bu nedenle de iç denetim örgütünde bilgisayar konusunda daima dikkatli davranmalı ve yapılacak olağan denetimlerde olası bilgisayar suçlarını özenle araştırmalıdırlar.

Denetçiler ayrıca, kendi terminalinden istediği raporları alabilmek için geliştirilmiş yazılımları kullanmalıdırlar.Bir çok ülkede olduğu gibi ülkemizde de şubeler açarak faaliyet gösteren dış denetim kuruluşları muhasebe denetiminde kullanılmak üzere özel olarak hazırlanan yazılımları başarıyla kullanmaktadır (Hicks vd. 1981: s. 334, 335; Thomas vd. 1983: s. 277, 278). Bu yazılımlardan iç denetimlerde de yararlanılmaması için, kanımızca hiç bir neden yoktur.

Bilgisayar teknolojisi çok hızlı bir şekilde -geometrik orandagelişmektedir (Black vd., 1973: s. 231). Kurmay işlev yükleyen iç denetçilerin yazılım ve donanım teknolojisinin günümüzdeki ve gelecekteki gelişmelerine karşı kendilerinin yenilemeleri sağlanmalı ve bu çalışmaları son gelişmelerden yararlanmalarını sağlayan denetim proğramları sağlanarak desteklenmelidir.

Kullanılan proğramlarda ve çalışma sisteminde yapılacak değisiklikler uygulanmaya konmadan önce muhakkak titizlikle gözden geçirimelidir.

3. Güvenlik Cihazlarının Kullanılması:

Güvenlik cihazları elektronik bilgi işlemede güvenliği sağlamak için yakın geçmişte geliştirilmiş özel elektronik aygıtlardır. Bu cihazlardan bazıları telefon hatları ile taşınacak veriyi şifrelemekte ve tekrar çözümlemektedir. Bir kısmı ise, sisteme proğramlara ve/veya verilere sadece yetkili kullanıcıların girebilmesi ve diğer girişlerin önlenmesinde kullanılmaktadır. Bu aygıtlar ayrıca bilgisayar suçu işleme girişimlerini otomatik olarak tanıyıp tespitleyebilmektedir.

IV. BİLGİSAYAR SUÇU İŞLEME YÖNTEMLERİ

Bilgisayar ve/veya bilgisayar bağlantılı suç olarak tanımlanabilen suçlar veya bu suçların işlenmesinde kullanılan yöntemler oniki ana grupta toplanabilmektedir (Wilson vd. 1989: s, 25 6-9: Porter vd. 1984 s. 435, 436).

Bu yöntemlerin bazıları basit, bazıları ise oldukça karmaşıktır. Ayrıntılı bir şekilde açıklanabilmesi için bilgisayar teknolojisinin ve programlama tekniklerinin iyi bilinmesi gerekmektedir.İncelemenin bu bölümünde bu yöntemler ve potansiyel suçlular örneklerle tanıtılmaya ve soruşturulma yöntemleri açıklanmaya çalışılmıştır.

Bu yöntem ve\veya suç türleri şunlardır:

1. Veri Hileciliği

2. Truva Atı,
3. Dilimleme Teknikleri,
4. Superzapping,
5. Tuzak Kapıları,
6. Mantık Bombaları,
7. Zaman Uyumu Sağlanmayan Hareketler (Asnkorone Hareketler)
8. Çöpçülük
9. Veri Sızıntısı
10. Sırtta Taşıma ve Başkasının Yerine Geçme
11. Hatlara Giriş
12. Benzetişim ve Modelleme

1. Veri Hileciliği

Bilgisayar suçu işlemede en yaygın olarak kullanılan yalın ve emin bir yöntemdir. Bu yöntemle veri; sisteme girilmeden önce ve/veya bir grup suçlu tarafından verinin sisteme girilebilmesi için hazırlanması kayıtlanması, kotlanması test edilmesi, denetimi, elektronik veri işleme sistemine girilebilir ve bu ortamda işlenebilir biçime dönüştürülmesi sürecinin herhangi bir noktasında yapılabilir. Örneğin, suç işleyebilmek için; önceden bu amaca uygun olarak hazırlanmış olan manyetik bantlar, kartlar, disketler doğru program ve/veya verileri taşıyanlara değiştirilebilir.Delikli kartların kullanılması durumunda ise suçu işleyebilmek için kartlarda yeni delikler açılabilir ve/veya açılmış olan delikler kapatılabilir.

Bu yöntemi;

-Bir işlemcinin katılımcıları,

-Verileri hazırlayanlar,

-Kaynak verileri sağlayanlar ve

-Giriş imkanı olan üçüncü kişiler kullanabilirler

-Veri hileciliği suçu ve/veya suçluları;

-Veriler kıyaslanarak,

-Belgelerin geçerliliği araştırılarak,

Elle yapılan kontroller ve bu kontrollerin bilgisayara uygulanan analizleri yaparak,

-Sistemin güvenirliğini inceleyerek ve onaylayarak,

-Rapor analizleri yapılarak.

-Bilgisayar çıktıları incelenerek,

-Doğruluk testleri yapılarak tespitlenebilir (Porter v.d. s. 437).

Bu suçun işlendiği ve kimin tarafından işlendiğinin tesbit ve ispatlanmasında yararlanılan kanıtlar ise, verilere ait belgeler, veri saklama ortamları, bilgisayar kullanımına ilişkin elle tutulan kayıtlar, bilgisayarın otomatik olarak tuttuğu kullanım kütükleri, özellikli durumlara ilişkin raporlar ve yanlış bilgisayar çıktılarıdır.

Bilgisayar kütüğü; her işi, çalışmayı, işlenmenin aldığı süreyi, işletimcinin hareketlerini ve gerekli diğer verileri kapsayan veri işleme ekipmanı çalışma kaydıdır (Wilson, v.d, s. 26/49).

Verilere ilişkin belgeler ise; verinin ilişkin olduğu ticari işlenmin doğuş noktasında düzenlenen fatura v.b. kaynak veya işletme içi belgeler yada barkot (barcode) gibi sadece optik okuyucularda okunabilen diğer belgelerdir.

Manyetik bantlar, delikli kartlar, disk ve disketler ile modüller ise; veri saklama ortamlarıdır.

2. Truva Atı:

Bir programın; temel hazırlanma amaçlarının gerçekleşmesi engellenmeden; suçluların, program komutlarını arzuladıkları işlevleride gerçekleştirebilecek şekilde değiştirdikleri bir suç türü ve/veya yöntemidir.

Suç işlemeyi sağlayıcı komutlar yazılımcılar tarafından programa programın yazılımı sırasında da eklenebilir.Bu durumda bu komutlar programın korumalı bölümünde ve özel kullanımlar için oluşturulan veri kütüklerinde de etkili olur.

Komut; bilgisayarın belirli bir işlem yapmasını sağlayan ifadeler topluluğudur.Komutlardan oluşan setler, rutin olarak tanımlanır. Bir komut genellikle 40-300 rutinden oluşur (Çarıkçıoğlu, 1977, s. 30).

Programların sonradan yeni komutlar eklenmesine izin verecek şekilde yani rutinler arasında boşluklar bırakılarak yazılımı durumunda bu suç daha da kolay biçimde işlenebilir.

Eğer suç akıllıca işlenmiş ise, araya sonradan eklenen ve programın amaç dışı kullanımına olanak veren "Truva Atı" olarak tanımlanan komutları bulmak ve önleyici tedbirleri almak icin pratik yöntemler yoktur. Çünkü işletmecilik alanında kullanılan tipik bir program yüzbinin üstünde komut ve rutiden oluşmaktadır (Porter v.d. s. 48). "Truva atı" komutları belli bir program içinde eklenme yerine işletim sistemini oluşturan beş-altı milyon komut içine de saklanabilir.Bu durumda genellikle utility (hizmet) programları ile birlikte kullanabilir.

"Truva Atı" komutlarının araştırılarak bulunması durumunda bile, suçun kimin işlediğine ilişkin bir iz kalmadığı için suçlunun belirlenmesi mümkün değildir.Suçlular, bu suçu işleyebilecek bilgi, yetenek sahibi ve bilgisayar kullanma imkanı olan programcıların sıkı bir şekilde izlenmesi ile tesbit edilebilir.Böyle bir hilenin yapıldığının anlaşıldığı durumlarda suçlunun tespiti için firmada halen çalışan, eskiden çalışmış ücretli ve vazılım satan firmaların çalışanlarının durumları dikkatlice soruşturulmalıdır.

Bu yöntemi kullanan suçlu, genellikle tek başına veya başkalarının yardımını sağlayarak haksız bir yarar sağlamayı hedefler. Eğer işletme varlıklarının hareketleri iyi bir şekilde tespitlenip kayıtlanırsa; suçlunun bulunma ihtimali artar. Eğer bir programa **"Truva Atı"** yöntemi ile yetkisiz eklemeler yapıldığından şüphelenilirse, şüphelenilen program kopyası ana programla veya yetkisiz hiçbir değişikliğin yapılmadığı kesinlikle bilinen diğer bir kopya ile karıştırılmamalıdır. Genellikle programların birer kopyeleri gerektiğinde kullanılmak üzere emin bir yerde saklanırlar. Eğer suçlu akıllı davranıp, yedek kopyeye ulaşarak onu da değiştirirse; kötü niyetle yapılan değişikliklerin tesbiti güçleşir. Ancak programlar, kullanımda duyulan gereksinmeler sonucu zaman zaman iyi niyetli olarak değiştirilebilmektedir.Eğer program yedek kopyeleri ihmalkarlık nedeniyle düzeltilmemiş ise, bir karşılaştıma anında tespitlenen değişikliklerin hangilerinin iyi niyetli, hangilerinin kötü niyetli olarak yapıldığının belirlenmesi oldukça zorlaşır (Robertson vd, 1988: s. 446-448; Porter vd, 1984: s. 438).

3. Dilimleme Teknikleri

Büyük tutardaki değerlerin ilgilileri dikkatini çekmeyecek küçük dilimler halinde, surekli olarak çalınması yöntemi dilimleme-salam-tekniği olarak isimlendirilmektedir. Bu yöntem işletmecilik alanında yuvarlama hilesi olarak bilinmektedir.Bu yöntemin uygulanabilmesi için, bankacılık sektöründe olduğu gibi çok sayıdaki finansal işleme ilişkin bilgilerin işlendiği bir bilgisayar sistemine gerek vardır.Bu suç işlenirken; kullanılan programlara ve/veya işletim sistemine "Truva Atı" yönteminde açıklanan biçimde eklemeler yapılarak, sistemce işlenen ve sayıları bir kaç yüzbini aşan mevduat hesaplarının dönem faizlerinden küçük miktarlarda kesinti yapılmakta ve bunlar yasal biçimde açılan bir hesaba aktarılmaktadır. Sistemden yasal olmayan bir yolla para çekilmediği için işlenen bu suç günlük kontroller sırasında yetkililerin dikkatini çekmemektedir.

Bu işlem; genel nakit hareketlerinde bir dengesizliğe neden olduğunda ilgililerin dikkatini çekebilmektedir.Ancak, dengesizliğin nedeninin bulunabilmesi için tüm hesapların teker teker incelenmesi gereklidir.Araştırılması oldukça zor ve maliyeti de yüksektir.

Ancak örnekleme yoluyla seçilecek hesapların özellikle personelin ve/veya yakınlarının hesaplarının inclenmesi yoluyla tespitlenir.Örneklemede istatistiksel yöntemlerden ziyade denetçinin bilgi ve deneyimine dayanarak oluşan kişisel yargılarının ön planda tutulduğu iradi örnekleme yöntemin kullanılması yararlıdır (Robertson vd. 1988: s. 446-448: Porter vd. 1984: s. 438). Bu tür bir yolsuzluğun soruşturulmasında öncelikle personelin açtırdıkları hesapların inceleneceği bilindiği için suçluları suçun ve/veya suçluların araştırılması yöntemleri ve araştırmada yararlanılacak kanıtlar aşağıda sistematik olarak belirtmeye çalışılmıştır.

Dilimleme yöntemini kullanabilecek potansiyel suçlular:

- Finansal işlemlerde kullanılabilen bilgisayarların sistem programcıları,
- Bilgi işlem birimi çalışanları,
- Sözleşmeli personel ve
- Donanım ve yazılım satıcısı firmaların çalışanlarıdır.

Bu yöntemle işlenebilecek suçlar;

- Verilerin ayrıntılı bir şekilde analizi,
- Programların ana kopyelerle karşılaştırılması,
- İşlemlerin denetimi ve
- Şüphelenilen finansal faaliyetlerin gözlenmesi ile tespitlenebilir.
- Küçük miktarlarda uğranılan zararlar,
- Desteklenmemiş hesap grupları ve

-"Truva Atı" kodu şüphelilerin değistrilmiş veya olağan olmayan kişisel finansal işlemleri dilimleme yönteminin ve kullanıcıların araştırılmasında yararlanılabilecek başlıca kaynaklardır.

4. Superzapping:

Bu yöntemin adı IBM firmasınca üretilen ve yaygın olarak kullanılan bir utility-hizmet-programı olan superzap'den türetilmiştir.Superzap ve benzeri hizmet programları çok kuvvetli programlardır.Yanlış ellere geçmesi ve bu ellerce kullanılması çok tehlikelidir.Bu tür programlar normal olarak sadece sistem analistleri ve işletim programlarını sisteme yükleyen programcılır tarafından kullanılır ve kötü niyetli kullanımlara karşı korunur.

Bu programı; kullanmasını bilen programcı veya işletimciler program kitaplıklarının iyi korunmadığı durumlarda elde edebilmektedirler.

Sistem analisti; sistemin düzenli olarak kullanabilmesi için gerekli bilgileri çözümleyen, verilerin ne şekilde işleneceği tespitleyerek sistemi derleyen ve bulgularını programcıya veren kişidir (Çömlekçi, s. 25-26).

Programcı; bu bulgulardan yararlanarak programlama mantıklarını ve akış şemalarını hazırlar, programları kotlar, tamamlanan programları dener ve gözden geçirir.Uygulama programcısı; sistemin işletimciler tarafından çalıştırılabilmesi için gerekli yazılımların hazırlanması içi yardım eder, birbiri ile ilişkili programlar arasındaki bağlantıları kurar (Robertson vd. 1988: s 442: Erdoğan, 1988: s. 19).

İşletimci, sistemi klavye veya bağlı terminaller yardımıyla çalıştıran, ortaya çıkan aksaklıkları tesbitleyen bilgi işlem görevlisidir.

Superzap programı kullanılarak dosyalarda yapılan değişiklikler iz bırakmadığı ve ancak çok gelişmiş teknikler kullanılarak belirlenebildiğinden bu hile çok az bir ihtimalle tesbitlenebilir.

Bu yöntem New Jersey'de bir bankada uygulanmış ve banka $128.000 zarara uğratılmıştır.Bu bankada reorganizasyon çalışmalarında dikkatli bir seçim yapılamadığı ve muhasebe sistemi yetersiz olduğu için çek hesaplarında hatalar oluyordu.Bilgisayar sistem yöneticisi bu hataları düzeltmek için yönetiminin gözetiminde superzap programını kullanıyordu.

Bu proğramı olağan düzeltmeler ve günlük kayıtların yapılması dışında kullanabilme imkanı bulan sistem işletimcisi müşteri hesaplarini değiştirecek bu hesaplardan önemli tutarı üç arkadaşının adına açılan hesaplara aktardı. Bu suistimal uzun bir süre devam ettirilince, hesabındaki eksikliğin farkına varan müşterinin şikayeti üzerine suçlular yargılanmış ve cezalandırılmıştır (Wilson v.d. s. 25/8).

Superzap programını;

-Elinde superzap programı ve bunu kullanabilme imkanı olan programcılar ve

-Bu programı kullanmasını bilen işletimciler yasal olmayan biçimde kullanabilir.

Bu yöntem;

-İşlem dosyaları, ikinci kopyeleri ile kıyaslanarak,

-Çıktılarda beklenmedik sonuçlar olup olmadıgı bunları alanlar tarafından dikkatlice araştırılarak.

-Bilgisayar kullanım günlükleri incelenerek aşağıdaki kanıtlar elde edilmeye çalışılarak tesbitlenebilir.

-Programların işletimi sonucu ortaya çıkan beklenmedik çıktılar

-Belgelendirilmemiş işlemler ve

-Bilgisayar kullanımının ve kütük (dosya) talep günlükleri superzap programının kötü niyetli olarak kullanıldığının başlıca kanıtlarıdır.

5. Tuzak Kapıları:

Büyük uygulama ve sistem programları yazılırken kullanılan bir yöntemdir.Bu programlar yazılırken programın yapısı içinde ileride istenilen eklemelerin yapılabileceği boşluklar bırakılır.Tuzak kapıları olarak adlandırılan bu boşluklar büyük ve karmaşık programların dizaynı sırasında sistem analisti veya programcı tarafından program mantığının yetersizliğinden yararlanılarak bırakılır. Bu boşluklar veya buralara yapılacak eklemeler sistemin veya programın gerektiği gibi çalışmasını önleyerek istenmeyen işlev ve yanlış çıktılara neden olabilir.Tuzak kapısı olarak tanımlanan bu boşluklar sistemin işletim devresi içine de yerleştirilebilir. Örneğin; işletim sisteminde kullanılan kotların tüm kombinasyonları sistemin işletimi için kullanılan komutlarda kullanılımaz, İşletim kılavuzlarında da açıklanmaz. Bu tanımlanmamış komutlar kullanıldığında işletim sistemi bilgisayarın uygunsuz çalışmasına izin vererek istenilmeyen sonuçlara neden olur.

Bu yöntemin sistem analistleri veya programcılar tarafından uygulanmasına karşın; daha önce açıklanan "Truva Atı" yöntemi uygulama progamcıları veya işletimciler tarafından kullanılır.

Bu hileyi araştıran denetçi; donanımın ve yazılımın kötü kullanımlara karşı hiç bir zaman kesinlikle güvenli olmadığını bilmelidir. Bu hile ve suçlular superzap yönteminde açıklanan esaslar doğrultusunda soruşturularak tespitlenir.

Bu yöntemin potansiyel suçluları, araştırma yöntemleri ve kanıtları tablolaştırılarak özetlenmiştir.

<u>Tuzak Kapıları Yöntemini Kazanabilecek Potansiyel Suçlular</u>

-Sistem programcıları

-Alanlarında uzmanlaşmış uygulama programcıları

<u>Bu Yöntemle İşlenebilecek Suçların Araştırma Yöntemleri</u>

-Programın herkesçe bilinen yazılım amacının dışında işlevleri olup ol-

madığına tespitleyici ayrıntılı testlerin yapılması

-Şüphelilerin bu suçu işleyebilecek niteliklere sahip olup olmadıklarının araştırılması ve

-Kanıtlara dayandırılan özel nitelikli testler uygulanması

Kanıtlar

-Sistemin olağan dışı çalıştığını gösteren bilgisayar çıktıları

6. Mantık Bombaları:

Bu yöntem, bilgisayara arzulanan zamanlarda veya belirli aralıkları suç işlemeyi kolaylaştırıcı koşulları sağlamak için yerleştirilen programlardır. Bir mantık bombası programı önceden tanımlanmış koşula veya veriye dayalı olarak arzulanan işlemin gerçekleştirilmesini sağlamaktadır. Bu veri veya koşul tetik görevi görerek bombayı patlatmaktadır.Mantık bombaları bilgisayara "Truva Atı" yönteminden yararlanılarak yerleştirilir. Bu hileyi bulmak için "Truva Atı" yönteminde açıklanan teknikler kullanılabilir.Bu yöntem işini emniyete almak isteyen bir programcı, kullanılmış personel dosyalarının tutulmasında kullanılan proğrama iş sözleşmesinin sona ermesi durumunda patlayacak bir mantık bombası -gizli bir MS-DOS kod- yerleştirilerek tüm personel dosyasının silinmesine.neden olmuştur.

Mantık bombası yöntemine verilebilecek en güncel örnek Michelangelo (Mikelanj) virüs programıdır.Kimliği tespitlenemeyen bir bilgi işlemci tarafından 6 Mart 1475'de doğan ünlü İtalyan resim ve heykel ustasının 517. doğum gününde virüslerin harekete geçmesi şeklinde hazırlanmıştır. Ancak 1992'nin artık yıl olduğu programlama sırasında dikkate alınmadığı sanıldığından virüsler normal koşullarda 5 Mart 1992 günü harekete geçmiştir. MS DOS işletim sistemlerine yerleşecek ve çok çabuk bulaşacak şekilde üretilen bir virüs zamanında haberi olmayan ve tedbir alamayam bir çok bilgisayar kullanıcısının IBM uyumlu bilgisayarını felce uğratmıştır.

Bir başka tür virüse saldırıya geçmesi nedeni ile programlanan süreden önce canlanmasıyla varlığından haberdar olunmuş bir çok ülkede devlet düzeyinde tedbirler alınmıştır (Hürriyet Gazetesi, 7 Mart 1992, s. 11). Virüsleri tesbitleyen programları belirlenerek antivirüs programları ile yok edilmiştir. Ya da bilgi işlem sistemlerinin otomatik olarak işleyen takvimleri manipule edilerek veya virüsü harekete geçeceği beklenen günler sistemler açılmayarak virüsün harekete geçmesi önlenmiştir. Buna rağmen bir çok ülkede habersiz yakalanan bir çok kuruluşların sistemleri devre dışı kalmış ve ülke düzeyinde zararlı durumlar oluşmuştur.

7. Zaman Uyumu Sağlanmayan Hareketler (Askrone Hareketler):

Bu hile sistemce bir sıra içinde gerçekleştirilmesi gereken işlemlerin sıralanmasının bozulmasına neden olur.Saptanması işletim sisteminin ve bilgisayar teknolojisinin karmaşıklığı nedeni ile ileri düzeyde teknik bilgi gerekmektedir.Sistemin uyumsuz çalışması suçlunun işletim sistemine yüklenilmiş program ve/veya verilere ulaşarak haksız kazanç sağlamasına imkan verir.

Sisteme girilen verilerin bilgi haline dönüsebilmesi için belirli işlemlerden geçmesi gereklidir.Bu işlemlerin ise, belirli işlemlerden geçmesi gereklidir. Bu işlemlerin ise belirli bir sıra ve yöntemle gerçekleştirilmesi gereklidir.

Sistem ve/veya programın akış şemaları bilgisayardan istenilen işlerin bir mantık dizgesi içinde birbirleriyle uyumlu olarak gerçekleşmesini sağlar. Sistem akış şeması, verilerin geldigi ve saklanacağı yerleri yapılması gereken işleri gösteren iş akış şemasıdır (Çarıkçıoğlu, s. 30).

Program akış şeması ise; belirli bir sistem içersindeki yer alan verilerin bilgisayarın birimlerinde yapılacak işler alınacak kararların niteliğini gösteren bir şemadır (Şanlı 1974, s.77).

Kullanıcının talepleri birbirine zıt, karışıklık yaratıcı işlemleri kapsayabilir. Örneğin değişik raporların çıktı halinde alınması gibi değişik işler aynı anda istenebilir.

İşletim sisteminin bu talepleri yerine getirilmesi mümkün oluncaya dek belleğinde saklar. Talebin karşılanması için gerekli koşular gerçekleştiğinde talep edenin talep önceliğine göre değil de işletim sistemindeki mantık önceliğine göre karşılar. Bu işlem işletim sisteminin; bir işi diğeri ile karıştırabileceği ölçüde karmaşık olabilir. Örneğin; uzun bir süre kullanılan uygulama programlarında bir aradan sonra tekrar çalıştırılabilmesi için bir kontrol noktasının bulunması program hazırlamada bir gelenektir. Bu kullanıcıya ileride programı önceden verilmiş veriler kaybolmadan tekrar çalıştırabilecek bir noktada çalışmasına ara vererek sistemi kapatmasına izin verir. Bu güncelleştirilmiş verinin kontrol noktasında işletim sistemince emniyete alınması gerektirir.İşletim sisteminin ayrıca programın durdurulduğu anda işin yapılmış biçimini ve emniyet düzeyini tanımlayan sistem parametrelerini de emniyete alması gereklidir.Eğer veri ve sistem parametreleri kontrol noktasına ulaştırılamassa tekrar bırakılan noktadar çalışma ya başlanılamaz.

Ayrıca bu yöntemle sistem parametreleri değiştirildiğinde program tekrar çalıştırılmaya başlandığında; işletim sistemi, daha yüksek bir emniyet

düzeyinde işlev görür. Böylelikle işletim sistemi sistemde yüklü program ve verilere yetkisiz girme imkanı verir.Bu yöntemi kötü niyetli olarak kullanabilecekler ve bu yöntem kullanılarak işlenecek suç ve suçluların tesbitlenmesinde kullanılacak teknik ve kanıtlar aşağıda özetlenmiştir.

Zaman Uyumu Sağlanamayan Harketler Suçunun Soruşturulması

Potansiyel Suçlar:

-Konusunda ileri düzeyde bilgi ve beceri sahibi olan, iş ahlakından yoksun sistem programcıları ve

-Konusunda ileri düzeyde bilgi ve beceri sahibi olan işletimciler

Araştırma Yöntemleri:

-Şüpheli hareketlerin sistem kontrolü

-Bir işin doğal ve emin koşullarda tekrarlamalı olarak yapılması

Kanıtlar:

-Sapma gösteren çıktılar

-Bilgisayar kullanımlarının niteliklerini gösteren kütükler.

8. Çöpçülük:

Bir çalışmadan sonra bilgisayarın içinde ve/veya çevresinde bırakılan bilgilerin elde edilme yöntemidir.Bu yöntemin en yalın şekliyle uygulanış biçimi bütün halinde veya parçalanarak atılan bilgisayar programlarının çöp sepetinden toplanmasıdır.

Daha teknik uygulaması ise; donanımda bırakılan verinin toplanmasıdır. Bilgisayar kullanıldıktan sonra işletim sistemi; sistem ile çıktı birimi arasındaki hız farkı dengesini sağlayan ara -tampon- bellek temizlememiş olabilir. Bazı işletim sistemleri, büyük miktarlarda bilgisayar saatinin kullanılması gerektiğinde manyetik disk veya bantları silmezler. Bu nedenle sistemden çıkılsa bile; yeni veri girilinceye dek, eski bilginin okunabilme imkanı vardır. Zaman ayrımlı sistemlerde bir kullanıcı tarafından depolama alanı, daha sonraki kullanıcıya da kullanılırsa ikinci, kullanıcı depolama alanına yani bu alana az miktarda veri girildikten sonra bu depolama alanını okuyarak önceden girilmiş verileri elde edebilir.

Teksas'da bu yöntemle gerçekleştirilen, aynı zaman ayrımlı bilgisayar sisteminin abonesi olan rakip petrol şirketlerinin sismik araştırma verilerinin çalındığı bir sanayı casusluğu, merkezi işlem birimindeki işletimcinin belirli bir kullanıcının sisteme her girişinde sisteme takılı bulunan bandı okuma düğmesinin yazma düğmesinden önce yandığının farkına varması üzerine yapılan basit bir soruşturma ile ortaya çıkarılmıştır (Porter v.d. s. 449).

Bu yöntemin potansiyel suçluları ve araştırma yöntemleri aşağıda tablolaştırılmıştır.

Çöpçülük Suçunun Araştırılması

Potansiyel Suçlular:

-Bilgisayar kullanıcıları/ Bilgisayarın bulunduğu yere veya yakınındaki alanlara girebilen kişiler

Araştırılma Yöntemleri:

-Çalındığının farkına varılan bilginin tekrar kaynağına taşınması

-Kullanılan harf karakterleri

-Şüphelenilen yollarla benzer şekillerde üretilmiş bilgi.

9.Veri Sızıntısı:

Yaygın bir şekilde işlenen bilgisayar ilişkili bir suçtur. Bilgisayar ve eklentilerinden verilerin veya kopyelerinin çalınmasıdır. Sistemlerin yoğun bir şekilde kullanıldığı bir ortamda kolaylıkla işlenebilir ve gizlenebilir. Bu suç, genellikle işletimci veya sistemin diğer kullanıcıları tarafından işlenir. Sistemden veri çalmak için değişik teknikler kullanılmaktadır. Bunlardan biri, dışarıya çıkarılması yasak olan veriyi kapsayan çıktıların, zararsız veri çıktılarının arasına gizlenerek dışarıya taşınmasıdır ya da taşınması istenen veriye eklemeler yapılarak, kamufle edilerek, ilk bakışta dışarıya taşınan verinin gizli veri olduğunun anlaşılması önlenmeye çalışılır. Kontrolün sıkı olduğu durumlarda daha karmaşık tekniklerden yararlanılır. Şifreler kullanılarak dışarıya taşınmak istenen verinin şekli değiştirilir.

Gizli bilgi, değişik uzaklıktaki satırlar, her satırdaki kelime sayısı noktalama işartleri gibi yollarla karışık bir hale getirilerek dışarıya çıkarılır. Daha sonra çözümlenerek kullanılır hale getirilir. (Porter, v.d. s. 450).

Bilgisayar teknolojisi; sistemi oluşturan ekipmanın belli bir sistem içersinde çalışmasını sağlamaktadır. Örneğin; o ve binary hanelerin (Binery sistem için bkz. Hicks Jr. vd. s. 543) bir manyetik bandın okunması veya yazılması işlemi sırasında band makarasının belirli kalıplar içersinde sağa ve sola dönmesini gerektirmektedir.Band makarasının bu hareketleri gözlenerek gizli veri elde edilebilir.

Yazıcının bir çıktının alınması sırasında çıkardığı sesler belirli kalıplar halindedir. Bu sesler bir ses cihazıyla kayıt edildikten sonra cihaz daha yavaş çalıştırılarak binary bilgiye dönüştürülebilir.Son olarak açıklanan teknikler yüksek riskli verilerin saklandığı, çok iyi güvenlik önlemlerinin alındığı ortam larda nadiren kullanılır.Çok iyi güvenlik önlemlerinin alındığı ortamlarda bile

çok değişik amaçlarla veri sızıntısı suçunun işlendiği görülmektedir.Örneğin; savaş sırasında Amerika Birleşik Devletleri'nin Wietnam'da kullandığı bir çok bilgisayarın merkezi işlem birimine uzaktaki alıcılara sinyal ulaştırabilecek güçteki telsiz vericilerinin yerleştirildiği ancak, sistem Amerika'ya geri götürüldügünde tespitlenmiştir (Porter v.d., s. 450).

Veri sızıntısı suçu hassas veri harerketlerinin gözlemlenmesi ve/veya ne zaman ulaşıldığı sistem işletim günlükleri incelenebilir.

Bu suç; "Truva Atı", "Mantık Bombası", "Çöpçülük" yöntemleri de kullanılarak işlenebilir. Veri sızıntısı suçunun işlendiğinden şüphelenilirse bu yöntemlerin olası kullanıcıları da soruşturulmalıdır.

Bu suçun ortaya çıkarılmasında araştırılacak deliller, çöpçülük yönteminin kanıtları ile büyük benzerlikler gösterir.

Bu yöntemin potansiyel kullanıcıları araştırma yöntemleri ve kanıtları, konuyu birleştirirek özetlemek amacıyla aşağıda tablolaştırılmıştır:

Veri Sızıntısı Suçlarının Soruşturulması

Potansiyel Suçlular:

-Bilgisayar kullanıcıları,

-Personel,

-İşten ayrılmış personel,

-Geçici personel ve

-Satıcı firmaların çalışanlarıdır.

Soruşturma Yöntemleri:

-Bilgi çalındığının farkına varılması ve

-Bilgisayar depolama araçlarının tekrar bilgisayara taşınmasıdır.

Kanıtlar:

-Bilgi işlem saklama ortamları,

-Bilgisayar çıktıları

-Yazı kalıpları ve

-Truva Atı ve Çöpçülük Suçunun tanıtıldığı kesitte belirtilen diğer kanıtlardır.

10. Sırtta Taşıma ve Başkasının Yerine Geçme

Fiziksel veya elektronik olarak işlenebilen bir suç türüdür.Elektronik veya mekanik olarak kilitlenen kapılarla kontrolden geçtikten sonra girilebilen alanlara yasal olmayan bir giriş hakkı kazanma fiziksel sırtta taşımadır (Porter v.d. s. 451). En tipik örneği, sadece yetkili belirli kişilerin girebileceği bir yerin kapısı önünde elleri kapıyı açamayacak kadar bilgisayar malzemeleri ile dolu bir şekilde beklenerek, yetkili bir kişinin kapıyı açmasından yararlanarak onun arkasından içeri girilmesidir.

Yetkisiz girişleri önlemek için alınan tedbirlerin başlıcaları turnikeler, adam tuzakları ve sabit korumalardır. Bilindiği üzere turnikeler elektronik veya metal anahtarı olan ya da şifreli kilitin şifresini bilen sadece bir kişi geçebilir. Adam tuzağı ise; anahtarın bir kullanımı ile sadece bir kişinin geçebileceği iki kapılı bir dolaptır.

Elektronik sırtta taşıma suçu; bir terminalden sisteme girmek isteyen kullanıcının yetkili bir kullanıcı olup olmadığının anahtar, şifre, kod ve/veya diğer bazı özel bilgiler yardımıyla sistem tarafından tespitlendigi on-line sistemlerde işlenir.

Yasal terminal kullanıcısının devrede olmadığı zamanlarda; onun telefon hattı kullanılarak gizli terminalin devreye sokulması yoluyla da işlenbilmektedir.Böyle durumlarda sistem bazen faklı terminal kullanıldığını anlayamamaktadır.

Yasal kullanıcının gerekli işlemleri tamamlamadan çalışmasına son verdiği durumlarda devre açık kaldığı için sırtta taşıma suçu kolaylıkla işlenebilmektedir.

Başkasının yerine geçme, yasal giriş hakkı olan kullanıcının kimliğine bürünmedir. Yukarıda da açıklandığı üzere sistem ancak, elektronik olarak ulaşan veriler uyumlu bir kombinasyon gösterdiğinde kullanıcının yetkili biri olduğunu anlayabilmektedir.

Bu veriler; yetkili olan kullanıcının bilmesi gereken şifre veya kod ile sahip olacağı manyetik ve/veya metal anahtar ile kullanıcının ses, parmak izi, el şekli gibi kişisel özelliklerine ait bilgilerdir.

Her hangi bir kişi doğru bir tanıtım kombinasyonu sağlayarak bir başkasının kimliğine bürünebilir. Bu suç türü aşağıdaki olayla örneklenebilir.

Telefon şirketine kendisini bir derginin zarı gibi tanıtan suçlu şirketi tanıtıcı bir yazıda yararlanmak için kullanılan bilgi işlem sistemi hakkkında bilgi edinmek istemiştir.

Bu talep üzerine kendisine, kullanılan bilgisayar sistemi ayrıntılı bir şekilde tanıtılmış ve bu yolla, elde ettigi bilgiler sayesinde güvenlik sistemini kırarak, yanıltarak da şirketten bir milyon değerinde alet, edavat çalmıştır.Oldukça ilginç ve ülkemiz açısından güncel bir diğer olay ise şöyle gerçekleşmiştir.

Otomatik vezne makinaları (ATM Atomatic Teller Mechine) para çekmek de kullanılan kartları çalan bir kişi bu kartları çaldıranlara telefon ederek kendini banka yetkilisi gibi tanıtmış ve kartların iptal edilerek yenilerinin çıkartılabilmesi için şifrelere/kodlara ggerek olduğunu söylemiştir.Bu yalana inanan kart sahipleri para çekme işleminin gerçekleşebilmesi için gereken ikinci veriyi de kendisine sağlamışlardır. O da en kısa zamanda bu kartları kullanarak mumkun olan en yüksek tutarlarda para çekmiştir.

Elektronik kapılar bilgisayarca kontrol edilir; bu alanlara yapılan girişlerin tarih ve zamanı sistemce kaydedilir.Yüksek güvenlik alanlarının girişlerinde çalıstırılan güvenlik görevlileri de bu alanlara girenlerin kaydını tutarlar.Bazı alanlarda özel kameralar kullanılır.Bu gereçlerin ve görevlilerin kayıtlarından yararlanılarak bu suçları işleyenler tesbitlenerek yakalanmaya çalışılır.Ayrıca güvenlik görevlilerin bu görgü tanıklarının verecekleri bilgiler suçun çözümlenmesinde büyük yararlar sağlarlar.

Bu suçun; potansiyel işleyicileri, araştırma yöntemler ve suç kanıtları aşağıda özetlenmiştir:

Potansiyel Suçlular:

-Personel,

-İşten ayrılmış personel,

-Satıcı firmada çalışan personel,

-Sözleşmeli personel ve

-Üçüncü kişiler

Araştırma Yöntemleri

-Bilgisayar kullanımlarının gözlenmesi,

-Görgü tanıklarıyla yapılan görüşmeler,

-Kullanımlarının kayıt edildigi defterler, belgeler ve bilgisayar kütüklerinin incelenmesi

-Bilgisayar kullanıcılarının sisteme girişlerinin niteliklerini analiz edebilecek özellikli bilgisayar programlarının kullanılması

Kanıtlar:

-Bilgisayar kullanım kütükleri (log).

-Bilgisayar kullanımlarının kayıt edildiği defterler

-Sistemin kullanım miktarını ölçen aletler

-Diğer fiziksel kanıtlar

11. Hatlara Giriş

Haberleşme imkanlarının artması ve bilgisayarların ucuzlaması sonucunda, her gün daha fazla sistem modem kullanılarak telefon hatlarıyla birbirine bağlanmakta; bir sistemde depolanmış ve/veya veriler diğerine kolaylıkla taşınabilmektedir.

Bu veri taşınması bilgi bankalarından abonelerine doğru olabileceği gibi firmaların değişik coğrafik bölgelerde yerleşik birimleri arasında da yapılmaktadır. Ayrıca bilgisayarı olan gençler kendi aralarında özel bilgi bankaları -Bulletinboard System-kulüpleri-kurmaktadırlar. Bu kulüplerin üyeleri zaman zaman çeteler tarafından kandırılarak yukarıda açıklanan bilgisayar suçlarının işlenmesinde kullanılmaktadır (Wilson v.d. s. 25/10-20). Diğer yöntemler daha kolay olduğu için hatlara giriş suçu diğerlerine kıyasla daha az işlenmektedir. Bunun diğer bir nedeni de hatlara girecek olan irtikapçının elde etmek istediği verinin taşınma zamanı kesin olarak bilmemesidir. Bu nedenle de bu yöntem kullanıldığında çalınan oldukça çok miktardaki verinin arasından istenilenin araştırılıp bulunması gerekmektedir. Bu yöntemle işlenen suçun tesbitlenip kanıtlanması da güç olduğundan bu suç türüne ilişkin gerçekleşen bir olay henüz literatüre geçmemiştir.

Bir sistemden diğer sisteme telefon kanalları ile taşınacak veriyi korumanın en iyi yolu veriyi şifrelenmektedir.Veriyi şifrelendirmek için güçlü aletler üretilmektedir. Gelecek bir kaç yıl içinde taşınacak gizli verilerin tümünün bu cihazlar kullanılarak şifrelendirilmesi beklenmektedir. Bu da hatlara giriş tehdidini önemli oranda azaltacaktır.

12. Benzetişim ve Modelleme:

Bazı beyaz yakalı suçların işlenebilmesi için oldukça karmaşık yöntemlerin kullanılması ve ayrıntılı bir planlamanın yapılmasını gerektirebilir. Bu planlama işleminde bilgisayar teknolojisinden yararlanılmakta ya da suç işleme modeli sistemde denenmektedir.

Bu yöntem aşağıda literatürde geçen iki olayla örneklenerek açıklanmaya çalışılmıştır (Porter v.d. s. 454).

Serbest meslek faaliyeti icra eden bir muhasebeci bilgisayarında suç işlemek istedi firmanın muhasebe sisteminin bir benzerini oluşturarak işlemeyi düşündüğü zimnet suçunun muhasebe kayıtlarına etkisini belrlemek için doğru ve degiştirilmiş verileri sisteme yükledi. Gerçek geliştirdiği benzer sistemi muhasebe kayıtlarının istediği şekilde olmasını sağlayacak şekilde ters yönde çalıştırarak işlenecek zimnet suçunun gizlenmesi için muhasebe kayıtlarını belirledi.

İkinci olayda ise; 1973 yılında Los Angelas'da bilgisayarda bir sigorta şirketinin satışının sonuçları tesbitlendi. Bu modelleme ile bilgisayarca okunabilen formlarda altmışdörtbin sahte poliçe hazırlanarak reasurans şirketine devredildi. Benzetişim ve modelleme yönteminin kullanımı için çok fazla bilgisayar saatinin kullanılması ve bir çok programın hazırlanması gereklidir. Bu yöntem ancak konusunda uzman programcıların yardımı ile kullanılabilir.

Bugüne tesbitlenen benzetişim ve modelleme suçlarında kendilerini mesleklerine adamış bilgisayar uzman ve programcıların haberleri olmadan kötü niyetlikişilerce suç işlemede yararlandıkları da tesbitlenmiştir.

Benzetişim ve modelleme suçunu;

-Bilgisayar uygulama programcıları

-Büyük ve karmaşık zimnet suçunu örgütleyebilmek pozisyonundaki yöneticiler işleyebilirler.

Bu yöntemle işlenen suçlar ise; Şüphelenen tüm bilgisayar kullanımları incelenerek tesbitlenebilir.

-Programlar,

-Program dökümanları

-Bilgisayarda hazırlanmış raporlar,

-Bilgisayar kullanım kütükleri ve kayıt defterleri bu yöntemle işlenen suç ve suçluların tesbit ve ispatlanmasında yararlanılacak başlıca kanıtlardır.

SONUÇ:

Bilgisayar suçu gerçekleştirilmesi için bilgisayar teknolojisinin gerekli veya bilgisayarın temel hedefi olduğu yasadışı bir eylem olarak tanımlanabilir. Bu suçlar gerek iş hayatında ve gerekse günlük yaşamda bilgisayarın ve/veya bilgisayar teknolojisinin özellile açık devre, gerçek zaman esasına göre çalışan sistemlerin kullanılmasının yaygınlaşması sonucu artmış ve etkili olduğu alanlar genişlemiştir.

Bu suçların önlenebilmesi için bilgi işlem teknolojisinden yararlanılacak kuruluşlarda, bilgisayar kullanımına başlamadan önce kullanım amacı ve bu amaca en etkin bir şekilde ulaşabilmek için yararlanılacak yöntemler doğru bir şekilde belirlenmeli ve bilgi işlem biriminin örgütlenmesinde çok dikkatli davranılmalıdır. Ayrıca bilgi işlem teknolijisinden yararlanan kuruluşlarda iç denetim işlevi örgütlenmemiş ise, bu birim muhakkak kurulmalıdır.

Son yıllarda üretilmeye başlanan güvenlik cihazlarının kullanılmaya başlanılması ile bilgisayar suçlarının önlenmesinde önemli bir adım atılmıştır. Bu cihazların geliştirilip daha da modernize edilmesi durumunda suçlar daha da azalacaktır. Bilgisayar suçlarının önlenmesi için tedbirler alınırken bilgisayar teknolojisinden yararlanacak iş alanının uzmanlarının bilgili, deneyimli ve ahlaklı bilgisayarcılarla işbirliği yapmaları, bu önlemlerinbeklenen yararını artıracaktır.

SUMMARY

Statistics show that the criminal element of society is taking advantage of computer technology to defraud, embezzle, and abuse organizational resources. On the other hand, auditors, law enforcement agencies, and posecutors are still reluctant to invest the resources necessary to train their people in computer technology. The solution to computer crime is an aboundant supply of auditors and enforcement officials knowledgeable in computer crime and computer technology.

KAYNAKÇA

BLACK, Homer A. Champion, JOHN E. ve MILLER, Gibbes v. : (1973) Accounting In Business Decisions Theory, Method and USE, Prentice-Hall Inc. Englewood Cliffs, New Jersey.

ÇARIKÇIOĞLU, Peyami: (1977) **Elektonik Bilgi İşlem (EBİ) Sistemi Kullanılan Muhasebe Sistemlerinde Denetimin Özellikleri ve Bir Vaka Çalışması** Basılmamış Doçetlik Tezi, İstanbul Üniversitesi, İşletme Fakültesi, İstanbul.

ÇÖMLEKÇİ, Ferruh: (1980) **Muhasebe Denetimi**, Üçüncü Baskı, Eskişehir.

ERDOĞAN, Melih: (1988) **Bilgisayar Kullanılan Muhasebe Sistemlerinde Denetim Süreci**, Eskişehir.

GÜREDİN, Ersin: (-) **Denetim**, Muhasebe Enstitüsü Yayın No: 50, İstanbul.

HİCKS, Jr. JAMES O Leininger, WAYNE E.:(1981) **Accounting Information Systems**, West Publishing Company, St. Pail, Minnesota

Hürriyet Gazetesi, 7 Mart 1992 tarihli sayısı.

KEPEKÇİ, Celal: (1988) **Muhasebe Denetimi ve Mali Analiz Fasikül1-11**, Anadolu Üniversitesi Yayınları No: 118, Eskişehir.

MEİGS, Robert M, MEİGS, WALTER B: (1990) **Accounting: The Basis for Business Decisions**, McGraw-Hill Publishing Company, Boston, Massachusetts.

Resmi Gazete 14 Haziran 1991 tarih ve 20901 sayılı

ROBERSON, Jack C. DAVIS, Frederick G: (1988) **Auditing**, Fifth Edition. Business Publications Inc. Plano Texas.

SELEK, Seha. TEK, Nergis: (1987) **Türkiye'de Denetim İşletmelerinin Genel Görünümü ve Başlıca Sorunları** 30 Eylül-2 Ekim 1987 tarihlerinde Balçova-İzmir'de yapılan 14. Türkiye Muhasebe Kongresi'ne sunulan tebliğ. Yayın: **İstanbul Üniversitesi İşletme Fakültesi, Muhasebe Enstitüsü Dergisi** Yıl 13, Ağustos-Kasım 1967 Sayı: 49-50.

SELEK, A. Seha: (1990) **Muhasebenin Temel Verileri**, İzmir.

ŞANLI, Çetin: (1974) **Finansal Bilgi İşleme** (Basılmamış Doçentlik Tezi), İstanbul.

THOMAS, C. William, HENKE, Emerson O.: (1983) **Auditing Theory and Practice**, Kent Publishing Company, Belmont California.

WALLACE, Wanda A.: (1984) **Handbook of Internal Accounting Controls** Prentice-Hall Inc. Englewood Cliffs, New Jersey.

WİLSON, D. James, ROOT Steven J.: (1989) **Internal Auditing Manual**, Second Edition Warren, Gorham and Lamiont Inc. Boston, Massachusetts.