YMT 311-Bilgi Sistemleri ve Güvenliği

Bilgi ve Bilgi Güvenliği

Konu Başlıkları

- Giriş
- Bilişim Suçları
- Bilgi ve Bilgi Güvenliği
- Sonuç
- Sorular
- Kaynaklar

Giriş

- Bilişim dünyasında bilgi ve bilgi varlıklarının öneminin gün geçtikçe artması, buna paralel olarak bilişim güvenliğinin öneminin de artmasını sağlamıştır. Uluslararası bir ağ sistemi olan İnternet ortamındaki verilerin veya bilgilerin korunması için donanımsal ve yazılımsal güvenlik tedbirleri alınmaktadır.

- Ancak, bu tedbirler sisteme veya bilişim cihazlarına yapılan saldırıları tamamen engelleyememektedir. Bu bağlamda bilişim suçlarının incelenmesi, saldırganların tespit edilmesi için birçok akademik ve ticari çalışmalar yapılmaktadır.

Giriş

- Bu bölümde, bilişim suçları, bilgi ve bilgi güvenliği konuları genel olarak incelenmiştir. Ayrıca bu konularda bilişim suçlarına örnek teşkil edecek saldırılar belirtilmektedir.

Bilgi ve Bilgi Güvenliği
(.Bilgi, Bilginin Değeri)

- En basit tanımlaması ile bilgi kişi ya da kurumlar için kıymet teşkil eden ve para gibi korunması gereken kıymetli bir metadır. Meta ifadesi ile eşya kast edilirken bunun yerine varlık ifadesi de kullanılmaktadır.
- Günümüzde bilgi ön plana çıkmış gibi gözükse de, aslında bilgi; dünün ve bugünün anahtarları iken, geleceğin şekillenmesinde de her zaman anahtar rollere sahiptir.

Bilgi ve Bilgi Güvenliği
(Bilginin Gelişim Evreleri)

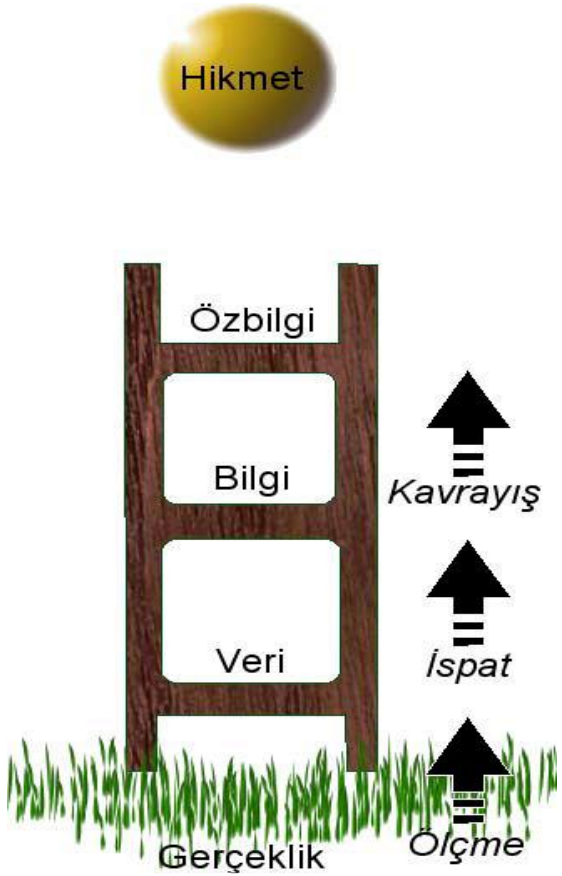
- İnsan bilincinden bağımsız olarak var olanlar veya hikmete ulaşmak için veri haline gelmeye hazır doğada bulunan her şey *gerçeklikdir*.
- Bilişim teknolojisi açısından *veri*, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir.
- *Bilgi;* verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. Bilgi; işlenmiş veri olarak ve bir konu hakkında var olan belirsizliği azaltan bir kaynak olarak da tanımlanabilmektedir. Kısaca, veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, v.s.) çıktısı, bilgi olarak ifade edilebilir.

Bilgi ve Bilgi Güvenliği
(Bilginin Gelişim Evreleri)

- *Özbilgi*; tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Verilerin bir araya getirilip, işlenmesi bilgiyi oluştursa da özbilgi, kullanılan bilgilerin toplamından daha üstte bir kavramdır. Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan özbilgidir.

Bilgi ve Bilgi Güvenliği
(Bilginin Gelişim Evreleri)

- Hikmet (wisdom), tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür. Hikmet, ayrıca, güvenilir yargıda bulunmak ve karar vermek için öz bilginin nasıl kullanılacağını kavramak olarak da tanımlanmaktadır.



Bilgi ve Bilgi Güvenliği
(Bilgi Güvenliği)

- *Bilgi güvenliği;* bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanır.
- Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür.

Bilgi ve Bilgi Güvenliği
(Bilgi Güvenliği)

- Bilgi güvenliğinin sağlanması için kullanılabilecek birçok yöntem olmakla beraber yeni sayılabilecek biometrik alanda yapılan bilgi güvenliği çalışmaları da mevcuttur. Bu biometrik korunma yolları arasında parmak izi ile çalışan sistemler, el ve parmakların şekline göre çalışan sistemler, ses tanıma sistemleri, dijital imza, gözün retina ve iris tabakasından yararlanılarak çalışan sistemler mevcuttur. Buna örnek olarak Kuzey Carolina'daki uluslararası havaalanında kullanılan iris ile çalışan güvenlik sistemi örnek olarak gösterilebilir [18].

Bilgi ve Bilgi Güvenliği
(Bilgi Güvenliği Sertifikasyonu)

- Büyüklüğü ne olursa olsun, ihtiyaç duyan tüm kurumların, kuruluşların bilgilerinin gizlilik, bütünlük ve erişebilirliklerini sağlamak amacı ile kurdukları bilgi güvenliği yönetim sistemini belgelendirmek ve bunu üçüncü taraflara kanıtlamak amacı ile aldıkları; bağımsız belgelendirme kuruluşlarının, yaptıkları denetim sonucu düzenledikleri ve kurumdaki bilgilerin güvenliklerinin sağlanmasına yönelik sistematik bir uygulamanın olduğunun kanıtını sağlamak üzere *kurum* adına düzenlenen sertifikaya veya belgeye TS ISO/IEC 27001 *Bilgi Güvenliği Yönetim Sistemi Belgesi* veya TS ISO/IEC 27001 *Bilgi Güvenliği Yönetim Sistemi Sertifikası* denir.

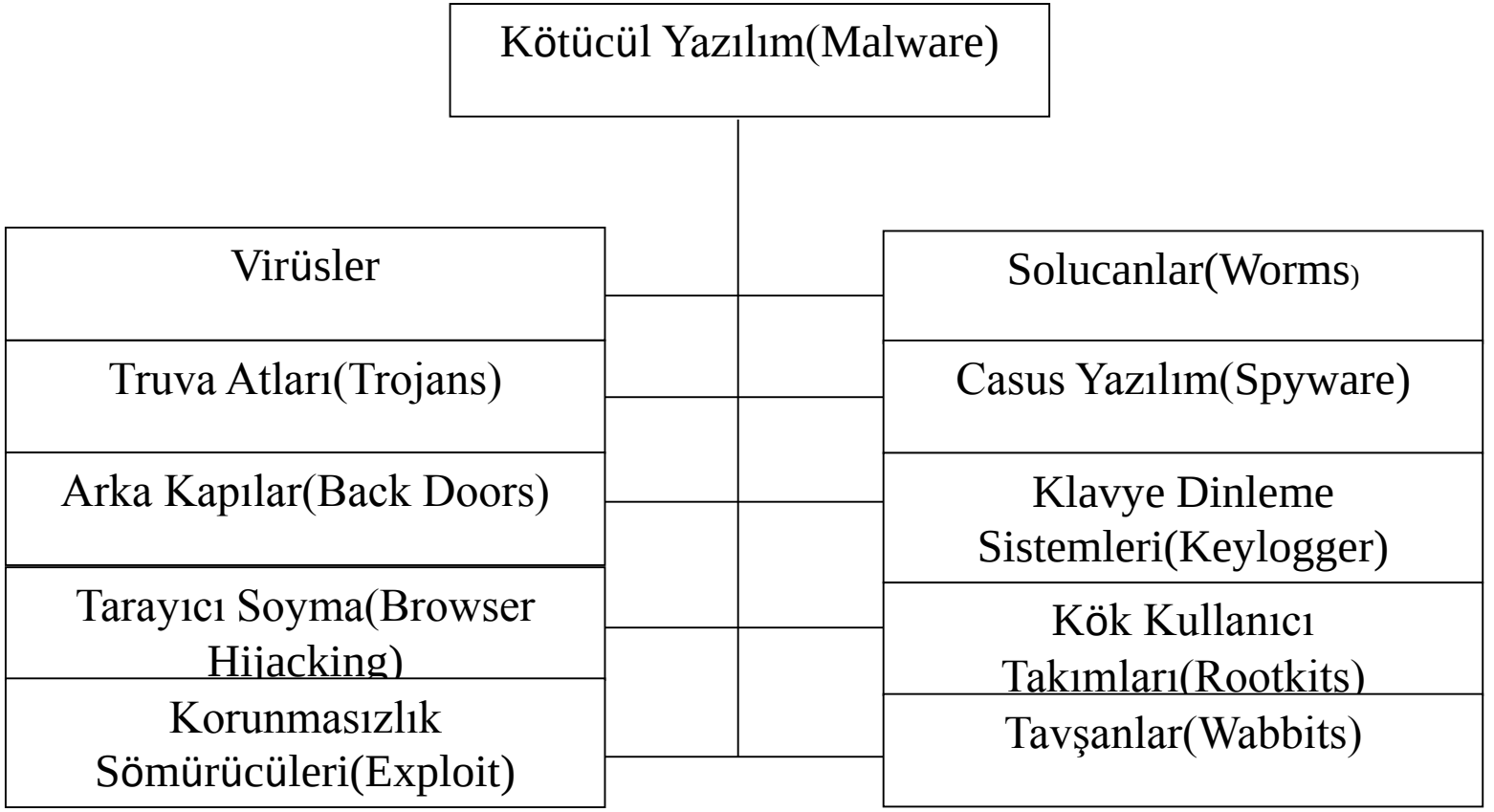
Bilgi ve Bilgi Güvenliği
(Bilgi Güvenliği Sertifikasyonu)

- TS ISO/IEC 27001 bilgi güvenliği yönetim sistemi kurmak ve belgelendirmek bir firmaya, şirkete veya kuruluşa bilgi güvenliği kavramının temel ilkelerini sağlamaktadır. Bilgi güvenliği kavramının temel ilkeleri kısaca G-B-U (C-I-A) kısaltması ile gösterilebilir. Bu kısaltmalar:
  - Gizliliğin korunması (bilgiye ulaşımın, sadece yetki sahibi kişilerce olabildiğinin garanti altına alınması)
  - Bütünlük (bilginin ve bilgi işleme yöntemlerinin, doğruluğunun ve eksiksizliğinin korunması)
  - Ulaşılabilirlik (gereken durumlarda yetkili personelin, bilgiye ve ilgili varlıklara ulaşabilmesinin garanti edilmesi), şeklinde tanımlanır.

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımlar)

- Kötücül yazılım (malware, İngilizce “malicious software”in kısaltılmışı), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır.

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımlar)



Tablo 1. Kötücül Yazılım Ana Türleri

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımlar)

VİRÜS İSMİ	TİPİ	KARIŞTIĞI OLAYLAR	YÜZDE
Win32/Ska	File	140	13.28%
Laroux	Macro	124	11.76%
Marker	Macro	122	11.57%
Ethan	Macro	69	6.55%
Class	Macro	59	5.60%
Win32/Pretty	File	52	4.93%
Win32/NewApt	File	48	4.55%
Melissa	Macro	47	4.46%
Tristate	Macro	44	4.17%
Freelinks	Script	42	3.98%
Win32/Babylonia	File	32	3.04%
Cap	Macro	31	2.94%
Win32/Fix	File	31	2.94%
Thus	Macro	29	2.75%
Win32/Explore.Zip	File	21	1.99%
Win95/CIH	File	19	1.80%

Tablo 2. En Meşhur Virüsler

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımlar)

Yeni kötücül yazılımlardan bir kısmı şunlardır:

- Sazan avlama (phishing),
- Koklayıcı (sniffer),
- Kandırıcı (spoofer)
- Şifre kırıcılar (password cracker),
- Reklâm yazılım (adware),
- Ağ taşkını (flooder),

bununla beraber daha birçok yeni kötücül yazılımın varlığından bahsedilmektedir [26].

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımların Bulaşma Yöntemleri)

- Çoğunlukla ücretsiz dağıtılan uçtan uça dosya paylaşımı (P2P) programları, ekran koruyucular ve oyunlar içine casus yazılım bohçalanması ile bulaşma,
- Faydalı bir yazılım kurulumunun yanında; dosya, klasör ve sistem kütüğü isimlerini zararsız, bilindik veya sisteme ait isimler vererek saptanmasını ve sistemden kaldırılmasını zorlaştırarak sisteme yerleşme,
- Uç kullanıcı lisans sözleşmelerinde yanıltıcı veya eksik bildirim ile kullanıcıya zararlı bir yazılımı bilgisayarına kurdurtma,

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımların Bulaşma Yöntemleri)

- Herhangi bir programın kurulumu sırasında, aslında casus yazılım özelliği taşıyan başka yardımcı ve ek yazılımların kullanıcıya belirtilerek kurdurulması,
- E-posta dosya eklentisi ile e-posta'da verilen bir web adresine gidildiğinde veya doğrudan HTML içerikli e-postaların okunması ile casus yazılım bulaşması,
- İnternet tarayıcılarında bulunan korunmasızlık ve açıklardan yararlanarak kurulum,
- Özellikle internet üzerinden kullanıcıyı aldatıcı mesajlarla yanıltıp; her hangi bir casus yazılımın kurulumunun başlatılması,

Bilgi ve Bilgi Güvenliği
(Kötücül Casus Yazılımların Bulaşma Yöntemleri)

- Çocukları ve bilinçsiz kullanıcıları aldatıcı taktikler kullanmak,
- Çok çeşitli sosyal mühendislik ve insan hatası kaynaklı yöntemler, olarak özetlenebilir.

Bilgi ve Bilgi Güvenliği
(Bilgisayarlarda Kötücül Yazılımların Belirtileri)

- Bilgisayarın her zamanki başarımı düşüyorsa,
- İnternet üzerinde tarayıcı ile sörf ederken istenmedik siteler açılıyorsa,
- İnternet tarayıcısındaki arama çubuğu bölümünde aranmak istenen anahtar kelime girildiğinde ayarlanmış olan arama motoru yerine başka bir arama motoru arama sonuçlarını gösteriyorsa,
- İnternet tarayıcısındaki Sık Kullanılanlar (Favorites) veya Yer İmi (Bookmark) bölümünde yabancı sitelere bağlantılar eklenmişse,
- İnternet tarayıcısının başlangıçta gösterdiği site olan “Başlangıç Sayfası” (Home Page), ayarlanandan başka bir siteyi gösteriyorsa ve bu ayar tekrar düzeltildiğinde yine farklı siteler açılışta ortaya çıkıyorsa,

Bilgi ve Bilgi Güvenliği
(Bilgisayarlarda Kötücül Yazılımların Belirtileri)

- İnternet tarayıcısında daha önce olmayan araç çubukları varsa,
- Sistem tepsisinde (system tray) daha önce bilinmeyen bir simge varsa,
- İnternet'e bağlantı olmadığı durumlarda bile kullanıcı adı ile hitap eden çıkıveren (pop-up) reklamlar görünüyorsa,
- İnternet sayfasında bazı tuşlar çalışmıyorsa (örneğin bir web formu doldururken bir sonraki yazım alanına geçmek için kullanılan sekme (tab) tuşu çalışmıyorsa),
- Bilgisayar ile faal olarak çalışılmadığı bir sırada bilgisayar kasasındaki sabit disk hareketini gösteren lamba sürekli yanıp sönüyorsa,

Bilgi ve Bilgi Güvenliği
(Bilgisayarlarda Kötücül Yazılımların Belirtileri)

- İnternet'e erişim olmadığı sırada sistem tepsisindeki ağ bağlantısını gösteren (iki bilgisayar şeklinde gösterilen) simgede veri aktarımını gösteren hareketler görülüyorsa,
- CD sürücüsü kendi kendine açılıp kapanıyorsa,
- Rastgele hata mesajları çıkıyorsa,
- İnternet'e modem ile bağlanıp da büyük meblağlarda telefon faturası geliyorsa, sistemde çok büyük ihtimalle casus yazılım bulunmaktadır [19,26].

Bilgi ve Bilgi Güvenliği
(Bilgisayarların Kötücül Casus Yazılımlardan Korunması)

Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Alınabilecek bazı güvenlik önlemlerini gerçekleştirmek bilgisayar güvenliği açısından iyi sonuçlar verecektir. Bu güvenlik tedbirleri aşağıdaki başlıklar halinde özetlenebilir:

- *Kötücül Yazılımlardan Korunma*
- *İşletim Sistemi Güncellemeleri:*
- *Anti-Spyware (Casus Karşı Yazılım):*
- *Host (Sunucu) Bloklama*
- *E-posta kontrolü*
- *Browser (İnternet Tarayıcısı) kullanımı*
- *Ofis Programları*
- *Güvenlik Duvarı (Firewall)*

Bilişim Suçları

- Büyük bir ivme ile önemi artmakta olan bilgi güvenliği ve gün geçtikçe artan bilişim suçlarının adli olarak incelenmesi konuları büyük önem kazanmaktadır.

- Bilişim suçları yakın zamanda ortaya çıkan bir ifade olduğundan bazı kavramların birleşimi ile kendisine tanım bulmaya çalışmıştır. Bu kavramlar tanımlanarak bilişim suçu tanımı daha iyi anlaşılabilecektir.

Bilişim Suçları

- Hukuki anlamda suç, bir toplumdaki hukuki kurumlar tarafından ceza veya güvenlik tedbiri yaptırımına bağlanmış fiildir [1]. Uygulamada ise suç; başka insanların veya tüzel kişiliklerin haklarına tecavüz etmek veya yanlış ya da zararlı olduğu için yasaklanan ve bazı durumlarda cezalandırılan davranış olarak tanımlanabilir [2]. Suçu gerçekleştiren kişiye suçlu denir. Hukuki anlamda bir kimsenin suçlu kabul edilebilmesi için suçun o kimse tarafından işlendiğinin hukuki süreçler sonucunda somut deliller ile ispatlanması gerekmektedir.

Bilişim Suçları

- En genel anlamıyla bilişim alanında kullanılan araçlardan yararlanılarak işlenilen suçlar, bilişim suçu olarak tanımlanmaktadır. Bununla beraber bilişim suçları TCK'de bilişim sistemleri kullanılarak işlenen suçlar olarak tanımlanmaktadır. Bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi veya kopyalanması da, bilişim suçları olarak tanımlanmaktadır [4].

Bilişim Suçları

- Bir bilişim suçunu işlemedeki nedenler arasında maddi kazanç elde etmek, kişilerin itibarını sarsmak, intikam almak, sosyal hayatta insanlara aktaramadığını sanal ortamda gerçekleştirmek, karalamak veya yakalanma ihtimalinin zor olduğunu düşünerek zevk amaçlı saldırı yapmak gibi sebepler ortaya çıkmaktadır.

Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- İnternetin yaygınlaşması ile bilişim suçu olarak tanımlayamayacağımız ancak millet menfaatine gibi görünen olaylarda mevcuttur. Bu olaylara somut bir örnek verilirse, mesai saatleri içerisinde bankada sıra bekleyerek işlemlerini tamamlamak isteyen müşterilerle ilgilenmeyen bir çalışanın, bilgisayarında oyun oynadığının görüntülenmesi ve görüntülerin internet ortamına aktarılması olayları da mevcuttur. Bu durum, suç kabul edilmeyip millet menfaatine gözüktüğünden görüntüyü internete aktaran kişi hakkında inceleme başlatılmamış olup, bilişim suçu kapsamına alınmamıştır.

Bilişim Suçları

(Ülkemizde Bilişim Suçlarının Durumu ve Örnekler)

- Ülkemizde artan bilişim suçlarının incelenmesi ve hukuki anlamda kontrolün sağlanması için çalışmalar yapıldığı görülmekte ancak uygulamada henüz istenen seviyeye ulaşılamadığı anlaşılmaktadır.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Delil:** İşlenen bir suç olayında fail/faillerin ortaya çıkarılabilmesi için ipuçları niteliğinde toplanan kaynaklar *delil* olarak tanımlanır. Bu deliller, aydınlatılması istenen olayın en önemli parçalarıdır. Bu elde edilen deliller bir araya getirilerek tüm resim görülmeye çalışılır. Böylece aydınlatılmak istenen olay bir çözüme kavuşturulmuş olur.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Delillendirme:** Suçların tespiti ve yargılanmasındaki en önemli husus *delillendirme* olarak tanımlanmaktadır. *Delillendirme* kısaca, bir suç ile ilgili o suçun kim tarafından ve ne şekilde işlendiğini ispat edici nitelikte bilgiler elde edilmesi ve bunun adli mercilere sunulması şeklinde tanımlanabilir.

Bilişim Suçları

(Bilişim Suçlarında Kullanılan Dijital Deliller)

- **Dijital Delil:** Sanal ortamda işlenen suçlardaki, suçluların tespit edilmesi için elde edilen kanıtlar *dijital delil* olarak isimlendirilmektedir. Bir bilişim suçu ile ilgili, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen bilgilere dijital delil denilmektedir. Bir suçun nasıl olduğunu veya suçtaki kritik elemanları adresleyen teorileri destekleyen veya çürüten, bilgisayar sistemleri kullanılarak kayıt edilen veya iletilen veriler" olarak tanımlamıştır. Dijital deliller "bir suçun işlendiğini gösteren veya suç ile kurban ya da suç ile faili arasında bir ilişki sağlayan veriler" olarak karşımıza çıkmaktadır [7].

Bilişim Suçları

(Dijital Delillerin Özellikleri)

- Dijital deliller, parmak izi veya DNA gibi gizli veriler olabilirler.
- Dijital deliller, kolaylıkla ve hızla sınırları aşabilirler.
- Dijital deliller, kolaylıkla değiştirilebilir, zarar verilebilir veya silinebilirler.
- Dijital deliller, bazen zaman ile sınırlı olabilirler.
- Dijital deliller, genellikle uçucu verilerdir.
- Dijital deliller, güvenliği sağlanmaz ise çabuk deformasyona uğrayabilirler.
- Dijital deliler, yapı itibariyle, fiziksel delillere göre daha hassas ve kolay bozulur niteliktedirler.

Bilişim Suçları

(Dijital Delillerin Özellikleri)

Dijital deliller, normal somut delillere göre yapı itibariyle bazı sıkıntıları barındırmaktadırlar. Bu sıkıntılar şu şekilde özetlenebilir:

1. Dijital Delillerin Bütünlüğü
2. Dijital Delillerin Doğrulanması
3. Dijital Delillerin İnkar Edilememesi
4. Dijital Delillerin Doğruluğu:
5. Dijital Delillerin Daha Sonradan Ele Alınabilirliği [7,11].

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Bilişim suçlarındaki dijital delillerin elde edildiği birçok kaynak olabilir. Bunlar genel olarak şu şekilde sıralanabilir:

- Bilgisayar sistemleri (Masaüstü, dizüstü, sunucu vb.)
- Bilgisayar bileşenleri (HDD, memory vb)
- Erişim kontrol araçları(Smart kartlar, biometrik tarayıcılar)
- Çağrı cihazları, Dijital kameralar, PDA ve PALM cihazları
- Harici harddiskler , Hafıza kartları, Network araçları (Modem, yönlendirici, anahtar)
- Yazıcılar, tarayıcılar ve fotokopi makineleri
- Çıkarılabilir yedekleme üniteleri (Disket, CD, DVD…)
- Telefonlar,Kredi kartı okuyucuları,GPS

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Dijital deliller birçok tipte karşımıza çıkmaktadır. Bunlardan bazıları şu şekildedir:

- Veri dosyaları
- Kurtarılmış, silinmiş dosyalar
- Kayıp alanlardan kurtarılmış veriler
- Dijital fotoğraf ve videolar
- Sunucu kayıt dosyaları
- E-posta
- Chat kayıtları
- İnternet geçmişi
- Web sayfaları
- Kayıt (log)

Bilişim Suçları

(Dijital Delillerin Bulunduğu Yerler)

Dijital delillerin elde edildiği alanlardan en çok göze çarpanları şunlardır:

- Bilgisayarlar (Masaüstü, dizüstü bilgisayar, PDA, sunucu, istemci)
- Elektronik aygıtlar
- Veri havuzları
- Bir sistemde yapılan işlemleri gösteren kayıtlar, geçmiş bilgileri, erişim listeleri
- Yedekleme üniteleri
- Yazılımlar
- E-Postalar
- Çerezler gibi internet ile ilgili dosyalar[7,11].

Bilişim Suçları

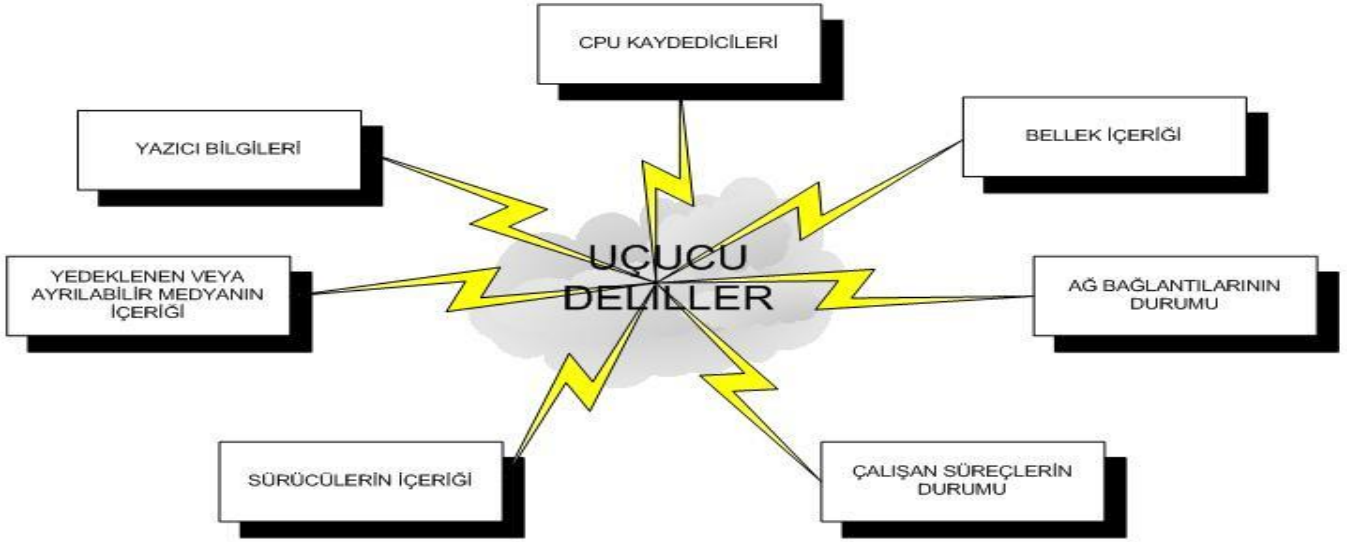
(Dijital Delillerin Toplanması)

- Sanal bir suçun varlığından şüpheleniliyor ise söz konusu suç veya vaka ile ilgili potansiyel delillerin toplanması gerekmektedir. Sürecin doğru bir şekilde işlemesi için öncelikle uygun prosedürleri ve gerekli hukuki şartları anlamak ve sağlamak büyük önem arz etmektedir. Geleneksel delil toplama, delillerin daha sonradan incelenmek üzere sahiplenilmesi anlamına gelmektedir. Fakat dijital delillerde durum biraz farklıdır. Delillerin doğrudan toplanması esnasında bazılarının kaybedilmesi, bozulması ile karşılaşılabilir.

Bilişim Suçları

(Dijital Delillerin Toplanması)

- Uçucu veriler (Ör: bellek, CPU kaydedicileri, çalışan süreçlerin durumu) dediğimiz elektrik kesildiğinde içeriği sıfırlanan ve tekrar kurtarılması mümkün olmayan delillerdir



Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Saldırı* ifadesi en bilindik anlamda kötülük yapmak, yıpratmak amacıyla, bir kimseye karşı doğrudan doğruya silahlı veya silahsız bir eylemde bulunma, hücum, taarruz veya bir sistemin kullanılamaz hale getirilmesi için yapılan her türlü meşru veya gayri meşru hareketler olarak tanımlanabilir. Bilişim sistemlerine yapılan saldırılar da *dijital saldırı* olarak tanımlanmaktadır. Dijital saldırılardaki amaç, bilgiyi çalmak, bozmak, sızdırmak veya bilişim sistemindeki yazılım ve donanımlara zarar vermek olarak belirtilebilir. Dijital saldırıları aktif ve pasif saldırı olarak ikiye ayırmak mümkündür.

Bilişim Suçları

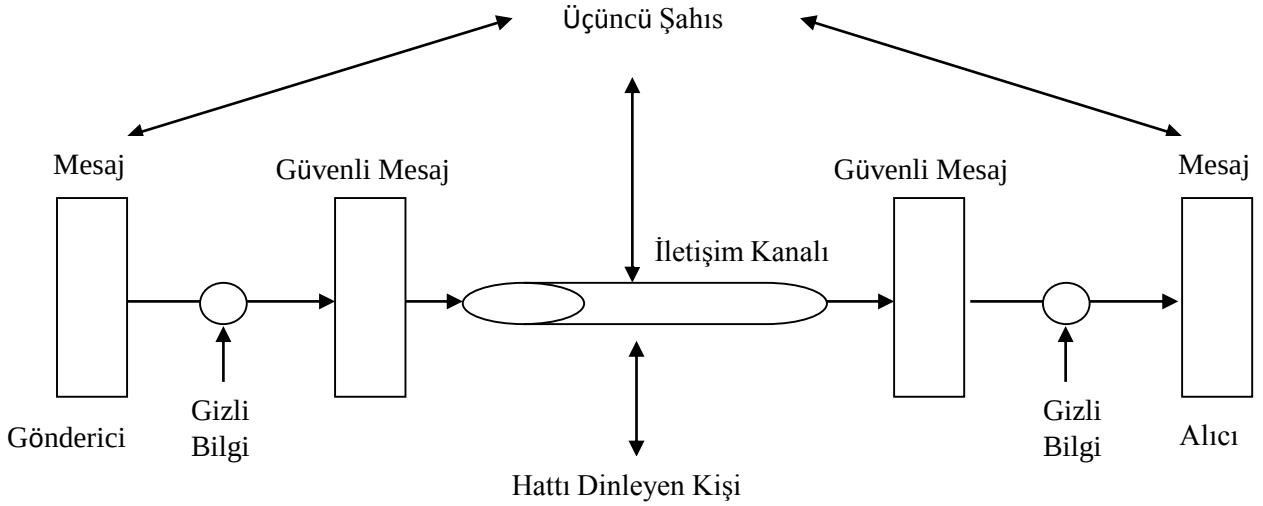
(Dijital Saldırılar ve Dijital Saldırganlar)

- *Pasif saldırıda,* saldırgan taraf pasif davranmakta ve çoğu zaman sadece sistemi gözetlemekle yetinmektedir. Bu saldırı şeklindeki saldırganın yakalanması çoğu zaman daha güç olmaktadır. Pasif saldırı yöntemlerine örnek olarak; Mesajın içeriğini edinme, trafiğin akışını takip etme gibi yöntemler verilebilir.
- *Aktif saldırı* yönteminde ise saldırgan aktif olarak rol oynar ve sistemin içerisine dahil olur. Sistemi savunan tarafın, saldırganı yakalama veya tespit etme ihtimali yüksektir. Aktif saldırı yöntemlerine örnek olarak olarak;
- Rol yapmak (Sniffer olayı, IP aldatmacası vb.)
- Eski mesajın tekrarlanması
- Aktarılan mesajı değiştirme
- Hizmet dışı bırakma/engelleme, gibi yöntemler sayılabilir.

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Şekilde görüleceği gibi aktif veya pasif saldırı mesajın çıkış noktasından başlayarak varış noktasına kadar üçüncü şahıs olarak adlandırılan saldırgan tarafından herhangi bir bölgede gerçekleştirilebilir.



Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Hackerlar (saldırganlar),* kültür ve bilgi düzeyi oldukça yüksek olan, en az bir işletim sisteminin yapısını tam olarak bilen, programcılık deneyimleri yüksek ve konusunda ileri eğitimler alarak uzun yıllarını bu işlere adamış kişilerdir [9]. Diğer bir tanımda ise işletim sistemlerini tam manası ile bilen, derinliklerine inen, bilgisayarla derinlemesine ilgilenen, programlamayı profesyonel düzeyde bilen bilgisayar uzmanlarıdırlar [8].

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Yapılan hacker tanımlamalarına bakılarak farklı niyette çalışan hackerler olduğu görülmektedir. Hackerlar; beyaz şapkalı hacker, siyah şapkalı hacker ve gri şapkalı hacker olarak sınıflandırılmaktadırlar.
- *Hacking* olarak ifade edilen kavram ise bir sisteme sızma ya da zarar verme anlamında yapılan saldırıların genel adıdır.
- *Beyaz şapkalı hackerlar* bilgi bakımından siyah şapkalılardan aşağı kalmamakla beraber; iyi niyetli, zarar vermeyen, amaçları bilgisayar güvenliğini sağlamak olan kişilerdir [8].

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- *Siyah şapkalı hacker* kavramı ise tamamen kötü niyetli, sırf kazanç elde etmek ve karşıya zarar verme amacıyla sistemlere sızan, bilgi çalan, korsanlar için kullanılır. Bu grup hackerların amacı bilgi çalmak veya sisteme zarar vermektir [8]. Siyah şapkalı hackerlar bazı çalışmalarda korsan, saldırgan veya 3. şahıs olarak da adlandırılmaktadırlar.
- Beyaz şapkalı ve siyah şapkalı grubun arasında kalan *gri şapkalı hacker* olarak adlandırılan bir grup vardır ki bunlar yerine göre siyah yerine göre de beyaz şapkalı hacker gibi hareket ederler.

Bilişim Suçları

(Dijital Saldırılar ve Dijital Saldırganlar)

- Bilişim sistemlerine zarar vermek amaçlı çalışan kişiler genelde *cracker* tanımlamasına dahildirler.
- Siyah şapkalı hackerlara nazaran daha zararsız olarak tanımlayabileceğimiz *Lamer* ifadesi genelde küçük yaşta ve hacker özentisi olan, birkaç hacker işlemini bilen ancak programlama bilgisi olmayan, herkesin yapabileceği işleri yaparak ün kazanmak isteyen kullanıcılardır. *Script Kiddie* ise genelde lise çağında olan, programlama bilgisi olmayan genellikle e-postalara saldırma işlemlerini öğrenen kişilerdir. Lamerlara göre fazla hacking bilgileri vardır [8].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Siber kelimesi bilgisayar ağlarına ait olan, internete ait olan, sanal gerçeklik manalarına gelmektedir.
- Soyut olarak iletişim kurulan sistemler *siber alan* olarak tanımlanmaktadır. Dünya üzerindeki en büyük iletişim sistemi olan interneti anlatan sanal alem ve siber alem kavramlarının ikisi de doğru birer önermedir. Siber alanın yaygınlaşması bazı kavramlarında beraberinde ortaya çıkmasına sebep olmuştur.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Zorbalık denince sözlü veya fiziksel şiddet anlamları akla gelir. *Siber zorbalık,* bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür. Elektronik zorbalık ve elektronik iletişim zorbalığı olmak üzere iki çeşit siber zorbalık mevcuttur.
- Siber zorbalık veya tehdidin en çok sosyal medya sitelerinde meydana geldiği görülmektedir. Genellikle fotoğraf ve video yayınlama tarzında gerçekleşen bu eylemler bazen sözlü alay ifadeleri ile mahremiyetlere zarar vermektedir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Elektronik zorbalık,* kişilerin şifrelerini ele geçirme, web sitelerini hackleme (bir sisteme izinsiz girmek), spam (zararlı virüs) içeren e-postalar gönderme gibi teknik olayları içeriyor. Bu tip saldırılar, bireylerin web siteleriyle sınırlı kalmayıp, kurumların ve devletlerin siteleri, yazılım ya da donanımlarını da olumsuz etkiliyor.
- *Elektronik iletişim zorbalığı* ise bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme (cyber-stalking), alay etme, isim takma, dedikodu yayma, hakaret ya da kişinin rızası olmadan fotoğraflarını yayınlama gibi ilişkisel saldırı davranışlarını içeriyor. Bu da direkt olarak insanın duygu ve psikolojisini etkiliyor [14].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Bilgi sistemleri doğrultusunda elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla, ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinlikler *siber saldırı* olarak isimlendirilmektedir. Siber saldırılar genellikle İnternet üzerinden yapılan tecrübeli hackerların yapabildiği saldırı biçimidir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Siber Terörizm(Savaş)* belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır [13].
- Siber terörde, saldırganların elektronik bir saldırı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğalgazı kapatabilecekleri, bilgisayar sistemlerini karmakarışık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve finans sektörünü çökertebilecekleri, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dahilindedir.

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- *Siber ordular* ulusal güvenliği sanal ortamda sağlayan ordulardır. Siber orduların öneminin farkında olan Amerika Birleşik Devletleri gibi gelişmiş ülkeler sanal ortamda saldırı tespit yöntemleri oluşturmaya yönelik yarışmalar düzenleyerek konu hakkında yetenekli kişileri bu ordularına dahil etmektedirler. Pentagonun düzenlediği güvenlikle ilgili bir yarışmada birinci olan bir Türk öğrencinin Pentagon'dan davet mektubu alması buna bir örnektir [15].

Bilişim Suçları

(Siber Alan ve Siber Güvenlik)

- Bilişim dünyasında yeni bir kavram olarak yer bulmaya başlayan siber ahlak olarak da tanımlayabileceğimiz siber etik en genel anlamı ile gerçek hayatta iyi bir birey olmak için yapılan fiillerin sanal ortamda da yapılması olarak tanımlanmaktadır.
- Sanal alemde davranış kuralları konusunda özellikle genç kuşağın eğitilmesi gerekmektedir. Günlük yaşamında hırsızlık yapmayı ahlaki değerleriyle veya toplumsal statüsü ile bağdaştıramayan bir genç net ortamında rahatlıkla hırsızlık yapabilmekte veya başkalarına zarar verebilmektedir.

Bilişim Suçları

(Adli Bilişim)

- Adli kelimesi TDK'nin sözlüklerinde adliye teşkilâtı ve hizmeti ile ilgili, adaletle ilgili olarak tanımlanmaktadır. Bu bağlamda adalete intikal etmesi gereken hadiselerin tamamına ise *adli vaka* veya *adli olay* denmektedir.
- Adli bilişim teriminin kökeni, İngilizce orijinal ismi ile Computer Forensics'tir

Bilişim Suçları

(Adli Bilişim Çeşitleri)

1. **Bilgisayar Adli Bilişimi (Computer Forensics) :** Daha çok bir bilgisayar üzerinde yapılacak araştırmalarla ilgilenir. Örneğin: Harddisk, RAM, işletim sistemi üzerinde yapılacak araştırmaları kapsar.
2. **Bilgisayar Ağlarına Yönelik Adli Bilişim (Network Forensics) :** Ağ sistemleri ve iletişimine yönelik incelemeyi kapsar.
3. **Bilgisayar Ağ Cihazlarına Yönelik Adli Bilişim (Network Device Forensics):** Yönlendirici, switch gibi cihazlar üzerinde yapılacak incelemeyi kapsar.
4. **İnternet Adli Bilişimi (İnternet Forensics):** Genel olarak internet kaynakları ve internet sistemleri üzerinde yapılan araştırmayı kapsar.
5. **Bilgi Adli Bilişimi (Information Forensics):** Bütün olarak bilgiyi içeren her türlü materyali barındıran sistemler üzerinde yapılan incelemeyi kapsar.

Bilişim Suçları

(Adli Bilişim Çalışma Alanları)

- Adli bilişimin çalışma alanlarından bazıları ana başlıklar halinde şöyle sıralanabilir:
- Veri kurtarma
- Veri imha etme
- Veri saklama
- Veri dönüştürme
- Şifreleme(Kriptografi)
- Şifre çözme
- Gizlenmiş dosya bulma.

Bilişim Suçları

(Adli Bilişimin Faydaları)

- Adli bilişim, yalnızca bilişim suçlarına has bir delil toplama metodu değildir. Bilişim suçlarından başka, klasik suçlara ilişkin olarak da ihtiyaç duyulan deliller, yine elektronik aygıtlar içerisinde de yer alabilir. Örneğin, bir bilişim suçu olmayan bir hırsızlık vakasında, soygun planı ve buna ilişkin haritalar bilgisayar ile hazırlanmış ve halen bilgisayarda mevcut olabilir. Bu bilgilere ulaşmada da yine adli bilişim devreye girecektir. Bu duruma en bariz örnek olarak; hala devam etmekte olan *Ergenekon* soruşturması ile alakalı bazı verilere, bilgisayar kayıtlarından ulaşılması gösterilebilir.

Bilişim Suçları

(Adli Bilişim Uzmanlığı)

- *Adli bilişim uzmanı*, bilişim sistemleri konusunda ileri derecede bilgi sahibi olan kimsedir.
- Adli bilişim uzmanı kabul edilmek için birtakım sertifika programları mevcuttur. Bu programlardan birine devam ederek sertifika almak ve adli bilişim uzmanı sıfatına sahip olmak mümkündür.
- Bu sertifika programlarından en çok kabul edilenleri şunlardır: EnCase Certified Examiner (ENCE), Certified Computer Examiner (CCE), Certified Computer Crime Investigator (CCCI), Computer Forensic Computer Examiner (CFCE), Certified Information Forensics Investigator (CIFI), Professional Certified Investigator (PCI) [16].

Bilişim Suçları

(Adli Bilişimde Dijital Delillerin Kanıt Olarak Kullanılabilmesi)

- Adli bilişimde elektronik bulgunun, bir hukuki delile dönüştürülme süreci belli prosedürleri takip eder. Uygulanan bu prosedürlerden sonra dijital delil, kendisini bir hukuki delil olarak ortaya koyar. İşte bu prosedüre, *adli bilişim safhaları* denilmektedir. Adli bilişimde dijital delillerin kanıt olarak kullanılabilmesi için incelenmesi gereken dört safha şu şekildedir [16]:
- Toplama (Collection)
- İnceleme (Examination)
- Çözümleme (Analysis)
- Raporlama (Reporting)

Sonuç

- Bilgi güvenliği konusunda güvenlik açıklarının önlenebilmesi için, kişilerin ve kurumların basitten en karmaşık yöntemlere kadar bir dizi önlemler alması gerekir. Ancak, tüm önlemler alınmış olsa da, sürekli gelişen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş kendini %100 güvende hissetmemelidir. Saldırılar; kötü niyetli kişiler, arkadaşlarımız veya tanıdığımız kişilerden gelebilir.

Sonuç

- Alınması gereken en temel önlemler, risklere karşı sürekli uyanık olmak, bu çalışmada açıklanan saldırı tekniklerine karşı uyanık olmak, yeni gelişmeler ışığında gerekli güncellemeleri yaparak saldırılardan etkilenme olasılığını en aza indirgemek olarak belirtilebilir. Güvenliğin statik değil dinamik bir sürece sahip olduğu, koruma ve sağlamlaştırma ile başladığını, bir hazırlık işlemine ihtiyaç duyulduğu, saldırıların tespit edilmesinden sonra hızlıca müdahale edilmesi gerektiği ve sistemde her zaman iyileştirme yapılması gerektiği unutulmamalıdır.