ÜÇÜNCÜ KISIM

BİLGİ GÜVENLİĞİ VE BİLİŞİM SUÇLARI

BİRİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ

1.1. GİRİŞ

Bireylerin ve toplumların yaşamlarını devam ettirmek ve refah seviyelerini yükseltmek açısından temel bir ihtiyaç olan bilgi; insanlık tarihi boyunca inceleme, araştırma, deneme, öğrenme, düşünme ve ilham alma yoluyla üretilmiş ve mevcut bilgi varlığı genişletilmiştir.

İnsanoğlu bilgiyi yaşamını devam ettirmek, refah seviyesini yükseltmek, ürün ve hizmetleri üretmek ve organizasyonları oluşturmak amacıyla kullanmıştır. Yaşadıkları dönem itibarıyla daha fazla ve daha nitelikli bilgiye sahip olan toplumlar diğerlerine göre daha yüksek bir refah seviyesine erişmiş ve güçlenmiştir.

Her ne kadar bilgi ilk insan topluluklarından beri hayati önem taşıyor olsa da özellikle 20'nci yüzyılın ortalarından itibaren elektronik alanında yaşanan gelişmeler bilginin elde edilmesi, depolanması, işlenmesi ve iletilmesi açısından bir çığır açmış ve bilgi toplumuna dönüşüm sürecini de önemli ölçüde hızlandırmıştır. Son yıllarda ise bilgi ve iletişim teknolojileri sosyal hayatın başta hukuk olmak üzere tüm alanlarında kullanılan ve bu alanlardaki gelişmeleri etkileyen temel faktör haline gelmiştir.

Bireyler toplumun ve ekonominin bir parçası olarak bilgi ve iletişim teknolojilerine dayalı yaşam ve iş süreçlerine dâhil olmanın ötesinde kişisel yaşamlarında daha fazla ve yoğun biçimde elektronik ortamı kullanır hale gelmektedir. Geleneksel sosyal yaşamda bilgi ve iletişim teknolojilerinin etkileri hissedilirken bilgi ve iletişim teknolojilerine dayalı sosyal ağlar gibi yeni sosyal yaşam pratikleri ortaya çıkmaktadır.

Ekonomik, sosyal ve bireysel yaşamda bilgi ve iletişim teknolojilerine dayalı olarak meydana gelen bu gelişmeler olumlu etkilerinin yanı sıra bazı olumsuzluklara da neden olabilmekte ve riskler barındırmaktadır. Bu teknolojilerin kullanımına bağlı olarak ortaya çıkan riskler de mevcuttur. Bu çerçevede; bilgi güvenliği ve kişisel bilgilerin korunmasına ilişkin bireysel, mali ve ulusal güvenlik problemleri ön plana çıkmaktadır.

Bu teknolojilerin kullanımı ile geleneksel tipteki suçların işlenmesi kolaylaşabilmekte, yeni suç tipleri de ortaya çıkabilmektedir. Öte yandan, sanal ortamın sınırsız dünyası, bireysel yaşam ve sosyal ilişkiler üzerinde meydana getirdiği değişimler ile bazı olumsuzluklara da neden olabilmektedir.

Sanal ortam pek çok açıdan tali bir seçenek olmaktan çıkarak ekonomik, sosyal ve bireysel yaşamın gerçekleştiği bir ortama dönüşmektedir. Bu nedenle sanal ortamın, mevcut hukuk düzeni ve kamu politikalarının türevleriyle yönetilmesinde güçlükler ortaya çıkmakta, yeni politika yaklaşımlarına ihtiyaç duyulmaktadır.

1.1.1. Temel Kavramlar

Siber güvenlik konusunda kullanılan temel teknik terimler, bu bölümde açıklanmıştır.

Açıklık: Yazılım veya donanımda, programlama hatası nedeniyle bulunan ve bilgisayarın kötü niyetli kişiler tarafından kullanılmasına sebep olan hatalara, açıklık denmektedir. Açıklıklar, kötü niyetli kişiler tarafından bilgi sistemlerinde bulunan bilgileri silmek, çalmak, değiştirmek veya diğer sistemlere saldırı düzenlemek amacıyla istismar edilmektedir.[668]

Arka Kapı (Backdoor): Sistem ve sistem kaynaklarına sıradan prosedür dışında bir yöntem ile erişim sunan yazılım ya da donanım mekanizması.

Atlatma (Bypass): Bir hedefe erişim için alternatif bir yöntem izleyerek alınan güvenlik önlemini etkisiz bırakmaya verilen isimdir.

[668] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.11.

Bot: Bilişim dünyasında "robot" anlamında kullanılan yaygın bir terimdir. Pek çok bilgisayar işlemini yarı-otomatik olarak yapabilen robotlar bilişimin tüm alanlarında kullanılır. Bir bot programı bağımsız olarak otomatik işleri gerçekleştirebilmektedir. Bot programları arama motorlarında kullanılan, web siteleri hakkında bilgi almak için kullanılanlar gibi masum olabilir. Fakat aynı zamanda daha farklı zararlı eylemlerin gerçekleştirilmesi için de kullanılabilir. Örneğin, bir bot, bilgisayarınızdaki tüm bilgiye ulaşmak ve diğer kişi veya kurumlara karşı suç içeren eylemlerde kullanılabilir. Aynı zamanda yetkisiz olarak erişim sağlanan bir bilgisayara kurulmuş olan bot programı o bilgisayarın yasadışı faaliyetlerde kullanılmasına sebebiyet verebilir. Bu türlü bilgisayarlar için bot ismi kullanılmaktadır.

Botnet: Bot programları kullanılarak, bilgisayarların belli bir merkezdeki kontrol sunucusuyla veya birbirleriyle haberleşmesi sağlanarak bir veya birkaç merkezden yetkisiz olarak yönetilen bilgisayar ağlarına botnet ismi verilmektedir. Bir botneti tek bir kişi merkezi veya birkaç merkezden yönetebilmektedir. Botnet sahipleri botnetleri suç işlemek için kendileri kullanılabilmekte veya suç işlenmesi için kiraya verebilmektedir.

Bütünlük: Bu prensibin amacı veriyi göndericiden çıktığı gibi alıcıya ulaştırabilmektir. Bu prensibin başarıyla yerine getirilmesi durumunda orijinal veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, verinin bir kısmı veya tamamı tekrar edilmemiş ve veri akışının sırası değiştirilmemiş bir şekilde alıcıya ulaşmaktadır.[669]

Casus Yazılım (Spyware) : Kullanıcıya ait bilgileri ele geçirmek amacı ile yazılan programlardır. Sürekli açılan pencerelere neden olabilirler. İnternet tarayıcısında istem dışında araç çubukları kurabilirler. İnternet tarayıcının ana sayfasının değişmesine neden olabilirler.

Dağıtık Servis Dışı Bırakma (Distributed Denial of Service – DDoS) Saldırıları: Servis dışı bırakma saldırıları bilgi sistemlerinin servis vermesini engelleyen saldırılardır. Dağıtık servis dışı bırakma saldırıları, birçok bilgisayardan bir sisteme e-posta gönderilmesi, belirli bir ağ trafiğinin yönlendirilmesi ile

[669] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.9.

gerçekleştirilen saldırılardır. Bu durumda internet bağlantısının kapasitesi veya sunucu bu ağır trafiği kaldıramamakta ve çalışamaz hale gelmektedir. Bu saldırılarda bazı durumlarda saldıran bilgisayar sayısı yüz binleri bulabilmektedir.

Dolandırıcılık (Scam) : Dolandırıcılık (Scam) terimi kişilerden para çalmak için yapılan dolandırıcılık eylemlerinin tamamından bahsederken kullanılmaktadır.

Gelişmiş Siber Casusluk Tehdidi (APT-Advanced Persistent Threat): İleri seviyede ve uzun süreli tehditler içeren zararlı yazılımlar için kullanılan bir tabirdir. APT'lerin en temel özellikleri; ileri seviyede oldukları için, profesyonel kadro, kurumlar ve teknik imkânlar gerektirmesi ve kalıcı ve yaşam sürelerinin uzun olabilmesi için, geçerli sertifikalar ile imzalanma ve sıfırıncı gün açıklıkları ile yayılma gibi tespit edilmesini engelleyecek teknikler kullanmalarıdır.

Gizlilik: Bilginin yetkisiz kişilerin eline geçmesinin engellenmesi prensibine verilen isimdir.[670]

Güvenilirlik: Sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Başka bir deyiş ile güvenilirlik, sistemden ne yapmasını bekliyorsak, sistemin de eksiksiz ve fazlasız olarak bunu yapması ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir.[671]

Güvenlik Prensipleri: Bilişim sistemleri güvenliğinin de temeli kabul edilen "Gizlilik, Bütünlük ve Süreklilik" kavramlarından oluşan üç temel prensibe verilen isimdir. Bu prensiplerin başarılı bir şekilde yerine getirilmesi durumunda sistem güvenliği sağlanmış kabul edilmektedir. Bu prensiplerin uygulanmasındaki problemlerin tamamı sisteme yönelik güvenlik problemleridir. Prensiplerin ihlalini sebebiyet verebilecek her türlü saldırı tehdidi de, sistemin güvenliğine yönelik saldırı tehdidi olarak değerlendirilmektedir. Belirtilen 3 temel prensibin haricinde, bu prensiplerle de kesişimi olan ve önemli kabul edilen; izlenebilirlik (accountability), kimlik sınaması (authentication), güvenilirlik (reliability-consistency), inkâr

[670] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.8.
[671] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.11.

edememe (non-repudiation) prensipleri de, sıkça kullanılan güvenlik prensibi kavramları olması nedeniyle bu bölüme dâhil edilmiştir.[672]

İnkâr Edememe: Göndericinin alıcıya bir mesaj gönderdiğini inkâr etmesini önleme ve aynı zamanda alıcının göndericiden bir mesaj aldığını inkâr etmesini önleme prensibine verilen isimdir. Bu prensip daha çok gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır ve gönderici ile alıcı arasında çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaktadır.[673]

İstenmeyen E-posta (SPAM) : Çok sayıda alıcıya aynı anda gönderilen gereksiz veya uygunsuz iletilerdir. İstenmeyen e-postalar genelde reklam amaçlı olmaktadır. Aynı zamanda bu e-postalar kullanıcıların zararlı sitelere yönlendirilmesini sağlayarak, tıklama sahteciliği, yetkisiz erişim veya bilgi çalma gibi amaçlarda sıklıkla kullanılmaktadır.

İstismar Etmek (Exploit): Sistemdeki bir zayıflıktan faydalanarak sisteme yetkisiz erişim sağlamaktır. Sistemdeki zayıflıktan faydalanarak sistemlere yetkisiz erişim sağlayan kod parçacıklarına da sömürü kodu (exploit code) ismi verilmektedir.

İzlenebilirlilik: Sistemde gerçekleşen işlemleri, daha sonrasında analiz edebilme adına kayıt altına alma prensibidir. Herhangi bir siber saldırı sonucunda bu prensibin uygulanmadığı sistemleri analiz etmek mümkün değildir. İlgili bilgisayar olaylarına müdahale ekibi, bu prensibin yeterli ve gerekli seviyede uygulanmadığı sistemlerde analiz işlemlerinde çok zorlanmaktadır.[674]

Kimlik Sınaması: Ağ güvenliği açısından kimlik sınaması; alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilebilir. Günümüzde kimlik sınaması, sadece bilgisayar ağları ve

[672] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.8.
[673] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.11.
[674] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.11.

sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir.[675]

Köle Bilgisayar: Bot tarafından enfekte olmuş bilgisayarlara zombi veya köle bilgisayar denmektedir. Bu bilgisayarlar botnet'in bir parçasını oluşturmakta ve bilişim suçlarında saldırganı gizlemek veya saldırının etki derecesini artırmak amacıyla kullanılmaktadır.

Kritik Altyapı veya Kritik Bilgi Sistem Altyapıları: Devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir.

Oltalama (Phishing) Saldırıları: Kişisel bilgilerin toplanması amacıyla yapılan eylemlerdir. Toplanan kişisel bilgiler, bankacılık işlemleri, kredi kartı kullanarak büyük alışverişler yapılması gibi suçlarda kullanılmaktadır. Bu eylemlerde kullanıcılar, sahte siteler, e-postalar yoluyla gerçeğe çok yakın senaryolarla aldatılmaya çalışılmaktadır. Bu tür saldırıların başarılı olabilmesinde kullanıcının rolü büyüktür.

Ortadaki Adam Saldırısı (Man-in-the-Middle-Attack) : Bir ağ üzerinde kurban bilgisayar ile diğer ağ araçları (yönlendirici, switch, modem ya da sunucu gibi) arasına girerek verileri yakalama ve şifrelenmemiş verileri görebilme ilkesine dayanan bir saldırı çeşididir. Ağ üzerinde veri paketleri serbestçe dolaşır. Özellikle ortak yayın olarak salınan paketler, aynı ağa bağlı tüm cihazlar tarafından görülebilir. İlkesel olarak hedefinde kendi IP'si olmayan bir paketi alan makinelerin, bu paketlerle ilgili herhangi bir işlem yapmamaları gerekir. Ancak istenirse bu paketlere müdahale edebilir ya da içeriğini öğrenebilirler. Aradaki adam saldırısı ağ üzerindeki paketleri yakalayarak manipüle etmek olarak özetlenebilir.

Payload: Bir sistemde yetkisiz erişim elde edilmesi sonrasında, kod çalıştırıp, saldırganın sistemde yapmak istediği değişikliği yapmasını sağlayan, yetkisiz

[675] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.11.

işlevleri gerçekleştiren kod parçacıkları veya bunların derlenerek çalıştırılabilir dosya haline getirilmiş şeklidir. İstismar kodları ile birlikte kullanılmaktadır.

Port veya Zafiyet Taraması: Bir bilgisayar üzerindeki portların, o bilgisayarda hangi ağ servislerinin çalıştığının hızlıca anlaşılması için teker teker yanıt verip vermediğinin kontrol edilmesidir. Bu işlem otomatik yazılımlar sayesinde kısa sürede gerçekleştirilebilmektedir. Tarama işlemi sonucu saldırgan, bilgisayarda hangi açıklıkları kullanabileceği hakkında bilgi sahibi olur. Otomatik yazılımlar ile bu portlarda çalışan servislerin sürüm bilgilerine göre, bu servislerin açıklıklarını tespit etmeye de zafiyet tarama denmektedir. Bir sisteme sızmayı planlayan bir saldırganın kullanacağı ilk yöntemlerden birisi port veya zafiyet tarama olacaktır.

Reklam Yazılımları (Adware): Reklam yazılımları, bilgisayarda çoğu zaman farkında olmadan kurulan küçük programlardır. Bedava yazılımların içinde bulunabilmektedir. Reklam yazılımları açılır pencere (pop-up) reklamlarının ekranınızda çıkmasına izin vermekte ve aynı zamanda internette ne ile ilgilendiğinizin izini sürmek için kullanılmaktadır. Reklam yazılımı internette gezdiğiniz tüm sayfaları kaydetmektedir. Bu bilgiler periyodik olarak reklam programının sahibine gönderilmekte ve size özel reklamlarının iletilmesinde kullanılmaktadır.

Servis Dışı Bırakma (Denial Of Service) Saldırısı: Verilen hizmetin kesilmesine veya aksamasına sebebiyet verebilecek saldırılardır. Hizmet kesilmesine sebebiyet veren saldırgan bilgisayarlar çok farklı yerlerden dağıtık durumda olduğunda DDOS terimi kullanılmaktadır.

Sıfırıncı Gün Açıklığı: Herhangi bir üründe bulunan, o ürünün üreticisi veya diğer bilgisayar güvenliği ile ilgilenen kişi ve kuruluşların bilmediği fakat saldırganların farkında olduğu ve kullandığı açıklıklardır. Gelişmiş zararlı yazılımlar hızlı bir şekilde yayılabilmek için sıfırıncı gün açıklığını kullanmaktadır.

Sızma (Penetrasyon): Bir sistemin güvenlik mekanizmalarındaki tasarımsal, donanımsal veya yazılımsal açıklıkların istismar edilerek yetkisiz erişim elde etmenin genel adıdır.

Sosyal Mühendislik: İnsan faktörünü kullanan saldırı tekniklerinden ya da kişiyi etkileme ve ikna yöntemlerinden faydalanarak normal koşullarda bireylerin gizlemeleri / paylaşmamaları gereken bilgileri bir şekilde ele geçirme sanatı sosyal mühendislik olarak ifade edilir.

Süreklilik: Bu prensip, sistemlere kurum içinden veya dışarıdan gelebilecek, sistemlerin performansını düşürücü etkiler yapacak saldırı tehditlerinin veya tasarımsal hataların önlenmesi prensibidir.[676]

Solucan: Solucan kendini mümkün olduğunca çok bilgisayara dağıtmak için tasarlanan programlardır. Solucanların virüslerden farkı, yayılmak için kullanıcıya veya dosyalara bulaşmaya ihtiyaçlarının olmaması ve aynı zamanda kendi kendilerini bulundukları yerlerde tekrarlıyor olmasıdır.

SQL Sorgu Enjeksiyonu: Web uygulamalarında kullanılan uygulama-veritabanı ilişkisine sahip sistemlerdeki kullanıcının ilgili sorgulamaları yapabilmesi için oluşturulmuş olan sorgu alanı manipüle edilerek sistemdeki bilgilere yetkisiz erişim sağlayan saldırı yöntemine verilen isimdir.

Şaşırtma (spoof): Ağ iletişiminde kendisini başka biri göstererek, yapmış olduğu saldırıda kimlik belli etmemek veya trafiği izlemek ve bilgi çalmak amacıyla yapılan saklanma eylemidir.

Trafiğin Dinlenmesi (Sniffing): Ortadaki Adam Saldırısı ile benzer bir saldırı yöntemidir. Haberleşme esnasında gelip-giden veriye yetkisiz erişimin gerçekleştirilmesine izin veren saldırı türüdür.

Truva Atı: Truva atı bilgisayar için yararlı gibi gözüken ve kullanıcının çalıştırması ile aktif olan zararlı yazılımlardır. İsmi efsanevi Truva Atı'ndan gelir çünkü çalışmaları için kullanıcının kendi isteği ile Truva atını içeri (bilgisayara) alması gerekir. Kendilerini virüsler gibi kopyalayamazlar. Kullanıcı bilgisayara Truva atı içeren programı yüklemedikçe zarar veremezler.

Tuş Kaydedici (Keylogger) : Tuş kaydedici klavyedeki hangi tuşlara basıldığını kaydeden bir programdır. Gelişmiş klavye kaydediciler fare hareketlerini

[676] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.10.

ve ekran görüntüsünü resim dosyası olarak kaydedebilmektedir. Klavye kaydedici daha sonra tuttuğu kayıtları fark edilmeden kötü niyetli kişilere e-posta veya diğer yollarla göndermektedir. Klavye kaydediciler casus yazılımların bir çeşididir.

Veri Tabanlı Kontrol ve Gözetleme Sistemi (Supervisory Control and Data Acquisition (SCADA): Bir tesise veya işletmeye ait tüm ekipmanların kontrolünden üretim planlamasına, çevre kontrol ünitelerinden yardımcı işletmelere kadar tüm birimlerin otomatik kontrolü ve gözlenmesi sağlayan ve anlık olay ve alarmları saklayarak geçmişte meydana gelen olayları da tekrar günün tarihinde ve saatinde gözlemlenebilmesine imkân veren geniş kapsamlı endüstriyel sistemlere verilen isimdir.

Virüs: Bilgisayara bulaşmak için dosyalara tutunan ve kendini çoğaltabilen programlardır. Virüsler çoğalarak yayılmak ve bulaştıkları sistemlerde çalışarak zarar vermek için yaratılırlar. Virüslerin aktif olabilmesi için bir şekilde kullanıcı tarafından çalıştırılmaları gerekir.

Zehirleme (Poisoning) : Haberleşme esnasında adres ve makine bilgileri gibi eşleştirme değerlerinin tutulduğu tablolarda değişiklik yaparak, kullanıcının haberleşmesini manipüle etme veya kesme saldırılarına verilen isimdir. ARP tablosu ve DNS Önbellek değerlerinde yapılan değişikliklerle ARP Zehirlenmesi ve DNS Önbellek zehirlenmesi gibi saldırılar yapılmaktadır.

Zararlı Yazılım: Tüm kötü amaçlı yazılımlar için ortak kullanılan bir terimdir. Virüsler, solucanlar, tuş-kaydediciler, casus yazılımlar, reklam yazılımları kötü amaçlı yazılımlar içinde yer almaktadır.

1.1.2. Bilgi Güvenliğine Yönelik Tehditler

Bilgisayarların birbirine bağlanması ile ortaya çıkan ve merkezi bir yöneticinin olmadığı internet üzerinden veya işleyişi kolaylaştırmak, üretimi hızlandırmak ve bilgiye erişim imkânını artırmak amacıyla kurulan bütün ağ sistemleri üzerinden izin verilmeyen erişimlerin sağlanması bilgi güvenliğine yönelik en temel tehdittir. Bu tehdidi "Siber Tehdit", bu doğrultuda gerçekleştirilen her türlü eyleme "Siber Saldırı", ekonomik, politik, askeri veya psikolojik amaçlar için, hedef

seçilen ülkeye, kurum veya kuruluşa, bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırıların tamamına "Siber Savaş" (Cyber Warfare) denilmektedir.

Günümüzde "Siber Saldırılar" bireysel, kurumsal ve toplumsal hedeflere yönelik olabilmektedir. Bireysel saldırılarda hedef bireylerin kişisel bilgilerini ele geçirmek ve manipüle etmektir. Bu tür saldırılar kişisel bilginin gizliliğine yönelik bir tehdittir.

Kurumsal ve toplumsal hedeflere yönelik yapılan saldırılar kurumları ya da devletleri zarara uğratmayı amaçlamaktadır. Siber Savaş kabul edilebilecek bu tür saldırılarda, Kritik Bilgi Sistem Altyapıları hedef alınmaktadır. Bu sistemlerin zarar görmesi halinde sağlık, enerji, ulaşım, haberleşme, su dağıtımı, bankacılık acil hizmetler gibi kamu hizmetlerinin aksaması gibi tehditler söz konusudur.

Genel bilgileri kısaca verilen siber saldırılar ve bilgi güvenliğine yönelik tehditleri "Siber Dünya'da Gerçekleşebilecek Saldırılar" ve "Siber Saldırı Çeşitleri" başlıkları altında değerlendirmek mümkündür.

1.1.2.1. Siber Dünya'da Gerçekleşebilecek Saldırılar

Siber Dünya'da gerçekleştirilen siber saldırılar, farklı amaçlarla farklı hedeflere farklı yöntemlerle yapılabilmektedir.

Şekil 54'te gerçekleştirilebilecek saldırı türleri, motivasyonları, hedef kitlesi ve kullanılan metotları verilmiştir.[677]

[677] Pro-G Proje Bilişim Güvenliği ve Araştırma San. ve Tic. Ltd. Şti., 2003, Sy.10.

Şekil 54 - Siber Dünya'da Gerçekleştirilebilecek Saldırılar

Saldırı Türleri	Motivasyon	Hedef Kitle	Metot
Siber Suçlar	Ekonomik fayda	Kişisel Kullanıcılar, Firmalar	Kullanıcı Bilgilerini Çalma, Sahtekarlık, Şantaj, Saldırı, Güvenlik Açığı Kullanımı, Lisanssız Yazılım Kullanımı vb.
Hactivism (Siber Korsanlık)	Politik amaçlar ve değişiklikler, kişisel tatmin	Kurumlar, Devletler	Siber ortamdaki saldırı yöntemlerinin kullanımı
Siber Casusluk	Ekonomik fayda ve kritik bilgi kazanımı	Kişisel Kullanıcılar, Firmalar, Devletler	Siber ortamdaki saldırı yöntemlerinin kullanımı, Güvenlik Açığı Kullanımı,
Siber Terör	Politik değişiklikler	Devletler	Bilgisayar-tabanlı şiddet ve yıkım
Siber Sabotaj	Ekonomik fayda, kişisel tatmin	Kurumlar, Devletler	Güvenlik Açığı Kullanımı, İnsan faktörü,
Siber Savaş	Politik veya askeri fayda	Kritik Bilgi Sistem Altyapıları, askeri bilgi sistemleri	Siber ortamdaki saldırı yöntemlerinin kullanımı, Güvenlik Açığı Kullanımı

1.1.2.2. Siber Saldırı Yöntemleri

Siber saldırılarda gerçekleştirilebilecek saldırılar noktasında herhangi bir sınırlandırma olmamakla beraber, siber saldırı yöntemleri verdikleri zararlar ve gerçekleştirilme şekilleri göz önünde bulundurulduğunda temel kavramlar kısmında kısaca açıklaması verilen 5 başlık altında gruplandırılabilir:

1. Servis Dışı Bırakma Saldırıları (DDOS, DOS)
2. Zararlı Yazılımlar

Zararlı yazılımlar hedefleri, oluşturulma ve bulaştırılma yöntemleri göz önüne alındığında 6 farklı başlıkta sınıflandırılabilirler:

a) Bilgisayar Virüsleri
b) Solucan (Worm)
c) Truva Atı (Trojan)
d) Tuş Kaydedici (Key-Logger)
e) Reklam Yazılımları (Adware)

f) Casus Yazılımlar (Spyware)

3. Oltalama (Phishing)
4. İstenmeyen E-posta
5. Trafiğin Dinlenmesi (Sniffing)

1.1.3. Son Yıllarda Yaşanan Önemli Olaylar

Dünya ve Türkiye genelinde son yıllarda karşılaşılan siber saldırıların bilgi sızması, işleyişin bozulması, prestij kaybı gibi büyük riskler taşıyor olma nedeni ile devletler, kurum ve kuruluşlar siber güvenlik alanında ciddi eylem planları hazırlamaktadırlar.

Dünya ve ülke genelinde son yıllarda ciddi tehditlerin hatırlandığı başlıca siber saldırılar ve siber saldırı hazırlıkları şunlardır:

Gelişmiş Siber Casusluk Tehdidleri

Stuxnet Gelişmiş Siber Casusluk Tehdidi

"Stuxnet ilk defa 2010 yılının haziran ayının ortalarında Beyaz Rusya'daki küçük bir firma olan VirusBlokAda tarafından tespit edildi. İlk incelemeler virüsün standart bir solucan olmadığını zaten gösteriyordu fakat karmaşık yapısı yüzünden uzayan incelemeler devam ettikçe işin boyutu gittikçe değişti. Özellikle solucanın çok karmaşık yapısı, kullandığı taktikler ve hedefi göz önüne alınınca, siber savaş adı altında yıllarca dillendirilen senaryoların aslında çok da gerçek dışı olmadığı ortaya çıktı.

Solucanı inceleyen araştırmacılar tarafından ortak olarak dile getirilen ilk gerçek şu ki, Stuxnet çok karmaşık bir yapıya sahip. Bu yüzden bu solucanın birçok farklı alandan uzmanların bir araya gelerek üzerinde uzun süre çalıştığı ve kayda değer bir bütçeye sahip bir projenin ürünü olduğu görüşü hâkim. Yine birçok araştırmacı tarafından bu tür bir projenin basit bir suç örgütünden ziyade devlet desteğindeki bir kuruluş tarafından gerçekleştirilmiş olması daha gerçekçi gözükmekte.

Stuxnet kendi karmaşık yapısı içinde hâlihazırda bilinen birçok zararlı yazılım yöntemini kullanmanın yanında daha önce hiçbir zararlı yazılımda olmayan

dikkat çekici birkaç özelliğe daha sahip. Özellikle dört tane sıfır gün (zero-day) yani daha önceden bilinmeyen açıklığı beraber kullanması, kendini gizlemek için kullandığı çekirdek (kernel) sürücülerini rahat yükleyebilmek için güvenilir firmalardan çalınmış kök sertifikalar ile sürücülerini imzalaması ve en önemlisi hedef olarak sanayi ve enerji tesislerindeki fiziksel süreçleri gizlice değiştirmeye çalışmasıdır"[678]

Stuxnet, Veri Tabanlı Kontrol ve Gözetleme Sistemlerini hedef alan bir yazılımdı. En çok görüldüğü bölge ise İran ve civar bölgesi idi. Symantec firmasının hazırlamış olduğu rapora göre virüsün en çok etkilediği ülke İran ve en çok etkilediği sistemler İran'daki nükleer santrallerdi.

Stuxnet virüsü'nün gün yüzüne çıkması ile birlikte, siber saldırının organize bir şekilde belli hedeflere yönelik olarak ve büyük güçleri arkasına alarak gerçekleştiği görülmüş oldu.

Duqu Gelişmiş Siber Casusluk Tehdidi

"İlk olarak, 14 Ekim 2011 tarihinde, Budapeşte Teknoloji ve Ekonomi Üniversitesi, Kriptografi ve Sistem Güvenliği Laboratuvarı(CrySyS) tarafından tespit edilen virüse, bu ismin verilmesinin nedeni; virüse ait tuş kaydedicinin "~DQ..." ile başlayan geçici bir dosya oluşturmasıdır. Duqu virüsünün amacı ise gelecekteki atakları daha rahat yapabilme adına endüstriyel kontrol sistemleri ve çalışma mekanizmaları hakkında bilgi toplamak gibi gözükmektedir. Yani Duqu virüsünün kaynak kodu endüstriyel sistemlere yönelik herhangi bir kod parçacığı içermiyor. Şu an için elde edilen örnekler, bu virüsün, temelde bir truva atı RAT(RemoteAccessTrojan)-olduğunu göstermektedir.

Symantec Firmasının, 1 Kasım 2011 tarihinde güncellediği, Duqu için hazırlamış olduğu "Security Response" raporuna göre, 8 ülkede 6 kuruluş Duqu virüsünün bulaştığını doğrulamaktadır. Bu 6 kuruluşun A,B,C,D,E,F kuruluşları dersek, bu kuruluşların ülkeler göre dağılımı şu şekildedir; A Kuruluşu: Fransa,Hollanda,İsviçre,Ukrayna; B Kuruluşu: Hindistan; C Kuruluşu: İran; D Kuruluşu: İran; E Kuruluşu: Sudan; F Kuruluşu: Vietnam

---

[678] Pamuk, http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/stuxneti-ozel-yapan-ne.html, Erişim Tarihi: 22.07.2012

Diğer güvenlik firmaları ise Avusturya, Macaristan, Endonezya, Büyük Britanya ülkelerindeki bazı kuruluşların ve İran'da D ve C kuruluşlarından başka kuruluşların da etkilendiği raporunu vermişlerdir.

Sonuç olarak, Stuxnet gibi en çok İran'daki kuruluşlar etkilenmiş fakat henüz Türkiye'den bir kuruluşun etkilenip etkilenmediği doğrulanmamıştır"[679]

Diğer Gelişmiş Siber Casusluk Tehditleri

Yukarıda bahsedilen APT (Advanced Persistent Threat-Siber Casusluk Tehdidi) lerin dışında yakın tarihte gündeme gelen Flamer, Tinba gibi zararlı yazılımlar da tespit edilmiştir. Bu zararlı yazılımlar da benzer hedefleri doğrultusunda oluşturulmuş karmaşık zararlı yazılımlardır.

Bu tür yazılımların varlığı ve tespiti siber savaşın daha önemli boyutlara geldiğini gözler önüne sermektedir.

Bilgi Sızdırma Saldırıları

2012 yılı içerisinde ülkemizi etkileyen bir diğer önemli saldırı da, Ankara Emniyet Müdürlüğü'ne yönelik Redhack saldırgan grubu tarafından üstlenmiş, bilgi sızdırma saldırılarıdır. Bu saldırıda da Ankara Emniyet Müdürlüğü'ne yönelik, bazı kullanıcıların şifre seçimindeki zafiyetten faydalanılarak, Müdürlüğe ait ağa sızılmış ve yine Müdürlüğe ait gizli bilgiler internet ortamında herkesle paylaşılmıştır.

Hükümetlerin ve organizasyonların hassas bilgilerini yayınlayan Wikileaks organizasyonu da dünya geneli bir saldırgan ve protesto grubu olarak kendini tanımlayan Anonymous grubu ile işbirliği içerisinde ulaşılması gereken hedef sistemlere yönelik sızma saldırıları yapmakta ve elde ettiği hassas bilgileri Wikileaks organizasyonu ile paylaşmakta olduğu, 2012 yılı içerisinde anlaşılmıştır.

Bu tür saldırılar, basına bilgi sızdırmak şeklinde yapıldığında genel prestij kaybına sebebiyet vermektedir. Fakat bazı elde edilen bilgilerin kimsenin haberi olmadan kötü amaçla kullanılması da söz konusu olabilmektedir.

Servis Dışı Bırakma ve İçerik Değiştirme Saldırıları

---

679 Haltaş, http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/duqu-yeni-nesil-kesif-ucagi.html, Erişim Tarihi:22.07.2012

Servis dışı bırakma saldırılar genel olarak hedef sisteme ekonomik olarak zarar vermeyi ya da organizasyona prestij kaybettirmeyi hedeflemektedir.

Benzer şekilde içerik değiştirme saldırılarında da amaç organizasyona ait internet sitesini içeriğini değiştirmek sureti ile organizasyona prestij kaybettirmektir.

Servis dışı bırakma saldırıları ve içerik değiştirme saldırıları da geçtiğimiz yıllarda sıklıkla gözlemlenen saldırılardır. Yukarıda belirtilen amaç doğrultusunda Anonymous saldırgan grubu ve Redhack saldırgan grubu, Türkiye Cumhuriyeti'nin önde gelen kurumları olan Emniyet Genel Müdürlüğü, Telekomünikasyon İletişim Başkanlığı, Adalet Bakanlığı, İçişleri Bakanlığı gibi kamu kurumlarına Servis dışı bırakma ve içerik değiştirme saldırıları düzenlemiş bir kısmında başarılı olmuşlardır, bir kısmında ise başarısız olmuşlardır.

1.2. DÜNYADAKİ DURUM

Bilgi güvenliği ve bilişim suçları alanında başta ABD ve Avrupa Birliği ülkeleri olmak üzere dünya çapında birçok ülkede politikalar ve faaliyetler gerçekleştirilmektedir.

1.2.1. Ülkelerin Politika ve Stratejileri

Amerika Birleşik Devletleri (A.B.D.)

ABD, Siber savunma alanında dünyada öncülük eden ülkeler arasında yer almaktadır. ABD'de siber savunma alanındaki faaliyetlere ilişkin temel belge şubat 2003 tarihinde yayınlanmıştır. Federal Yönetim, yerel makamlar ile özel sektörü içermesi nedeniyle ulusal nitelikte ve geniş kapsamlı olarak anılan belgede, kendi görev alanları itibarıyla öncü rol üstlenecek devlet kurumları da belirtilmektedir. Bahsedilen strateji belgesinin, "National Strategy for Homeland Security" belgesinin uygulama boyutunu oluşturduğu ve "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" belgesini tamamlayıcı nitelikte olduğu belirtilmektedir.

Bahsi geçen belge ve 17 Aralık 2003 tarihli İç Güvenliğe ilişkin Başkanlık Direktifi uyarınca, İç Güvenlik Bakanlığına (Department of Homeland Security) siber savunma konusunda önemli sorumluluklar verildiği görülmektedir. İç güvenlik bakanlığının internet sitesinde, bünyesinde "Ulusal Siber Güvenlik Bölümü" bulunduğu da ayrıca belirtilmiştir.

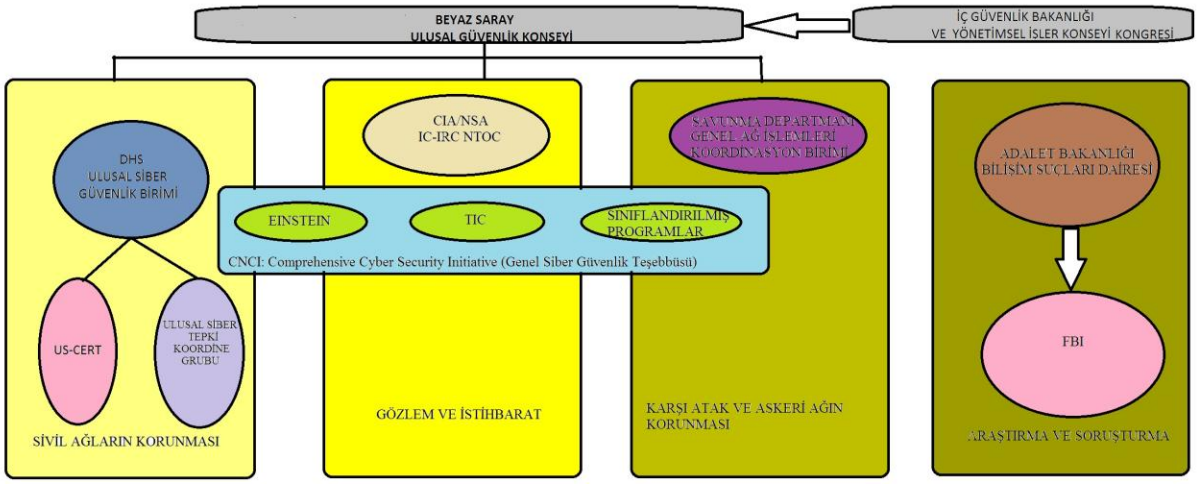
2008 yılında ABD siber politikası yenilenmiştir ve Comprehensive National Cybersecurity Initiative başlığı altında bir politika dokümanı hazırlanmıştır.

Aynı zamanda bir DHS programı olan ve hükümetin internet sitelerinden diğer sitelere olan trafiğin ve giden-gelen verinin incelendiği, daha önceki dönemlerde hazırlanmış EINSTEIN programının kapsamı genişletilmiş ve program Ulusal Güvenlik Birimi'ne (National Security Agency) devredilmiştir.

Son olarak hazırlanan raporda Beyaz Saray içerisinde bir Siber Güvenlik Ofisi'nin kurulması tavsiye edilmiştir.

2008 yılındaki rapora göre hazırlanan Siber Politikayı anlatan şema ve Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü tarafından yapılmış olan şemaya ait açıklama aşağıda verilmiştir.

Şekil 55 - ABD Siber Güvenlik Konseyi'nin Yapısı



TIC: Trusted Internet Connections (Güvenli Internet Bağlantıları)

IC-IRC: Intelligence Community-Incedence Response Center (İstihbarat Topluluğu-Olay Müdahele Merkezi)

NTOC: NSA/CSS Threat Operation Center (Tehdit Operasyonları Merkezi)

"Bu şemaya göre, Beyaz Saray'da görevlendirilen ve Ulusal Güvenlik Konseyi üyesi olan ve kongreye bağlı olarak çalışan bir başkanlıkta 4 ana iş kavramı

altında federal kuruluşların birbirleriyle olan bağlantıları resmedilmeye çalışılmıştır.

Federal Sivil Ağların Korunması ve Tepki Konması süreci içinde DHS içerisinde yer alan Ulusal Siber Güvenlik Biriminin (National Cyber Security Division) liderliğinde US-CERT ve Ulusal Siber Tepki Koordinasyon Grubu (National Cyber Response Coordination Group) gibi kuruluşların çalışması öngörülmüştür. Ulusal Siber Tepki Koordinasyon Grubu ulusal çapta etki yaratabilecek bir siber saldırı durumunda 19'dan fazla federal kuruluş arasında koordinasyonun sağlanması ile görevlidir. US-CERT (United States Computer Emergency Readiness Team) ise daha önce var olan CERT/CC (Computer Emergency Readiness Team Coordination Center) yerine görevlendirilmiştir.

İzleme ve İstihbarat sürecinde ise Merkezi İstihbarat Ajansı (Cetral Intelligence Agency, CIA) ve Ulusal Güvenlik Ajansı (National Security Agency, NSA) işbirliği altında İstihbarat Toplumu-Vaka Tepki Merkezi (Intelligence Community-Incident Response Center, IC-IRC) ve Ulusal Güvenlik Kuruluşu Tehdit Operasyonları Merkezi(NSA/CSS Threat Operations Center, NTOC) gibi kuruluşlar görev almaktadır.

Karşı atak ve Ordu Ağı Savunması sürecinde ise Savunma Departmanı'na bağlı (Department of Defense) Birleşik İş Gücü – Global Ağ Operasyonları (Joint Task Force – Global Network Operasyonları) başkanlığında çalışmalar yürütülmektedir.

Soruşturma ve adli takibat sürecinde ise Adalet Departmanı'na (Department of Justice) bağlı Bilgisayar Suçları ve Fikri Mülkiyetler kuruluşu liderliğinde (Computer Crime and Intelligence Property) Federal İstihbarat Bürosu (Federal Bureau of Intelligence) tarafından çalışmalar yürütülmektedir "[680]

Almanya

Almanya siber saldırılara karşı almakta olduğu önlemleri Federal İçişleri Bakanlığı tarafından hazırlanmış olan "Enformasyon Altyapı Savunması İçin Ulusal Plan" başlıklı belgede tanımlamıştır. Siber saldırıların başlıca hedeflerinin büyük

[680] Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, 2012, Sy. 15.

şirketler, bankalar veya kamu kuruluşları olduğu belirlenmiş ve siber güvenlik açısından öncelikli olarak belirlenmiştir. Belirlenmiş olan bu ulusal planın gerçekleşmesi ise "Enformasyon üyeliğinden Sorumlu Federal Ofis" (BSI) tarafından yürütülmektedir. Siber saldırılara karşı koyabilmek için Federal Hükümet, Ulusal Plan'da üç stratejik hedef belirlemiştir:

- Önleme: Bu başlık altında, enformasyon altyapısının, güncel ve güvenli teknoloji ürünlerinin kullanımı ve mevcut risklerin bilinciyle uygun şekilde korunması öngörülmektedir.

- Hazırlıklı olma: Meydana gelebilecek elektronik saldırılara etkin şekilde karşı koyabilmek için BSI bünyesinde Enformasyon Teknolojisi Kriz Müdahale Merkezi tesis edilmesi planlanmakta, bu merkezin ulusal komuta, kontrol ve analiz merkezi görevlerini üstlenmesi ve bu amaçla bir algılayıcı ağı kurulması hedeflenmektedir. Aynı şekilde, Federal Hükümet, halkın ve özel sektörün mevcut riskler ve alınabilecek önlemler hakkında bilinçlendirilmesini hedeflemektedir.

- Sürdürülebilirlik: Bu başlık altında, Almanya'nın elektronik güvenlik alanında yeterliliğinin artırılması amaçlanmaktadır.

Belirlenmiş olan bu politika ve uygulamaların sadece yetkili makamlar tarafından yerine getirilmesinin yeterli olmayacağı bunun yanında özel kuruluşlar ile iletişim ve etkileşimin de önemli olduğu söz konusu belgede vurgulanmıştır. Ayrıca özel kullanıcıların da mevcut risklerin bilincinde olmalarının ve gerekli bireysel önlemlerin alınmasının önemine dikkat çekilmekte, öte yandan ülkelerarası işbirliğine de vurgu yapılarak, Almanya'nın uluslararası standartların ve normların tesis edilmesini savunduğu kaydedilmektedir.

İngiltere

İngiltere'de siber saldırılara karşı savunma konusu "bilgi güvenliği" (information assurance) kapsamında ele alınmaktadır. Bilgi güvenliği konusundaki çalışmalar, teknolojik gelişmelere paralel olarak İngiltere'de 1999 yılından sonra ağırlık kazanmıştır. Kamu ve özel sektörün bu kapsamdaki ihtiyaçlarının karşılanması amacıyla üçlü bir yapı tesis edilmiştir. Başbakanlık ofisine bağlı olarak görev yapan "Central Sponsor for Information Assurance", "cyber defense"

konusunda politika, strateji ve siyasa geliştirme çalışmalarını yürütmektedir. Hazırlanan söz konusu politikaların uygulamasından ise "Center for Protection of National Infrastructure" (CPNI) ve "The Communications-Electronics Security Group" (CESG) sorumludur.

CPNI özel sektör ve iş çevrelerinin, CESG ise kamu kuruluşlarının bu alandaki ihtiyaçlarının karşılanmasında rol almakta, elektronik altyapı ve bilgi ağlarına yönelik olarak gerçekleştirilebilecek saldırılar konusunda ilgili kurumlara tavsiyelerde bulunmaktadır. Bu iki kuruluş, hükümetin bilgi güvenliği genel stratejisinin uygulanmasının genel gözetimini gerçekleştirmekte ve bilgisayar ağlarına ve elektronik ortamdaki işlemlere karşı olabilecek saldırılar konusunda erken uyarı işlevi görmektedir. Elektronik ortamdaki bilgi, belge ve işlemlerin güvenliğinin sağlanması amacıyla IT çözümleri geliştirilmesinin, temelde her bir kamu veya özel sektör kuruluşunun kendi sorumluluğunda olduğu kabul edilmektedir. Bu alanda önleyici işlev gören yazılım ve donanımların serbest piyasa koşullarında bu kuruluşlar tarafından temin edilmesi beklenmektedir.

Bu alandaki çalışmaların koordine edilebilmesi amacıyla "Chief Information Officer's Council" (CIOC) kurulmuş olup, ayda bir düzenli olarak toplanan söz konusu Konsey'e CPNI ve CESG'e ilaveten silahlı kuvvetler ve istihbarat servisinin ilgili birimleri katılmaktadır. Buna ilaveten, daha kapsamlı eşgüdüm ihtiyacının karşılanması için "Information Assurance Policy and Program Board" (IAPPB) oluşturulmuştur. Kamu ve özel sektörle ilgili bilgi güvenliği politikası uygulamalarının ele alındığı söz konusu Kurul, üç ayda bir toplanmakta ve toplantılara CIOC'a ilaveten Savunma Bakanlığı, Dışişleri Bakanlığı ve İş, Girişim ve Reform Düzenlemeleri Bakanlığı'ndan yetkililer iştirak etmektedir.

İtalya

İtalya'da Telekomünikasyon ve bilgi işlem sistemleriyle ilgili ulusal kanunlar ve AB mevzuatı çerçevesinde Yenilikler ve Teknoloji Bakanlığı, Telekomünikasyon Bakanlığının mutabakatıyla, 16 Ocak 2002 tarihinde bir kararname yayımlayarak Kamu Sektörünün elektronik ortamlarda savunulması için Ulusal Güvenlik Komitesi kurulmasına karar vermiştir. Bu iki Bakanlık 24 Temmuz 2002'de imzalanan müşterek bir kararname ile Ulusal Güvenlik Komitesi aracılığıyla uluslararası güvenlik standartlarına uyum ve risklere karşı konulması gibi gereksinimleri

yanıtlayacak bilgi işlem ve telekomünikasyon güvenlik planları oluşturulmasında müşterek programlar izlenmesi konusunda da mutabık kalmışlardır.

Komitenin belli başlı görevleri arasında bilgi işlem güvenlik sistemlerinin uluslararası standartlara uyması için proje ve öneriler hazırlamak, kamu kurumlarında güvenlik sistemlerinin oluşturulması için programlar oluşturmak, yapılan çalışmaları değerlendirmek ve gerektiği hallerde uyarılarda bulunmak, kamu personelinin güvenlik konusunda eğitimi için programlar hazırlamak gibi hususlar yer almaktadır. Komite her dört ayda bir yaptığı çalışmalara ve elde edilen somut neticelere ait bir rapor hazırlar ve bunları Telekomünikasyon Bakanlığına ve Yenilikler ve Teknoloji Bakanlığına göndermektedir.

Bu kararname kapsamında tüm kamu kuruluşları kendi bünyelerinde bilgi işlem güvenliği için bir birim oluşturmakla yükümlü kılınmışlardır. Komite ayrıca, "Computer Emergency Response Team" adlı bir birim oluşturmuştur. Bahsedilen bu birim içerisinde bilgi işlem hataları ve elektronik saldırılar konusunda kamu idarelerine destek vermek için özel bir birim bulunmaktadır (GovCERT). GovCERT "Computer Emergency Readiness" görevi yapmakta ve her bir Kamu idaresi bünyesinde kurulan yerel birimlere destek vermektedir. Komite, Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency) ile de işbirliği yapmaktadır.

Finlandiya

Finlandiya'da elektronik ortamdaki saldırılara karşı savunma (cyber defense) bağlamında, yetkili makam Fin İletişim Düzenleme Kurulu (Finnish Communications Regularity Authority)'dur. Elektronik ortamdaki saldırılarla mücadele dâhil olmak üzere, bilgi güvenliğinin sağlanması için önlemler alınması ve bilgi güvenlik durumunun geliştirilmesinde yetkili ve sorumlu en üst makam Hükümet'tir. Hükümet, Eylül 2003'te Ulusal Bilgi Güvenliği Stratejisi hakkında kararı kabul etmiştir. Bu stratejinin desteklenmesi ve kaydedilen gelişmelerin gözetimi, Ulusal Bilgi Güvenliği Danışma Kurulu (National Information Security Advisory Board) tarafından 2007 yılı başlarına kadar yerine getirilmiştir. Bilgi güvenliğinin sağlanması için 2008 yılında Bakanlıklar arası bir çalışma yapılarak yeni bir strateji belgesi hazırlanmıştır. Bu çalışmayı "Ubiquitous Information Society

Advisory Board" (Geniş Bilgi Toplumu Danışma Kurulu) altında kurulan yeni bir bilgi güvenliği grubu yerine getirmiştir.

Olağan durumlarda, bilgi güvenliğinin sağlanması ve bu konuda yapılacak düzenlemelere öncülük edilmesi, Ulaştırma ve İletişim Bakanlığı, söz konusu Bakanlığa bağlı Fin İletişim Düzenleme Kurulu ve Ekonomi ve İstihdam Bakanlığı tarafından gerçekleştirilmektedir. Kamu sektöründe bilgi güvenliğinin geliştirilmesi ise, temel olarak Maliye Bakanlığı ile İçişleri Bakanlığı'nın sorumluluğundadır. Ulaştırma ve İletişim Bakanlığı, iletişim hizmetlerinde bilgi güvenliğiyle ilgili mevzuat ve strateji geliştirmeden sorumludur.

Bilgi güvenliği, son dönemde, pek çok ülkede ve AB çerçevesinde, çeşitli çalışma grupları tarafından izlenmektedir. Girit'te bulunan Avrupa Ağı Bilgi Güvenliği Ajansı (European Network and Information Security Agency), bu konuda AB'nin bir kurumu olarak faaliyet göstermektedir.

Danimarka

Danimarka'da sanal âlemden gerçekleştirilen saldırılara karşı koymakla görevli tek bir otorite bulunmamakta, görev ve yetki; Danimarka İstihbarat ve Güvenlik Servisi (PET), Savunma Bakanlığı'na bağlı Danimarka Kriz Yönetim Makamı (DEMA), Bilim, Teknoloji ve Yenilik Bakanlığı'na bağlı Danimarka Ulusal Bilgi Teknolojileri ve Telekomünikasyon Kurumu (ITST), Bağımsız idari otorite statüsünde bulunan ve teknoloji ile ilgili konularda, parlamento ile kamu kurumlarını bilgilendirmekle görevli Danimarka Teknoloji Kurulu arasında paylaştırılmış durumdadır.

Danimarka Teknoloji Kurulu himayesinde "IT- Security Beyond Borders" adıyla kurulan bir çalışma grubunca 2007'de sınırı aşan bilgi teknolojileri güvenliği meselelerine dair Danca bir rapor yayımlanmıştır. Raporda, bu alanda uluslararası yardımlaşmanın önemine ve somut adımlar atılması gerektiğine özel vurgu yapıldığı anlaşılmaktadır.

Danimarka İstihbarat Servisi konuya dair kamu kurum ve kuruluşlarına rehberlik ve yardım hizmetlerinde bulunmakta, yine korunmasında kamu yararı bulunan bilgileri haiz kişilere de gerekli yardımları yapmaktadır. Öte yandan, son yıllarda elektronik verilerin depolanması ve iletilmesindeki artışın sonucu olarak

PET bünyesinde bilgi teknolojileri güvenliği kısmı (IT securitysection) tesis edilmiştir. Bu bağlamda PET ulusal ve uluslararası makamlarla (istihbarat makamları dâhil) işbirliği halinde faaliyetler yürütmektedir.

1.2.2. Diğer Ülkelerin Gerçekleştirdiği Çalışmalar

1.2.2.1. Kurumsal Organizasyon ve Kurumlar Arası İşbirliği

TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü'nün yapmış olduğu araştırmalar ve katılmış olduğu uluslararası siber güvenlik tatbikatları ve konferanslarından edinmiş olduğu bilgiye göre genel olarak, ülkelerde siber güvenlik kurumsal organizasyonu ve koordinasyonu ülke yönetimi tarafından görevlendirilmiş bir ulusal bilgisayar olaylarına müdahele ekibi veya ülke ordusu aracılığı ile yapılmaktadır. Ülkenin kamu ve özel sektör kuruluşlarının her birine ait bir BOME olması sağlanmaya çalışılmakta ve siber güvenlik alanında çalışmalar gerçekleştiren enstitüler kurulmakta ve çalışmaları takip edilmektedir. Aynı zamanda yine birçok ülkede bu alanda araştırma yapması için üniversiteler teşvik edilmektedir.

Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü'nün hazırlamış olduğu "Siber Güvenlik Raporu" ve TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü'nün edinmiş olduğu tecrübeye göre, birkaç ülkenin Siber Güvenlik adına oluşturmuş olduğu organizasyon yapısı ve koordinasyon şekli aşağıda örnek olarak verilmiştir. Bu örneklerin birçoğunda ülkeler yukarıda bahsedildiği gibi benzer bir mekanizmaya sahiptirler.

Amerika Birleşik Devletleri:

Department of Homeland Security (DHS) birimi Amerika Başkanı Barack Obama'nın direktifi üzerine kurulmuş ve siber internet güvenliğinin sağlanması için bütün sorumluluğu üzerine almıştır. Daha önceki yıllarda ise her kurumun kendisine ait Bilgisayar Olaylarına Müdahele Ekibi (BOME) nin olması istenmiştir. Hükümete ait; askeriye, istihbarat gibi kurum veya kuruluşların kendilerine ait kapalı bir siber savunma mekanizması kurulmuştur. Fakat özel sektör ve diğer kurumlarda BOME kurulması istenilen anlamda gerçekleştirilememiştir. Kurulanlar arasında

koordinasyonu sağlamak ve aynı zamanda diğer stratejilerin belirlenmesi ve uygulamaya geçilmesi amacıyla doğrudan Beyazsaray'a bağlı bir DHS kurulmuştur.

İlk olarak sivil ağın korunması sorumluluğunu özel sektöre ve federal olarak desteklenmiş olan CERT/CC gibi kuruluşlara havale eden ABD, CERT/CC işbirliği ve DHS organizasyonu içerisinde bulunan Ulusal Siber Güvenlik Birimi altında ulusal bir CERT (BOME) yani US-CERT organizasyonunu kurmuştur. İzleme ve istihbarat süreci ise CIA ve NSA (National Security Agency) işbirliği çerçevesinde yürütülmektedir.

Çin Halk Cumhuriyeti:

Çin Halk Cumhuriyeti, Siber Güvenlik konusunda Çin Halk Kurtuluş Ordusu'nu (People Liberation Army - PLA) görevlendirmiştir. Çin Halk Cumhuriyeti, ülkenin güvenliği yanında siber güvenliği de büyük oranda ordunun denetimine bırakmış durumdadır [2].

PLA'nın Genel Personel Bölümü'nün (General Stuff Deparment) 3. ve 4. bölümleri, bilişim sistemlerinin güvenliğinin sağlanmasından sorumludur. Bu birimler tüm kuvvet komutanlıkları ile birlikte ülke sınırları içerisindeki trafiğin izlenmesinden sorumludur. 3. Departmanda yaklaşık 130.000 personel çalışmaktadır. Bunların yanında ülkede siber güvenlik alanında Ar-Ge çalışması yapan 3 enstitü bulunmaktadır. Bu enstitüler, ülkenin en iyi üniversitelerinden destek almaktadır. Bu enstitülerin çalışması PLA tarafından kontrol edilmektedir ve ülkede "Altın Kalkan" adında bir verilerin dışarıya çıkmasını önleyen "Büyük Çin Firewall" ı da olarak bilinen bir filtreleme sistemi uygulanmaktadır.

Birimler arası koordinasyon, çalışmaların yürütülmesi ve Siber Güvenlik ile ilgili düzenlemenin yapılması ve uygulamaya geçirilmesi PLA'in sorumluluğunda gerçekleştirilmektedir.

Almanya:

Almanya Devleti içerisinde Siber Güvenlik, diğer birçok ülkede olduğu gibi, Almanya Ordusu tarafından sağlanmaktadır. Almanya Devleti de kamu ve özel kurum ve kuruluşların kendi bünyeleri içerisinde Bilgisayar Olaylarına Müdahele Ekibi'nin kurulu olmasını tavsiye etmektedir. Bu birimler arası koordinasyonun sağlanması adına Ulusal Siber Müdahele Merkezi kurulması planlanmaktadır.

Bu merkez, Bilgi Güvenliği Federal Dairesi, Anayasayı Koruma ve Sivil Koruma Federal Dairesi ve Afet Yardımı Federal Dairesi'ne rapor vererek doğrudan işbirliği yapacaktır. Ulusal Siber Müdahale Merkezi, ilgili tüm makamların yasal görevleri ve yetkilerine, sıkı işbirliği anlaşmaları temelinde uyacaktır. Federal Kriminal Dairesi (BKA), Federal Polis (BPOL), Gümrük Kriminolojik Ofisi(ZKA), Federal İstihbarat Servisi (BND), Alman Ordusu ve kritik altyapı işletmecileri denetleme makamlarının hepsi kendi kanuni görevleri ve yetkileri çerçevesinde bu çatı altında toplanmıştır. IT ürünlerinin zayıflıkları, hassas noktaları, saldırı formları, fail profilleri, hızlı ve yakın bilgi paylaşımı için Ulusal Siber Müdahale Merkezi, IT olaylarının analiz ve eylemleri için birleştirilmiş tavsiyeler vermeyi planlamaktadır.[681]

Aynı zamanda, ülkede bu alanda çalışmakta olan birçok Siber Güvenlik Enstitüsü bulunmaktadır. Bu enstitüler, istihbarat birimleri ile de koordinasyon halinde, ülkenin güvenlik ile ilgili ihtiyaçlarına yönelik Ar-Ge faaliyetlerini yürütmektedir.

İngiltere:

İngiltere'de, Ulusal Altyapının Korunması Merkezi (Center for the Protection of National Infrastructure), internet ve iletişim altyapıları da dâhil olmak üzere ülkenin kritik altyapıların korunması konusunda çalışmakta; ilgili özel sektör altyapı kuruluşları ile devamlı iletişim halinde bulunmaktadır. Türkiye'de de internet ve iletişim altyapılarının korunması için ilgili özel sektör kuruluşları ile devamlı iletişim halinde olacak ve altyapıların korunması için bilgi alış verişinde bulunacak bir kuruluşun kurulması önemlidir.[682]

Siber Güvenlik alanında eğitim ve araştırmanın ilerletilmesi adına Siber Güvenlik Enstitüsü kurulması planlanmaktadır. Bu kapsamda üniversitelerde bu alanda verilen dersler ve yapılan araştırmaların artırılması yönünde, söz konusu merkez girişimde bulunmaktadır.

[681] Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, 2012, Sy. 33.
[682] Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, 2012, Sy. 30.

İsviçre:

İsviçre'de elektronik ortamdaki tehdit unsurlarına karşı kontrol ve mücadele, türlerine göre farklı kurumlarca yürütülmektedir. Devlet kurumları, kamu kuruluşları ve ulusal güvenliği alakadar eden bilişim atakları ile mücadele hususunda görevli olan birim Federal Analiz ve Önleme Dairesi'dir ve sivil ve askeri istihbarat kapasitelerinden yararlanmaktadır.

Federal İnternet Suçları ile Mücadele Koordinasyon Dairesi (CYCO) koordinasyonunda faaliyet gösteren Federal Polis Teşkilatı, elektronik ortamdaki bireysel ve örgütsel tehdit unsurlarının araştırılması, takibi ve ele geçirilmesi çalışmalarını yürütmektedir.

İş dünyası ile münferit internet kullanıcılarının elektronik ortamdaki saldırılara karşı korunması, bilgilendirilmesi, olası saldırıların algılanıp karşı önlemlerin alınması ile yasal ve idari düzenlemelerin yapılması hususlarında Bilgi Güvenliği Analiz ve Bildirim Servisi (MELANI) sürekli araştırmalar yapmakta, gelen ihbarları ilgili birimlere yönlendirmekte ve yılda iki kez, ülke içi ve uluslararası internet güvenliği durum raporu düzenleyerek kamuoyunun bilgisine sunmaktadır.

İsviçre Hükümeti 1 Ekim 2004 tarihinden beri MELANİ servisini İsviçre'nin özellikle iletişim ve veri toplama hususundaki hassas kurumlarını korumak ile görevlendirmiş ve önlemler hususunda Zürih ETH üniversitesi ile müşterek çalışılmasını sağlamıştır.

Güney Kore

İnternet kullanımının son derece yaygın olduğu Güney Kore'de elektronik ortamdaki saldırılara karşı savunma, farklı yönleriyle farklı kuruluşları ilgilendirmektedir.

Toplantılarını Cumhurbaşkanı başkanlığında gerçekleştiren ve Cumhurbaşkanına iç ve dış politika ile askeri konuların ulusal güvenlik boyutu hakkında bilgi vermekten sorumlu olan "Ulusal Güvenlik Konseyi'nin sekretaryası, ulusal kriz uyarı sisteminin işleyişi ve geliştirilmesi, ulusal kriz durumlarına ilişkin bilgilerin toplanması, özetlenmesi ve dağıtılması ile "siber" tehdit uyarısı yayınlanmasından da sorumludur. "Ulusal Güvenlik Konseyi" bünyesinde yer alan

"Ulusal Siber Güvenlik Strateji Konseyi" (National Cyber Security Strategic Council) ise ulusal "siber" güvenlik sisteminin kurulması ve geliştirilmesi, "siber" güvenlik politikaları ve çeşitli kuruluşlar arasında eşgüdümün sağlanması ve Cumhurbaşkanının "siber" güvenliğe yönelik kararlarının uygulanmasından sorumludur. Güney Kore Ulusal İstihbarat Servisinin başkanı aynı zamanda bu Konseyin de başkanıdır.

"Ulusal Siber Güvenlik Strateji Konseyi'nin altında, "Ulusal Siber Güvenlik Konseyi" (National Cyber Security Council) yer almaktadır. "Siber" güvenliğin sağlanması ve "Ulusal Siber Güvenlik Strateji Konseyi" tarafından alınan kararların uygulanması "Ulusal Siber Güvenlik Konseyi'nin görev alanına girmektedir. Konseyin başkanlığını, Güney Kore Ulusal İstihbarat Servisinin başkan yardımcısı yapmaktadır.

Elektronik ortamdaki saldırılara karşı savunma politikalarının hayata geçirilmesinden özel sektörü ilgilendiren konularda "Enformasyon ve Haberleşme Bakanlığı" bünyesindeki "Kore Enformasyon Güvenlik Ajansı'na bağlı "Kore Internet Güvenlik Merkezi", ülke savunmasını ilgilendiren konularda Savunma Bakanlığına bağlı "Enformasyon Savaş Müdahale Merkezi", ulusal güvenliği ve kamu sektörünü ilgilendiren konularda ise Ulusal İstihbarat Servisine bağlı "Ulusal Siber Güvenlik Merkezi" sorumludur. Ayrıca, Güney Kore ulusal polis teşkilatı bünyesinde de "Siber Terör Müdahale Merkezi" (Cyber Terror Response Center) bulunmaktadır.

Estonya:

2007'de Estonya'ya yönelik gerçekleştirilen siber saldırılar, ülkenin siber yeteneklerini ve politikalarını ciddi şekilde sorgulamasına neden olmuştur. Olaylar neticesinde Estonya'da siber savunma faaliyetleri Savunma Bakanlığı gözetiminde gerçekleştirilmektedir.

Bunun yanı sıra, ülkede Defence League (Savunma Ligi) adı verilen bir organizasyon da, ülkenin siber savunma yeteneklerini geliştirmek için çalışmalarda bulunmaktadır.

Estonya, üyesi olduğu NATO çatısı altında Bilişim Güvenliği alanında uluslararası işbirliğinin önemini gören ve bu alanda aktif rol alan ülkelerden biridir.

Bu işbirliği, kendi savunma yetkinliğinin artmasının yanı sıra NATO üyesi diğer ülkelere de önemli katkılarda bulunmasını sağlamaktadır. Bir NATO kuruluşu olarak 2008 yılında Tallinn kentinde faaliyete geçen Cyber Defence Centre of Excellence (Siber Savunma Mükemmeliyet Merkezi), üye ülkeler arasında işbirliğini artırma, bilgi paylaşımı sağlama ve siber güvenlik alanında araştırmalar yapma hedefine yönelik faaliyetlerde bulunmaktadır. Merkezin destekçileri olan ülkeler; Estonya, Almanya, Macaristan, İtalya, Letonya, Litvanya, Slovakya ve İspanya olarak sıralanabilir.[683]

Teknik Çalışmalar

Siber güvenlik alanında gerçekleştirilen çalışmalar, ülkelerde kurulu olan güvenlik enstitüleri ve üniversiteler tarafından gerçekleştirilmektedir. Ulusal BOME grupları, yapılmış olan Ar-Ge faaliyetlerinin neticesinde elde edilen bilgi birikimleri ile inceleme işlemlerini gerçekleştirmekte veya üretilen ürünleri ve bulunan güvenlik çözümlerini, ulusal çapta uygulanması gerekenleri ulusal düzeyde uygulamakta veya kamu ve özel sektörden ulusal güvenliği sağlama adına beklentilerini belirlemekte ve uygulanması yönünde yaptırım uygulamaktadır.

Bu kapsamda, Bilgi Üniversitesi'nin hazırlamış olduğu "Siber Güvenlik" raporuna ve Dünya'daki Durum başlığı altında verilen bilgilere göre, söz konusu üniversiteler ve enstitüler tarafından alınan en temel birkaç teknik önlem özetle şu şekildedir:

- Ulusal bir güvenlik duvarı hazırlanması ve uygulanması
- Kamu veya özel kurumları ve kuruluşları alınması gereken önlemler hakkında bilgilendirmek, eğitmek ve bu kapsamda gerekli olan internet veya uygulama yazılımları hizmetini sunmak
- Zararlı yazılım incelemesini geniş kapsamlı yapabilmek adına zararlı yazılım analiz laboratuarları kurmak
- Ulusal güvenlik ürünleri üretmek
- Adli analiz yapabilecek teknik ekibi yetiştirmek ve güncel saldırı teknikleri hakkında bu ekibin Ar-Ge yapmasını temin etmek

[683] Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, 2012, Sy. 33.

- Kamu kurum ve kuruluşları ile kritik altyapı işletmecisi olan özel sektör kuruluşlarına düzenli olarak ve güncel bir içeriğe sahip sızma testleri yapmak ve/veya yapılmasını temin etmek.

1.2.2.2. Kanuni Düzenlemeler

Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü'nün hazırlamış olduğu rapora ve Dünyadaki Durum başlığı altında verilen bilgilerden de anlaşılabileceği üzere birçok dünya ülkesi henüz siber güvenlik alanında yapılması gereken yasal düzenlemenin çok uzağında bulunmaktadır.

Bu konuda ileriye gitmiş olan ABD, Çin ve Almanya gibi ülkelerde ise kanuni düzenleme organizasyonel yapının kanuna aktarılması şeklinde olmuştur.

Siber saldırılarda analiz ve tespit yeteneklerinin kısıtlı olması nedeni ile suçlulara karşı yaptırım hakkındaki kanuni düzenleme gelişmiş ülkelerde bile yeterli seviyede değildir.

1.3. TÜRKİYE'DEKİ DURUM

1.3.1. Ülkemizde Bilgi Güvenliği İle İlgili Hâlihazırda Gerçekleştirilen Çalışmalar

Öncelikle Türkiye'de bilgi güvenliği ile ilgili çalışmalar gerçekleştiren kurumlar ve bu kurumların rollerini belirtmek gerekir.

TÜBİTAK bünyesinde bulunan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nün misyonu, "bilgi güvenliği, haberleşme veileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan

teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Ülkemizin bilgi toplumuna dönüşüm sürecinin koordinasyonu amacıyla yürütülen e-Dönüşüm Türkiye Projesi kapsamında hazırlanan ve 2006-2010 dönemini kapsayan Bilgi Toplumu Stratejisi ve Ek'i Eylem Planı, 2006/38 sayılı Yüksek Planlama Kurulu Kararı ile onaylanmış ve 28 Temmuz 2006 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Eylem Planında yer alan "Ulusal Bilgi Sistemleri Güvenlik Programı" başlıklı 88 numaralı eylem ile Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'ne (TÜBİTAK - UEKAE);

Siber alemdeki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir "bilgisayar olaylarına acil müdahale merkezi (CERT)" kurma,

Kamu kurumları için gereken asgari güvenlik seviyelerini belirleme, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyelerini tespit etme ve eksikliklerini giderme konularında öneriler geliştirme görevleri verilmiştir. 5809 sayılı Elektronik Haberleşme Kanunu ile; bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi, izinsiz erişime karşı şebeke güvenliğinin sağlanması, elektronik haberleşme sektörüne yönelik olarak, millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması görevleri Bilgi Teknolojileri ve İletişim Kurumuna verilmiştir.

Uluslararası Telekomünikasyon Birliği (ITU) tarafından düzenlenen ve ilk aşaması aralık 2003'te Cenevre'de, ikinci aşaması ise kasım 2005'te Tunus'ta gerçekleştirilen Dünya Bilgi Toplumu Zirvesi'nin sonuç dokümanlarında 11 ana faaliyet alanı belirlenmiştir. Bu faaliyet alanlarından biri de "Bilgi ve İletişim Teknolojilerinin Kullanımında Gizlilik ve Güvenliği Tesis Etmek"tir. Söz konusu Zirvede bu faaliyeti uygulamaya koyma görevi uluslar arası toplum tarafından ITU' ya verilmiştir. ITU bu görev doğrultusunda çalışmalar yapmakta olup, BTK,

Ülkemizi ITU nezdinde temsil eden taraf olarak bu çalışmalara katılmakta ve katkı sağlamaktadır.

1.3.2. Türkiye'de Bilgi Güvenliğine İlişkin Çalışmalar ve Bulgular

Bilgi güvenliği ile alakalı gerçekleştirilen ulusal çalışmalar:

Türk Ceza Kanununda yapılan değişiklikler

- Bölümünde (Bilişim Alanında Suçlar) yer alan Bilişim Sistemine Girme Suçunu Düzenleyen 243. madde

- Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçunu Düzenleyen 244. madde

- Banka veya Kredi Kartlarının Kötüye Kullanılması Suçunu Düzenleyen 245. madde

Ulusal Bilgi Güvenliği Kapısı (www.bilgiguvenligi.gov.tr)

Ulusal Bilgi Sistemleri Güvenlik Programı'nın en önemli unsurlarından birisi de Ulusal Bilgi Güvenliği Kapısı Projesi'dir. Ülkemizde bilgi güvenliği konusunda web üzerinden bilgi paylaşım ortamı sağlamayı amaçlayan site www.bilgiguvenligi.gov.tr adresinden yayın yapmaktadır. Sitede, bilgi güvenliğiyle ilgili özel konularda okuyucuyu bilgilendirmeyi amaçlayan teknik yazılar, bilgi güvenliği ile ilgili kılavuzlar, ülkemizde yapılan etkinlik, toplantı, sempozyum vs. gibi organizasyonların duyuruları, önemli açıklıklarla ilgili güvenlik bildirisi sayfası bulunmaktadır. Ulusal Bilgi Güvenliği Kapısı'nın, şu anda iki binin üzerinde kayıtlı kullanıcısı, yirmi altısı kurum dışından olmak üzere altmış yedi yazarı, yayınlanmış yetmiş iki makalesi, otuz kılavuzu ve üçyüzün üzerinde güvenlik bildirisi mevcuttur. Bilgi birikimine katkının sadece TR-BOME tarafından değil, ülkemizde bilgi güvenliği alanında yetkinliğe sahip her türlü kurum veya kişi tarafından yapılmasına imkân sağlanmaktadır. Kişilerin siteye kayıt olduktan sonra, bilgi güvenliği konularında oluşturduğu rehber, doküman veya makale, oluşturulacak değerlendirme komitesinin gözden geçirmesini takiben web kapısında yayınlanmaktadır.

TÜBİTAK – BİLGEM – Siber Güvenlik Enstitüsü (SGE)

TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü (SGE) bilgi ve iletişim sistemleri güvenliğine yönelik çalışmalar yürütür

Enstitü, siber güvenlik ve ilgili konularda bilgi birikimi ve araştırma kapasitesine sahip olmayı, ülkemizde siber güvenlik konusunda yürütülen teknik faaliyetleri yönlendirme ve eşgüdümü sağlayıcı önerilerde bulunmayı, ülkemizde siber güvenlik konusunda bir referans merkezi olarak görev yapmayı, ülkemizdeki kritik altyapıların siber güvenliğinin sağlanmasına katkıda bulunmayı hedeflemektedir.

TÜBİTAK - Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)

1972 yılında kurulan UEKAE, bilgi güvenliği, haberleşme ve ileri elektronik konularında faaliyet göstermektedir. Bünyesinde bulunan Kripto Analiz Merkezi, Ürün Geliştirme Bölümü, İLTAREN, Yarı İletken Teknolojileri Araştırma Laboratuarı, EMI/EMC/TEMPEST Test Laboratuarı, Akustik Test ve Analiz Laboratuarı, Ortak Kriter Test Merkezi ve Optoelektronik Laboratuarları ile araştırma ve geliştirme çalışmalarını sürdürmektedir. Milli imkânlar ile kriptografik ürünler, Milli Açık Anahtar Altyapısı (MA3), Güvenli Elektronik Posta (GEPosta), tempest ürünleri, Linux tabanlı PARDUS işletim sistemi, Elektronik Kimlik Doğrulama Sistemi (EKDS) gibi siber güvenlik alanında ürünler geliştirmektedir.

Ulusal Bilgi Sistemleri Güvenliği Programı

DPT (Kalkınma Bakanlığı) tarafından yayımlanan "Bilgi Toplumu Stratejisi 2006-2010" belgesinin ekinde yer alan ve bu belgenin uygulanmasına yönelik hususları içeren "Eylem Planı" belgesinin 88 nolu eylemi "Ulusal Bilgi Sistemleri Güvenlik Programı"nı gerçekleştirme sorumluluğu UEKAE'ye verilmektedir. Bu Eylem Planı çerçevesinde TÜBİTAK UEKAE projeler oluşturmuş ve 2007'den itibaren çalışmalarına başlamıştır. Yapılan çalışmalar TÜBİTAK UEKAE'nin Ulusal Bilgi Güvenliği Kapısı web sayfasında belirtilmekte olup aşağıda verilmiştir:

"Prototip olarak seçilen kamu kurumlarına Bilgi Güvenliği Yönetim Sistemi kurulum danışmanlığı verilmesi ve bu kurumların bilgi sistemlerinde bulunan güvenlik açıklarının tespit edilmesi, Bilgisayar Olayları Müdahale Ekibi - Koordinasyon Merkezi'nin kurulması ve kamu kurumlarına Bilgisayar Olay

Müdahale Ekipleri kurulması amacıyla danışmanlık verilmesi, Kamu kurumlarına ait bilgi sistemlerinin internet üzerinden maruz kalacağı tehditlerin tespit edilmesi amacıyla sanal ortam savunma sistemi kurulması,

Ulusal Bilgi Güvenliği Kapısı'nın kurulması ve işletilmesi,

Kamu kurumlarına bilgi güvenliğinin değişik alanları ile ilgili uygulamalı eğitim verilmesi,

Bilgi güvenliği ile ilgili rehber dokümanlar ve teknik yazılar yazılması".

TR-BOME Bilgisayar Olaylarına Müdahale Ekibi

Bilgisayar olaylarına müdahale ekipleri belirli bir sorumluluk alanı dâhilinde faaliyet gösteren, bu sorumluluk alanında bilgi sistemleri güvenlik olaylarına müdahale hizmeti ve bilgi sistem güvenliği ile ilgili diğer önleyici veya düzeltici hizmetleri veren ekiplerdir.

TR-BOME'nin görevi, ülke genelinde kurum ve kuruluşlara bilgisayar güvenlik olaylarına müdahale yeteneği kazandırmak ve gerçekleşen bilgisayar güvenlik olaylarına müdahale etmektir. TR-BOME bilgisayar güvenlik olaylarıyla ilgili ulusal danışma birimidir. TÜBİTAK UEKAE'nin Siber Güvenlik Enstitüsü bünyesinde faaliyet gösteren TR-BOME Türkiye'nin tamamına hizmet vermektedir. Siber olaylar çoğu zaman kurum ve ülke sınırlarını aşmasından dolayı TR-BOME bu durumlarda ilgili kurum ve kuruluşlar arasında koordinasyonu ve diğer ülkelerle işbirliğini sağlamaktadır. TR-BOME, kurum ve kuruluşlarda BOME kurulması veya bilgisayar güvenlik olaylarına müdahale yeteneği kazanılması amacıyla eğitim ve danışmanlık hizmetleri vermektedir.

Ulusal Siber Güvenlik Tatbikatları

Ulusal Siber Güvenlik Tatbikatları (USGT) finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin; adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan kamu kurumlarının, özel sektör kuruluşlarının ve sivil toplum kuruluşunun (STK) katılımıyla gerçekleştirilmektedir. Tatbikatta katılımcı kurum/ kuruluşlardan bilgi teknolojileri ve iletişim, hukuk ve halkla ilişkiler uzmanı statüsündeki personeller görev almaktadır. Katılımcı kurumların siber saldırı durumunda verecekleri tepkilerin

gerçek ortamdaki ve simülasyon ortamındaki saldırılarla ölçülmesiyle, kurumların hem teknik kabiliyetleri hem de kurum içi ve kurumlar arası koordinasyon yetenekleri değerlendirilmektedir. Ülkemizde 2008 ve 2011 yılında gerçekleştirilen tatbikatlar ile katılımcı kurumların teknik kabiliyetlerini tespit etmek ve kurumlara olası saldırılara karşı müdahalede deneyimi kazandırmak amacıyla hem gerçek saldırılar hem de yazılı ortamda senaryolar gerçekleştirilmiştir.[684]

Siber Güvenlik Yaz Kampı

TÜBİTAK ve Bilgi Güvenliği Akademisi, Türkiye'de siber güvenlik uzmanı eksikliğinin giderilmesine destek olmak ve kapasite geliştirilmesini sağlamak amacıyla üniversite öğrencilerine yönelik "Siber Güvenlik Yaz Kampı" düzenlemektedir. Resmi internet sitesinde yer alan bilgilendirme yazısı aşağıdaki gibidir.

"Kamp süresince bilişim sistemleri güvenliği konusunda teknik eğitimler verilmiştir. Teknik eğitimlerin yanı sıra, kamp katılımcıları bilgi güvenliği alanındadeneyim sahibi akademisyenler, kamu ve özel sektör yöneticileri ile bir arayagetirilmiştir. Kamp sırasında, öğrenciler, siber dünyadaki tehditler, alınması gereken önlemler ve bu alandaki kariyer fırsatları konusunda bilgi sahibi olmuşlardır. Aynı zamanda kamp esnasında uygulamalı eğitim amaçlı yarışmalar düzenlenmiştir.

Siber Güvenlik Yaz Kampı, Kalkınma Bakanlığı tarafından hazırlanan 2012 yılı Yatırım Programı'nda yer alan Kamu Bilgi Sistemleri Güvenliği Programı kapsamında gerçekleştirilmektedir. "

Bilgi Toplumu Stratejisi ve Eylem Planı (2006 - 2010)

Türkiye'nin bilgi ve iletişim teknolojilerinden etkin olarak yararlanması ve bilgi toplumuna dönüşmesi ile ilgili uygulanacak stratejileri içeren "Bilgi Toplumu Stratejisi 2006-2010" belgesi Devlet Planlama Teşkilatı'nın (Kalkınma Bakanlığı) koordinatörlüğünde hazırlanmıştır. "Bilgi Toplumu Stratejisi 2006-2010" belgesinin

[684] TÜBİTAK, https://www.bilgiguvenligi.gov.tr/raporlar-kategorisi/ulusal-siber-guvenlik-tatbikati-2011-sonuc-raporu.html, Erişim Tarihi: 22.09.12

ekinde yer alan ve bu belgenin uygulanmasına yönelik hususları içeren "Eylem Planı" belgesinde, siber güvenliğe ilişkin bazı eylem maddeleri tanımlanmıştır.[685]

Planın 87. maddesi (Bilgi Güvenliği ile İlgili Yasal Düzenlemeler) ve 88. maddesi (Ulusal Bilgi Sistemleri Güvenlik Programı) şeklindedir.

Kişisel Verilerin Korunması Kanunu Tasarısı

Adalet Bakanlığı tarafından kişisel verilerin korunması kanun tasarısı 22 Nisan 2008 tarihinde TBMM başkanlığına sunulmuştur.

Bu kanunun amacı; kişisel verilerin işlenmesinde kişinin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemektir.

Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı

Tasarıyla; Devletin bilgi güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların üretilmesi ve belirlenmesi, bunu gerçekleştirmeye yönelik planların hazırlanması, buna yönelik metodolojilerin oluşturulması ve ilgili yasal düzenlemelerin yapılması gerekliliği karşısında, Ulusal Güvenlikle ilgili hassas bilgilerin uluslararası standartlarda korunması amacıyla hazırlanması öngörülen Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı taslağı ile ilgili komisyon kurulması yönündeki hazırlık çalışmaları devam etmektedir.[686]

Ulusal Sanal Ortam Güvenlik Politikası

Türkiye'de siber güvenlik alanındaki ilk resmi belge olan Ulusal Sana lOrtam Güvenlik Politikası, Cumhurbaşkanlığı, Başbakanlık, Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Adalet Bakanlığı, Milli Savunma Bakanlığı, Maliye Bakanlığı, Ulaştırma Bakanlığı, İçişleri Bakanlığı, Devlet Planlama Teşkilatı Müsteşarlığı (Kalkınma Bakanlığı), Dış Ticaret Müsteşarlığı (Ekonomi Bakanlığı), Hazine Müsteşarlığı, Türkiye Cumhuriyet Merkez Bankası, Milli Güvenlik Kurulu Genel Sekreterliği, Milli İstihbarat Teşkilatı Müsteşarlığı, Bankacılık Düzenleme ve Denetleme Kurumu, Emniyet Genel Müdürlüğü, Bilgi Teknolojileri ve İletişim

[685] T.C Başbakanlık Devlet Planlama Teşkilatı, 2010

[686] Adalet Bakanlığı Kanunlar Gen. Müd., http://www.kgm.adalet.gov.tr/Tasariasamalari/Uzerindecals/uzrencal.htm, Erişim Tarihi: 22.07.2012

Kurumu ve TÜBİTAK-UEKAE'nin katılımı ile ocak 2009'da oluşturulmuştur. Bu belgenin amacı Türkiye'yi siber ortamdaki saldırılara karşı hazır hale getirecek ve siber ortamda yaşanacak problemlerin sonrasında hızlı bir şekilde toparlanmayı sağlayacak sanal ortam güvenlik adımlarını belirleme olarak verilmiştir. Bu politikada Türkiye için bilgi ve iletişim sistemleri ile ilişkili tehditler ve açıklıklar genel hatları ile ortaya konulmuştur. Bu belgenin son bölümünde ise gelen olan tehditleri bertaraf etmek ve açıklıkları kapatmak için yapılması gereken güvenlik adımları verilmiştir. Bunlar:

- Yasal düzenlemelerin oluşturulması,
- Ülke yeteneklerinin geliştirilmesi,
- Ulusal bilgisayar olaylarına müdahale organizasyonunun kurulması,
- Bilgilendirme ve bilinçlendirme çalışmaları yapılması,
- Ulusal Kritik Bilgi Sistem Altyapıları'nın güvenliğinin sağlanması,
- Uluslararası eşgüdümün sağlanması,
- Kurumsal bilgi ve iletişim sistemleri güvenliğinin sağlanması,
- Ulusal sanal ortam güvenlik stratejisinin hazırlanması olarak verilmiştir.[687]

Avrupa Konseyi Siber Suç Sözleşmesi

Siber suçlarla ilgili olarak düzenlenen ilk belge olma özelliğini taşıyan ve temel amacı, toplumları siber suçlara karşı korumak, siber suçlarla uluslararası alanda etkin bir şekilde mücadele etmek ve bu suçlarla mücadelede ortak bir anlayışı benimsemek olan Avrupa Konseyi Siber Suç Sözleşmesi'ni 39'u Avrupa Konseyi (AK) üyesi ve AK dışından ABD, Kanada, Japonya ve Güney Afrika olmak üzere toplam 43 ülke imzalamıştır. Türkiye de 10 Kasım 2010 tarihinde Dışişleri Bakanlığı düzeyinde bu belgeyi imzalamıştır. Uluslararası bir antlaşma olarak ve tüm kanunların üzerinde işlem görecek olan 48 maddeden oluşan bu belgede; özellikle telif haklarının ihlalleri, bilgisayarlarla ilişkili sahtekârlık eylemleri, çocuk pornografisi ve network güvenliği ihlaline ilişkin suçlar tanımlanmakta, cezai soruşturma ve kovuşturma yöntemleri belirlenmektedir.[688]

---

[687] Ulusal Sanal Ortam Güvenlik Politikası, Ocak 2009, Bölüm 1,2,4.

[688] AvrupaKonseyi, 2011, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=12&DF=02/02/2011&CL=ENG, Erişim Tarihi: 17.09.12

Ulusal Siber Güvenlik Stratejisi Raporu (Bilgi Güvenliği Derneği)

Bilgi Güvenliği Derneği tarafından hazırlanan bu rapor, Türkiye'nin Ulusal kapsamda Siber Güvenliğine yönelik ilkelerini, stratejik hedeflerini, bu hedeflere ulaşmak için ele alması gereken temel uygulamaları ve ilk planda atması gereken somut adımları özetlemektedir.

Siber güvenlik; yönetimsel, teknik, sosyolojik, tarihsel, yasal, politik, askeri ve akademik gibi çok sayıda alanın devreye girdiği bir konudur. Bu konuların etkin bir şekilde ele alınıp en doğru yöntem ve doğrultuda yönetilmesi, pek çok gelişmiş ve bu konuyu ciddiye alan ülkenin yaptığı gibi ilke ve stratejilerin belirlenmesi ile mümkündür.

İlke ve stratejilerin belli olmadığı her türlü girişimin başarısız olmaya mahkûm olduğunu göz önüne alarak; Siber Uzay gibi geleceğin şekillendiği bir ortamda, Türkiye'nin dönüşümünü; vatandaş, devlet, kamu kurum ve kuruluşları, özel sektör, üniversite ve sivil toplum kuruluşları gibi tüm paydaşlarının işbirliği ve emeği ile başarılı bir şekilde gerçekleştirmek için Siber Güvenlik Stratejisinin oluşturulması ve uygulanması büyük önem arz etmektedir.[689]

1.3.3. Türkiye'de Bilgi Güvenliğine İlişkin Çalışmalar Ve Bulgular Hakkında Genel Değerlendirme

1.3.3.1. Ulusal Siber Güvenlik Tatbikatı Sonuçları

Yapılan çalışmalar tatbikata katılan kurum ve kuruluşlarda bilgi güvenliği açısından azımsanmayacak miktarda açıklık olduğu sonucunu gözler önüne sermektedir.

Açıklıkların kapatılması konusunda bilişim teknolojilerine yapılacak donanım-yazılım satın alımı ve benzeri yatırımların yeterli olmayacağına, başta kurum yöneticileri olmak üzere kurum çalışanlarının tamamının bilgi güvenliği konusunda eğitilmesi, ilave olarak bilgi güvenliğine ilişkin kurumsal iş süreçlerinin hayata geçirilmesi gerektiğine dikkat çekmek isteriz.

[689] Bilgi Güvenliği Derneği, http://www.bilgiguvenligi.org.tr/files/Ulusal_Siber_Guvenlik_Stratejisi.pdf, Erişim Tarihi: 10.09.2012

Elde edilen bulgular genel olarak değerlendirildiğinde ülkemizde siber güvenliğin sağlanması için özetle, bilgi güvenliği yönetim sistemi, iş sürekliliği, insan kaynakları, kurum içi ve kurumlar arası iletişim ve koordinasyon alanlarında çalışma yapılması gerektiği görülmektedir.[690]

Bilgi Güvenliğine Kurumsal Yaklaşım İçin BGYS

Kurumsal olarak siber güvenliğin sağlanmasına çalışılırken gerçekleştirilecek faaliyetlerin çalışanların kişisel bilgi ve yeteneklerine bağımlılığını azaltacak, ölçüm, denetim ve sürekli iyileştirme anlayışını kuruma yerleştirecek Bilgi Güvenliği Yönetim Sistemleri (BGYS) önem arz etmektedir. Tatbikat kapsamında gerçekleştirilen senaryolarda bilgi güvenliği olaylarına müdahale aşamalarında BGYS'ye sahip kurumların daha sistematik olarak sorunları çözmeye çalıştıkları görülmüştür.

İş Sürekliliği

Hizmet kesintilerini önlemek, bir kesinti durumunda ise kısa zamanda sistemin çalışır hale gelmesini sağlamak için iş sürekliliği çalışmaları önem taşımaktadır. Yapılacak analizlere göre kurumlar öncelikle iş sürekliliği planlarını oluşturmalıdır. Daha önce iş sürekliliği ile ilgili çalışma yapmış olan kurumların tatbikat esnasındaki senaryolarda hizmet kesintileriyle daha etkin mücadele edebildiği ve daha kısa zamanda sistemlerini çalışır hale getirdikleri görülmüştür.

İnsan Kaynakları Çalışmaları

Siber güvenliğin sağlanması için gerçekleştirilecek insan kaynakları çalışmalarında personel istihdamı ve eğitim önemli yer tutmaktadır. Bu kapsamda, öncelikle yedekliliği sağlayacak şekilde yetişmiş personel istihdam edilmeli, sistem yöneticilerine işlettikleri sisteme hakim olmalarını sağlayacak eğitimler planlanmalı, devamında ise bilgi güvenliği konusunda çalışacak uzman personel (mümkünse ayrı bir birim olacak şekilde) için bilgi güvenliği uzmanlık eğitimleri planlanmalıdır. İnsan kaynakları çalışmaları siber güvenliği sadece teknik bir olgu olarak görmemeli, siber güvenlik için gerçekleştirilecek eğitimlerde tüm bilgi sistemi kullanıcıları için düzenli bilinçlendirme çalışmaları yapılmalıdır.

---

690 TÜBİTAK Ulusal Bilgi Güvenliği Kapısı, http://www.bilgiguvenligi.gov.tr/raporlar-kategorisi/ulusal-siber-guvenlik-tatbikati-2011-sonuc-raporu.html, Erişim Tarihi: 14.09.12

Kurum İçi ve Kurumlar Arası Koordinasyon

Son olarak, yaşanan bilgi güvenliği olaylarının çoğuna kurumların tek başına müdahale etmesi ya da kurum içindeki bilgi işlem biriminin tek başına çözüm üretmesi mümkün olmamaktadır. Siber güvenlik tehditleriyle mücadele edebilmek için gerek kurum içi (bilgi işlem birimi, hukuk birimi, iletişim birimi vs.) gerekse kurum dışı paydaşlarla iletişim arttırılmalı ve gerekli koordinasyon sağlanmalıdır.

1.3.3.2. Ticari Kuruluşların Periyodik Raporları

Symantec 2011 Tehdit Raporu

Symantec güvenlik firmasının 2011 yılı için yayınladığı tehdit raporuna göre dünya genelinde yeni güvenlik açıklıklarının yüzde 20 oranında düştüğü belirtilirken kötü niyetli saldırıların yüzde 80 oranında artış gösterdiği belirtilmiştir.[691] Türkiye, Avrupa, Ortadoğu ve Afrika bölgesinde (EMEA) en çok saldırı alan ilk 10 ülke arasında 4. sırada yer alıyor. 2011 yılında EMEA'da tespit edilen kötü amaçlı yazılımların %6'sını barındıran Türkiye bu oran ile bulunduğu coğrafyadaki ülkeler arasında 4. sıraya yerleşti.

Türkiye için bu raporda önemli olan bir başka sonuç ise bot aktivitelerinde ve network saldırılarında 8. sırada yer alması. Mobil cihazların güvenliği ise gelecek için endişe yaratıyor.

Bu süreçte istenmeyen e-posta seviyesi önemli oranda azalırken keşfedilen yeni güvenlik açıkları da yüzde 20 oranında azaldı. Zararlı yazılım oranındaki artışla kıyaslandığında bu istatistikler oldukça ilginç bir görünüm kazanıyor. Saldırganlar mevcut zafiyetlerden verimli şekilde faydalanabilmek için kullanımı kolay saldırı araçlarını benimsiyor. Siber suçlular saldırılarını gerçekleştirmek için istenmeyen e-postaların da ötesine geçerek sosyal ağları kullanıyorlar. Söz konusu ağların doğası itibariyle kullanıcılar yanlış bir varsayımla risk altında olmadıklarını ve saldırganların bu sitelere dönmelerinin amacının yeni kurbanları hedef almak olduğunu düşünüyor. Oysa sosyal ağların viral doğaları ve sosyal mühendislik teknikleri düşünüldüğünde tehditlerin bir kişiden diğerine yayılması da kolaylaşıyor.

[691] Symantec, http://www.symantec.com/threatreport/, Erişim Tarihi: 12.09.12

Gelişmiş saldırılar her ölçekten kurumu hedef alıyor. Rapora göre 2011'in sonu itibarıyla günlük hedefli saldırılar gün bazına 77 saldırıdan 82 saldırıya kadar artmış bulunuyor. Hedefli saldırılarla, sosyal mühendislik ve kişiselleştirilmiş zararlı yazılımları kullanarak hassas bilgilere yetkisiz erişim sağlamaya çalışıyorlar. Geleneksel olarak kamu sektörü ve hükümetlere karşı yoğunlaşan bu gelişmiş saldırılar 2011 yılında daha da fazla çeşitlenmiş bulunuyor.

Hedefli saldırılar artık yalnızca büyük kurumları hedef almıyor. Söz konusu saldırıların yüzde 50'den fazlası 2 bin 500'den daha az çalışana sahip kurumları hedef alırken, saldırıların neredeyse yüzde 18'i 250'den az çalışana sahip kurumlara yönelik oldu. Söz konusu kurumlar daha büyük bir şirketin tedarik zincirinde yer aldıkları ya da büyük şirketin ekosisteminin bir parçası oldukları için hedef alınmış olabiliyorlar. Hedef alınmalarının bir diğer sebebi de daha az savunuluyor olmaları. Dahası saldırıların yüzde 58'i insan kaynakları, halkla ilişkiler ve satış gibi yönetici pozisyonunda olmayan çalışanları hedef alıyor. Söz konusu pozisyonlardaki bireyler bilgilere doğrudan erişim sahibi olmasalar da şirketin içerisine doğrudan bir bağlantı olarak konumlanabiliyorlar.

Bu çalışanlar online olmaları, proaktif talepler almaları ve bilinmeyen kaynaklardan ek dosyalar aldıkları için hedef saldırganlar için hedef teşkil edebiliyorlar.

Veri ihlalleri yükseliyor, kayıp cihazlar gelecek için endişe yaratıyor. 2011 yılında veri ihlali başına çalınan kimlik sayısı yaklaşık 1,1 milyon olarak gerçekleşirken bu artış diğer tüm yıllardan fazla oldu. 2011 yılında bilgisayar korsanlığı etkinlikleri 187 milyon kimliğin açığa çıkmasıyla birlikte en büyük tehdidi teşkil etti. Bu rakam geçen yılki tüm ihlal türleri arasında en yüksek sayı olarak kayıtlara geçti. Buna rağmen veri ihlallerinin en yaygın sebebi hırsızlık ya da kayıp bilgisayarların yanı sıra verilerin depolandığı akıllı telefon, USB anahtarı ve yedekleme cihazı gibi taşınabilir cihazlar oldu. Bu hırsızlık ya da kaybolma ilintili ihlaller 18,5 milyon kimliği açığa çıkardı.

Tablet ve akıllı telefon satışları PC satışlarını geride bıraktıkça hassas bilgilerin daha çok mobil cihazlarda depolanacağı öngörülüyor. Çalışanların, iş ortamlarına kendi akıllı telefon ve tabletlerini dâhil etme hızı birçok kurumun onları

güvenlik altına alma ve yönetme becerilerinin gelişmesinden daha hızlı seyrediyor. Mobil cihazların bilgilerin iyi korunmadıklarında kaybolmalarının veri ihlallerinde bir artışa yol açabileceği düşünülüyor. Symantec tarafından yakın zamanlarda yapılan bir araştırma, kaybolan telefonların yüzde 50'sinin geri dönmediğini ve yüzde 96'sının (geri dönmüş olanların dâhil) veri ihlali yaşayacağını ortaya koyuyor.

Mobil tehditler kurumları ve tüketicileri tehdit ediyor. Mobil zaaflar 2011 yılında yüzde 93 oranında artış göstermiş bulunuyor. Aynı dönemde Android işletim sistemine yönelik tehditlerde de artış gözleniyor. Mobil ortamdaki zaaflar arttıkça zararlı yazılım üreticileri mobile özel tehditler üretmeye başladılar. 2011 bu bağlamda mobil ortamdaki zararlı yazılımların kurumlara ve tüketicilere tehdit oluşturduğu ilk yıl oldu. Söz konusu veriler, veri toplama, içerik gönderme ve kullanıcı takibi gibi amaçlar için tasarlanmış bulunuyor. 65 milyondan fazla mobil abone, 31 milyondan fazla 3G abonesi bulunan Türkiye'de de bireyler ve kurumların mobil tehditlere karşı dikkatli olması gerekiyor.

Kaspersky firması 2011 Raporu

Güvenli içerik ve tehdit yönetimi çözümleri lideri Kaspersky Lab'in 2011 üçüncü çeyrek spam raporuna göre dünya genelindeki spam oranı ikinci çeyreğe oranla %2.7 düşüş göstererek 3. çeyrekte %79.8'e geriledi. Aynı rapora göre, dünyadaki spam e-postaların %50'den fazlası Hindistan (14.8%), Endonezya (10.6%), Brezilya (9.65%), Peru (6.65%), Güney Kore (5.85%) ve Ukrayna (3.7%)'dan yayılıyor. Türkiye ise bu ülkelerden farklı olarak %0.59 gibi oldukça düşük bir spam oranı ile listede 29. sırada yer alıyor.

Spam e-postaların en çok yayıldığı ilk 10 ülkenin Güney Amerika, Asya ve Doğu Avrupa'da bulunduğunu, bu ülkelerde çok sayıda kullanıcı bulunması ve kullanıcıların çoğunlukla da bilgili olmamasının spam e-postalarının neden yayıldığını açıkladığını söyleyen Kaspersky Lab Spam Analiz Uzmanı Maria Namestnikova, raporda tüm e-posta antivirüs taramalarında maruz kaldığı %1.78 spam e-posta oranıyla listede 14. sırada yer alan Türkiye hakkında ise şunları söylüyor: "Bu rakam, çok sayıda spam e-postaların Türkiye'ye gönderildiğini gösteriyor. Bunun önemli nedenlerinden bir tanesi Türkiye'deki internet kullanıcı sayısının ilk 20 ülke içerisinde yer alıyor olması. Buna paralel olarak, Türkiye'deki deneyimsiz internet kullanıcıları botnet ve e-dolandırıcılık için potansiyel birer

kurban olarak dikkat çekiyor. Türkiye'yi ziyaret eden turistler de e-dolandırıcılık ile kişisel ve finansal bilgileri çalan kötü niyetli yazılımların kurbanı oluyor" diyor.

Türkiye'de saptanan kötü amaçlı yazılımların en popüleri Trojan-Downloader uzantılı spamlar.

Rapora göre dünya genelinde 2011 yılı 3. çeyrek döneminde e-posta ile yayılan kötü amaçlı yazılım programları arasında ilk 3 sırada Trojan-Spy.HTML.Fraud.gen, Email-Worm.Win32.Mydoom.m, Trojan.Win32.FraudST.atc. yer alıyor. Bu üç zararlı yazılım, e-dolandırıcılık ile finansal kayıtları ele geçirme, bilgisayarlara virüs bulaştırarak kişisel bilgileri çalma ve ilaç konusunda spam e-posta gönderimi ile dikkat çekiyor. Ancak Türkiye'deki e-posta yoluyla yayılan ilk 10 kötü amaçlı yazılımlar bu listeden farklılık gösteriyor. Türkiye sonuçlarını yorumlayan Namestnikova, e-dolandırıcılık yazılımı Trojan-Spy.HTML.Fraud.gen'in Türkiye sıralamasında yer almamasını oldukça ilginç bulduğunu ve bunun nedenini Türkiye'deki kullanıcıların e-dolandırıcılar için daha az popüler olması olarak açıklıyor.

Türkiye'de saptanan kötü amaçlı yazılımların en popüleri olan Trojan-Downloader uzantılı spamlar, sıralamanın yarısından fazlasını oluşturuyor. Bu programlar internete bağlanıyor ve belirli URL adreslerinden dosya indirme komutu veriyor. Listelenen Trojanlar genellikle bots (spam e-posta yazan yazılım) indirmek için kullanılıyor.

Spam araştırma sonuçlarına göre Türkiye'nin kendine has özellikleri bulunuyor. Bunlar arasında kullanılan dilin Türkçe olması ilk sırada yer alıyor. Spam e-postaların çoğu, bölgede müşteri arayan ve reklamlarını spam yoluyla yapan yerel şirketler tarafından gönderiliyor. Ancak çoğunlukla İngilizce olan ilaç sektörü ve taklit ürün spamları düşük kar sebebiyle göndericiler tarafından Türkçe'ye çevrilmiyor. Bir diğer önemli özellik ise kültür ve dini inançlar konusudur. Spam e-posta gönderenler, ulusal tatil ve dini günleri de bölgesel spam e-postalarında sıklıkla kullanılıyor.

Türkiye'deki güvenlik bilinci bilgisayar kullanıcı sayısı ile paralel artmıyor, siber suçlular Türkiye'yi tercih ediyor.

Kaspersky Lab'in gerçekleştirdiği 2011 yılı 3. çeyrek kötü amaçlı yazılım raporu, Türkiye'deki internet kullanıcı sayısının etkin bir şekilde arttığını, ancak güvenlik bilinci seviyesinin bu artışa paralellik göstermediğini ortaya koyuyor. Ayrıca, Türkiye'deki kullanıcıların interneti kullanma şekilleri, bilgilerin basit bir şekilde araştırılmasından, Avrupa ülkelerine benzer bir şekilde farklı servislere doğru bir kayma gösteriyor. Türkiye, Körfez Arap Ülkeleri İşbirliği Konseyi (GCC)'nde yer alan ülkelerden farklı olarak devlet düzeyinde internet filtreleri kullanmıyor ve bu nedenle Avrupa'ya daha çok benziyor.

Kaspersky Lab, Türkiye'nin kötü amaçlı yazılımlarla ilgili durumunu değerlendirmek için, Türkiye'de 2011 yılı 3. çeyreğinde her bir Kaspersky Security Network kullanıcısı tarafından algılanan ve engellenen kötü amaçlı programların ortalama sayısını hesapladı.

2011 3. çeyrek kötü amaçlı yazılım raporunda Türkiye'de her bir aktif Kaspersky Security Network kullanıcısı başına 15,6 kötü amaçlı yazılım örneğinin engellendiği veya kaldırıldığı ortaya çıktı. Bu rakam Avrupa'nın 13,7 olan ortalamasından biraz; kullanıcı başına yaklaşık iki olan Körfez Arap Ülkeleri İşbirliği Konseyi ülkelerine oranla ise oldukça yüksek. Sonuçlar Türk bilgisayar kullanıcılarının siber suçluların hedefi olduğunu ortaya koyuyor. Siber suçlular tarafından tercih edilen Türkiye bu nedenle Avrupa ve Amerika'ya benzerlik gösteriyor.

Bir diğer önemli sonuç da Türkiye'de kötü amaçlı veya istenmeyen yazılımların kullanıcıların bilgisayarlarına nasıl sızdığıdır. Kaspersky Lab, ürünlerinin kullanıcının bilgisayarındaki kötü amaçlı bir programı ne sıklıkta algıladığını veya engellediğini, internette sörf yaparken, taşınabilir bir cihazla bağlantı kurarken ya da sadece sabit diski tararken analiz etti. Analiz sonucunda, web'den veya e-postadan ve dosya veya taşınabilir aygıttan olmak üzere iki temel saldırı tipi olduğu belirlendi.

Türkiye'de internet kullanıcıları Avrupa'ya göre kötü amaçlı yazılımlara daha fazla maruz kalıyor.

Kullanıcıların bilgisayarlarına web aracılığıyla virüs bulaşma riskinin en yüksek olduğu ülkeler arasında ilk beşte Bangladeş, Sudan, Ruanda, Tanzanya,

Angola yer alıyor. Türkiye'de üçüncü çeyrek boyunca saldırıya uğrayan internet kullanıcılarının oranı %27,7 olup dünya sıralamasında 36. sırada yer alıyor. Bu oran Avrupa ülkelerinde %25,5, GCC ülkelerinde ise %31,8. Bu da Türkiye'deki kullanıcıların, Avrupa'daki kullanıcılara kıyasla interneti kullanırken kötü amaçlı yazılımlara daha fazla maruz kaldığını ortaya koyuyor.

Türkiye'de kullanıcıları hedef alan saldırıların oranının Avrupa'ya kıyasla daha yüksek olması, Türkiye'de bilgisayarların saldırılara karşı daha savunmasız olmasından kaynaklanıyor. Bunun sebepleri arasında güncellenmeyen veya eski bilgisayarlarda kullanılan Windows XP oranının %42 olması öne çıkıyor. Bu sebeple bilgisayarlar sanal suçlular için oldukça basit hedefler haline geliyor.

Dünya çapında onlarca web sitesi Türk saldırganların kurbanı oldu. Kaspersky Lab Kötü Amaçlı Yazılımlar Uzman Analisti Yury Namestnikov; "Türk siber suçluların kendilerine özgü özellikleri olduğunu belirtmemiz gerekiyor. Türkiye'de bilgisayar korsanları diğer ülkelerde olduğu gibi ekonomik kazanç sağlamak için zararlı kod yazmakla vakit harcamıyor. Esas ilgilendikleri nokta, protestolarını sert bir şekilde göstermek için çeşitli site ve çevrimiçi servisleri çökerterek zarar vermek. Dünya çapında onlarca web sitesi Türk saldırganların kurbanı oldu" dedi. Suç türü açısından bakıldığında Türkiye'deki hukuk sisteminin bu konuda iyi çalıştığını söyleyen Yury Namestnikov Türkiye'de 3. çeyrekte 32 kişinin "Anonymous" grubunun bir parçası olarak DDoS saldırılarını başlattıkları şüphesiyle tutuklandığını hatırlatıyor.[692]

ESET Firması 2011 Tehdit Raporu

2011 yılı BT güvenliği açısından neler getiriyor? Kendimizi hazırlamamız gereken tehditler neler olacak? ESET'in kıdemli araştırma uzmanı David Harley ve ESET Sanal Tehdit Analiz Merkezi (CTAC) uzmanları, 2011 tehdit eğilimlerini açıkladı. Buna göre Facebook, Twitter gibi sosyal platformların yanı sıra Google, Yahoo, Bing gibi popüler arama motorlarına yönelik sosyal mühendislik saldırıları artacak. Yine taşınabilir cihazlara yani internet bağlantılı akıllı telefonlara yönelik tehditlerde yoğunlaşma olacak. ESET uzmanlarına göre, Botnetler yani virüslü çok sayıda bilgisayarın uzaktan yönetilmesi tehdidinin, 2011 yılında da büyümeye devam

[692] Kaspersky, http://usa.kaspersky.com/resources/knowledge-center/spam-report-january-2011, Erişim Tarihi: 12.09.12

edeceğini öngörülüyor. Öte yandan 2010 yılında "bilinen" bulaşıcı örnek sayısının 40 milyon olarak belirlendiğini aktaran ESET uzmanları, 2011 yılı içerisinde bu sayının "iyimser" bir tahminle 50 milyonu geçmesini bekliyor.

ESET'in kıdemli araştırma uzmanlarından David Harley ve ABD'nin San Diego kentinde bulunan ESET Sanal Tehdit Analiz Merkezi (CTAC) uzmanları 2011 tehdit eğilimlerini şöyle aktardı:

ESET Sanal Tehdit Analiz Merkezi takımı Facebook ve Google kullanıcılarının hali hazırda karşılaştıkları sosyal mühendislik saldırılarının artacağında ve hatta LinkedIn, Orkut ve Twitter gibi diğer sosyal ağ sitelerinin ve Bing, Yahoo gibi arama motorlarının da bu saldırılara maruz kalacağı konusunda hemfikir. Facebook özel bir tehlike barındırıyor: Facebook, sosyal medya gizliliği meselesinin müşterilerinin talebi olması gerekçesi ile neyin paylaşılıp neyin paylaşılmaması gerektiğini müşterilerinin sorumluluğuna bırakmaya devam eder ise hastalıktan çok belirtileri tedavi etmeye de devam eder.

Taşınabilir cihazların (akıllı telefonların) hedef alınması giderek artacak. Yüklenen uygulamaları ciddi şekilde kontrol eden markaların cihazları zararlı yazılım saldırılarına daha az maruz kalacak. Yine de dolandırıcılık içeren sosyal mühendislik saldırıları devam edecek.

Yeni bir tehdit çeşidi sayılmasalar da botnetler (Virüslü birçok bilgisayarın aynı anda tek bir amaca yönelik uzaktan yönetilmesi ile oluşturulan grup) 2011 yılında da büyümeye devam edecekler. ESET verileri botnetlerdeki genişlemeyi işaret ediyor. 2010 yılı boyunca Twitter aracılığı ile kontrol edilmiş olan botnetlerin önümüzdeki yıl içerisinde diğer kanalları kullanarak da kontrol edilebilmesi bekleniyor. İyi haber ise botnetleri tespit ederek kapatma çalışmalarındaki başarı da giderek artacak.

Çeşitli uygulamalarla birden çok platformu etkileyebilecek zararlı yazılımlarda artış bekleniyor. Örneğin hem Windows hem de Windows olmayan işletim sistemlerine sahip virüslü bilgisayarlardan oluşan botnetler var.

İndeks zehirlemesi olarak da adlandırılan ve "BlackHat SEO" yani "Kara Şapkalı Arama Motoru Optimizasyonu" olarak nitelendirilen arama sonuçlarının

manipüle edilmesi de yeni değil ama yükselen bir tehdit olarak yerini alıyor. Özellikle sosyal medya kullanımı, arama sırasında trafiğin zararlı siteler üzerinden yönlendirilmesine yönelik geniş bir alan sunuyor.

Sosyal mühendislik en büyük sorunlardan biri olmaya devam edecek. Birçok zararlı yazılım e-posta, bulaşıcı URL, forumlar, haber grupları gibi bilindik yollardan saldırmaya devam edecek. Yine de LNK açığı (Windows işletim sistemlerinin kabuk yapısında tespit edilmiş bir açık) gibi sorunlarla karşılaşmaya da hazırlıklı olunmalı. İran ve ABD'deki elektrik santrallerini hedef alan SCADA türü endüstriyel veri hırsızlığına yönelik truva atları ile daha çok karşılaşabiliriz.

Zararlı yazılımlar ile savaşan güvenlik yazılımı üreticileri, analizler ve tersine mühendislik yöntemi ile zararlı yazılım inceleme işlemlerini giderek bulut-tabanlı alanlara kaydıracak. 2010 mayısında Helsinki'de düzenlenen CARO çalışma grubunda "bilinen" bulaşıcı örnek sayısı 40 milyon olarak belirlendi. 2011 yılı içerisinde bu sayının 50 milyonu geçeceğini öngörebiliriz. Aslında bu rakamlar oldukça iyimser fakat gerçek rakamlara ulaşmak firmaların sayma yöntemleri arasındaki farklılıklar ve kopyaların ayıklanabilmesi için gerekli zaman gibi zorlu nedenlerle imkânsız gibi görünüyor.[693]

1.4. TÜRKİYE İÇİN ÖNERİLER

1.4.1. Ulusal Bilgi Güvenliği Politikası ve Stratejisi

Ulusal Bilgi Güvenliği Politikası ve Stratejisinde yer alması gereken adımlar aşağıdaki tabloda gösterilmiştir. Eylem planı beş ana başlıktan oluşmaktadır. Bunlar:

- Ulusal Siber Güvenlik Koordinasyon Kurulu'nun kurulması,
- Siber güvenlik konusunda yasal düzenlemenin yapılması
- Ulusal siber güvenlik altyapısının güçlendirilmesi
- Ulusal siber güvenlik kabiliyetlerinin geliştirilmesi
- Siber güvenlikte ulusal/uluslararası işbirliğinin sağlanması

şeklindedir.

[693] Eset, http://www.eset.co.uk/Download/Collateral/Threat-Reports, Erişim Tarihi: 12.09.12

Tablo 120. Ulusal Bilgi Güvenliği Politikası ve Stratejisinde Yer Alması Gereken Adımlar

No	Eylem	Açıklama
1	Ulusal Siber Güvenlik Koordinasyon Kurulu'nun kurulması	Ulusal Siber Güvenlik Koordinasyon Kurulu oluşturulur. Kurul ulusal siber güvenlik eylem planında yer alan maddelerin uygulanması için yöntem belirler, sorumluları atar, planın uygulanmasını takip eder, gerektiğinde plana ek ve düzeltmeler yapar.
2	Siber güvenlik konusunda yasal düzenlemenin yapılması	Yasal düzenleme ile siber güvenliğin tanımı yapılmalı, kapsam ve sorumluluklar belirlenmelidir. Bu konuda detaylı açıklama dokümanın Ulusal Siber Güvenlik Kanunu bölümünde yer almaktadır.
3	Ulusal siber güvenlik altyapısının güçlendirilmesi	
3.1	Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı	Siber tehditlerin doğrudan hedefi haline gelen ve zarar görmesi halinde toplum düzenini bozabilecek kritik altyapılar tespit edilecek, bilgi teknolojilerinin kullanımından kaynaklanan risklerin analizi yapılacak, risklerin kapatılması için gerekli karşı önlemler belirlenecek ve uygulanacaktır.
3.2	Kamu Bilgi Güvenliği Programı	Belirlenen kamu kurumlarına, kurum bazında özelleştirilmiş test ve denetim prosedürleri kullanılarak düzenli aralıklarla güvenlik test ve denetimleri gerçekleştirilecektir.

No	Eylem	Açıklama
3.3	Ulusal Internet Sürekliliği Programı	Kamu kurumları ve özel kurumlar tarafından İnternet aracılığı ile verilen hizmetlerin geniş kapsamlı saldırılardan korunması için Ulusal Internet Ağı İzleme Sistemi kurulacak ve tüm paydaşların işbirliği ile saldırılara gerçek zamanda müdahale edilecektir.
3.4	Yazılım Güvenliği Programı	Ulusal kritik bilgi sistemlerinde çalışmakta olan ya da geliştirilen yazılımların sağlaması gereken güvenlik fonksiyonları belirlenecek, yazılımların bu güvenlik fonksiyonlarını icra ettiklerini doğrulayacak metodoloji ve yöntemler geliştirilecektir.
3.5	Kötücül Yazılımla Mücadele Programı	Ulusal ağlarda dolaşan zararlı yazılımlar ve bulaştıkları sistemlerde yaptıkları etkiler belirlenecek, bu zararlı yazılımlara karşı uygulanacak korunma önlemleri geliştirilecektir.
3.6	Kamu Güvenliği Ağı	Kamu kurumlarının güvenli, hızlı ve sürekli iletişimini sağlamak üzere VPN teknolojileri kullanılarak Kamu Güvenli Ağı kurulacaktır.
4	Ulusal siber güvenlik kabiliyetlerinin geliştirilmesi	
4.1	Siber Güvenlik Enstitüsü	Siber uzaydan kaynaklanan tehditleri incelemek, tehditlere karşı alınması gereken önlemleri belirlemek, siber güvenlik alanında kullanılacak yazılım, donanım ve benzeri bilişim teknolojilerini geliştirmek için Ar-Ge faaliyetleri yapmak ve her türlü faydalı bilgiyi üretmek ve yayınlamak üzere Siber Güvenlik Enstitüsü kurulacaktır.

No	Eylem	Açıklama
4.2	Siber güvenlik uzmanı destekleme programı	Siber güvenlik konusunda uzmanlaşmak isteyen başarılı öğrenciler desteklenecek, bu konuda dünyada yetkinliğini ispatlamış üniversitelerde doktora ve yüksek lisans yapmaları için burs verilecektir.
4.3	Üniversitelerde siber güvenlik eğitimi	Üniversitelerde siber güvenlik ile ilgili derslerin sayısı arttırılacak, içerikleri zenginleştirilecektir.
4.4	Siber güvenlik personelinin eğitimi	Kanun kapsamında yer alan kurumların bilgi sistemlerinden ve siber güvenliğinden sorumlu personeli eğitime tabi tutulacaktır.
4.5	Bilgisayar kullanıcılarının eğitimi	Kapsam dışında yer alan bilgisayar kullanıcılarının bilinç düzeyini arttırmak için milli eğitim olanakları, basın ve yayın organları kullanılacaktır.
4.6	Ar-Ge faaliyetlerinin teşvik edilmesi	Siber güvenlik ile ilişkili yazılım, donanım ve benzeri bilişim teknolojisi ürünlerine yönelik ulusal araştırma – geliştirme faaliyetleri teşvik edilecektir.
4.7	Test yapan firmaların sertifikasyonu	Bilgi sistemlerinin güvenlik testlerini yapan firmaların standardizasyonu ve sertifikasyonu sağlanacaktır.
4.8	Açık kaynak kodlu ürünler	Kamu ve özel sektör kurumlarının kullanabileceği, belirlenmiş minimum güvenlik kriterlerini sağlayan açık kaynak kodlu mevcut güvenlik ürünleri hakkında bilgilendirme yapılacak, kılavuzlar yayınlanacak, açık kaynak kodlu yeni ürünlerin geliştirilmesi için platformlar oluşturulacaktır.

No	Eylem	Açıklama
5	Siber güvenlikte ulusal/uluslararası işbirliğinin sağlanması	
5.1	Ulusal Siber Güvenlik Forumu	Kamu ve özel sektörün, üniversite, STK ve benzeri tüm bilgi güvenliği paydaşlarının katılacağı bir forum oluşturulacaktır. Forum katılımcıları araştırma, geliştirme, koordinasyon ve diğer bilgi güvenliği ihtiyaçlarının karşılanması konusunda iletişim ve işbirliği yapar.
5.2	Milli ürünlerin teşvik edilmesi	Kurumların bilgi ve iletişim sistemlerinde milli olarak geliştirilmiş ürünleri tercih etmeleri, Milli ürünlerin mevcut olmadığı durumlarda güvenlik değerlendirmesi ve sertifikalandırması milli olarak gerçekleştirilmiş ürünleri tercih etmeleri, Güvenlik değerlendirmesi milli olarak gerçekleştirilmiş ve sertifikalandırılmış güvenlik ürünlerinin mevcut olmadığı durumlarda uluslar arası standartlar uyarınca değerlendirilmiş ve sertifikalandırılmış ürünleri tercih etmeleri için teşvik mekanizmaları oluşturulacaktır.

Yukarıdaki tabloda önerilen maddlerle ilgili detaylı açıklama aşağıda yapılmıştır.

Yasal ve Kurumsal Düzenlemeler

Yasal altyapı ile beraber hem ülke çapında bilgi güvenliğinden sorumlu olan kurum/kurumlar tespit edilmeli hem de bu kurumun/kurumların sorumlulukları açıkça tanımlanmalıdır. Ulusal çapta bilgi güvenliğinin sahibi olacak olan organizasyon kurulmalıdır. Bu organizasyonda ulusal bilgi güvenliği politikasını ve

stratejisini belirleyecek, güncelleyecek, bu politika ve stratejiye göre eylem planı oluşturacak ve bu planın uygulanmasını takip edecek, konuyla ilgili kurumlardan üst düzey katılımla oluşturulacak bir **bilgi güvenliği kurulu** olmalıdır. Ayrıca bilgi güvenliği ile ilgili olarak her bir kamu kurumunun ve özel sektörün görev ve sorumlulukları da belirlenmelidir. Yapılacak olan yasal düzenlemelerde kişisel bilginin mahremiyeti bir ilke olarak göz önünde bulundurulmalıdır. İlgili mevzuat kapsamında, kanun başta olmak üzere bu kanunu tamamlayacak olan alt hukuki düzenlemeler de oluşturulmalıdır.

Kritik Altyapı Güvenliği

Savaş halinde savaş suçlarının da işlenebileceğinden hareketle Türkiye'nin kritik altyapı güvenliğini öncelikli olarak sağlaması, ilave olarak kendisine yapılan saldırılarla ilgili delil üretmek üzere kritik altyapı sistemlerini mükemmelen çalışan kayıt sistemleri ile izlemesi gerekir. Kayıt sistemleri aracılığı ile Türkiye'nin kendisine yapılan saldırının doğrudan ve dolaylı etkilerini ve saldırının nereden yapıldığını doğru olarak belirleme kabiliyetine sahip olması şarttır. Aksi halde meşru müdafaa hakkının kullanılması bile mümkün olmayabilir.

Bu amaçla aşağıdaki adımlarda sıralanan faaliyetler gerçekleştirilmelidir:

- Ülkedeki kritik bilgi altyapıları tespit edilmelidir.

- Tespit edilen her bir kritik bilgi altyapısının diğer kritik bilgi altyapılarıyla ilişkisi analiz edilmeli ve bağımlılıkları ortaya konmalıdır.

- Kritik bilgi altyapıları önem derecesine göre sınıflandırılmalı ve her bir sınıf için alınması gereken minimum güvenlik önlemleri belirlenmelidir.

- Belirlenen minimum güvenlik önlemlerinin uygulanması denetlenmelidir.

Siber Güvenlik Hukukuna Hakim Personel Yetiştirilmesi

Uluslararası ilişkiler, uluslararası hukuk ve milli savunma stratejileri konusunda çalışan stratejist ve bürokratlar arasında bu konuları siber güvenlik açısından ele alabilecek bilgiye sahip kişilerin yetiştirilmesi çok önemlidir. Bu kişilerin siber savunma ve uluslararası siber güvenlik hukuku konularında fikir, politika ve strateji üretmelerine çok fazla ihtiyaç bulunmaktadır. Bu sebeple Mili

Savunma Bakanlığı, Dışişleri Bakanlığı ve Türk Silahlı Kuvvetlerinde söz konusu yetkinliklere sahip personel istihdam edilmeli ya da mevcut personelin bir bölümünün bu yetkinliklere sahip olmaları sağlanmalıdır.

Bilgi Güvenliği Araştırmalarını Destekleme

Bilgi güvenliği konusunda ülkemizin ihtiyaçlarının kendi kaynaklarıyla karşılanması için çalışmalar yapılmalıdır. Bu kapsamda, öncelikle ülkemizin ihtiyaçları analiz edilmeli, bu ihtiyaçların ülke içinden temin edilebilmesi için araştırma yapılacak konular tespit edilmeli, bu konulardaki çalışmalara destek sağlanmalıdır. Bilgi güvenliği konusunda ülkede var olan birikimin artırılması ve paylaşılabilmesi için üniversitelerde bilgi güvenliği derslerinin yaygınlaştırılması teşvik edilmeli ve bu derslerin içeriklerinin sadece kriptoloji konularıyla sınırlı kalmaması, yazılım ve sistem güvenliği konularının da kapsama alınması gerekmektedir. Kamu kurumları, üniversiteler ve özel sektörün, araştırma, geliştirme ve gerekli diğer ihtiyaçların karşılanmasında işbirliği içerisinde çalışması sağlanmalıdır.

Ulusal Bilgisayar Olaylarına Müdahale Organizasyonu

Bilgi ve iletişim sistemlerine yönelik tehditlerin hızlı tespiti, tehditlerle ilgili bilgi paylaşımı ve yaşanan olayların yıkıcı etkilerini ortadan kaldırmaya ve azaltmaya yönelik hızlı tedavi metotlarının geliştirilmesi ve paylaşılması aktivitelerinin ulusal seviyede etkili bir şekilde ve eşgüdüm içerisinde yapılabilmesi için **Ulusal Bilgisayar Olaylarına Müdahale Organizasyonu** kurulmalıdır. Sorumluluk alanı, ülkedeki tüm sistemler olan Ulusal Bilgisayar Olaylarına Müdahale Organizasyonu'nun alt birimleri oluşturulmalıdır. Alt birimlerin sorumluluk alanları arasında ilgili kritik altyapı birimlerinin korunması yer almalıdır. Bu ekiplerin oluşturulması kapsamında eğitim başta olmak üzere yapılması gereken tüm çalışmalar bu organizasyonun bir görevi olmalıdır. Bu organizasyon, ülkenin tamamını veya bir kısmını etkileyen tehdit ve saldırılara karşı 7/24 hizmet veren bir "acil işlem merkezi" şeklinde faaliyetlerini sürdürmelidir. Acil işlem merkezi yaşanan bilgi sistemleri güvenlik olayları ile ilgili diğer ülkeler ve uluslararası kuruluşlar ile teması ve koordinasyonu sağlamalıdır. Ulusal Bilgisayar Olaylarına Müdahale Organizasyonu ülkemizin olası bir sayısal ortam savaşına karşı ne kadar

hazırlıklı olduğunu ölçmek ve ardından var olan eksiklikleri tespit etmek amacıyla tatbikatlar düzenlemelidir.

Bilgi Güvenliği Eğitimleri ve Bilinçlendirme Çalışmaları

Bilgi ve iletişim sistemlerini işleten personelden kurumun stratejisini belirleyen üst düzey yöneticilere kadar herkes bilgi ve iletişim sistemlerinin güvenliği ve üzerine düşen sorumluluk konusunda bilinçli olmalıdır. Bunu sağlamak için son kullanıcıları, sistem yöneticilerini, teknoloji geliştiricilerini, denetçileri, orta ve yüksek seviyeli yöneticileri kapsayan eğitimler hazırlanmalı ve bu eğitimlerin ilgili personele verilmesi sağlanmalıdır. Sistem yöneticileri için hazırlanacak olan eğitimde, bu personele işlettikleri sistemlerin güvenlik yapılandırmalarının nasıl olması gerektiği ve güvenlik açısından dikkat edilmesi gereken hususlar anlatılmalı ve eğitim sonunda yapılacak sınavla sertifika verilmelidir. Sertifikanın belli bir geçerlilik süresi olmalı, bu sayede personelin teknik olarak kendini yenilemesi sağlanmalıdır. Yeni neslin bilgi güvenliği bilinciyle yetişmesini sağlamak için okullarda bilgi güvenliği konusunda eğitimler verilmelidir. Ulusal güvenlik açısından kritik olarak değerlendirilen kuruluşlara bilinçlendirme posterleri asılmalı, belirli aralıklarla seminerler verilmelidir. Tüm vatandaşların bilgi güvenliği bilincini artırmak amacıyla medya aktif kullanılmalı, televizyonlarda programlar yapılmalıdır. Tüm vatandaşlara hitap eden bir İnternet sitesi aracılığıyla bilgi güvenliği konusundaki temel dokümanlara ulaşım kolaylaştırılmalıdır. Bu site e-öğrenme altyapısıyla son kullanıcılar için bilgi güvenliği eğitimleri vermelidir.

Kamu Kurumları Bilgi Güvenliği Programı

Kamu kurumlarının bilgi güvenliğini sağlamak amacıyla öncelikli atılması gereken adım bu kurumlarda bilgi güvenliğinden sorumlu personelin belirlenmesidir. Kurumlarda bilgi güvenliğinin sağlanması ancak üst yönetimin desteği ile sağlanabilir dolayısıyla bilgi güvenliği sorumluluğu öncelikli olarak kurumun en üst yöneticisine aittir. Kamu kurumlarında bilgi güvenliğinin sorumluluğu en üst yöneticiye verilmekle beraber operasyonel ihtiyaçları karşılamak amacıyla gerekirse organizasyon yapısında değişikliğe giderek bilgi güvenliği birimi kurulmalıdır. Bu birim kurum içi Bilgisayar Olaylarına Müdahale Ekibi (BOME) olarak hizmet vermeli, kurumda bir güvenlik olayı yaşanmaması için gerekli önlemleri almalı ve meydana gelen güvenlik olaylarına ilk müdahalede bulunmalıdır. Kamu

kurumlarında atılması gereken bir diğer adım ise dünyada kabul görmüş Bilgi Güvenliği Yönetim Sistemi standardı olan ISO 27001:2005'e uyumluluğun sağlanması olmalıdır. Bu sayede güvenliğin sadece anlık olarak ulaşılacak bir hedef değil devam eden bir süreç olduğu kavranılacak ve çalışmalarda devamlılık sağlanacaktır. Yine bu standardın bir gereği olarak kurumlar risk analizi yaparak eksikliklerini tespit edecekler ve bunları kapatma yoluna gideceklerdir. Bilgi ve iletişim sistemlerinde çok sayıda yazılım ve donanım kullanılmaktadır. Gelişen teknolojiyle beraber yazılım ve donanım ihtiyacını karşılamak amacıyla çok sayıda ürün ortaya çıkmıştır. Bu ürünlerin tedariğini yaparken kurumlar Ortak Kriterler (Common Criteria) sertifikasına sahip ürünleri tercih etmelidirler.

1.4.2. Organizasyon Önerisi

Ülkemizde bilgi güvenliğiyle ilgili yapılacak yasal düzenleme ile kurumların sorumlulukları belirlenmeli, denetim mekanizması kurulmalı ve ülkenin siber güvenlikle ilgili politika, strateji ve eylem planını oluşturmak ve takip etmekten sorumlu olan Ulusal Siber Güvenlik Koordinasyon Kurulu oluşturulmalıdır.

Ulusal Siber Güvenlik Kanunu aşağıdaki özelliklere sahip olmalıdır:

a. Kapsam: Yasa kapsamında yer alacak kurum ve kuruluşların tanımını kapsamalıdır (Bilgi ve iletişim sistemlerinde kritik bilgi bulunduran veya taşıyan, bilgi ve iletişim sistemleri aracılığı ile kritik sistem çalıştıran tüm kamu ve özel sektör kurum ve kuruluşları kapsam dâhilinde yer almalıdır).

b. Sorumluluk: Her kurum kontrolü altındaki bilgi varlıklarının ve sistemlerin güvenliğini sağlamakla yükümlü olmalıdır.

c. Kurum içi organizasyon: Kurumlarda siber güvenlikten sorumlu bir yetkili ve siber güvenlik sürecini çalıştıracak birim bulunmalıdır.

d. Asgari güvenlik önlemleri: Kurumlar tarafından alınması gereken asgari güvenlik önlemlerini tanımlamalıdır.

e. Kurum içi siber güvenlik süreci: Kurum tarafından düzenli aralıklarla yapılması gereken risk analizi, risk tedavisi, tetkik, eğitim, gözden geçirme toplantısı vb. faaliyetler tanımlanmalıdır.

f. Tetkik makamı: Kurumlar üstü bir tetkik makamı tanımlanmalı ve kurumların siber güvenlik sürecini çalıştırıp çalıştırmadığını denetleme yetkisi ile donatılmalıdır.

g. Ulusal siber güvenlik koordinasyon kurulu: Kurumlar üstü bir siber güvenlik koordinasyon kurulu tanımlanmalıdır. Kurul ulusal siber güvenlik ile ilgili durumu izlemeli, ihtiyaçları belirlemeli ve planlama yapmalıdır.

h. TR-BOME, yasal düzenleme ve kaynak tahsisi ile tam zamanlı Ulusal BOME işlevini gerçekleştirecek şekilde güçlendirilir. TR-BOME, (kanununda tanımlanan) kurum içi siber güvenlik birimleri ile koordinasyon içinde çalışarak aşağıdaki işlevleri yerine getirir:

- Bilgi ve iletişim sistemleri üstünde gerçekleşen ulusal ve uluslar arası bilgi güvenliği ihlallerine ve saldırılarına etkin müdahale için koordinasyon görevini üstlenir.
- Bilgi ve iletişim sistemlerinde bulunan açıklıklar, bunları kullanabilecek tehditler ve açıklıkları kapatmak için alınması gereken önlemlerle ilgili güncel mesajlar yayınlar.
- Konferans, WEB sitesi ve benzeri her türlü olanağı kullanarak bilgi güvenliğinin teknolojik ve idari boyutlarına ilişkin bilgilendirme ve bilinçlendirme çalışmaları yapar, danışmanlık ve eğitim hizmetleri verir.

1.4.2.1. Bilgi Güvenliği Kurumu/Kurulu

Ulusal Siber Güvenlik Koordinasyon Kurulu oluşturulur. Kurul ulusal siber güvenlik eylem planında yer alan maddelerin uygulanması için yöntem belirler, sorumluları atar, planın uygulanmasını takip eder, gerektiğinde plana ek ve düzeltmeler yapar.

Oluşturulmuş olan Siber Güvenlik Koordinasyon Kurulu doğrudan başbakanlığa bağlı olarak Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Bilim, Sanayi ve Teknoloji Bakanlığı, Milli Savunma Bakanlığı, TÜBİTAK ve BTK başta olmak üzere diğer bakanlıklarla ve kurumlarla koordineli bir şekilde çalışır.

1.4.2.2. Siber Ordu

Siber ortamda savunma sadece bir kuruma ait birimin sağlayabileceği bir işlev değildir. Her kurum ve kuruluşun kendi bilgi ve sistemlerini koruyacak yetkinliğe kavuşturulması siber güvenliğin esasıdır. Kurum ve kuruluşların siber saldırılara karşı koyma adına gerçekleştireceği çalışmalarda eğitim, danışmanlık ve bilgi desteğini TÜBİTAK BİLGEM'in hâlihazırda sağladığı ve desteğin çok daha fazla kurum ve kuruluşa ulaşması adına gerekli kapasite artırım çalışmalarının yapılması gerektiği değerlendirilmektedir.

Siber saldırılara dönük savunma konusunda özellikle internet servis sağlayıcılarına ve internet servis sağlayıcılarını düzenleyen kurumlara çok önemli görevler düşmektedir.

Siber suçları önleyici faaliyetlerin gerçekleştirilmesi ve siber suçluların tespit edilmesi Emniyet birimlerince gerçekleştirilmektedir. Bu yeteneğin daha da artırılması sağlanmalıdır.

Üniversitelerde açılması gereken siber güvenlik araştırma merkezlerinin gerekli akademik çalışmaları ve Ar-Ge çalışmalarını gerçekleştirmesi gereklidir.

Siber ortamda gereken durumlarda saldırı yapılması konusunda sorumluluk, hedeflerin niteliğine ve saldırının amacına göre farklı kurumlarda bulunmalıdır. Örneğin siber ortamdan istihbarat elde edilmesi amacına yönelik eylem yeteneğinin istihbarat kurumlarında bulunması gereklidir. Ayrıca açık kaynak istihbaratına, internet üzerinden otomatik veri elde edilmesi, bu verilerin sınıflandırılması ve kullanılabilecek hale getirilmesi faaliyetlerinin dâhil edilmesi çok önemlidir. Düşman ülkelerin siber saldırı potansiyelleri, ulusal ve uluslararası hacker gruplarının tespiti ve takibi gibi konuların istihbarat kurumlarınca ele alınması gereklidir.

Bir savaş halinde askeri bilgi sistemlerini hedef alacak siber saldırıların silahlı kuvvetler birimlerince yapılması gereklidir. Siber saldırı kavramı normal askeri saldırı kavramından ayrı tutulmamalı, siber saldırının sadece düşman tarafından gerçekleştirilebilecek olası siber saldırılara karşı yapılabilecek bir eylem olarak düşünülmemesi, normal bir saldırıda da kullanılabilecek ana ya da tamamlayıcı bir unsur olarak ele alınması gerektiği değerlendirilmelidir.

Herhangi bir ülkenin kritik bilgi sistem altyapılarının hedef alınmasının, can ve mal kaybının hem askeri, hem sivil kesimi etkilemesi açısından uluslararası savaş hukukunun "ayrım" ve "orantılılık" ("distinction" ve "proportionality") ilkelerine aykırı olacağı değerlendirilmektedir.

1.4.3. Hukuki Düzenleme Önerisi

Bilişim teknolojilerinde yaşanan sürekli değişim, hayatın tüm alanlarını (sağlık, eğitim, çalışma, haberleşme, eğlence, ticaret, vs.) etkilemekte ve bunun sonucunda mevcut kurum ve kuralları da değişime zorlamaktadır. Bu değişim süreci içerisinde, geleneksel yönetim yapıları şekil değiştirmekte, mevcut hukuk kuralları da toplum dinamikleri arasındaki bu yeni etkileşime ayak uydurmaya zorlanmaktadır. Yeni ve temel değişiklikler içeren yasal düzenlemelerin yapılması, varolan yasal düzenlemelerin ise yeniden gözden geçirilmesi gerekmektedir. Bilişim toplumu olma yolunda muadillerine göre özellikle 2000'li yıllardan sonra etkili şekilde ilerleyen Türkiye'nin bilgi toplumu hedefine varmasını hızlandıracak temel hukuki düzenlemeleri hızla gerçekleştirmesi gerekmektedir.

Teknoloji, kültürü, ahlaki kabulleri ve sosyal yaşam pratiklerini etkileyen, zaman zaman dışlayan önemli bir olgudur. Teknoloji ile kültürün birbirinden kopmasının, kültürsüz kalan teknolojinin yarattığı kaosun insanlığın bugününü, yarınını etkiler, değiştirir ve tehdit eder olması hukuki düzenlemelerin teknolojik gelişmeleri de kapsar şekilde yapılmasını kaçınılmaz kılmaktadır. Bilgi güvenliği ve bilişim suçlarına dair düzenlemeler ulusal ve uluslararası hukuk bütünlüğü içerisinde yapılmalıdır.

Bugünkü adıyla, bilişim teknolojilerini takip açısından, Türkiye'de politika oluşturma çalışmaları 1960'lı yıllarda başlamış ve "Türk Bilim Politikası 1983-2003" ve "Türk Bilim ve Teknoloji Politikası 1993-2003" ile hız kazanmış, ancak bilim ve teknoloji alanında önerilen politikaların ilgili bütün kesimler (siyaset, kamu, özel sektör ve üniversiteler vs.) tarafından sahiplenilmemesi nedeniyle, bu politikaların hiçbiri tam olarak uygulamaya konulamamıştır.'[694] Bilişim teknolojilerindeki gelişmeler sanal dünya olarak isimlendirilmiş, fizik dünyanın bir parçası olarak kabul edilmemiştir. Fiziki işleyişe ikincil bir alternatif olarak; belli bilgilerin kuralsız, sınırsız, düzensiz erişim imkânı, gençlerin bir hevesi olarak görülmüş ve düzenleme ihtiyacı karşılanmamıştır. Ancak toplumdaki değişime sosyolojik olarak bakıldığında, bilişim dünyasının pek çok açıdan tali bir seçenek olmaktan çıkarak ekonomik, sosyal ve bireysel yaşamın gerçekleştiği bir ortama dönüştüğü görülmektedir. Bilişim dünyasının, mevcut hukuk düzeni ve kamu politikasıyla yönetilmesinde güçlükler ortaya çıkmış, yeni politik, hukuki ve sosyal yaklaşımların zorunluluğu kabul edilmiştir. Ulusal ve uluslar arası sahada bu ihtiyacı karşılamak üzere pek çok düzenleme yapılmaktadır. Ancak bilişim teknolojilerinde gelişme hızı kural koyuculardan çok daha süratlidir.

1991 yılında ülkemize giren internetin, etkilerinin araştırılmasının 2012 yılında yapılması, ülkemizdeki "farkındalığın" oluştuğunu göstermektedir. Birçok ülkede bu analizin yapılmamış olduğu gerçeği karşısında bu çalışma ayrı bir önem kazanmaktadır.

Yasal düzenleme eksikliklerinin giderilmesi, uluslararası toplumun bir ferdi olmanın gereği, yürütülmekte olan Avrupa Birliği üyelik sürecinin etkisi ve cezai, mali, hukuki ihtiyaçların birleşmesi ile de ötelenemez hal almaktadır. Bu anlamda temel bazı düzenlemelerin bütüncül yapılamaması eleştirilere konu olmaktadır. 2011 yılında İzmir'de düzenlenen Türkiye Bilişim Hukuku 2. Kurultay'ında bu talep "bilgi toplumuna geçiş sürecinde ülkemizin vizyonu; toplumsal ve bireysel yaşamın her alanında belirleyicilik işlevi üstlenen bilginin, fikri emeğin ve yaratıcılığın değerinin tanındığı, saygı gösterildiği ve korunduğu dinamik bir hukuki alt yapının, düşünce ve ifade özgürlüğü başta olmak üzere, hukuk devleti temel ilke ve kuralları çerçevesinde

[694] Berber, Keser Leyla, İst. Bilgi Ün. "Bilgi Ve İletişim Teknolojileri Hukuku" Karşılaşılan Sorunlar ve Çözüm Önerileri Sunumu, 24.05.2012

gerçekleştirilmesi" olarak belirlenmiştir.[695] Bilgi toplumu olma yolunun temel çizgilerini belirleyen bir mevzuatın oluşturulması sektörün bütün oyuncularının talebi olarak kayıtlara girmektedir. Bir bilişim sisteminde kayıtlı en basit bir verinin hukuki değeri konusundaki tartışmaları anlamsız bırakacak düzenlemenin olmayışı, devletin elektronik arşivini düzenlememiş olması gibi hususlar ortadaki sorunu çok net figüre etmektedir. Bilişim dünyasının gerek kamu ve gerekse özel yaşam alanındaki yaygın etkisi itibariyle hem özel hukuk hem de kamu hukukunun kapsadığı bütün alanlarda düzenleme yapılması gerekmektedir. Özetle yapılması gereken hukuki düzenleme temel ilkeleri anılan Kurultay'da aşağıdaki şekilde belirlenmiştir.

"1. Demokrasi, hukukun üstünlüğü ve insan haklarına saygı ilkelerinin temel öğesi ifade ve bilgi özgürlüğüdür. Bu temel hak ve özgürlük; her kişinin, sosyal, ekonomik, kültürel ve siyasal gelişimi için gerekli olduğu gibi sosyal ve kültürel grupların, ulusların ve uluslararası toplulukların da uyumlu bir biçimde gelişmesinin koşuludur. Sınırlar dikkate alınmaksızın ve kaynağı ne olursa olsun bilginin ve düşüncelerin ifade edilmesi, araştırılması, edinilmesi ve yayılmasında bilişim ve iletişim teknolojilerindeki gelişmeler bu hakkın her geçen gün daha çok güçlenmesine hizmet etmektedir. O halde devletlerin de, vatandaşlarının ifade ve bilgi özgürlüğüne yapılacak olan müdahalelere karşı güvence getirmek göreviyle yükümlü olduğu açıktır. Temel olan hak ve özgürlüklerin korunması ve geliştirilmesi asıl olup, hak ve özgürlük sınırlandırmaları istisna kabul edilmelidir. Bu bağlamda bilişim ve iletişim teknolojileri alanında yapılacak olan tüm hukuki düzenlemelerin en temel ilkesi; "başta ifade özgürlüğü olmak üzere kişisel tüm hak ve özgürlüklerin korunması, geliştirilmesi ile demokratik toplum düzeninde hukukun üstünlüğünü sağlayan, koruyan, geliştiren hukuk devleti temel ilkelerine saygılı bir çerçeve içinde kalmak"olmalıdır.

2. Bilişim ve iletişim teknolojilerinin, insanların, ulusların ve her ülkenin gelişimi için sunduğu benzersiz olanaklar, her geçen gün akıl almaz bir hızla artarak yayılmaktadır. Aslında bu gelişme bilişim ve iletişim teknolojilerinin, herhangi bir merkezi bulunmadığı halde, bilginin paylaşımına dayanan ve çok taraflı katılımcı

[695] http://www.ubhk.org.tr/anasayfa, 2011 yılında İzmir de düzenlenen Türkiye Bilişim Hukuku 2. Kurultayı Raporu

yapısından kaynaklanmaktadır. Bu nedenle, bu alanda yapılacak tüm hukuksal düzenlemeler, saydam ve paylaşımcı bir süreç içerisinde gerçekleştirilmelidir; bilişim ve iletişim teknolojisi ile doğrudan ve dolaylı olarak ilgili olan tüm taraflar bu sürece katılabilmelidir. Yani kullanıcılar başta olmak üzere, akademik kurumların, teknoloji geliştiricilerin, hizmet üreticilerinin, iş dünyasının, yargı mensuplarının ve sivil toplum kuruluşlarının etkin katılımı ve işbirliği sağlanmalı ve geliştirilmelidir. Aksi takdirde, kendine özgü kuralları olan bu alanda yapılması düşünülen ve gerekli olan hukuksal düzenlemeler 1. maddede yazılı olan amacı gerçekleştirmekten uzaklaşarak, yapıya uygun ve uygulanabilir olmaktan çıkacaktır.

3. Bilişim ve iletişim teknolojilerinin, yukarıda belirtilen kendine özgü yapısının bir başka boyutu da uluslarüstü doğasıdır. Bu nedenle, bilişim ve iletişim teknolojileriyle ilgili olarak yapılacak her türlü hukuksal düzenlemede, diğer ülkelerdeki uygulamalar ile Avrupa Birliği başta olmak üzere çeşitli uluslarüstü platformlarda geliştirilen uluslararası düzenlemeler ve sözleşmeler gözönünde bulundurulmalıdır.

4. Ülkenin yararı için büyük önem taşıyan bilgi toplumuna giden yolun tıkanmaması, ülke içinde dijital uçurumun derinleştirilmemesi gerekir. Yapılacak hukuki düzenlemelerle, bilgi toplumuna giden yolu geliştirici ve teşvik edici bir ortamın yaratılması için çaba gösterilmelidir. Asıl olan uluslararası sınırlara bakılmaksızın bilgiye ulaşılması, elde edilmesi, elde edilen veya oluşturulan bilginin başkalarına ulaştırılması sürecinde kamu makamlarının müdahale ve sınırlandırmalarının minimum düzeye indirilmesidir. Bilişim ve iletişim teknolojileri alanındaki hukuksal düzenlemeler, ülkeyi bilgi toplumuna taşıyacak seferberliğe katkıda bulunmalı ve insanların, ulusların gelişime açık bir hukuksal koruma sağlayan hukuk yoluyla temel hak ve özgürlüklerin korunduğu bir zemin yaratmalıdır. Bu çerçeveye, dijital bölünmenin önüne geçecek, teknolojiyi ülkenin her yerine yaymak için teknoloji erişimini kolaylaştıracak, ucuzlatacak ve herkes için ulaşılabilir kılacak teşvik kararları, özelleştirme mevzuatı, kamusal teknoloji erişimiyle ilgili düzenlemeler vb. dâhildir.

5. Bilişim ve iletişim teknolojileriyle ilgili her türlü hukuksal düzenlemenin genel yapısı itibariyle; yasaklayıcı, engelleyici, baskı kurucu ya da teknik açıdan uygulanamaz olmamasına büyük önem atfedilmelidir. Hukuksal düzenlemeler,

teknolojideki hızlı gelişime ayak uydurabilmek ve hem sosyal adaleti hem de teknik uygulanabilirliği sağlayabilmek için; esnek, teknolojik açıdan nötr, platform-bağımsız, jenerik-işlevsel ve mümkün olduğunca minimalist bir yapıya sahip olmalıdır. Böyle bir çerçeve hukuksal düzenlemenin teknolojik gelişmeye uyum göstermesinin teminatı olacaktır.

6. Ülkenin bilgi toplumuna dönüşmesi, bilişim ve iletişim teknolojilerinin etkin bir biçimde kullanımıyla kamu yönetiminde şeffaflığın ve katılımın sağlanması ve yargı sürecinin şeffaf ve adaletli bir biçimde işleyebilmesi için, temel insan hak ve özgürlüğü olarak kabul edilen"**Kamu Bilgilerine Erişim Özgürlüğü**", açık ve net bir şekilde anayasa ile teminat altına alınmalı ve ayrıca özel bir bilgi edinme hak ve özgürlüğü yasası çıkarılmalıdır.

7. Bilgiye erişimin, özellikle de internet erişimi hakkının evrensel haklardan olduğu, anayasayla teminat altına alınmalıdır.

8. Bilişim ve iletişim teknolojilerinin ülkede kalıcı bir gelişim ivmesi yakalayabilmesi ve teknoloji-bağımlılığının azaltılabilmesi için büyük önem taşıyan fikri mülkiyet haklarının korunmasına büyük özen gösterilmeli; ancak, bu konudaki düzenlemelerde, kamu yararı, hak sahipliği ve bireysel haklar arasındaki dengelere dikkat edilmelidir.

9. Bilişim ve iletişim teknolojileri alanında hukuksal düzenlemelere girişilirken, yukarıdaki ilkelerden hareketle ve bilgi toplumunun gelişimi için en uygun hukuksal zeminin kurulması gözetilerek; öncelikler tespit edilmeli; düzenlemeler arasında uyum gözetilmeli ve böylelikle olası uygulama sorunlarının önüne geçilmelidir.

10. Belli bir periyodik süreç öngörülerek, bilişim ve iletişim teknolojileri alanındaki gelişmelerin izlenmesi ve bilgi toplumu politikalarının hayata geçirilebilmesi için bu alanla ilgili hukuksal düzenlemelerin hem teknik hem de ilkesel olarak gözden geçirilmesi ve güncellenmesi gereklidir. Bu ihtiyaç için kurumsal bir mekanizma yapılandırılmalıdır. Bu mekanizma,"Bilişim Hukuku Şurası" olarak yansız ve bağımsız yapılanma biçiminde önerilebilir. Bu şura, Başbakanlık, Adalet Bakanlığı, diğer ilgili bakanlık ve kamu kurumları, Türkiye Barolar Birliği, Barolar, konuyla ilgili sivil toplum kuruluşları, özel sektör ve

akademik kurum temsilcilerinin geniş katılımıyla gerçekleştirilmeli ve belli aralıklarla toplanmalıdır. Bu konuda koordinasyon sürecinin, yine ilgili tarafların katılımı ve uzlaşmasıyla yapılandırılması, kurumsal mekanizmanın sağlıklı bir biçimde işlemesini garanti altına alacaktır.

11. Teknoloji ve hukuk koordinasyonunu sağlayabilmek için, yargı sürecinde yer alan tüm tarafların bilişim ve iletişim teknolojileri konusunda eğitimi ve bilinçlendirilmesi çok büyük önem taşımaktadır. Bu kapsamlı eğitim ve bilinçlendirme çalışmasında, konuyla ilgili akademik kurumlar, özel sektör ve sivil toplum kuruluşları destek ve işbirliği içinde olmalıdır. Bu eğitim iki farklı düzeyde gerçekleştirilmelidir:

a. Yargı sürecine katılacak yeni nesillerin eğitimi ve bilinçlendirilmesi için, eğitim kurumlarında gerekli müfredat değişiklikleri yapılmalı ve etkin bir biçimde uygulanmalıdır.

b. Hakim ve savcılardan kolluk kuvvetlerine kadar yargı sürecinin bütün aşamalarında yer alan tüm görevlilerin konuyla ilgili eğitimleri için özel programlar geliştirilmelidir. Bilişim alanında verilen yargı kararlarına konu taleplerin büyük kısmının kolluk birimlerinden iletildiği bilinmektedir. Bu konuda kolluktan gönderilen talebin bütün teknik ayrıntısının işlenerek gönderilmesi de büyük önem taşımaktadır.

Emniyet Genel Müdürlüğü'nün Bilişim Suçları Daire Başkanlığı kurması ve bu organizasyonu illerde de temsil ettirmesi önemli gelişme olarak görülmektedir. Yine Hâkimler ve Savcılar Yüksek Kurulu'nun basım merkezi olan yerlerde Cumhuriyet Başsavcılıkları altında Bilişim Suçları Bürolarının kurulmasını teşvik etmesi ve ilgili Başsavcılıkların Bilişim Savcıları olarak görevlendirmesinin sağlanması da önemli gelişmelerdir. Hâkim ve Cumhuriyet savcı adaylarının mesleğe kabul aşamasına kadar eğitimlerinden sorumlu Türkiye Adalet Akademisinin eğitim programına "Bilişim Suçlarını" alması önemlidir.

12. Bilişim ve iletişim teknolojilerinin yargı reformuna entegrasyonunun etkin bir biçimde sağlanarak, adalet sürecinin hızlandırılması, bir ulusal politika konusu haline getirilmelidir. "Benzer şekilde sağlık reformu, tapu ve kadastro reformu, ilköğretimden lisansüstü aşamayı da kapsayan veri ambarlarıyla eğitim

reformu vs. hedefine vardırılmalıdır. "UYAP Bilişim Sistemi" gibi bu konudaki mevcut çalışmalar teşvik edilmeli, duyurulmalı, etki ve kapsamı hızla genişletilmelidir.

13. Gerek ilgili yasal düzenlemelerin yapılması, gerekse ortaya çıkan sorunların çözümünde, bilişim ve iletişim teknolojilerinin yapısına ve hukuka uygun çözümler üretilmesi için çalışmak üzere barolarda bilişim hukuku komisyonları kurulmalı; hukuk fakültelerinde doğrudan bu alanla ilgili eğitim veren bölümler açılmalı; özerk bilişim ve iletişim hukuku enstitülerinin kurulması teşvik edilmelidir.

14. Bilişim ve iletişim teknolojileri alanında yaşanan sorunlara yönelik olarak, ihtiyaca cevap verecek yasal düzenlemeler yapılmalıdır. Yapılacak yasal düzenlemelerde tanımlar, yetkilendirilen birimler, bu birimlerin görev ve sorumluluk alanları açık ve net bir biçimde belirtilmelidir. Bilişim ve iletişim teknolojilerindeki suçların araştırılması, soruşturulması ve kovuşturma aşamasında gerçekleştirilecek olan usuli işlemler sırasında yetkililerce, gerekmediği halde özel hayatın gizliliğinin bozulmasına ve iletişim özgürlüğünün kısıtlanmasına yol açabilecek uygulamalar yapılması olasılığı göz önünde tutularak; suç soruşturma ve kovuşturma usullerinin neler olduğunun yasalarla detaylı bir şekilde belirlenmesi ve tüm usuli işlemlerin yargıç kararı ile yargı denetiminde bulunduğunun hukuki güvenceye bağlanması esas alınmalıdır.

15. Yargı sürecinin içinde çeşitli aşamalarda yer alan görevlilerin eğitilmesine ilişkin programlar uygulanmaya konulmalı, bilişim iletişim teknolojileri alanında delil tespiti, zararlı içeriğin tespiti gibi ihtisas gerektiren konularda özel prosedürler belirlenmeli ve uzmanlık isteyen konularda ihtisas mahkemelerinin tesisine zemin oluşturacak bir biçimde yapılanmanın sağlanmasına yönelik çalışmalar yürütülmelidir."

1.4.3.1. Ulusal Bilgi Güvenliği Alanında Düzenleme

Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak için bir mevzuat gerektiği açıktır. Devletin bilgi

güvenliği faaliyetlerinin geliştirilmesi, gerekli politikaların belirlenmesi, planların hazırlanması, metodolojilerin oluşturulması, özetle ulusal güvenlikle ilgili hassas bilgilerin uluslararası standartlarda korunmasını temin edecek Ulusal Bilgi Güvenliği Hakkında bir kanun çıkarılmalıdır.[696]

E-devlet alanında kurumların geldiği aşama önemsenerek elektronik yazışma, elektronik bilgi ve belge paylaşımını esas alan entegrasyon metodolojisi etkinleştirilmelidir.

Siber güvenlikle ilgili olarak her kurumda alınacak önlemleri belirlemek ve etkin olarak uygulamak için yeteri kadar siber güvenlik uzmanı istihdamı özellikle büyük ölçekli bilişim sistemi işleten kurumlarda teşvik edilmeldir.

1.4.3.2. Kişisel Verilerin Korunması Hakkında Düzenleme

Kişisel veri, bireylerin kimliklerini belirli hale getirmeye elverişli her türlü bilgi olarak tanımlanabilir. Bu bağlamda kimlik, iletişim ve sağlık bilgileri ile malî kayıtlar, özel hayat, dini inanç ve siyasi görüşe dair bilgiler kişisel veri olarak nitelendirilebilmektedir. Bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin akli, psikolojik, fiziki, kültürel, ekonomik, sosyal ve sair özelliklerine ilişkin verilerdir. Toplumda yasal dayanak olmaksızın kişisel verilerin işlenebilmesi ve etkin bir denetim mekanizmasının bulunmaması "fişleme" olarak adlandırılan olumsuz bir algının oluşmasına da sebebiyet vermiştir. Kişisel veriler düzenlemesine dair değerlendirmeler hep bu "fişleme" eksenine göre yapılmaktadır. İnsan haklarının korunması bilincinin gelişmesine paralel olarak, kişisel verilerin korunmasına dair farkındalık daha belirgin hale gelmektedir. Bu anlamda uluslararası kabule uygun "kişisel veri" kavramını örneklendirmek yararlı olacaktır.

AB Veri Koruma Direktifiyle uyumlu olan yukarıdaki tanım geniş anlamıyla;

- Cinsiyet, medeni hal, doğum yeri, diğer kişisel bilgiler ile ilgili bilgileri içeren uygulamaları (Nüfus sayımı),

[696] http://www.kgm.adalet.gov.tr/Tasariasamalari/Uzerindecals/uzrencal.html.

- Polis kayıtları gizli olsa bile polis tarafından parmak izi, fotoğraf ve diğer kişisel bilgilerin kaydedilmesini,

- Tıbbi verilerin toplanması ve tıbbi kayıtların tutulmasını,

- Vergi makamları tarafından kişisel harcamaların detaylarını (ve böylece özel hayatın detaylarını) açıklama zorunluluğu getirilmesini,

- Sağlık, sosyal hizmetler, vergi gibi idari ve sivil konuları ele alan bireysel kimlik belirleme sistemi gibi uygulamaları kişisel veri içeren uygulama olarak değerlendirmektedir.

Kişisel veriler, özel sektör ve kamu tarafından bilişim sistemlerine kaydedilmekte, bu sistemler üzerinden işlenmekte ve otomatik yollarla sıkça kullanılmaktadır. Bilgi çağı olarak nitelendirilen günümüzde kişisel verilerin kullanılmasının bireyler, mal ve hizmet sunanlar bakımından bazı kolaylıklar veya avantajlar sağlamasının yanında söz konusu bilgilerin istismar edilmesi riskini de barındırmaktadır. Bu verilerin yetkisiz kişiler tarafından elde edilmesi, işlenmesi, kullanılması ve ifşa edilmesi, uluslararası sözleşmeler ve 1982 Anayasa'sında koruma altına alınan temel hakların ihlali olarak karşımıza çıkmaktadır. Bu iki menfaat arasında makul bir dengenin oluşturulması gerekmektedir. En son yapılan değişiklikle bu yasal düzenlemelerin tamamının anayasal zemini oluşturulmuştur. 07/05/2010 tarih ve 5982 Sayılı Kanunun 2. maddesiyle 1982 Anayasası'nın 20. maddesine eklenen 3. fıkrayla "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." denilerek yasal düzenlemelerin çerçevesi gösterilmiştir.

Türkiye'de kişisel verilerin korunmasına ilişkin değişik kanunların içerisinde serpiştirilmiş çok çeşitli hükümler yer almakta ise de, konuyu bütüncül olarak düzenleyen bir kanun bulunmamaktadır. Buna ilaveten kişisel verilerin işlenmesi süreçlerini kontrol edecek ve denetleyecek bir kurum da bulunmamaktadır. Bunun bir sonucu olarak, halen kişisel verilerin hiçbir kurala ve denetime tabi olmaksızın,

yetkili-yetkisiz birçok kişi veya kurum tarafından kullanılması mümkün olmakta ve bu durum birey ve devlet arasında veya devletler arasında sorun yaşanmasını netice vermektedir. Kişisel verilerin korunmasına yönelik uluslararası belgeler göz önüne alındığında; bu konuya ilişkin hazırlanacak kanunda, kişisel verilerin işlenme şartlarının, bireylerin aydınlatılmasının, bu alanı denetleyecek ve düzenleyecek bağımsız bir veri koruma otoritesinin oluşturulmasının, veri güvenliğine ilişkin gerekli tedbirlerin alınmasının temel ilkeler olarak kabul edildiği görülmektedir. Ülkemizde kişisel verilerin korunmasını sağlayacak bir kanunun yürürlüğe girmesini gerektiren değişik sebepler bulunmaktadır. Bu bağlamda;

a. Kişisel verilerin korunması konusu 1980'lerden itibaren uluslararası belgelerde yer almaya başlamıştır. İlk olarak, ülkemizin de üyesi bulunduğu, İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından 23/09/1980 tarihinde "Kişisel Alanın ve Sınır Aşan Kişisel Bilgi Trafiğinin Korunmasına İlişkin Rehber İlkeler" kabul edilmiştir. Avrupa Konseyi tarafından, tüm üye ülkelerde kişisel verilerin aynı standartlarda korunması ve sınır ötesi veri akışının ilkelerinin belirlenmesi amacıyla hazırlanan, "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması'na ilişkin 108 sayılı Sözleşme, 28 Ocak 1981 tarihinde imzaya açılmış ve ülkemiz tarafından da imzalanmıştır. Ancak Sözleşmenin 4'üncü maddesi gereğince, iç hukukta kişisel verilerin korunmasına yönelik yasal düzenleme yapılmasının zorunlu olması ve ülkemizde buna yönelik bir yasal düzenleme bulunmaması nedeniyle, Sözleşme Türkiye Büyük Millet Meclisi tarafından henüz onaylanamamıştır.

b. Öte yandan 12 Eylül 2010 tarihinde yapılan halkoylaması sonucu kabul edilen 5982 sayılı Kanunla Anayasanın 20 nci maddesine yapılan ekleme ile kişisel verilerin korunması temel bir insan hakkı olarak koruma altına alınmış ve detayların kanunla düzenlenmesi öngörülmüştür.

c. 5237 sayılı Türk Ceza Kanunun 135 ve devamı maddelerinde, kişisel verilerin hukuka aykırı olarak elde edilmesi, kaydedilmesi veya ifşa edilmesi fiilleri suç olarak düzenlenmiş ve yaptırıma bağlanmıştır. Bununla birlikte, kişisel verilerin işlenmesine yönelik bir kanunun bulunmaması sebebiyle, bu fiillerin ne zaman hukuka aykırı, ne zaman hukuka uygun olduğunun belirlenmesinde tereddütlerin yaşandığı görülmektedir.

d. Avrupa Birliği tam üyelik sürecinde, müzakere fasıllarından dördü, doğrudan kişisel verilerle ilgilidir. Bu fasıllarla ilgili sürecin ilerleyebilmesi için ülkemizde kişisel verilerin korunmasına ilişkin temel bir kanunun yürürlüğe girmesi gerekmektedir. Avrupa Birliği'nin Türkiye ile ilgili olarak hazırladığı ilerleme raporlarında Türkiye'de veri koruma alanındaki yasal boşluğa işaret edilmektedir. Ülkemizde kişisel verilerin korunmasına ilişkin yasal bir düzenleme olmaması sebebiyle, polis birimleri arasında etkin bir işbirliğini hayata geçiren EUROPOL ile ülkemiz güvenlik birimleri arasında işbirliği anlaşması yapılamamakta ve elektronik bilgi değişimi gerçekleştirilememektedir. Ayrıca çalıntı oto, sahte pasaport, aranan şahıslar, istenmeyen yabancılar gibi konularda önemli bir veri bankasına sahip olan SCHENGEN Bilgi Sistemi ve SİRENE Ofisinin imkânlarından ülkemiz güvenlik birimleri yararlanamamaktadır. Çok sayıda Türk vatandaşının yaşadığı bazı ülkelerle (Fransa, Belçika) güvenlik ve yargı alanında işbirliği anlaşması yapılamamaktadır.

e. Avrupa Konseyi ayrıca, kişisel verilerin korunmasına yönelik, tıbbi veri bankaları, bilimsel araştırma ve istatistik, doğrudan pazarlama, sosyal güvenlik, sigorta, polis kayıtları, istihdam, elektronik ödeme, telekomünikasyon ve internet gibi çeşitli sektörlerde uygulanacak ilkeleri belirleyen tavsiye kararları da kabul etmiştir. Sağlık kuruluşlarında hastalara ilişkin çok sayıda özel nitelikli veri tutulması, bu verilerin tutulmasına ilişkin kanuni dayanağın olmayışı, bu verilerin güvenliğinin sağlanmasına yönelik yeterli önlemlerin alınamaması ve yetkisiz kişilerce bu nitelikteki bilgilerin ifşa edilmesi, Avrupa İnsan Hakları Mahkemesince özel hayatın gizliliğine müdahale olarak nitelendirilmekte ve ülkemiz aleyhine ihlal kararları verilebilmektedir.

f. Öte yandan, Avrupa Birliği, üye ülkelerin kişisel verilerin korunmasına ilişkin mevzuatları arasında uyum sağlamak üzere, 24.10.1995 tarihinde "Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Direktifi"ni (95/46/EC) yürürlüğe sokmuştur. Bu Direktifle, üye ülkelerde "kişisel verinin" üst düzeyde korunması ve kişisel verilerin Avrupa Birliği içerisinde özgür dolaşımını sağlayacak açık ve kalıcı bir düzenleme yapılması amaçlanmıştır.

g. Türkiye'de yaşayan yabancılar ile yurtdışında yaşayan Türk vatandaşları bakımından Dışişleri Bakanlığı askerlik, vatandaşlık, kimlik ve malvarlığı gibi konularda veri paylaşımında sorunlar yaşamaktadır.

h. Sınır aşan suçlarla ilgili değişik ülkelerin yargı mercilerinin ortak operasyonlar yapabilmesi amacıyla oluşturulan EUROJUST ile çok sayıda sınır aşan suçun işlendiği geçiş güzergâhında bulunan ülkemiz arasında bu suçlarla mücadeleye yönelik işbirliği yapılamamaktadır.

i. Kişisel verilerin korunması konusunda kanun hazırlanması, Ülkemizin Katılım Ortaklığı Belgesine cevap olarak hazırladığı 2003 Ulusal Programında taahhüt ettiği yükümlülüklerdendir.

j. Kişisel verilerin korunması konusu daha ziyade kamu sektörünü ilgilendiren bir sorun gibi algılanmakla birlikte, ekonomik alanla da yakından ilgilidir. Zira yabancı sermayenin ülkemizde yatırım yapması ve başka ülkelerdeki yatırımları ile ülkemizdeki yatırımlarını etkin bir şekilde yönetebilmesi için ihtiyaç duyduğu veri aktarımı, ülkemizde yasal düzenleme olmaması sebebiyle gerçekleştirilememekte ve bu durum yabancı sermayenin ülkemizde yatırım yapması bakımından caydırıcı bir etken olarak değerlendirilmektedir. Yine işadamlarımızın yabancı ülkelerdeki yatırımları ve ortaklıklarıyla ilgili ihtiyaç duydukları veri aktarımında sorunlar yaşanmaktadır.

Tüm bu açıklamalar ülkemizde kişisel verilerin korunmasına ilişkin kanunun bir an önce yürürlüğe girmesini gerekli kılmaktadır.

Kişisel Verilerin Korunması Hakkında AİHM Kararları (Özet)

Telefonların gizlice dinlenmesinin, hem özel hayat, hem haberleşmeye saygı gösterilmesi hakkının açık ihlali olduğunun belirtildiği, AİHM'deki Klass vs.(Almanya) ve Malone (Birleşik Krallık) kararlarında AİHM, kişinin konutunun kanuna aykırı olarak aranmasını, telefonlarının gizlice dinlenmesini özel hayata açık bir müdahale saymıştır.

Friedl (Avusturya) davasında AİHM, devlet ajanlarınca başvuranın evine girip evinde fotoğraf çekmek suretiyle özel hayatın "iç alanına" bir müdahale edilmediğine, fotoğrafların davacının kendi isteği ile katıldığı bir kamu olayına, kamuya açık bir alanda birden fazla kişinin yaptığı gösteriye ait olması, fotoğrafların daha sonra suçların soruşturulmasında, sadece gösterinin özelliğini ve gösteriye

katılanların davranışlarını kaydetmek amacıyla çekilmesi gerekçeleriyle özel hayata müdahale niteliğinde olmadığına karar vermiştir.

AİHM başka bir başvuruda geçmişteki ceza davaları hakkında tutulan kayıtların özel hayata müdahale olduğunu; ancak, bunun hafif olması ve suçun önlenmesi için modern bir demokratik toplum sisteminde "gerekli" olarak değerlendirilebileceği görüşünü belirtmiştir. Terörizm de kişisel verilerin kullanılmasını haklı kılan nedenlerden sayılmıştır. Mesela MC Veigh- O'neill ve Evans (Birleşik Krallık) davasında anti-terörizm kanunları kapsamında sorgulanıp, kişilerin üst aramasına tabi tutulması, parmak izlerinin alınıp fotoğraflarının çekilmesi ve bu kayıtların saklanması, bu "bilgiler istihbarat için gerekli olduğundan ve terörizmle savaşmak konusunda toplumsal ihtiyacın kişilerin özel hayatı ve aile hayatına saygı gösterilmesi hakkından daha üstün olduğu kabul edilerek," özel hayata müdahale niteliğinde görülmemiştir.

Hakkında veri toplanan bireyin hakkının korunması çerçevesinde; kişilerle ilgili bilgilerin elektronik ortamlarda işlenmesiyle ilgili esas ve usullerin düzenlenmesi, bu düzenlemelerin uluslararası veri değişimine elverişli olması, düzenlemelere uymayanlar hakkında ceza ve yaptırımların getirilmesi, ayrıca bunlar yapılırken AB direktiflerine uygunluk, kişilik haklarına mutlak riayet edilmesi ve yasal güvencelerin sağlanması zorunlu olmalıdır. AB'nin, aşağıda belirtilen dört temel esas üzerine kurulduğu değerlendirilmektedir. Bunlar;

- Malların (Maastricht Antlaşması md.9-30),
- Kişilerin (Maastricht Antlaşması md.42-48),
- Hizmetlerin (Maastricht Antlaşması md.59),
- Sermayenin (Maastricht Antlaşması md.73b), serbest dolaşımıdır.

AB yukarıda sayılı temel antlaşmalarda belirlenen temel değerler doğrultusunda üye ülkelerle birlikte, birliğe girmek isteyen ülkeleri de etkilemekte ve yönlendirmektedir. AB baştan beri birey söylemini kullanmış ya da bireyi ön planda tutmaya özen göstermiştir. AB antlaşmasının 6/1 maddesinde AB'nin deklare edilmiş hedefleri sıralanmıştır; bu hedefler özgürlük, demokrasi ve hukukun üstünlüğü

ilkelerini korumaktır. Yine aynı antlaşmanın 7 ve 8'inci maddelerinde ise, insan haklarının ve temel özgürlüklerin korunmasıyla birlikte, söz konusu bu ilkelerin ihlal edilmesi halinde tedbirler alınması öngörülmektedir.

1.4.3.2.1. AB Veri Koruma Direktifi

AB veri koruma direktifi'nin birinci maddesinde açık bir şekilde ifade edilen iki hedef vardır: Üye devletlerin, kişilerin temel hak ve özgürlüklerini ve özellikle kişisel verilerin işlenmesi ile ilgili olarak özel yaşamlarının gizliliğine saygı gösterilmesi haklarını koruyacakları, üye devletlerin, kendi aralarında yukarıdaki hedefte belirtilen nedenlere dayanarak kişisel verilerin dolaşımını yasaklayamayacakları ve engelleyemeyecekleri, hüküm altına alınmıştır. 34 maddeden teşekkül 95/46/EC sayılı "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması ve Verilerin Serbest Dolaşımı Direktifi'nde amacın, gerçek kişilerin haklarının korunması ve özellikle özel hayatın korunması gibi sebeplerle veri trafiğinin engellenmesinin önüne geçilmesi olduğu belirtilmiştir. "Veri Kalitesine İlişkin İlkeler" başlıklı 6'ncı maddesinde ise kişisel verilerin hukuka ve dürüstlük kuralına uygun şekilde işlenmesi için şu ilkeler öngörülmüştür:

1. Amaca Bağlılık,
2. Belirli Amaçların Varlığı Halinde Amaca Bağlılık Varsayımı,
3. Gereklilik İlkesi ve Depolama Yasağı,
4. Maddi Gerçeklik, Veri Güncelliği, Silinme ve Düzeltme,
5. Saklanma Süresi.
6. Direktife göre kişisel verilerin işlenmesi yasağına, ulusal düzenlemelerle getirilen istisnalar şunlardır:
    a. Devlet güvenliği ve ülke savunması,
    b. Kamu güvenliği,
    c. Hukuki düzenlemeye tabi mesleki kuralların ihlali ve suçların önlenmesi, soruşturulması ve kovuşturulması,

d. AB'nin üyesi devletin iktisadi çıkarlarının korunması,

e. Kamusal gücün kullanılmasını gerektirecek durumların varlığı,

f. İlgilinin ve üçüncü kişilerin hak ve özgürlüklerinin korunması,

g. Bilimsel araştırma ve istatistik.

Avrupa Konseyi'nin ana amacı, kişi özgürlüğü, siyasal özgürlük ve hukukun üstünlüğüne bağlı olarak bu amacı paylaşan üyeler arasında hukuki bütünleşmeyi temin etmektir. Konsey bu hedefe yönelik olarak birçok sözleşme ve tavsiye kararı kabul etmiştir. Bu sözleşmelerden en önemlisi 4 Kasım 1950 tarihinde Roma'da imzalanmış olan İnsan Hakları ve Ana Hürriyetleri Korumaya Dair Sözleşme, "Avrupa İnsan Hakları Sözleşmesi"'dir. Türkiye AİHS'yi 10 Mart 1954'te onaylayarak Türk hukuk düzeninde yürürlüğe koymuştur. AİHS'nin 8. maddesinde "özel hayatın ve aile hayatının korunması" başlığı altındaki hüküm:

"Herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir."

Devlet ajanları tarafından bir kişi hakkında, rızası dışı bilgi toplanması ve bu bilgilerin saklanıp kullanılması da "özel (bireysel) hayat"ın kapsamına girer. Cinsiyet, medeni hal, doğum yeri ve diğer kişisel bilgilerle ilgili zorunlu yanıtlanacak soruları içeren nüfus sayımları, polis tarafından parmak izi, fotoğraf ve diğer kişisel bilgilerin kaydedilmesi, tıbbi verilerin toplanması ve tıbbi kayıtların tutulması, vergi makamlarının kişisel harcamaların (dolayısıyla özel hayatın) detaylarını açıklama zorunluluğu getirmesi gibi hususlar " özel (bireysel) hayat"ın kapsamında sayılmıştır.

Sonuç olarak, kişisel verileri korumak, hukuk devletinin bir gereği olarak keyfiliği önlerken bilgi toplumu olma ve şeffaf bir toplum olma yolunu da açacaktır. Ancak bu yapılırken de kişisel verilerin korunması konusunda çok karmaşık bir mevzuat düzenlemesi yapılarak birçok faydalı iş yapılmasının önüne kişisel verilerin

korunması mevzuatı engel olarak çıkarılmamalıdır. Kaldı ki e-Devlet projelerinin sayısının artması da başlı başına kişisel verilerin korunması mevzuatının bir an önce yürürlüğe girmesini zorunlu kılmaktadır.