

# Bilgi Teknolojileri Güvenliđi: Ulusal Bilginin Korunmasına Pragmatik Bir Yaklaşım ve Türkiye Perspektifi

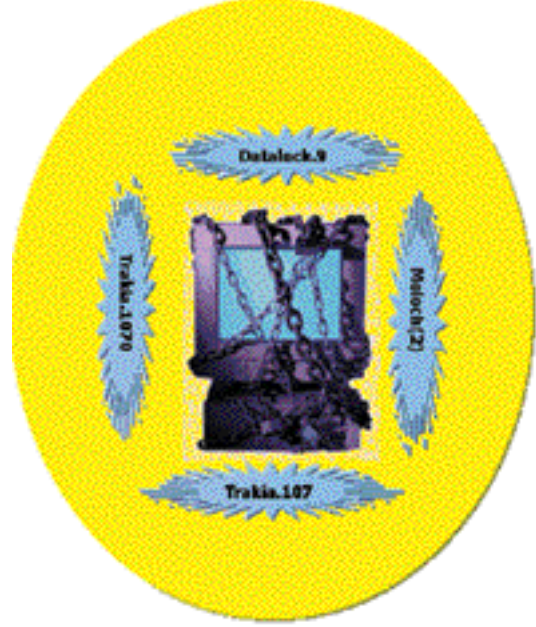
74

**Mustafa SAĞSAN\***

Bilgi çağında, İnternet ortamındaki bilgi kullanımının ve akışının artması, bilginin kontrol altına alınmasını da giderek zorlaştırmıştır. Bu bilgi akışını daha güvenli hâle getirebilmek amacıyla devletler, ulusal bilgi güvenliđi kavramı ile tanışmışlardır. Bu makale, bilgi teknolojileri güvenliđinin gerçekleşmesi için hedeflenen noktaların ne olduğunu açıklamaktadır. Ayrıca, bilgi teknolojilerinde kullanılan güvenlik protokolleri ile toplam sistem güvenliđi için yapılması gerekli kriptografi çalışmalarından bahsetmektedir. Türkiye'nin de ulusal bilgi güvenliđi açısından durumu kısaca analiz edilmeye çalışılmış ve önerilerde bulunulmuştur.

Today it is getting more and more difficult to control information on the internet due to the increasing flow. The states are slowly realizing the importance of "national information security". In this article, the author explains the cryptology studies that should be done in order to secure the system and the security protocols that are being used along with information technologies. Finally, Turkey's situation in connection with the National Information Security has been briefly analyzed and some suggestions are given regarding this topic.

**Stratejik Analiz**, Cilt 2, Sayı 22, Şubat 2002



## Giriş

Bruce Schneier'in de söylediđi gibi "Güvenlik bir ürün deđil, süreçtir" sözü, ulusal bilgi güvenliđinin ne derece önemli olduğunu açıkça ortaya koymaktadır. Ulusal bilgi güvenliđi denildiđi zaman, genellikle devletin ulusal çıkarları doğrultusunda güvenliđini tehdit edecek bilgilerin korunması anlaşılmaktadır. Fakat bunun yanında ulusal bilgi güvenliđi, bir ülkedeki her türlü bilginin (bilimsel, teknolojik, ekonomik, vs.) dış tehditlere karşı korunmasını da hedef almaktadır. Çünkü devletlere karşı gelebilecek tehditleri içeren bilgiler, devletin iç ve dış politikalarına bađlı olarak zamanla deđişebilmektedir. Özellikle, devletlerin özel sektör güvenliđinin gelişmesine karşı takındıđı tavır, bu tehditlerin belirlenmesinde önemli rol oynamaktadır. Bu nedenle, ulusal bilgi güvenliđinden bahsedilirken, sadece devletin ulusal çıkarları doğrultusunda oluşturulan bilgiler deđil; daha geniş manada özel sektörü de ilgilendiren bilgilerin korunması anlaşılmalıdır. Zaten devletler de, özel sektörü tehdit eden bilgilerin korunmasına yönelik çalışmalarda bulunmak zorundadırlar. Aksi takdirde, özel sektöre karşı gelebilecek iç ve dış tehditlerden devlet de etkilenecek zor durumda kalabilecektir.

\* ASAM, Dokümantasyon ve Enformasyon Merkezi,  
Bilgi Uzmanı.  
E-posta: msagsan@avsam.org

Ulusal bilginin güvenliği, bir zincirin halkalarını oluşturacak şekilde organize olmaktadır. Bu düzenleme ise, kişisel bilgisayarların kullanımını koruyacak bir güvenlik sisteminden başlayarak ağların ağı olarak bilinen internet ortamında kullanılan çok fonksiyonlu bilgi sistemlerinin korunmasına kadar geniş bir yelpazeye sahiptir.

Bu makalede özellikle anlatılmak istenen nokta, bilgi teknolojilerinde kullanılan güvenlik sistemlerinin neler olduğu ve nasıl çalıştığı ile bunların ulusal bilginin korunmasında ne gibi fayda sağladığını açıklamaktır. Bahsedilecek olan bu tür güvenlik sistemleri, ulusal bilginin gerek yurt gerekse uluslararası plâformlarda korunmasına doğrudan doğruya katkı sağlamaktadır. Bu tür güvenlik uygulamaları sayesinde, elektronik ortamda bulunan her türlü bilgi akışı, güvenli bir şekilde gerçekleşmektedir.

### Ulusal Bilgi Teknolojileri Güvenliği

İnternette çeşitli ortamlar sayesinde gerçekleşen bilgi akışının sınırlarının olmaması, bilginin gelecekteki güvenliğini ciddi boyutlarda tehlikeye sokmuştur. Bu sayede bilgi, izinsiz olarak kolayca elde edilebilmekte ve tehdit altında kalabilmektedir. Özellikle, OECD ve Avrupa Birliği belgelerinde bilgi güvenliği koşullarının yerine gelmesi, kişisel hak ve gizliliğin uluslararası alanda kabul görmesi ve bilginin dolaşımının açık ağlar üzerinden yapılması<sup>1</sup> gibi koşullar, bilginin güvenli bir ortamda hizmete sunulabileceğini açıkça ortaya koymaktadır. Bilgide yaşanan tüm bu gelişmeler, yeni bir çalışma ürününün gerekliliğini ortaya koymuş ve “bilgi güvenliği” terimi ortaya çıkmıştır. Bilgi güvenliği, kısaca bilginin ağ üzerinde güvenli iletiminin sağlanması<sup>2</sup> şeklinde değerlendirilebilir. Daha geniş bir ifade ile

“bilginin değişimine veya yetkisiz erişimine karşın bilginin korunmasını; sistemi kullanmak isteyen yetkisiz kullanıcılara karşı korunan bilginin depolandığı, işlendiği ve akışının sağlandığı sistemler”<sup>3</sup>

şeklinde ifade edilmektedir.

<sup>1</sup> “Açık Ağlarda Bilgi Güvenliği ve Dünya’daki Eğilimler”, <http://e-kimlik.bilen.metu.edu.tr/net/yayinlar/aabg.jsp>

<sup>2</sup> TÜBİTAK-ODTÜ-BİLTEN, *Türkiye İçin Elektronik Ticarete Geçiş Durum Değerlendirmesi ve Pilot Uygulama Projesi Raporu*, Ankara, Bilgi Teknolojileri Elektronik Araştırma Enstitüsü, 1999, s. 7.

<sup>3</sup> Don M. ve Sinn M. Darragh, “On the 6th Day: A Nonprofessional’s View of *Information System Security*, Cilt 10, (5), Kasım/Aralık 2001, s. 2.

## ►► İnternette çeşitli ortamlar sayesinde gerçekleşen bilgi akışının sınırlarının olmaması, bilginin gelecekteki güvenliğini ciddi boyutlarda tehlikeye sokmuştur. ◀◀

Ulusal bilgi sistemleri güvenliğine ulusal açıdan yaklaşılarak verilen tanım ise, “Ulusal Bilgi Güvenliği Teşkilâtı ve Görevleri Hakkında Kanun Tasarısı Taslağı”<sup>4</sup> isimli kaynakta şu şekildedir:

“Ulusal güvenliği ilgilendiren, yetkisiz ellere geçtiği takdirde devletin güvenliğini tehlikeye sokabilecek veya devlet aleyhine kullanılabilecek her türlü bilgiyi; üretim, kullanım, işleme, saklanma, nakledilme ve imha sırasında yetkisiz kişilerin erişimine ve olası her türlü fiziksel ve elektronik müdahaleye karşı korumaya; bilgiye erişim ve kullanıma ait usulleri açık şekilde belirlemeye ve bilgiyi gerektiğinde hazır bulundurmaya yönelik tedbirler”.

### Bilgi Güvenliği ile Hedeflenen Nokta

Bilgi güvenliği ile ilgili hedeflenen nokta, bilgi sistemleri güvenliğine karşı gelebilecek tehditlerin neler olduğu sıralanmakla açıklanabilir. Bunlar genel anlamda, *kurumlara ve bireylere ilişkin yapılan casusluk faaliyetlerinden tutun da, bilgisayar korsanlarının saldırıları, virüslerin yayılması, kaynakların kötüye kullanımı, yetkisiz erişim, belirli bir amaçla yönelik olarak gönderilen sahipsiz elektronik postalar (spam mail), IP spoofing, güvensiz yazılımlar ve test edilmemiş yedeklere kadar*<sup>5</sup> geniş bir yaygınlık alanına sahiptir. Herhangi bir tüzel kişi veya kuruluşa karşı gerçekleştirilebilecek ihtimali yüksek olan bu saldırıları, saldırıya uğrayan tarafın yönetebileceği tehditler şeklinde de nitelendirebiliriz. Bilgi güvenliğinin hedefi, gerek kurum/kişinin elinde olan veya gerekse olmayan bu tür saldırılara karşı tedbirler almak ve güvenlik sistemleri geliştirmektir. Bu tehditler belirlenirken kurum içerisinde dikkat edilecek noktalar, Uğur Gökhan Can, “Güvenliğe Giriş” adlı sunumunun 10. slaytında şu şekilde dile getirilmiştir:

<sup>4</sup> Ulusal Bilgi Güvenliği Teşkilâtı ve Görevleri Hakkında Kanun Tasarısı Taslağı, [http://www.webbuilder.gen.tr/net\\_hukuk/u\\_bil\\_guv/ulusal\\_bilgi\\_guvenligi\\_teskilati01.html](http://www.webbuilder.gen.tr/net_hukuk/u_bil_guv/ulusal_bilgi_guvenligi_teskilati01.html)

<sup>5</sup> Uğur Gökhan Can, “Güvenliğe Giriş”, TEPUM Danışmanlık, Slayt No:7, <http://www.tepum.com.tr/guvenlik.pdf>

- @ alıřanlar,
- @ Eski alıřanlar,
- @ Canı sıkılan alıřanlar,
- @ Rakipler,
- @ Profesyonel bilgi hırsızları,
- @ Müşteriler,
- @ Profesyonel saldırganlar,
- @ Güvensiz yazılımlar,
- @ Eğitimsiz kullanıcılara
- @ Eğitimsiz veya eksik eğitimli sistem yöneticileri,
- @ İnternet ve extranet bağlantılarının fiziksel güvenliđi.

Bütün bunlara ek olarak, kurumsal açıdan herhangi bir tehdit unsuru yaratmayacak kullanıcıların da dikkate alınması gerekmektedir. Bu açıdan bakıldığında, teknolojiye dayalı kurumlarda, kurum içi bilgi akış hiyerarşisi güvenlik protokolleri de dikkate alınarak belirlenmeli, test edilmeli ve sistem tarafından denetlenmelidir.

#### **Bilgi Teknolojileri Güvenliđi: Kavramlar, Tanımlar, Uygulamalar ve Öneriler**

76

Bu kısımda amacımız, herhangi bir ortamda bulunan (internet, ağ, bilgisayar) bilgi sistemlerinin nasıl korunması gerektiđine yönelik olarak oluşturulan güvenlik sistemlerinin hangi kavramlar çerçevesinde ele alınıp değerlendirildiđini ve bu kavramların neyi ifade ettiđini anlatmaktır. Ayrıca, bilgi sistemleri güvenliđi ile ilgili dünyada hangi tür uygulamaların var olduđunu göstermek ve bunların daha iyi yapılandırılmasına yönelik nelerin yapılabileceđini açıklamaktır.

Ulusal bilgi teknolojilerinin güvenliđinde genellikle yedi adet sistemden söz edilmektedir.<sup>6</sup> “Toplam Güvenlik” kavramı içerisinde değerlendirilen bu başlıklar, İşletim Sistemi Güvenliđi, Web Sunucu Güvenliđi, Ağ Güvenliđi, Güvenlik Duvarları, Virüse Karşı Koruyucu Araçlar, Güvenlik Politikası ve Sistem Güvenliđi şeklinde sıralanabilir. Tüm bunlara ek olarak, teknoloji güvenliđinin başlatılması için gereken nokta olan bilgisayar güvenliđini de ilk sırada söylemek gerekmektedir.

**Bilgisayar Güvenliđi** : Aslında en genel anlamda konuya yaklaşmak gerekirse, “*güvenli bilgisayar internete bađlı olmayan bilgisayardır*” yargısını söylemek gerekir. Fakat bu söz, hızla gelişen bilgi

ve iletişim teknolojileri sayesinde geçerliliđini yitirmiş durumdadır. İyi bir bilgisayar güvenliđi, iyi alıřan bir işletim sistemi sayesinde sağlanabilir. Bu nedenle, bilgisayarın işlevini yerine getiren unsurların güvenliđinin sağlanması gereklidir ki, bunlar da genel olarak işletim sistemi ve yazılım programlarının dış tehditlere karşı korunması ile gerçekleştirilebilir. Bilgisayara iyi bir güvenlik duvarı (**firewall**) yazılımının entegre edilmesi ve etkili bir anti-virüs programının yüklenmesiyle bu tehditlerin azaltılacağını söylemek mümkündür.

**İşletim Sistemi Güvenliđi:** İşletim sistemleri genel olarak çok esnek ve karmaşık bir yapıya sahip olduklarından güvenlikle ilgili yapılandırılmaları konusunda çok dikkatli olmak gerekir. İşletim sistemlerinin güvenliđinin sağlanmasına yönelik olarak yapılan güvenlik duvarı koyma alıřmaları yetersiz kalmaktadır. Bu nedenle, bu sistemlerde güvenlik duvarının yanında, güvenlik tarayıcıları da kullanılmalıdır.<sup>7</sup> Bu tarayıcılar, Windows 2000 Server, Windows NT, Windows XP, OS/2, Unix ve Linux gibi işletim sistemlerinin zayıf noktalarını tarayarak bulur ve bu konuda alınması gereken tedbirleri önerir. Daha ayrıntılı şöyle ifade edilebilir:

“Tarayıcı, bir sistemdeki (uzak ya da yerel bir sistem olabilir) zayıflıkları otomatik olarak tarayarak bulan programdır. Tarayıcılar yerel sistemde ya da ağda alışabildiđi gibi, internet üzerinde de alışabilir. Yani siz İnternet’e bađlı herhangi bir sunucuyu uygun bir tarayıcıyla uzaktan tarayabilir ve sistemdeki zayıflıkları öğrenebilirsiniz. Ağlardaki ve sistemlerdeki zayıflıkları ortaya ıkardığı için tarayıcılar İnternet güvenliđinde çok önemlidirler. Daha önce de belirtildiđi gibi, tarayıcılar yeraltı dünyası için önemli olduđu kadar bu kişilere karşı sistemini korumak isteyen sistem yöneticileri için de çok önemlidir. (çođu zaman göz ardı edildiđi hatta çođu kişinin böyle bir şeyin varlıđından haberi bile olmamasına rağmen). Sistem yöneticileri tarayıcıları kullanarak kendi ağlarının güvenliđini artırabilirler.”<sup>8</sup>

**Web Sunucu Güvenliđi:** Web sayfasının güvenliđi, web tabanlı bilginin güvenliđi ile aynı anlamı taşımaktadır. Bu kısım, hipermetin işaretleme bağlantıları yapılmış belgelerin bulunduđu sayfalar olarak adlandırılan “*web sayfası*” ve hazırlanan HTML dokümanları ve ilgili sayfaları okuyarak sunuma hazırlayan http sunucusu yazılımı olan “web

<sup>6</sup> “Elektronik Ticaret”, <http://www.adambilgisayar.com.tr>

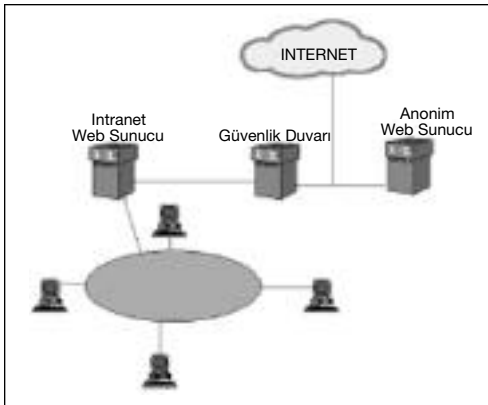
<sup>7</sup> <http://www.adambilgisayar.com.tr/guvenlik.html>

<sup>8</sup> <http://astavilla.kolayweb.com/tarayicinedir.htm>

sunucu” sunun güvenliği ile ilgilidir.<sup>9</sup> Web tabanlı bilgilerin iki önemli özelliği bulunmaktadır ki bunları Michael Otey, “*tazelik*” ve “*dünya çapında erişilebilirlik*” olarak tanımlamaktadır.<sup>10</sup> Güvenlik ile ilgili bilgiler, web sayfalarının artmasıyla birlikte daha fazla bilinir hâle gelmiştir. Buna karşın, web sayfalarının sayı ve çeşitlerinin artması da bunların ciddi anlamda korunması zorunluluğunu getirmiştir. Web sayfalarının güvenliği için, öncelikle web sunucusuna güvenlik duvarı (*firewall*) konulmalıdır. Alınacak tedbirler, site isimlerinin ve şifrelerin konulmasından sitede yer alan kelimelerin olmadığı şifrelerin kullanılmasına kadar geniş bir dizgeye sahiptir. Herhangi bir işletmeye web sunucusu kurulurken bunun birçok yönteminin olduğu ve bu yöntemlere uygun olarak geliştirilen güvenlik teknolojilerinin bulunduğu unutulmamalıdır. Örneğin, Şekil-1’de de görüldüğü üzere, iki ayrı web sunuculu uygulanan kurumlarda, doğal olarak güvenlik duvarının korunması dışında kalan web sunucusu saldırılara açıktır ve çevrimiçi siparişlere uygun değildir. Eğer intranete girilmesine izin verilecekse (Şekil-2), kısıtlı ulaşımlı intranet sunucu kullanılmalı ve bunun her iki tarafı güvenlik duvarları ile korunmalıdır.<sup>11</sup>

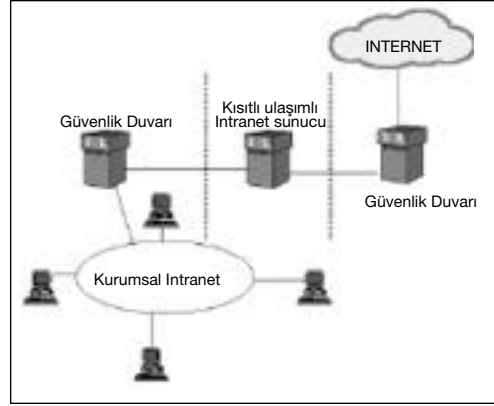
**Ağ (Network) Güvenliği:** Ağ, kısaca bir grup bilgisayarın ve ilgili birimlerinin iletişim araçları ile birbirlerine bağlanması ve en basit şekli ile kablolar, telefon ve diğer iletim bağlantı birimleri ile ka-

**Şekil-1. İki Ayrı Web Sunuculu Uygulama**



**Kaynak:** <http://www.adambilgisayar.com.tr/guvenlik.html>

**Şekil-2. İnternet Ulaşımına İzin Verilmesi Durumundaki Ağ Yapısı Önerisi**



**Kaynak:** <http://www.adambilgisayar.com.tr/guvenlik.html>

lı bir ortamın oluşturulması anlamına gelmektedir.<sup>12</sup> Güvenli bir bilgisayar ağı, öncelikle çok iyi tasarlanmış bir sistemin hayata geçirilmesi ile gerçekleşmektedir. Bu nedenle, ağ güvenliği için üç tür analiz yapılması zorunludur.<sup>13</sup> Bunların ilki, ağ için güvenlik risk analizinin yapılmasıdır. Risk analizinin amacı, güvenlik açısından tehdit oluşturan en zayıf halkayı belirlemektir. İkinci aşama olan güvenlik politikasının oluşturulması ise, bilgi teknolojilerindeki genel güvenlik politikalarının kendisini içermektedir ki bundan da makalenin “Bilgi Teknolojileri Güvenliği” kısmının son bölümünde bahsedilecektir. Son aşama ise, ağ güvenliği ile ilgili güvenlik çözümlerini içermektedir. Örneğin İnternet protokolü ve *Domain Name System*’ler için nasıl bir güvenlik oluşturulması hususuna bu aşamada karar verilir.

**Güvenlik Duvarları (Firewall):** İnternet üzerinde yüzde yüz güvenliğin olmaması, bilgi teknolojileri güvenliği konusundaki çalışmaların bireysel olarak sayıca artmasına neden olmuştur. Bu kişisel çalışmalar, genellikle tedbir amaçlı internetten indirilen ve “*güvenlik duvarı*” olarak Türkçe’ye çevrilen Firewall yazılımlarıdır. Koruma programlarına verilen genel bir ad olarak da nitelendirebileceğimiz güvenlik duvarları,<sup>14</sup> verilen direktifler doğrultusunda kişileri uyarmakta ve internet bağlantıları ile port’ların güvenliğini kontrol altında tutmaktadır. *PC Magazine Türkiye* dergisinin Ağus-

<sup>9</sup> Naci Altan, “Web sunucu”, *Bilgisayar Terimleri Ansiklopedik Sözlüğü*, İstanbul, Sistem Yayıncılık, 2000, s.s. 574-575.

<sup>10</sup> Michael Otey, “Web’deki Güvenlik Kaynakları”, *Windows2000 Magazine Türkiye*, Kasım 2001, s. 89.

<sup>11</sup> <http://www.adambilgisayar.com.tr>

<sup>12</sup> Naci Altan, “Network”, s. 363.

<sup>13</sup> Uğru G. Can, “Bilgisayar Kullanımında Toplam Güvenlik”, *Elektronik İş ve Ticaret Dergisi*, Kasım, 2000, s. 26.

<sup>14</sup> Kerem Köseoğlu, “Test: Kişisel Firewall Yazılımları”, *PC Magazine Türkiye*, Sayı:81, Ağustos 2000, s. 166.

tos 2000 yılında yaptığı bir test çalışmasına göre en iyi güvenlik duvarının *Norton Internet Security* (NIS) olduğu görülmüştür. Kurum ve kişilerin bütçelerine göre internetten rahatlıkla indirilebilen bu yazılım programları sayesinde internette rahatça sörf yapılabilmektedir.

**Virüse Karşı Koruyucu Araçlar:** Virüs, kısaca bilgisayarımıza değişik şekillerde zarar verebilen ve genelde kötü niyetli kişiler tarafından yazılan bilgisayar programlarıdır. Virüsler genel olarak üç gruba ayrılmaktadır: Bilgisayarın sistem alanlarına bulaşanlar, dosyalara yayılanlar ve makro virüsler.<sup>15</sup> Bu virüslerin sistemi etkisiz kılabilmesi yayılmasına ve virüsün cinsine bağlıdır. Aslında virüsler tek başlarına etkinlik göstermezler. Genel olarak istem dışı bir sisteme eklenerek aktif hâle geldiklerinden, bulaştığı program dosyalarının çalıştırılmasını beklemektedirler. Kodlardan oluşan bu programlar sayesinde, virüsler yayılma alanı bulmaktadır. Virüslerin yayılması dosya ile gönderilmelerinden dolayı şu şekilde olmaktadır:

Açılan dosya otomatik olarak ilintili diğer son kullanıcılara da iletilmekte ve virüsün yayılma hızı ve etkinlik kapasitesi artmaktadır. Ayrıca, elektronik posta, gruplar arası tartışma listeleri ve internet gibi teknolojik iletişim ve bilgi kanalları ile de virüs rahatlıkla genişleme alanı bulmaktadır. Özellikle bu tür araçlardan yapılan veri transferleri ile bulaşan virüslerin neden oldukları zararlar aşağıdaki şekilde açıkça görülmektedir.

78

**Şekil-3. Virüsleri Yol Açtığı Zararlar**



**Kaynak:** National Computer Security Association

Bu nedenlerden dolayı virüslerden korunmak için anti-virüs programları oluşturulmuştur. Anti-virüs programları, özellikle geniş ağlarda kolayca kurulabilen ve yeni virüslere karşı sık sık güncellenen yazılımlar olma özelliklerini taşımaktadır.<sup>16</sup> Bilinen en iyi anti-virüs programları içerisinde Norton Anti-Virüs, McAfee Scan Associates, IBM Anti-Virüs, F-Prot (F-Secure) ve Thunderbyte Antivirüs vardır.

**Güvenlik Politikası:** Üretime dayalı kurumlarda güvenlik birimlerinin oluşturulması kaçınılmazdır. Bu nedenle, bu tür yerlerde uygulanacak güvenlik politikaları öncelikle iş akış şemasını ve işin yapılış tarzını kolaylaştırıcı yönde olması gerekmektedir. Bu tarz, işin uygulanabilirliğini ve kullanılabilirliğini denetleyecek şekilde organize edilmelidir. Bu şekilde oluşturulması hedeflenen güvenlik politikaları, ayrıca bir yönetim gerektirmeyerek kendi kendine işler ve kendisini yönetir bir tarz ile yapılandırılmalıdır. Güvenlik politikası oluşturulurken, gözden kaçmaması gereken bir diğer önemli nokta da kurumun kültürüne uygun bir şekilde tasarlanmasıdır. Aksi takdirde, kurumun bilgi altyapısı güvenliği ile faaliyetleri arasındaki oluşturulması gereken hassas dengede aksaklıklar meydana gelecektir.

**Sistem Güvenliği:** Yukarıda açıklanan altı maddenin analiz edilerek kontrol edilmesinden oluşmaktadır. Sistemler arası entegrasyonun güvenliğinin sağlanması ve kurulan bilgi sistemi ile ilgili toplam ne kadar güvenliğe sahip olduğumuzun değerlendirilmesi çalışmalarını içermektedir.

## Toplam Sistem Güvenliği İçin Kriptografi ve Kriptolamada Güvenlik Protokolleri

### 1-Kriptografi ve Kriptolama

Toplam Sistemin Güvenliği'nin (TSG),<sup>17</sup> ağ güvenliği yöntemleri ve kriptografi ile sağlandığı, yukarıdaki bölümlerde izah edilmiştir. Şimdi de kısaca, güvenli veri iletimi ve saklanması amacıyla şifreleme ve şifre çözme yöntemleri<sup>18</sup> hususunda sistem geliştiren "*Kriptografi*" biliminden bahsedilecektir. Kriptolama, bazı kaynaklarda "şifreleme" ve "şifre çözme" terimlerinden farklı olarak gösterilse de, genel manada işlevsel yaptırımlarının aynı olması itibarıyla eşanlamlıdır. "Kriptolamada

<sup>16</sup> <http://www.tepum.com.tr/virus.htm>

<sup>17</sup> Toplam Sistem Güvenliği, kişisel, kurumsal, bilgi ve sistem güvenliğinden oluşmaktadır.

<sup>18</sup> TÜBİTAK-ODTÜ-BILTEN, s.7

<sup>15</sup> Aslan İnan, *İnternet El Kitabı*, İstanbul, Sistem Yayıncılık, 2001, s.412.

amaç, elektronik bir haberleşmenin, sadece gönderen ile alıcının tekrar okuyabileceği biçimde oluşturulmasıdır.” Genel olarak 3 grupta toplanmaktadır.<sup>19</sup>

- 1- *Gizli (Simetrik) Anahtar Kriptolaması,*
- 2- *Genel (Asimetrik) Anahtar Kriptolaması,*
- 3- *Gizli ve Genel (Simetrik ve Asimetrik) Anahtar Kriptolaması,*

Kriptografi literatürü oldukça geniş ve kapsamlı teknikleri içerdiğinden ve makalemizin amacı ve konusuyla doğrudan doğruya ilişkili olmadığından konuyla ilgili detaylara değinilmeyecektir. Fakat, kriptografi bilimi çerçevesinde Avrupa Birliği ülkelerinin de önemle üzerinde durduğu **“Sayısal İmza”** kavramından söz edilecektir. Sayısal imza, “elektronik ortamda iletilen verilerin bütünlüğünün bozulmadığını kontrol etmek ve imzayı atanın kimliğini doğrulanmak”<sup>20</sup> için kullanılır. Özellikle kamu kurumlarının resmî haberleşmelerinde, açık ağlar üzerindeki sözleşmelerin yapılmasında ve kimlik veya yetki tanımlamalarında kullanılmaktadır. Sayısal imzanın yasal durumu ülkeler arasında farklılık göstermekle beraber, sayısal imza içeren herhangi bir sözleşmenin yasal dayanağının olup olmadığı ülkelerin kanunlarında mutlaka belirtilmelidir.

Her ne kadar sayısal imzanın geçerli olduğu durumların kabulü az olsa da; şifreleme yöntemleri sayesinde güvenli iletişim gerçekleşmekte ve yaygın kullanım alanı bulmaktadır. Kriptolamanın ne denli önemli olduğunu ve bu şifreleri çözmenin ne kadar zamanda yapılabildiğini gösterir tablo aşağıda incelemeye sunulmuştur.

**Tablo-1. Bir Şifrenin Denenerek Bulunmasının Hesap Cetveli**

Anahtar Uzunluğu	Sayı Değeri	10 <sup>6</sup> şifre/s	10 <sup>9</sup> şifre/s	10 <sup>12</sup> şifre/s
32 bit	~4x10 <sup>9</sup>	36 dak	2.16 s	2.16 ms
40 bit	~10 <sup>12</sup>	6 gün	9 dak	1 s
56 bit	~7.2x10 <sup>16</sup>	1142 yıl	1 yıl 2 ay	10 saat
64 bit	1.8x10 <sup>19</sup>	292.000 yıl	292 yıl	3.5 ay
128 bit	1.7x10 <sup>38</sup>	5.4x10 <sup>24</sup> yıl	5.4x10 <sup>21</sup> yıl	5.4x10 <sup>18</sup> yıl

**Kaynak:** [http://inet-tr.org.tr/inetconf5/seminer/Aydogan\\_Karabulut/sld011.htm](http://inet-tr.org.tr/inetconf5/seminer/Aydogan_Karabulut/sld011.htm)

## 2-Güvenlik Protokolleri

İnternet üzerinde dolaşan birtakım bilgi paketleri, güvenlik protokolleri yardımları ile şifrelenerek gönderilmektedir. Bu bilgi paketleri, önce kriptoloji biliminin içerdiği şifreleme teknikleri ile şifrelendikten sonra aşağıda açıklayacağımız protokollerden geçmektedir.

**2a) SSL: Güvenli Bağlantı Katmanı:** (Secure Sockets Layer): Web uygulamalarında bilginin doğru kişiye güvenli olarak aktarılması için kullanılan standart bir ağ yazılımıdır. “SSL İnternet üzerinde SSL becerili sunucular ve tarayıcılar biçiminde yaygın olarak kullanılmaktadır. TCP/IP ağ yazılımı ile işbirliği yapan SSL ağ yazılımı veri şifreleme, sunucu ve tarayıcı doğrulama ve ileti bütünlüğü güvenlik tekniklerinin tamamını sağlamaktadır.”<sup>21</sup> SSL, bilginin doğru bilgisayardan geldiği ve doğru bilgisayara gittiğini teyit eder. Özellikle ticari amaçlı kullanılan ve kredi kartı kullanımının zorunlu olduğu web sayfalarında bağlantısının güvenilirliğinden emin olmak zorundayız. Bu bağlamda SSL içerisinde bulunduğumuz web sayfasının güvenli iletişim pozisyonunda olup olmadığını bilmiyoruz. SSL'nin gerçekleşmesi için,

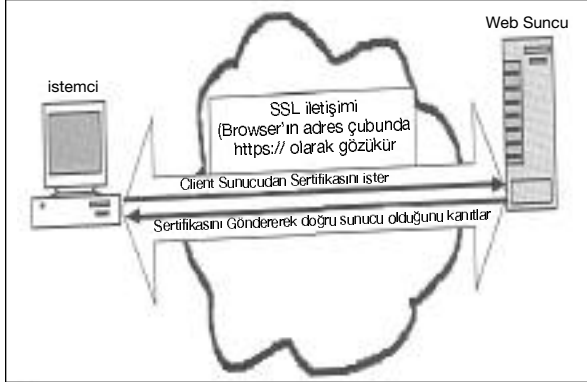
“istemci bir bilgisayar SSL'yi destekleyen bir sunucuya bağlandığı anda doğrulama işlemleri başlamaktadır. İstemci, kendi açık anahtarını sunucuya gönderir. Sunucu ise, bu anahtarı kullanarak şifrelediği bir mesajı istemciye geri gönderir. Daha sonra istemci sadece kendinde olan kapalı (private) anahtarı kullanarak gelen şifreli mesajı çözer ve sunucuya geri gönderir. Mesajı alan sunucu bunu kendisinin yolladığı orijinal mesajla karşılaştırır ve iki mesaj aynı ise doğrulama işlemi başarıyla tamamlanmış olur. Dolayısıyla, sunucu, istemciye o an gerçekleşen web oturumunda kullanılacak tüm önemli anahtarları göndererek güvenli iletişimi başlatmış olur.”<sup>22</sup>

<sup>19</sup> Hazırlayan Zeynep Ersoy, *E-Ticaret ve Noktaları*, Ankara, İGE-ME, 1999, s.36.

<sup>20</sup> <http://e-kimlik.bilen.metu.edu.tr/net/yayinlar/aabg.jsp>

<sup>21</sup> Sacit Ertaş, “Elektronik Ticaret: Tanımı, Gelişimi, Avantajları, Güvenliği”, Veysel Bozkurt (Der.), *Ekonomik, Toplumsal, Teknik ve Yasal Yönleriyle Elektronik Ticaret*, İstanbul, Alfa, 2000, s.s. 1-18.

<sup>22</sup> Adem Özbay, Devrim Jan, *İnternet Teknolojileri*, İstanbul, Pusula Yayıncılık, Eylül 2001, s. 245.

**Şekil-4. SSL İletişim Protokolü** 23

**Kaynak:** Zafer Demirkol, İnternet Teknolojileri

**2b) SET: Güvenli Elektronik İşlemler** (Secure Electronic Transaction): Kredi Kartı işlemlerini internet üzerinden işlemek üzere, Microsoft, Netscape, MasterCard ve Visa tarafından ortak geliştirilmiş bir güvenlik protokolüdür. SET, genel anahtar kriptolamasını kullanır ve dijital sertifikalar ile çalışır. Özellikle online hesap kontrolü ve aktarımı işlemlerinde güvenliği sağlar. Kredi kartı ile satış yapan bir site, müşterinin aldığı ürünlerin detayını bilirken, müşterinin hesabına ilişkin hiçbir bilgiye ulaşamaz. Sadece müşterinin kredi kartından gerekli miktarın kesildiği onayını alır. Öte yandan, kredi kartı ödeme onayını veren ve hesabı düzenleyen banka da, müşterinin alışveriş detayı hakkında hiçbir bilgiye sahip olmamaktadır.<sup>24</sup> SET protokolünü uygulayan firmalar, ödeme bilgisinin gizliliği, gönderilen bütün bilgilerin doğruluğu, kredi kart sahibinin yasal kullanıcı olup olmadığı ve yazılım ve ağ sağlayıcıları arasındaki işlemlerin sağlanması gibi avantajlara sahip olmaktadır.<sup>25</sup> SET, genellikle internette bilgi gönderilirken, güvenli bilgi göndermek için kullanılan VISA ve Mastercard'ın yanı sıra IBM, GlobeSet, HP gibi teknoloji liderlerinin olduğu bir teknoloji grubu tarafından geliştirilmiştir. Bu bağlamda sistem geliştirilirken bazı hedeflere ulaşılacak istenmiştir. Bu hedefleri şu şekilde sıralamak mümkündür:<sup>26</sup>

- @ Kredi Kartı bilgilerinin sadece bankalar tarafından görülebilmesi,

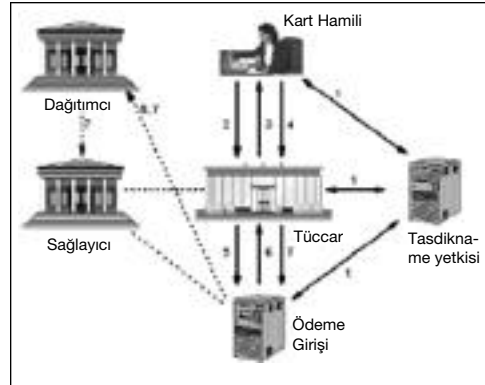
<sup>23</sup> Zafer Demirkol, İnternet Teknolojileri, İstanbul, Pusula Yayıncılık, Eylül 2001, s. 245.

<sup>24</sup> Zafer Demirkol, s. 246.

<sup>25</sup> İbrahim Kircova, İnternette Pazarlama, İstanbul, Beta, 1999, s.s. 166-167.

<sup>26</sup> Sedat Ekşi, "İnternet Üzerinden Alışverişlerde Güvenlik Altyapısı", Elektronik İş ve Ticaret Dergisi, Kasım Sayısı 2000, s. 54.

- @ bankaların, satıcıların ne sattıklarını bilmesi,
- @ bilginin, internet aracılığı ile bir yerden bir yere iletilirken değiştirilemeyeceği,
- @ bilginin tekrar tekrar gönderilemeyeceği.

**Şekil-5. SET İletişim Protokolü**

**Kaynak:** <http://www-3.ibm.com/software/ad/sanfrancisco/images/setimage.gif>

### Türkiye Perspektifinden Ulusal Bilgi Güvenliği

Türkiye'de ulusal bilgi güvenliği ile ilgili çalışmalarına genel olarak göz atıldığında, bu konuda devlet tarafından ciddi bir çalışma olmadığını görmekteyiz. Bu eksikliğin en büyük kanıtı ise, bu alanda yapılan bilimsel çalışmaların oldukça az ve yetersiz olmasıdır. Ulusal bilgi güvenliği için öncelikle, ulusal güvenliği ilgilendiren bilginin ne olduğunun bilinmesi gerekmektedir. Daha sonra, bu bilginin örgütlenmesi, gizlilik derecesi, nasıl üretilip korunacağı, nakledileceği ve kullanılacağı konularında devletin bilgi sahibi olması gerektiği halde herhangi bir çalışmasının bulunmadığı dikkat çekmektedir.<sup>27</sup> Türkiye'nin ulusal bilgi alt yapısına karşı yönelebilecek tehdit ve riskler, devletin ku-

►► **Türkiye'nin ulusal bilgi alt yapısına karşı yönelebilecek tehdit ve riskler, devletin kurum ve kuruluşları tarafından yeterince algılanamamıştır.** ◀◀

<sup>27</sup> TÜBİTAK-BİLTEN, Elektronik Kimlik Hizmetleri Web Sayfası, "Ulusal Bilgi Güvenliği Raporu ve Teknolojik Gelişmeler", <http://e-kimlik.bilten.metu.edu.tr/net/yayinlar/ubgrapor.jsp>

rum ve kuruluşları tarafından yeterince algılanmamıştır. Bu konudaki bilinç ve bilgi eksikliği, ülkemizi bu açıdan giderek daha zor duruma sokmaktadır.

Ulusal bilgi güvenliği teknolojileri konusunda Avrupa ülkelerinde ve ABD’de özellikle kamu sektörü tarafından olumlu örneklerine rastladığımız gibi, Türkiye’de de bilgi teknolojileri güvenliği ile ilgili altyapının sadece özel sektörde değil; özellikle kamu sektöründe de uygulanması zorunluluğu kendini açıkça göstermektedir. Hatta, gelişmiş ülkelerde olduğu gibi, bilgi teknolojileri güvenliği ile ilgili, özel sektör devlete değil; bilâkis devlet özel sektöre danışmanlık eder duruma gelmelidir.

Yapılan araştırmalarda, bilgi ve bilgisayar sistemleri konusunda devletin herhangi bir organına bağlı olarak yürütülen bir kurumun olmaması da dikkati çeken eksiklikler arasındadır. Bu konuda, örneğin Almanya’da söz konusu güvenlik uygulamalarının yapılandırılmasına ve uygulanmasına öncülük eden **Bundesamt für Sicherheit in der**

**Informationstechnik** adında bir kamu kuruluşu bulunmaktadır.<sup>28</sup>

Türkiye’de yaşanan tüm bu eksikliklere ilâveten, bir de 5680 sayılı kanuna 27. maddenin eklenmesi,<sup>29</sup> internetin sıkça kullanımı ve internet algılaması açısından Türkiye’yi büyük bir kayba uğratmıştır. RTÜK yasasına eklenen bu madde ile Türkiye’de internet, dergi veya gazete gibi bir yayın aracı olarak değerlendirilmiştir.

Görülüyor ki, devletlerin dünya sistemindeki etkinliğini önemli ölçüde belirleyen olguların başında, ulusal bilgi güvenlik sistemleri gelmektedir. Bu nedenle 21. yüzyıl bilgi teknolojileri çoğunlukla güvenlik odaklı olarak geliştirilmeye başlanmalıdır. Ulusal bilgi güvenliğinin korunması, devletlerin gelecekle ilgili bu alandaki tehditleri azaltacağı anlamına gelmektedir. Bu nedenle bulunduğu jeopolitik konum itibarıyla Türkiye de çok geçmeden ulusal bilgiyi koruma altına alacak bir politika gerçekleştirmeli ve bu politika değişen ve gelişen bilgi teknolojilerine uyarlanacak şekilde düzenlenmelidir.

**Bulunduğu jeopolitik konum itibarıyla Türkiye de çok geçmeden ulusal bilgiyi koruma altına alacak bir politika gerçekleştirmeli ve bu politika değişen ve gelişen bilgi teknolojilerine uyarlanacak şekilde düzenlenmelidir.**

<sup>28</sup> Detaylı bilgi için bkz. <http://www.bsi.de>

<sup>29</sup> <http://www.ntvmsnbc.com/news/85569.asp?0m=5vw>, NTV Yakın Plan Programı, 29 Mayıs 2001 Salı, 14:35.