Bilgisayar Dünyası

Alkım Özaygen

Şifreleme

Shell, kendi bilgisayar ağlarının dışarıdan girilemez olduğunu düşünüyordu. Bir anda, merkezlerinde bir bilgisayar korsanının (hacker) Doğu Asya'daki bölgesel ofisleri yoluyla ağlarına girdiğini öğrendiklerinde dehşet içinde kaldılar. "Bundan sonraki adımının ne olduğu konusunda hiçbir fikrimiz yoktu, ancak merkezdeki ateş duvarımızı aşmaya çalıştığında onu durdurabildik" diyor Shell'in bilgi güvenliği sorumlusu. İtinalı bir çalışmadan sonra Shell şirketi güvenli bir bilgi sisteminin testini bitirdi. Bunun amacı, şifreleme teknolojisi kullanarak verileri korumaktı.

Shell'de yaşananlar mesajların şifrelenmesinin, bir işyeri için çok önemli bilgilerin rakip firmaların, yabancı devletlerin, suçlu ve meraklı gözlerin bilgisayar saldırılarından korumak açısından önemli olduğunu göstermiştir. Ancak, sadece firmalar şifreleme yoluna gitmiyor. Aynı zamanda şifreleme, sahtekârlık, kişisel bilgilerin çalınması, çocuk pornografisi satışı, terör ve ekonomik ya da askeri casusluk, haber alma gibi birçok suçta kullanılıyor.

Şifreleme, yazının bulunması kadar eski. Yüzyıllardır siyasette de önemli bir rol oynadı. Fransız XIII Louis'nin pek de dürüst olmayan Richelieu Kardinali şifrelemeyi, gizli yazışma olarak adlandırdı.

Şifrelemedeki savunma yöntemlerini şifre çözümlemedeki gelişmeler izlemiştir. Ancak günümüzde güçlü bilgisayarlar sayesinde şifreleme, artık neredeyse kırılmaz hale geldi. Bu, bankalar için kendilerine para yatıranların güvenliği açısından çok önemli. Ancak suçluların da bu teknolojiyi aynı şekilde kullanabilmeleri devletlerin işine gelmiyor. Bu yüzden, Clinton yönetimi gelişmiş şifreleme yöntemleri ihracatının kesin kurallara dayandırılmasını istiyor. Soğuk savaşın bitmesine rağmen, Clinton yönetimi şifrelemenin askeri teknoloji konusuna girdiğini ve bunun da karşı güçlerin ellerine geçmemesi gerektiğini iddia ediyor. Şirket yöneticileri, Amerikan kongresindeki yaklaşık bir düzine üye ve birçok Batı Avrupa hükümetleri, bu sınırlamaların hiçbir şeye yaramadığını; İnternet gibi bilgisayar ağlarının gelişmesini önlediğini ve gizliliği bırakmadığını iddia ediyorlar. Bu ihracata getirilen sınırlamaların amacının, uyuşturucu kaçakçıları, teröristler ve diğer suçlular tarafından şifrelemenin kontrolsüz kullanmanın önlenmesi olduğunu başkan yardımcısı Albert Gore savunuyor. Georgetown Üniversitesi'nde hazırlanan rapora göre, teröristler bomba ve diğer ölümcül silahların yapımı ve patlatılması için şifreli talimatlar veriyor. Clinton yönetiminin üzerinde durduğu bu çok önemli anahtarlara ulaşım söz konusudur. Amerikan yönetimi, şifreleme teknolojisinin ihracatına ancak kanun uygulayıcı makamlar tarafından anahtara ulaşma izni verene müsade etmektedir. Fransa ve bir ölçüde İngiltere, Washington ile bu konuda görüş birliğindedir. ABD bu konudaki tutumu etrafında bir uluslararası görüş birliği sağlamaya çalışmaktadır. Bu çalışmalarını OECD ülkelerinin dışına da taşırarak Hindistan, İsrail ve Güney Afrika'yı da bu görüş etrafında toplamaya niyetli. ABD bu konuda bir anlaşmaya varmak için uğraş verirken, yeni bir sorun ufukta görünüyor. ABD dışındaki yasal şirketlerin şifreleme kullanımı çok hızlı şekilde artarken, özellikle Avrupa'da kanun uygulayıcı makamların, verilmesi gereken anahtar erişimini mecbur tutmayan ABD dışı firmalardan, yasal olarak satın alınan yazılım paketlerine yönelmektedirler. Hatta bazı hallerde bu yazılım, İnternet'ten bir fare tıklamasıyla yollanabilmektedir.

Amerikan ve Avrupalı şirketler bilgisayar güvenliği için 10 milyar dolar civarında para harcamaktadırlar. Avrupa'da İnternet ve diğer bilgisayar ağları çok hızlı bir gelişmeye adayken, bilgisayar teknolojisi için talep de aynı şekilde artacaktır.

DEC'in bilgisayar güvenlik bölümü olan AltaVista, şifreleme işinin her yıl yaklaşık %150 arttığını belirtmektedir. %150'lik bu artışın nedenlerinden biri de, bilgisayar suçlarındaki hızlı bir artıştır. Yılda 3 milyon dolarlık iş yapan bir Fransız şirketini yöneten Sarraut, Avrupa'da bilgisayar ağlarını suçlulardan ve diğer istenmeyen kişilerden (özellikle Rus ve Orta Avrupa mafyasının İnternet'e girdiği de düşünülürse) koruma sorununun muazzam ölçülere ulaştığını belirtmektedir. Sarraut'nun şirketi, müşterilerinin banka hesaplarından akıllı (smart) kartlara bağlanmış telefon hatlarından elektronik para çekmesini sağlayan yazılımlar satmaktadır. Sayısal parayla güvenli bir şekilde alışveriş yapabilmek için kredi kartı numaraları ve diğer gizli kişisel verilerin korunması gerekmektedir. Sarraut, şifrenin bu soruna en güvenli cevap olduğunu belirtmektedir. Bütün Avrupalı yöneticilerin hayalindeki kanun olarak tanımladıkları Fransız kanunlarına göre, şifreleme kullanan şirketler hükümetin kontrolündeki Fransız Merkez Bankası'na şifreleme anahtarını çözmeye yarayan çözüm anahtarını teslim etmek zorundalar.

Almanya'nın Brokart şirketi kendi şifreleme paketini yaklaşık 50 banka ve mali kuruluşa satmış. Almanya anahtar kodunun devlete verilmesini mecbur etmemiş. Washington bu durumdan pek memnun değil. Gerçekten Beyaz Saray, Amerikan ihracatındaki kontrolleri kaldırabilecek kanun tekliflerine karşı koymaktadır. Amerikan şirketleri, kendileri veya müşterilerinin önceden bir hükümetin kabul ettiği bir üçüncü tarafa anahtarı vermeyi kabul etmedikçe, gelişmiş şifreleme teknolojisinin ihracına izin vermemektedir. Siz evde yokken evin anahtarlarını bıraktığınız bir komşu gibi, TTP'de bir mahkeme kararının gösterilmesi halinde anahtarı hükümet yetkilisine vermekle yükümlü bulunmaktadır. Washington'un bu stratejisinin işe yaradığının ilk işaretleri bir düzine Amerikan şirketinin şimdiye kadar yasaklanmış şifreleme ürünlerini TTP koşuluyla ihraç etmek için lisans almalarıdır. Birçok şirket ise lisans almak için başvuruda bulunmuştur. Bunlar arasında IBM ve bu TTP sisteminin konusunda patenti olan ABD'nin önde gelen bilgisayar güvenliği firması olan Trusted Information System (TIS) vardır.

Şifreleme için Avrupa piyasasının geleceği ABD planının sahne gerisindeki tartışmasından çıkacak sonuca bağlı. Birçok ülkede şifrelemenin ulaşılabilir olması ve gizliliğinin korunması konusunda geniş bir görüş birliği vardır. Avrupalı yöneticiler, ABD usulü anahtar teslim sisteminin özel verilerin istenmeyen bir şekilde gizliliğinin kaybolmasına yol açmasından korkuyor. Daha açık bir şekilde ifade etmek gerekirse, bu yöneticiler şirket sırlarının rakiplere açılmasından korkmaktadırlar. Bu, özellikle Amerikan ve Avrupa sanayilerinin hızlı bir rekabette bulunduğu güçlü hükümet desteğine sahip Aerospace gibi duyarlı sektörlerde geçerli oluyor. Shell, IBM ve gelişmiş şifreleme bilgisayar ağlarına sahip diğer çok uluslu şirketler Fransa'dan kaçınmaktadırlar. Bir yöneticinin endüstriyel casusluğu ima ederek söylediği gibi, Fransa'da çok fazla kulak ve göz bulunmaktadır. FBI yetkilileri de ABD'de iş yapan Fransız firma ve devlet kuruluşları için de aynı şeyi söylemektedirler. Fransızlar bu konuda değişim işaretleri veriyorlar. Yetkililer Fransa'da çalışan çok uluslu şirketler için şifreleme kullanımını kolaylaştıracak planların bulunduğunu beyan ediyor. Bununla beraber bu konudaki mevcut mevzuatta bir değişiklik olmayacağını söylemektedirler. Bir yetkilinin belirttiği gibi, vatandaşlarının sırlarının saklanması konusundaki sorumluluk şahısların değil; devletin sorumluluğu altındadır. Şüphe yok ki Richelieu Kardinali bu görüşü onaylardı.