E-postama dokunma!

Büyük biraderin e-postalarınızı izlediğini düşünüyorsanız bu yazıyı okumanızda yarar var...

Eylem CÜLCÜLOĞLU

eylem@bilisimdergisi.org

Dünyayı sarsan NSA skandalından sonra, çoğu insan iletişim konusunda çekingen hale geldi. E-postalarım okunuyor mu, özel hayatım izleniyor mu, gizli ticari sırlarım güvende mi sorusu insanların zihinlerini meşgul etmeye başladı. Bu kaygıların ardında eskiden çok fazla dikkat edilmeyen güvensiz internet protokolleri yatıyor.

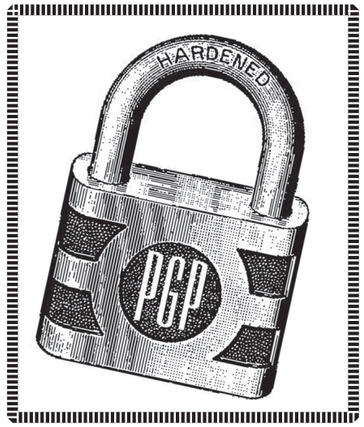
İnternet ticari kullanıma açıldığından bu yana çok değişti, devasa bir hale geldi ama kullanılan protokoller pek değişmedi. Örneğin e-posta için hala SMTP protokolü kullanılıyor. SMTP protokolü 1982 yılında geliştirilmiş, eskimiş güvensiz bir protokol. Dünya üzerindeki e-posta trafiğinin büyük bir kısmı herhangi bir şifreleme içermeyen SMTP üzerinden akıyor. SMTP üzerinde SSL şifrelemesine olanak tanıyan SMTPS kullanımı çok yaygın değil. Durum böyle olunca ağ üzerinde akan tüm e-posta trafiği kolayca izlenebilir oluyor. Yollanan bir e-posta, A noktasından B noktasına ulaşana kadar birden fazla atlama noktasından geçiyor. Bu atlama noktalarında bir ağ monitörü cihazı varsa tüm iletişim kolayca izlenebiliyor. Tüm dünyada internet trafiğini taşıyan büyük omurgaların sayısı bir elin parmaklarını geçmeyecek kadar az. Bu büyük servis sağlayıcıların neredeyse tamamına yakını ABD merkezli veya Amerikan ortaklı. NSA skandalı ile bu servis sağlayıcıların Amerikan İstihbaratı ile ortaklaşa çalıştığı ve NSA'ye veri trafiği servis ettiği ortaya çıktı.

Normal mektup daha güvenli!

Geleneksel postada, gönderici mektubunu yazar, bir zarfa koyar, üzerine adresini yazar, postaneye gider, postayı gönderir. E-postaya benzer şekilde geleneksel posta da birden fazla noktadan geçerek alıcıya ulaşır. Geleneksel postada zarf açılmaz ve mektubun içeriği gönderici ile alıcı arasında saklı kalır. E-postada ise durum tamamen farklı. E-postada ne içerik, ne zarf (protokol) ne de postacı (servis sağlayıcı) güvenli.

Radicati Group'un araştırma verilerine göre 2011 yılında dünyada 3.1 milyar adet e-posta adresi bulunuyordu. Bu rakamın 2015 yılında 4.1 milyara ulaşacağı öngörülüyor. E-posta adreslerinin yüzde 25'ini kurumsal hesaplar, yüzde 75'ini de bireysel hesaplar oluşturuyor. Bir kurumsal kullanıcı günde ortalama 78 e-posta alıyor ve ortalama 37 e-posta gönderiyor. Gün içinde internette milyarlarca e-posta dolaşıyor. Bu milyarlarca e-posta NSA'in süper bilgisayarları tarafından indeksleniyor, sınıflandırılıyor, anahtar kelime bazında filtreleniyor ve gerekirse de uzmanlar tarafından okunuyor. Amerika e-postaların sadece terörle mücadele için kullanıldığını söylese de bu dev içeriğin hangi amaçlar için kullanıldığını, kimlerin izlendiğini ve ne tür raporlamalar yapıldığını bilmek olanaksız.

İnternet kullanıcıları olarak bu kanunsuz izlemelere boyun eğmek zorunda değiliz. E-posta izlemelerine karşı bireysel veya kurumsal olarak kullanabileceğimiz çözümler bulunuyor. İsterseniz bu çözümlere yakından bakalım:



1 - PGP – Pretty Good Privacy

Amerikalı güvenlik gurusu Phil Zimmerman tarafından 1991 yılında geliştirilen PGP (Pretty Good Privacy) halen en güvenli e-posta şifreleme çözümü olmayı koruyor. PGP, mevcut SMTP e-posta protokolünü kullanan bir çözüm. PGP kullanıcıları e-postalarını bir gizli anahtar ve bir açık anahtar kullanarak şifreliyorlar. PGP yazılımı içeriği, şifrelenmiş bir ASCII formatına çeviriyor. Standart ASCII kullanıldığı için mesaj normal e-posta üzerinden kolayca yollanabiliyor. PGP üstün bir güvenlik sağlama amacıyla birden fazla yöntem kullanan bir çözüm. Mesaj sırasıyla harmanlanıyor (hashing), sıkıştırılıyor, simetrik anahtar kripto tekniği ile kriptolanıyor ve mesajın açılabilmesi için açık anahtar (public key) kriptolama tekniği kullanılıyor. PGP'nin sunduğu güvenlik o kadar yüksek ki, programı geliştiren Phil Zimmerman ABD'de büyük eleştirilere maruz kaldı. Bu kadar güçlü bir kriptolama sisteminin halka açık olmasından çekinen ABD hükümeti Phil Zimmerman'ı sürekli olarak sıkıştırdı. 11 Eylül saldırılarından sonra PGP'nin teröristler tarafından kullanılmış olabileceği iddiaları gündeme gelmişti. Saldırılardan hemen sonra Washington Post'a bir röportaj veren Zimmerman, terörist saldırılardan dolayı çok üzgün olduğunu ama güçlü kriptolamanın bir insan hakkı olduğunu ve PGP'nin insanlığa güvenli iletişim sunma yolunda devam edeceğini söylemişti. Sözünde duran Zimmerman, PGP'nin o zamanki sahibi Network Associates'den ayrıldıktan sonra PGP altyapısını kullanan Hushmail.com'un CEO'su oldu. Hushmail.com hala faaliyetine devam ediyor ve kullanıcılarına senelik 35 dolar karşılığında güvenli e-posta hizmeti satıyor.

PGP kriptolama tekniği günümüzde ticari olarak sunulan en güvenli çözüm. PGP'nin kırılabildiğine dair yayınlanmış herhangi bir bilgi bulunmuyor. 2003 yılında İtalyan polisi yaptığı bir baskında Kızıl Tugaylar'a ait bilgisayarlar ele geçirmişti. Bilgisayarların içinde bulunan PGP şifreli dosyalar asla kırılamadı. 2006 yılında ise PGP'nin Amerika tarafından bile kırılamadığı ortaya çıktı.

PGP'nin kurucusu Phil Zimmerman

Endüstriden Haberler

Olay, Kanada'dan Amerika'ya geçiş yapan Sebastian Boucher aldı şahıs dizüstü bilgisayarında çocuk pornosu bulunduğu iddiasıyla gözaltına alınmasıyla başladı. Yetkililer Boucher'ın dizüstü bilgisayarını açmaya çalıştıklarında sabit diskin PGP ile şifrelendiğini gördüler. Bocuher ise PGP şifresini polise söylemeyi reddetti. Bunun üzerine sabit disk FBI kriminal laboratuvarlarına yollandı. En gelişmiş teknolojilere sahip olan FBI bile Boucher'ın sabit diskindeki verilere ulaşamadı. Davanın hakimi ABD'de çok tartışılacak bir karara imza atarak Boucher'a PGP şifresini vermesini emretti. Şifresini vermezse ceza alacağı için Boucher şifresini vermek zorunda kaldı ve ilgili dosyalara ulaşıldı. Bu olay FBI kriminal laboratuvarlarının bile PGP şifresini kıramadığının bir belgesi olarak tarihe geçti. PGP günümüzde bile kırılabilmiş değil.

PGP, 2010 yılında Symantec tarafından satın alındı ve firma PGP altyapısını son kullanıcıya yönelik veri güvenliği çözümlerinde kullanmaya başladı. PGP yazılımı hakkında daha fazla bilgiyi www.symantec.com/encryption adresinde bulabilirsiniz. Ayrıca PGP altyapısını kullanan açık kaynak kodlu OpenPGP yazılımına www.openpgp.org adresinden ulaşılabilirsiniz.

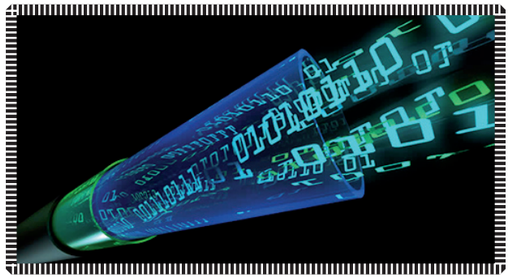
2 - Hushmail.com

PGP'nin kurucusu Phil Zimmerman'ın yöneticiliğini yaptığı Hushmail güvenli e-posta için iyi seçeneklerden birisi. Senede 35 dolara abone olunabilen Hushmail uçtan uca kriptolanmış bir web e-posta ortamı sunuyor. Bir Hushmail kullanıcısı başka bir Hushmail kullanıcısına e-posta yolladığı zaman mesaj otomatik olarak OpenPGP ile şifreleniyor. Hushmail sunucularında e-posta bu formatta saklanıyor. Alıcı e-postayı açtığı zaman kripto otomatik olarak açılıyor. Bu işlemler tamamen arka planda gerçekleştiği için kullanıcının şifreleme anahtarlarıyla uğraşması gerekmiyor. Hushmail'in koruması sadece Hushmail kullanıcıları arasında olan iletişimle sınırlı değil. Serviste dışarıdaki e-posta adreslerine yollanan e-postaları kriptolama özelliği bulunuyor. Alıcı gelen e-postayı önceden belirlenen şifreyi girerek okuyabiliyor.

Cliff Baltzley tarafından 1999 yılında Kanada'da kurulan Hushmail'in sunucuları Vancouver'da bulunmakta. Kanada bireysel haklar ve iletişim özgürlüğü konusunda ABD'den daha esnek yasalara sahip. Bunun yanında Kanada ve ABD arasında Karşılıklı Hukuki Yardımlaşma Anlaşması bulunuyor. Bu anlaşma yüzünden Hushmail 2007 yılında sunucularındaki e-postaların bir kısmını ABD'li federal ajanlara teslim etmek durumunda kalmıştı. ABD'deki bir mahkeme Çinli yasadışı streoid kimyasal maddeleri üreticilerinin Hushmail üzerinden haberleştiğini iddia etmişti. Mahkemenin kararı doğrultusunda Hushmail, FBI'a 12 CD dolusu e-postayı teslim etmişti. Bu olaydan sonra Hushmail'in güvenilirliği tartışılmaya başladı.

3 - Mailpile

NSA skandalının ardından güvenli e-posta çözümleri daha çok gündeme gelmeye başladı. Bu alanda ihtiyacı fark eden üç İzlanda'lı genç Mailpile adlı bir çözüm geliştirmeye başladılar. Indiegogo adlı kitle finansmanı sitesinde 163 bin dolar bağış toplanarak gerçekleştirilen çözüm bir anda güvenli e-posta konusunda bir umut ışığı oldu. Mailpile, e-postaya farklı bir anlayış getirerek merkezi e-posta sunucularını devre dışı bırakıyor.
Mailpile çözümünde her kullanıcı kendi bilgisayarına Mailpile yazılımını yüklüyor. Mailpile yazılımı içerisinde OpenPGP ve S/MIME kriptolama sistemleri bulunuyor. Kullanıcıların Mailpile'ın web arayüzü yüzünden diğer kullanıcılara şifreli e-postalar gönderebiliyorlar. Sunucu kullanıcının bilgisayarında bulunduğu için ve e-postalar tamamen şifrelenmiş olarak gönderildiği için e-postanın içeriğinin izlenmesi mümkün olmuyor.
Mailpile'ın en büyük dezavantajı ise ekstra bir yazılıma ihtiyaç duyması. Günümüzde e-posta kullanıcılarının büyük bir kısmı web arayüzlü bulut çözümlerini tercih ediyorlar. Mailpile çözümü farklı bilgisayarlar kullanan kullanıcılar için çok kullanışlı değil. Mailpile yazılımı istenirse bulut üzerinde herhangi bir sunucuya da yüklenebiliyor ama bu zamanda barındırmaya ücret ödemek ve güvenlikten fedakarlık etmek gerekiyor. Mailpile hakkında daha fazla bilgiye www.mailpile.is adresinden ulaşabilirsiniz.



4 - Flowingmail

Peer-to-peer (P2P) teknolojisi genellikle dosya paylaşımında kullanılan bir teknolojidir. Henüz geliştirme aşamasında olan Flowingmail bu teknolojiyi e-posta ortamına taşımak isteyen bir ağ protokolü. Flowingmail'in en büyük özelliği tamamen merkezi olmayan bir yapıya sahip olması. BitTorrent ve BitMessage protokollerinden esinlenerek geliştirilen Flowingmail'de 4096 bitlik RSA anahtarları kullanılıyor. Normal e-posta altyapılarında e-postalar merkezi sunucuya giderken, Flowingmail'de e-postalar ilk önce şifreleniyor, sonra parçalara ayrılıyor ve Flowingmail ağı üzerindeki diğer kullanıcılara gönderiliyor. Alıcı mesajı açacağı zaman tüm parçalar ağ üzerinden indiriliyor, anahtar ile açılıyor.

Flowingmail bu yapısı sayesinde diğer güvenli e-posta çözümlerinin tamamından daha etkin

Endüstriden Haberler

bir güvenlik sağlıyor. Flowingmail ağı üzerinden gönderilen e-postalar sabit bir yerde saklı olmadığı için herhangi bir kişinin ya da kuruluşun bu e-postaları okuması imkansız. Flowingmail haberleşmesini dinlemek isteyenin ağ üzerindeki tüm e-posta trafiğini dinlemesi gerekli. Bununla da kalmayıp daha sonra süper bilgisayarlarla bile yüzyıllarca sürecek 4096 bit şifreyi kırması lazım.

E-postaların herhangi bir sunucuda bulunmaması, ortada bir servis sağlayıcının bulunmaması Flowingmail'i yasal engellerden de koruyor. Hükümetlerin Flowingmail tarzı bir P2P e-posta altyapısını engellemesi mümkün görünmüyor.

Flowingmail henüz çok yeni. Protokolün geliştirilmesine geçtiğimiz Eylül ayında başlandı. Flowingmail geliştiricileri Indiegogo sitesi üzerinden bağış topluyorlar. Projenin başında Paola Brandoli adlı 30 senedir programcılık yapan bir İtalyan ve Mike Vorobyev adlı bir Rus C++ gurusu bulunuyor. Flowingmail hayata geçerse Brandoli ve Vorobyev'in isimlerini çok duyacağız gibi gözüküyor.

5 - Lockbin.com

Güvenli e-posta konusunda benim favorim ise kolay kullanımı ve ücretsiz olması nedeniyle Lockbin.com. Herhangi bir kullanıcı kaydı gerektirmeyen Lockbin, isteyen herkese istediği an güvenli e-posta yollama imkanı sunuyor. Kullanıcının tek yapması gereken Lockbin.com adresinde basit bir form doldurarak e-posta yazmak. Kullanıcı kendi e-posta adresini, alıcının adresini giriyor, mesajını yazıyor, gerekirse dosya ekliyor ve şifreyi belirliyor. Daha sonra Lockbin sunucuları belirtilen adrese bir e-posta gönderiyor. Bu e-postada sadece bir link bulunuyor. Kullanıcı linke tıklıyor, Lockbin sunucularına SSL bağlantısı ile bağlanıyor ve önceden kararlaştırılmış şifreyi girerek e-postayı açıyor. E-postalar AES-256bit kriptolama yöntemi ile şifrelendiği için herhangi bir üçüncü kişinin şifreyi bilmeden bu içeriği okuması mümkün olmuyor.

Lockbin.com'un tek dezavantajı ise ABD menşeili bir firma olması. Her ne kadar sitelerinde bize henüz NSA'den bir başvuru gelmedi deseler de, ileride ne olacağı bilinmiyor.