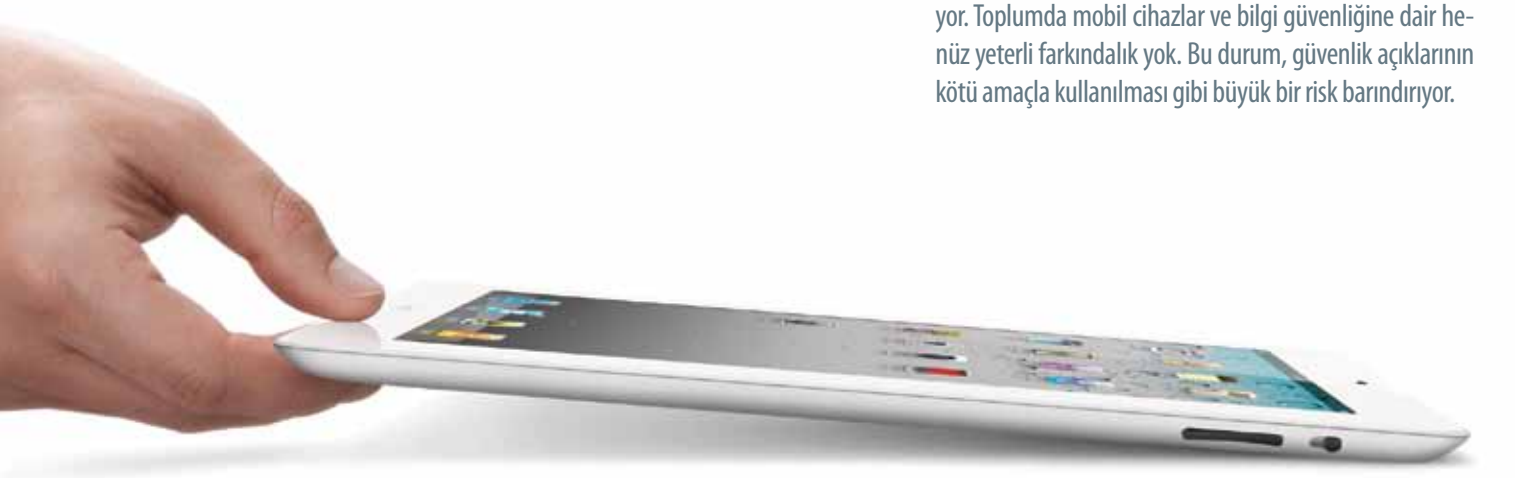
Oğuzhan Vıcıl

Dr, Bilimsel Programlar Uzmanı,
TÜBİTAK Bilim ve Toplum Daire Bşk.

Mobil Cihazlar ve Güvenlik Riskleri

Mobil cihazlar artık hayatımızın hemen hemen her alanında kullanılıyor. Çok değil, daha on yıl öncesine kadar sadece belirli bir kesimin sahip olabildiği mobil cihazlar, günümüzde teknolojik gelişmelerin sonucunda giderek ucuzlamaları ve kullanım alanlarının iyice yaygınlaşmasıyla yedisinden yetmişine hemen herkesin elinde. Cep telefonları, Ipodlar, mp3 çalıcılar ve Blackberry'ler ile başlayan bu akım günümüzde yerini Iphone'lara, Ipad'lere, akıllı telefonlara ve tablet bilgisayarlara bıraktı.

Kullanımlarının kolay olması, taşınabilir olmaları, veri depolama ünitelerinin kapasitelerinin artmış olması, kablosuz ağlara ve diğer cihazlara kolaylıkla (infrared, bluetooth, wi-fi, vs. yoluyla) bağlanabilmeleri, diğer elektronik cihazlarla uyumlu çalışabilmeleri mobil cihazların yaygınlaşmasındaki en önemli faktörler arasında. Ama bunlar, birtakım bilgi güvenliği risklerini de beraberinde getiriyor. Mobil cihazların sahip olduğu bu özellikler nedeniyle, sadece bilgi güvenliğine dair risklerin gerçekleşme olasılığı artmakla kalmıyor, riskler gerçekleştiğinde etkileri de artıyor. Toplumda mobil cihazlar ve bilgi güvenliğine dair henüz yeterli farkındalık yok. Bu durum, güvenlik açıklarının kötü amaçla kullanılması gibi büyük bir risk barındırıyor.



Günümüzde birçok kişi, kişisel bilgisayarlara yönelik bilgi güvenliği riskleri ve bu risklerden korunma yöntemlerinin neler olduğu konusunda belli bir birikime sahip. Hemen hemen herkes yalnızca güncel bir antivirüs yazılımı kullanmanın yeterli olmadığını, casus yazılımlar, Truva atları ve solucanlar için de önlem alınması gerektiğini, güvenlik duvarının etkin hale getirilmesi, farklı internet hesaplarında aynı şifrelerin kullanılmaması, bilinmeyen üçüncü parti uygulamaların kurulmaması gerektiğini biliyor. Bir taraftan da üretici firmalar güvenlik açıklarına karşı sürekli olarak işletim sistemi yamaları yayımlıyor ve bilgisayarlar raflardaki yerlerini güvenlik yazılımları kurulmuş olarak alıyor. Bu sebeple kötü niyetli kişilere, kullanıcıların henüz bilmediği risklerden faydalanmak daha cazip geliyor.

>>>

Veri Depolama Üniteleri

TB'lara ulaşan kapasiteleri ile hard diskler artık inanılmaz miktarda veri depolamaya imkân veriyor. Bu nedenle hard diskleri belirli aralıklarla gereksiz şeylerden temizlemeye, CD ve DVD gibi ortamlarda veri yedeklemeye gerek duyulmuyor. Özel resimler ve videolar, kişisel belgeler ve hatta finansal işlemlerinizi yürüttüğünüz hesaplar da dâhil çeşitli internet hesaplarının şifreleri hard disklerde veya flash belleklerde tutuluyor. Sadece bunlar da değil: Dijital fotoğraf makineleri, kameralar, mp3 çalıcılar ve cep telefonlarında bulunan dâhili ve harici bellek kartları da veri depolama ve veri paylaşımı için kullanılıyor. Bu nedenle, farklı elektronik cihazlardaki verilerin yönetilmesini ve senkronize edilmesini kolaylaştıran taşınabilir hard diskler ve diğer bellek ürünleri günümüzde hayli revaçta.

Peki, mobil cihazlar ve hard diskler gibi veri depolama üniteleri kaybolursa veya çalınırsa neler olabilir? Büyük ihtimalle pek çok kişinin aklına ilk gelen ve üzüntü doğuran şey ya yitirilen cihazdır ya da yedeği alınmadığı için kaybedilen verilerdir. Hâlbuki cihazınız çalındığında veya kaybolduğunda, eğer daha önceden gerekli birtakım önlemleri almamışsanız, kişisel bilgilerin ve gizlilik derecesi yüksek diğer verilerin yetkisiz kişilerin eline geçmesi sonucunda uğrayabileceğiniz maddi ve manevi zarar, çoğu zaman cihazın maddi değerinden ve yaşadığınız sıkıntıdan çok daha büyüktür.

Kablosuz İnternet Ağları ve Casus Yazılımlar

Kablosuz ağlar sayesinde artık hemen her yerden internete bağlanmak mümkün. Havalimanlarının bekleme salonlarında, otellerde, kafelerde, Wi-Fi noktası olan alışveriş merkezlerinde bilgisayarlarınızla, akıllı cep telefonunuzla ve internete bağlanma özelliği olan diğer mobil cihazlarınızla kablosuz ve ücretsiz olarak internete bağlanabiliyorsunuz. Kablosuz bağlantı noktalarını araştırdığınızda çoğunlukla birden fazla bağlantı noktası görülüyor. Ancak haklarında herhangi bir bilgiye sahip olmadığınız bağlantılar, özellikle de şifresiz olanlar, bilgi güvenliği açısından risk taşıyor. Herhangi bir ücret ödenmediği için şifresiz ağlar birçok kişiye cazip gelebilir. Fakat tüm internet trafiğinizin birileri tarafından siz farkında olmadan izleniyor olması muhtemel. Bütün internet hesaplarınızın şifreleri ve kişisel bilgileriniz kötü amaçlı kişilerin eline geçebilir. (Oysa SIM kartlar vasıtasıyla internete bağlanma yöntemlerinde, örneğin 3G modemlerde belirli ve onaylı iletişim protokolleri kullanıldığı için veriler güvenli bir şekilde iletiliyor). Bu riskten korunmak için bilinen ve güvenli olduğundan emin olunan bağlantıların kullanılması hayli önemli. Kablosuz internet güvenliğini sağlamaya ve iletişimi kriptolu yapmaya yarayan ticari yazılımlar da var.

Önemli bir başka risk de üçüncü parti uygulamaların mobil cihazlara kurulması ile ortaya çıkıyor. Çoğunlukla eğlence amaçlı olan ve herhangi bir ücret ödenmeden edinilen bu uygulamaların kurulması ile cihazınıza casus yazılımlar bulaşabiliyor. Casus yazılımların etkileri çok çeşitli. Hangi internet sitelerini ziyaret ettiğinize ilişkin bilgileri belirli bir merkeze göndermekten ve reklam gösteriminden tutun, tüm veri trafiğinizi izlemeye varıncaya kadar çeşitli amaçlara hizmet edebiliyorlar. Casus yazılımlar çoğunlukla antivirüs programları tarafından fark edilemez. Bunlar için geliştirilmiş özel yazılım kullanmadığınız sürece, ne varlıklarını fark etmeniz ne de sisteminizden silmeniz mümkündür. Casus yazılımların bilgisayarlara ve cep telefonlarına kurulması ile birlikte bilgisayarınızda güvenlik açıkları meydana gelir ve aldığınız diğer önlemler geçersiz kalır. Ne kadar güvenlik duvarı ve antivirüs yazılımı kullanmak gibi önlemler almış olsanız da, bu yazılımlar nedeniyle tüm veri trafiğiniz riske girebilir ve üçüncü şahıslar tarafından izlenip kayıt edilebilir. Hatta casus yazılımlar sayesinde cep telefonunuz veya kamera bağlantılı bilgisayarınız, haberiniz olmadan sizin resimlerinizi veya hareketli görüntünüzü çekip başkalarına da yollayabilir. Ayrıca GPRS özellikli telefonlar nedeniyle, bulunduğunuz yerler ve buralarda kaldığınız süreler de başkaları tarafından izlenebilir. Bu nedenle kaynağı tam olarak doğrulanmayan ve yayımcısı sertifikalı olmayan üçüncü parti uygulamalar konusunda çok dikkatli olmak gerekir. En iyisi bu tür programların mümkünse kullanılmamasıdır.

Aslında günümüzde kişisel bilgisayar güvenliğine yönelik belli bir farkındalık ve altyapı var. Ama ne yazık ki diğer mobil cihazlardaki tehlikeler konusunda henüz istenen seviyede birikim yok.

İkinci El Cihazlar

Dünya üzerinde şu an kullanılmakta olan milyonlarca cep telefonu var. Ülkemizde de cep telefonu abonelerinin sayısının 50 milyonun üstünde olduğu göz önüne alınırsa, yeni modellerin piyasa ömürleri çok da uzun olmuyor, dolayısıyla da birbiri ardına yeni ürünler piyasaya çıkıyor. Son yıllarda "moda" teknolojiye de bulaştı. Kullanıcılar ihtiyaçları olmamasına karşın daha üstün özellikli, daha şık tasarımlı ve daha fonksiyonel cep telefonlarına rağbet eder oldu. Bu anlayış sadece cep telefonları ile sınırlı değil, dizüstü bilgisayarlar, mp3 çalıcılar ve tablet bilgisayarlar için de geçerli. Örneğin günümüzde, ortalama bir kaç senede bir cep telefonu değiştiriliyor. Satın alınan her yeni cep telefonu, eskisinin atıl hale gelmesi, bir başkasına hediye edilmesi veya ikinci el piyasasında değerlendirilmesi anlamına geliyor. Durum böyleyken çoğu zaman sıradan bir silme işlemi ile bu cihazların içindeki verilerin tamamen silindiği varsayılıyor. Hâlbuki veriler, eğer özel bir yolla silinmediyse, verilerin geri döndürülmesi bazı yazılımlarla çoğu zaman mümkün. Adli tıp araştırmaları konusunda uzmanlaşmış ABD merkezli çeşitli şirketler, eBay gibi internet üzerinden alışveriş yapılan sitelerde satılan ikinci el cep telefonlarının çoğunun, sosyal güvenlik numarası gibi kimlik bilgilerini ve finansal bilgiler içerdiğini, bu verilerin de geri döndürülebildiğini belirtiyor. Cep telefonlarından ve SIM kartlardan silinen verilerin kurtarılmasını sağlayan ticari ürünler bulmak da mümkün. Örneğin, ABD'deki Utah merkezli Paraben, cep telefonlarından ve SIM kartlardan silinen verilerin geri döndürülmesini sağlayan ürünlere ek olarak, kısa süreliğine ödünç alınan cep telefonlarındaki tüm verilerin kopyalanmasını sağlayan ürünler de sunuyor. Esasında emniyet çalışanları ve bilgi güvenliği uzmanları için tasarlanmış bu ürünler, çocuklarının aktivitelerini izlemek isteyen ebeveynlere de hitap ediyor. Herkes tarafından temin edilebilecek bu tür ürünlerin piyasada olması, aynı zamanda çok fazla teknik bilgiye sahip olmayan saldırganların da bu ürünlere kolaylıkla erişebileceğini gösteriyor.

Şirketler Açısından Durum

Şirketlerde bilgi güvenliğinin sağlanması genellikle çok daha zor ve karmaşıktır. Veriler genellikle "çok gizli", "gizli", "hizmete özel" ve "herkese açık" olmak üzere farklı kategorilere ayrılır. Verinin bulunduğu kategoriye göre alınması gereken önlem değişir. Personel ve müşteri kimlik bilgileri ile finansal bilgiler gizlilik seviyesi yüksek bilgilerdir, dolayısıyla da bu tür bilgileri barındıran veri tabanları çoğunlukla dış ortama açılmaz. Şirket veri tabanına uzaktan bağlanmak yüksek güvenlikli protokoller ile sağlanır. Şirketin intranet ağı etkin güvenlik duvarları arkasındadır. Veri tabanları açısından fiziksel güvenlik de önemli bir unsur olduğundan, verilerin tutulduğu yerlere sadece yetkili kişiler erişebilir. Etkin ve güvenli kimlik doğrulama sistemleri uygulanır ve kullanıcılar şirket bilgisayarlarına ancak ondan sonra girebilir.

>>>

Yüksek veri depolama kapasiteleri ve kablosuz ağlara bağlanabilme yetenekleri nedeniyle kullanımları yaygınlaşan mobil cihazlar, şirket içi ve şirket dışı veri akışı üzerindeki kontrolün kaybolmasına da neden olabiliyor. Bunun sonucunda, gizlilik derecesi yüksek bilgilerin dışarı sızması ve yetkisiz kişilerin eline geçmesi riski doğuyor.

Ancak her ne kadar pahalı bilgi güvenliği çözümleri satın alınıp uygulamaya geçirilmeye çalışılsa da, insan faktörü devreye girip alınan önlemleri geçersiz kılabilir. Örneğin, güncel antivirüs ve antispyware yazılımları kullanılsa bile, çalışanlar tarafından şirket bilgisayarına takılan mp3 çalıcılar ve USB flash bellekler gibi cihazlar yüzünden, şirket bilgisayarlarına virüsler ve casus yazılımlar bulaşabilir. Sonuçta zararlı bir program sadece o bilgisayara zarar vermekle kalmayıp bilgisayarın bağlı bulunduğu tüm ağ bileşenlerini tehlikeye atabilir.

Mobil cihazlarla ilgili risk yönetimi nasıl olmalıdır?

Önce şirketlerin alabileceği güvenlik önlemlerini ve bunların olası etkilerini ele alalım. Alınabilecek en önemli ama bir o kadar da katı güvenlik önlemi, şirket bilgisayarlarına ve ağ bağlantılarına mobil cihazların erişiminin tamamen engellenmesidir. Örneğin şirket bilgisayarlarında CD-Rom, USB flash bellek, taşınabilir hard disk, Ipod ve mp3 çalıcı gibi cihazların kullanılması sistemsel olarak engellenebilir. Kablosuz ağlara cep telefonlarından ve kişisel dizüstü bilgisayarlardan erişim kısıtlanabilir. Bu önlemler ilk bakışta etkin bir çözüm gibi görünse de, iş yapma şekline ve kurum kültürüne göre, her şirket için uygun olmayabilir. Örneğin iletişimin hayli önemli olduğu şirketlerde, birçok çalışan bir yandan kendi taşınabilir bilgisayarları, Outlook tarzında e-posta uygulamaları barındıran Blackberry ve Iphone gibi akıllı telefonlarıyla şirket ağına bağlanırken, bir yandan da bir takım ofis uygulamalarını da bu cihazlar ile çalıştırıyor ve veri paylaşıyorlar. Özellikle satış, pazarlama, teknik destek ve danışmanlık gibi iş kollarında çalışanların hareket edebilme kapasitesi vazgeçilmez bir unsur. Bu nedenle, risk azaltıcı önlemler değerlendirilirken maliyet-fayda analizi dikkatli bir şekilde yapılmalı, mobil cihazların doğru ve yerinde kullanımı için bilgi güvenliği yöneticisinin de katılımıyla bir kurum politikası belirlenmelidir. Bu politikalar çalışanlara duyurulmalı ve onlar tarafından benimsenmesi için gerekli bilinçlendirme çalışmaları yapılmalıdır. Çalışanların bilgi sistemleri üzerindeki aktiviteleri güvenlik yöneticisi tarafından izlenmeli, şüpheli bir durum olduğunda müdahale edilebilmelidir.

Mobil cihaz güvenliğine yönelik kişisel ve kurumsal risk yönetiminde dikkat edilmesi gereken diğer hususlar şu şekilde sıralanabilir:

Güvenlik duvarı: Mobil cihaz güvenliğindeki önemli bileşenlerden biri de güvenlik duvarlarıdır. Dizüstü bilgisayarların kablosuz ağ bağlantıları açıksa, çevredeki çeşitli ağlarla sürekli olarak haberleşirler. Güvenlik duvarı, bilgisayarınıza gelen ve giden trafiği kontrol altına almaya yarar. Bir diğer ifadeyle internete bağlanmanızı sağlayacak olan ağlara izin verirken, davetsiz misafirlerden gelen erişimleri kısıtlar. Güvenlik duvarları, ağ bağlantılarınızı sürekli olarak izler ve saldırıları fark ederek otomatik olarak bu bağlantıları bloklar. Bu nedenle güvenlik duvarının aktif olması sistem güvenliği açısından çok önemlidir.

Güvenli ve etkin kimlik doğrulama: Mobil cihazlar parola korumalı olmalıdır. Belirli bir süre kullanılmadığında cihazın otomatik olarak kapanma özelliği ve tekrar açılması için de parola girilmesi özellikleri etkinleştirilmelidir. Bu sayede, bir yerde unutulduklarında ya da çalındıklarında bile cihazın içindeki verilere yetkisiz kişiler tarafından erişilmesi engellenir.

Antivirüs yazılımları: Artık sadece masaüstü ve dizüstü bilgisayarların değil, akıllı telefonların da internet ortamından yayılabilecek virüslere karşı korunması gerekiyor. Günümüzde cep telefonları gibi mobil cihazlarda antivirüs yazılımlarının kullanılması giderek daha önemli hale geliyor, yakın bir gelecekte bu yöndeki ürünler daha da yaygınlaşıp önem kazanacak gibi görünüyor. Şimdiden birçok yazılım firması, cep telefonlarına yönelik antivirüs yazılımlarını kullanıcıların hizmetine sunmuş durumda.

Günümüzde hayli popüler olan dosya paylaşımını kolaylaştıran USB flash bellekler de virüslerin bulaşmasında çok etkili. Kişiye özel olmayan, ortak kullanıma açık bilgisayarlarda sürekli kullanılıyorlar. Flash bellekleri tehdit eden virüslerin çoğu autorun.inf özelliğini kullanan virüsler. Bu şekilde, belleği cihazınıza taktığınız zaman, eğer güncel ve etkin antivirüs yazılımınız yoksa, bilgisayarınıza ya da o sırada kullandığınız cihaz her ne ise ona, otomatik olarak bu virüs bulaşır. Antivirüs yazılımının yanı sıra USB flash belleğinizdeki autorun özelliğini etkisiz hale getirmek de akıllıca bir önlemdir.

Uzaktan veri silme: Bazı cep telefonlarında uzaktan veri silme özelliği var. Eğer sizin cihazınızda da bu özellik varsa, çalınması durumunda, cep telefonunuza uzaktan bir mesaj göndererek cihazın içindeki tüm bilgileri silebilirsiniz. Bu özelliğin olmadığı telefonlarda ise satın alınacak bazı ticari yazılımlarla telefonun uzaktan kilitlenmesi ve içindeki verilerin silinmesi mümkün. Bu tür yazılımlar hayli çeşitlilik gösterebiliyor. Bazı akıllı telefonlar yalnızca SMS yoluyla açma şifresi gönderildiği zaman tekrar kullanılır hale geliyor. GPRS özelliği olan bazı telefonlar ise coğrafi konumunu, istenirse gerçek sahibine bildirebiliyor. Tabii ki tüm bunları yapabilmesi için cep telefonunun bataryasının tükenmemiş olması ve açık olması gerekiyor. Bu sebeple telefonunuzun çalındığını anladığınız an ile tepki vermeniz gereken an arasında zaman dilimi, çok kritik bir zaman dilimi.

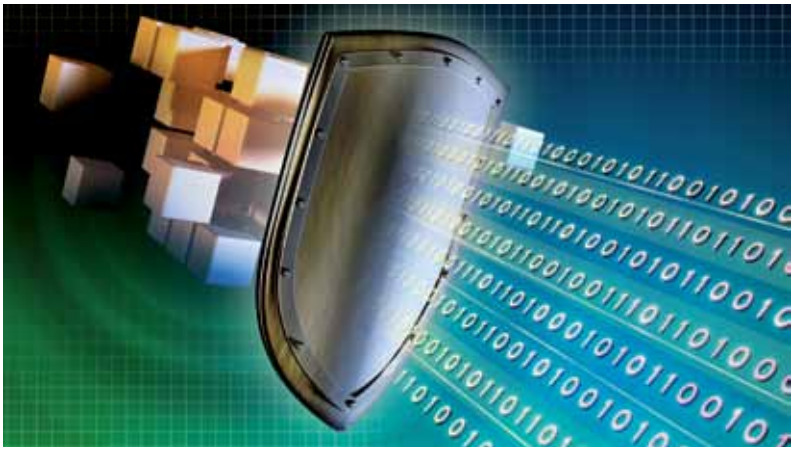
İmha ve yeniden kullanım: Kullanıcıların belki de en çok ihmal ettiği risklerden biri de artık kullanılmayacak olan veya el değiştiren cihazlardaki verilerin güvenliği. Örneğin bilgisayarınızı bir başkasına vermeden önce, hard disklerindeki verileri, özel yazılımlar kullanarak geri döndürülemeyecek şekilde silmelisiniz. Flash belleklerin manyetik disklere göre en büyük risklerinden biri ise güvenli veri silme işleminin daha zor ve karmaşık olmasıdır. Aralarında Michael Wei ve Steven Swanson'un bulunduğu San Diego Kaliforniya Üniversitesi (UCSD) araştırmacılarının gerçekleştirdiği güncel bir çalışma, katı hal disklerinden (SSD) ve USB flash belleklerden silinen verilerin aslında tam olarak kaybolmadığını, özel yöntemlerle geri getirilebildiğini ortaya koyuyor. Manyetik disklerde en güvenli silme yöntemi, silinecek verinin üzerine yeni verilerin çeşitli kereler yazılması. UCSD araştırmacılarına göre, bu yöntem SSD'lerde ve flash belleklerde tekli dosyaları silmek için kullanıldığında etkili olmuyor ve hâlâ verilerin önemli bir bölümü geri getirilebiliyor. (Çalışmanın detayları için http://nvsl.ucsd.edu/sanitize adresindeki "Reliably Erasing Data from Flash-Based Solid State Drives" başlıklı makaleye bakınız.)

Bu açıdan, verilerin bu belleklerde en baştan kriptolu olarak saklanması, cihaz artık kullanılamayacak duruma geldiğinde ise disk imha makineleri ile fiziksel olarak parçalanmaları en etkin yol. Gerçi bu son yöntem daha çok, çok hassas verilerle uğraşan savunma endüstrisinde ve bazı kamu kurum ve kuruluşlarında uygulanır. Cep telefonları için de "master reset" adı verilen silme işlemi yapılabilir. Bunun için cep telefonunuzun kullanma kılavuzundaki adımları izlemeniz yeterlidir. Bu yapıldığı takdirde cep telefonunuzdaki tüm log dosyaları telefon tekrar açıldığında silinir. Ancak telefonunuzda harici ek bellek kartı varsa, unutmayın oradaki bilgiler hâlâ orada!

Yedekleme: Yedekleme ilk bakışta bilgi güvenliği önlemi olarak görülmese de cihazınız çalınır veya kaybolursa, en azından verilerinizi kurtarmaya yarayan etkili bir yöntemdir. Bilgi güvenliğini ilgilendiren yönü ise çoğu zaman depolama ünitelerinde kesin olarak hangi verilerin olduğunun ve bunların gizlilik derecelerinin bilinememesidir. Yedeğiniz olduğunda ise kaybolan cihazda hangi verilerin olduğunu belirleyebilir ve ona göre elinizden ge-

len önlemi almaya çalışabilirsiniz. Örneğin internet bankacılığına ait şifrelerin veya kredi kartı bilgileri gibi kişisel bilgilerin çalındığını fark ettiğinizde, bankanızı arayıp kredi kartlarınızı iptal ettirebilir ve internet bankacılığı şifrelerinizi değiştirebilirsiniz.

Hırsızlıklar, günümüzde sadece cihazın kendisi için değil, barındırdığı veriler için de yapılmaya başlandı. Bu nedenle mobil cihaz güvenliğinde belki de en etkin yöntemler, çalındığı zaman cihazı ve içindeki verileri değersiz kılan yöntemlerdir.



Kriptolama: Mobil cihazlarda hassas verilerin saklanmaması, saklanacaklarsa da bunun belli standartlara uygun, kriptolu olarak yapılması gerekir. Taşınabilir bilgisayarlar için önemli bir güvenlik önlemi de hard diskteki belirli bir bölümün veya bir dosyanın şifreyle korunması yerine cihazın tam disk kriptolama adı verilen yöntemle şifrelenmesidir. Bu yöntemde hard disk tamamen şifreli olduğundan işletim sistemi üzerinde yapılan her şey otomatik olarak şifrelenerek hard diskte tutulur. Oturum kapatıldığında tüm hard disk şifrelenmiş olduğundan işletim sisteminin tekrar açılabilmesi için doğru parolanın girilmesi gerekir.

Piyasada 256 bit AES ile korunan donanım tabanlı USB flash bellekler ve hard diskler bulmak mümkün. Genellikle şirketler ve kamu kurumları için hayli önemli olan bu ürünlerin bazılarında güvenliği artırmak amacıyla yüksek çözünürlüklü entegre parmak okuyucular bulunuyor. Kaybolmaları veya çalınmaları durumunda, belirli bir deneme sayısından sonra tüm içeriğin kendiliğinden silindiği ürünler de var ve bu ürünler Windows, Linux ve Mac OS işletim sistemlerinde sürücü gerektirmeden çalışıyor. Ayrıca internetten kriptolama için bazı ücretsiz programlar indirmek de mümkün. Yalnız bu programların yayımcıları verilerin bozulmaması yönünde herhangi bir garanti vermiyor.

OLED ekranlı biyometrik USB bellek
www.ennovadirect.com

Günümüzde kişisel bilgisayar güvenliğine yönelik belirli bir farkındalık ve altyapı oluşmuş durumda. Buna karşın mobil cihazlardaki tehlikeler konusunda toplumun genelinde henüz gerekli birikim yok. Bu nedenle mobil cihazlardaki bilgi güvenliğini tehlikeye atan en önemli unsur bu cihazların kullanıcıları ve onlardan kaynaklanan açıklar. Eğer gerekli birtakım önlemler daha önceden alınmamışsa, mobil cihazınızdaki kişisel bilgilerin ve gizlilik derecesi yüksek diğer verilerin yetkisiz kişilerin eline geçmesi nedeniyle uğrayabileceğiniz maddi manevi zarar, sandığınızdan çok daha fazla olacaktır. Yazıda bahsedilen tüm önlemler, risklerin gerçekleşme olasılığını düşüren, riskler gerçekleştiği zaman da etkilerini en aza indiren önlemlerdir. Yoksa riskleri tamamen yok etmek çoğu zaman ya mümkün değildir ya da maliyet etkin bir çözüm değildir. Ancak alınabilecek basit önlemler bile bilgi güvenliği risklerinin gerçekleşme olasılığını hayli düşürecektir.