ÇATLAKTAN SIZANLAR

Bilgisayar Mühendisi Burak OĞUZ
burak@medra.com.tr

Wikileaks ile farkedilen sorun: Bilgi Sızıntısı

Wikileaks Cablegate'in belgelerinin neden olduğu sorular ve tatışmalar süredursun, bu skandalın perde arkasında yatan esas sorun bugünlerde bilgi güvenliği çevrelerinde daha geniş perspektifte konuşulmaya başlanıldı. Bilgi sızıntısı olayları Wikileaks'in özelinde belki büyük bir kitlenin isteği doğrultusunda bir bilgi akışına sebep olmuş olsa da, aslında hergün yaşadığımız bilgi sızıntısı olayları bireysel olarak bizlerin kişisel bilgilerimizin ve kurumsal olarak ticari bilgilerin yetkisiz ellere geçmesini sağlamaktadır. Özellikle kişisel verilerin (kimlik bilgileri, sağlık bilgileri, kredi kartı bilgileri, vb) serbest piyasada işlem gören bir mal haline gelmeye başladı.

İlk önce Wikileaks olayı özelinde bilgi sızıntısının nasıl gerçekleştiğini incelemek gerekmekte. WikiLeaks olayında içeriden sızmalara karşı gerekli önlemler alınmadığı için sızmaların tamamı bilinemiyor. Sadece Bradley Manning adındaki ABD ordusunda görevli istihbarat uzmanı, arkadaşı olduğunu düşündüğü birinin ihbarı sonucunda yakalandı. Ancak Wikileaks ile ilgili diğer sızmaların da içeriden yapıldığına kesin gözüyle bakılıyor. Zira sızan bilgiler, SIPRNet adındaki internetten bağımsız ve dışarıdan saldırılara karşı en üst düzeyde güvenli olan ABD devletine ait bir ağdan çalındı. Bu da gösteriyor ki dışarıdan gelen tehditlere yönelik mevcut güvenlik çözümleri ne kadar sofistike olursa olsun bilgi sızıntısı söz konusu olduğunda bu önlemler tamamen yetersiz kalıyor.

Bilgileri sızdıran istihbarat görevlisi Bradley Manning ise şu şekilde bir açıklama yapıyor. "Üzerinde 'Lady Gaga' gibi bişey yazan bir yeniden yazılabilir CD ile geleceğim... müziği sil... sonra ayrı bir sıkıştırılmış dosya yap. Kimse hiçbir şeyden şüphelenmedi... Muhtemelen ABD tarihinin en geniş bilgi döküntüsünü sızdırırken Lady Gaga'nın "Telephone" şarkısını dinleyip dudaklarımı oynatıyordum."

Bilgi Sızıntısına Detaylı Bir Yaklaşım

Son birkaç yıla kadar kamuoyunda bilinen bilgi güvenliği tehdidi, "hacker"ların kurumların web sitelerine yaptıkları saldırılardan ibaretti. Bu tip saldırılar iş sürekliliğini sekteye uğratıyor ve kurumların itibarını sarsıyordu. Dolayısıyla kamu kurumları ve iş çevreleri bilgi güvenliği yatırımlarını göz önündeki bu tehdidi engelleme yönünde yaptılar. Piyasada yer alan güvenlik çözümleri de genellikle dışarıdan gelen bu tip tehditlere yönelik çözümler olarak şekillendiler.

Ancak bu durum geçtiğimiz bir iki yıl içinde değişmeye başladı. Bilginin artık ülkemiz de dahil olmak üzere sayısal ortamlar üzerinde saklanmaya başlanmasından itibaren, bilgiye erişim yetkisi olan kullanıcıların kazara veya kötü niyetli olarak bu bilgileri sızdırdığı yoğun olarak gözlenilmeye başlandı. Bilgi sızıntılarının maliyetlerini hesaplamaya yönelik birçok araştırma yapıldı.

Datamonitor firmasının yaptığı bir araştırmaya göre, büyük şirketlerde yaşanan her bilgi sızıntısı olayı ortalama 1,8 milyon dolar maliyet oluşturuyor. Üstelik aynı araştırma bu şirketlerin %77'sinin, bilgi sızıntısı olaylarını tespit etme yeteneğinden de yoksun olduğunu gösteriyor. Dolayısıyla bilinmeyen bu maliyet hesaplanan ortalamaya katılamamış. Avrupa Ortadoğu ve Afrika bölgesinde ise 2000 adet küçük ve orta boy şirkette yapılan bir araştırma, bu şirketlerdeki bilgi sızıntısı maliyetinin olay başına ortalama 200.000 pound olduğunu gösteriyor.

Başka bir önemli nokta ise, bilgi sızıntısı olaylarında müşterilerin özel bilgilerinin de sızıyor olması. Müşteriler şahsi olarak zarar gördüğü için bu durum, "hacker" saldırılarından çok daha büyük prestij kaybına yol açıyor. Firmalar doğrudan maliyetlerin ve itibar kaybının yanında, iş ortakları ve müşterileri tarafından açılan davalar sonucunda da yüklü cezalar ödemek zorunda kalıyorlar. Gün geçtikçe çalışanlar arasında kullanımı yaygınlaşan Facebook gibi sosyal ağ servisleri ve bilgi paylaşımını kolaylaştıran her türlü platform şirketler için riskleri arttırıyor. Yakın bir zamana kadar bir çalışan stratejik bir bilgiyi sızdırdığında yapabileceği en kötü şey bu bilgiyi rakip şirketlere ulaştırmasıydı. Ancak bugün bir çalışan şirketinizin her türlü bilgisini kazara veya kötü niyetle sosyal ağ ortamlarında ve diğer internet ortamlarında binlerce hatta milyonlarca kişi ile paylaşabilir.

Bilgi sızıntısı olaylarını diğer bilgi güvenliği olaylarından ayıran başka bir nokta ise, kötü niyetli kişilerin yanı sıra personelin yaptığı kazara aktiviteler

de bu tip olaylara sebep olabiliyor. Proofpoint firmasının yayınladığı bir araştırmaya göre bilgi sızıntısı olaylarının %80' i çalışanların kurumun bilgi güvenliği politikasını bilmemesinden kaynaklanmaktadır. Aynı araştırmaya göre İngiltere'de bulunan kuruluşların %66'sında çalışanlar bilinçli veya bilinçsiz e-posta yoluyla bilgi sızdırmıştır. Ayrıca bu kurumlardaki tüm e-postaların %12'lik kısmının yasal sorunlara yol açabileceği saptanmıştır.

Bilgi sızıntıları şüphesiz ki giderek büyüyen bir sorun. Ancak uygun araçlar, politikalar ve eğitim ile bu sorun ortadan kaldırılabilir.

Yurtdışındaki kurumsal bilgi sızıntısı olaylarının oluşturduğu sorunlar ile ilgili http://datalossdb.org adresinden daha geniş bilgiye erişebilirsiniz.

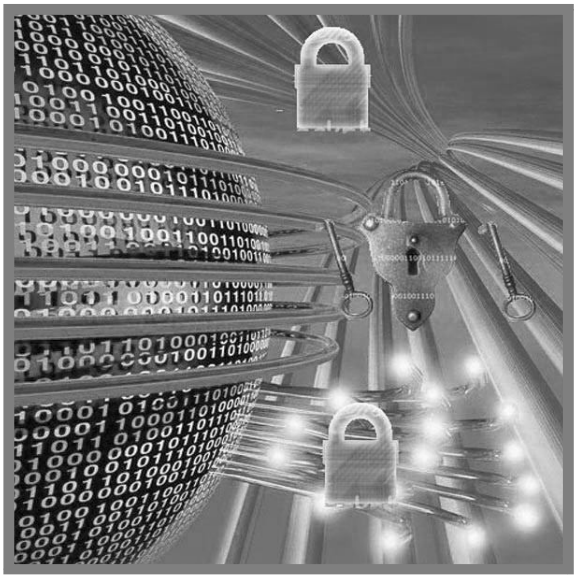
Türkiye'de de bilgi sızıntısı deyince akla gelen birçok olay bulunmaktadır.
1. KPSS sorularının e-posta ile çalınması
2. Milyonlarca kişinin bilgilerinin KEY ödemeleri sırasında İnternet üzerinden dağıtılması
3. Siyasilerin kişilik bilgileri üzerinden yapılan tartışmalar
4. Çalınan TC Kimlik Numaraları

Kişisel Verilerin Güvenliği

Bireysel bilgi güvenliği, hem bireyler hem de kurumlar tarafından özen gösterilmesi gereken bir konudur. Ülkemizde kişisel verilerin korunması konusunda kurumlar üzerinde herhangibir cezai yaptırım bulunmasa da Anayasa'nın yeni değişen 20. Maddesi diyor ki;
"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 islenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

2008 Ekim ayından itibaren TBMM Adalet Alt Komisyonunda görüşülen "Kişisel Verilerin Korunması Kanun Tasarısı"nda ise başta sağlık kurumları olmak üzere kişisel veri işleyen tüm kamu ve özel kurumlara bu verileri koruma görevi verilmiştir. Bu tasarının yasalaşması ile kişisel bilgilerin korunamaması cezai yaptırıma neden olacak.

Bunların yanında özellikle Sağlık Bakanlığı başta olmak üzere birçok kurumun iç hizmetlerinde kullandıkları bilgi işlem politikalarında kurumsal ve kişisel bilgilerin gizliliğine önem gösterilmesi gerekliliği vurgulanmaktadır. Diğer bir nokta ise 4857 sayılı İş Kanunu'nun 75. Maddesi gereği işverenler, çalışanlarının, kendileri ile ilgili bulunan kişisel verilerini korumakla yükümlüdür.



Kurumsal Bilgi Güvenliği Nasıl Sağlanmalı?

Öncelikle genel olarak bilgi teknolojisini sadece bir maliyet kalemi olarak değil bir yatırım olarak görmeniz gerekiyor. Özellikle bilgi güvenliği alanına doğru bir şekilde yapılan yatırım kurumunuzu risklerden koruyarak iş sürekliliğinize ve karlılığınıza doğrudan katkı yapacak, kurumunuzu itibar kaybından ve yasal sorunlardan kurtaracaktır.

Bilgi güvenliği konusunda çok basit bir test de yapılabilir. Öncelikle gidip rastgele bir personel bilgisayarının başına oturun. Bilgisayar üzerinde stratejik plan, mali rapor, ihale teklifi ya da firma için önemli olan ve üçüncü kişiler ile paylaşılması sorun yaratacak herhangi bir dosyayı seçin. Son olarak da bu dosyayı bir USB Bellek'e kopyalamayı deneyin veya dışarıdaki kendi mail adresine e-posta'ya ekleyip göndermeyi deneyin. USB Bellek'e kopyalayabiliyorsanız, e-posta ile gönderebiliyorsanız ya da böylesine basit herhangi bir yöntemle bu belgeyi dışarı çıkarabiliyorsanız, bilgi güvenliği konusunda firmanızın eksikleri var demektir. Bilgi sızıntısı tehditlerine karşı savunmasızsınız demektir.

Bunun dışında, bilgi sızıntılarının tam bir uyum ile engellenebilmesi için öncelikle kurumunuzun bir bilgi güvenliği politikasına sahip olduğundan ve bunu uygulandığından emin olun. Bu politikada kurumunuzda hangi bilgi tipleri işlenir, bu bilgiler nerelerde tutulur ve gizlilik dereceleri nedir, hangi kişiler bu bilgilere erişebilir, bu kişilerin görev ve sorumlulukları nedir, hangi koşullarda bilgiler diğer kişi veya kuruluşlarla paylaşabilir gibi soruların cevapları mutlaka olmalıdır. Bu politikanın sadece bilgi işlem personeli değil tüm personeliniz tarafından benimsenmesi ve gerekli iç ve dış denetim mekanizmalarının oluşturulması politikanın başarılı olması için gereklidir. Bu konuda COBIT gibi en iyi uygulamalar ve ISO 27001 gibi yayınlanmış kapsamlı standartlar bulunmakta, kurumunuzda bu standartları uygulayabilirsiniz.