

“Şirketler daha açık olmalı”

RSA'deki güvenlik açığı, Prof.Dr. Koç'a göre tüm şirketleri bu konuda açık konuşmaya itiyor. Ama teorideki bu gereklilik, pratikte pek uygulanmıyor.

Handan AYBARS



İmajı toparlamak zor olacak



İstanbul Şehir Üniversitesi'nden Prof.Dr. Çetin Kaya Koç, cihaz ve tanımlama teknolojisi odaklı bir çalışma yaptığını söyledi.

Prof.Dr. Çetin Kaya Koç'a göre, RSA'e saldırının arkasında profesyonel bir ekip, bunun da arkasında büyük bir devlet var. Saldırılan noktalardan birinin Lockheed Martin olmasının, ne kadar ciddi ve planlı bir hareket olduğunu gösterdiğine dikkat çeken Koç, şu önerileri yaptı: “Müşteri bilgisi, parola ve şifre bilgisi gibi bilgilerin sunucularda bir şekilde tutulduğu çözümlerden kaçınmak gerek. En iyi çözümler; cihaz-kullanıcı-bulut işbirliği ile çalışan işbirliği içinde çalışan ve bulutta kesinlikle kişisel değerli bilgileri tutmayan çözümler.”

EMC'nin güvenlik şirketi RSA'deki açık son ayların önemli gündem maddesi oldu. Lockheed Martin'in saldırı girişimini haber vermesi, RSA'nın SecurID çözümünü kullanan şirketleri de alternatif çözümlere itmeye başladı. Reuters'in 8 Haziran tarihli haberine göre, SecurID yaygın olarak kullanılan elektronik bir anahtar. Bilgisayar saldırganlarını uzak tutmak için de iki şifreli giriş sistemi uygulanıyor. Bunlardan biri sabit, diğeri ise güvenlik sistemi tarafından otomatik olarak birkaç dakikada bir üretilen şifreler. RSA'ı sarsan olay; Mart ayında haklayıcı SecurID cihazların etkisini azaltabilecek ve kurumsal bilgilere erişim olanağı sunabilecek bilgilerin çalındığını açıklaması ile başladı. İkinci darbeyi de RSA'den çalınan teknolojiyi kullanarak Lockheed Martin'e girmeye çalışan haklayıcılar vurdu. RSA, 6 Haziran'da 30-40 milyon adet SecurID kartını değiştireceğini bildirdi.

Hisse satışı soru işareti

Reuters'in haberine göre RSA, EMC'nin toplam gelirleri içinde küçük bir paya sahip. Ama RSA ile ilgili haberlerin EMC'nin borsadaki eğilimini etkilediği bir gerçek. Bir ilginç durum da; Lockheed saldırıları araştırırken, RSA Yönetim Kurulu Başkanı Art Coviello'nun da 24 Mayıs'ta bir işlemle 1.44 milyon dolar EMC hissesi satması. Reuters, bu konuda Coviello'dan bilgi alamamış. EMC sözcüsü Michael Gallant da hisse satışı konusunda yorum vermek istememiş. Sektör uzmanlarına göre bu güvenlik anahtarlarını yenilemek için geç olabilir ve birçok şirket, farkında olsun ya da olmasın, verilerine izinsiz erişimden olumsuz etkilenmiş olabilir. İstanbul Şehir Üniversitesi'nden Prof. Dr. Çetin Kaya Koç, RSA'nın 1978 yılında ARS algoritmasını bulan üç mühendisin şirketi olduğu bilgisini verdi. Tüm dünyada elektronik imzanın

temelini bu algoritmanın oluşturduğunu söyleyen Koç, “1970'lerin sonunda bu mühendisler bir şirket kurdu ve ben de bu şirketin 11'inci çalışanı oldum” dedi. Sistem şöyle çalışıyor: Örneğin internet bankacılığında kişiye ait bir şifreye ek olarak, 6 haneli bir sayı da giriliyor. Bankanın sunucusu bu sayıların nasıl değişeceğini biliyor, algoritmaya hakim. “Sürekli 6 haneli sayı üreten bir yapı var. Bu sayıyı, nasıl bir sayının takip edeceğini tahmin etmek de imkansız” diyen Koç, şöyle devam etti:

“Bu sayılar kendi içlerinde bir metodoloji, bir 'şifreleme algoritması' ile sistem içinde üretiliyor. Bu rakamların nasıl değişeceğini algoritmasını sunucu da biliyor. Zaten elinizdeki cihaz ve sunucunun verdiği sayı uyuşmazsa, giriş izni de verilmiyor. Sizin cihazınızı çalıp giriş yapmak istersem, siz çalındığını fark edip kayıp bilgisi verir ve benim girişime engel olabilirsiniz. Ama maalesef bu durumda; anahtarlar belli bir metotla üretilmiş ve gizli anahtarlar da seri numaraları. Hatta bu numaralar bir tablo halinde tutuluyordu. Amaç; anahtarın tehlikeye düşmesi halinde bunun bulunması ve devre dışı bırakılmasıydı. Bu bilginin, internet bağlantısı olmayan, güvenli bir bilgisayarda tutulması gerekirdi. Oysa bunlar ağda bir yerdedi. 17 Mart'ta birileri bu listeyi çaldı. RSA önce inkar etti, sonra bunun önemsiz bir durum olduğunu söyledi, ama sonra Lockheed Martin, 27 Mayıs'ta saldırı bilgisini verdi.”

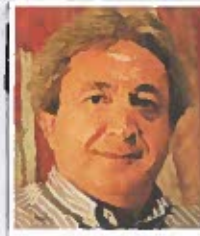
Yeni anahtar çözüm (mü?)

Elinde liste olanlar boş bir SecurID anahtar alıyor, seri numarasını yazıyor ve elinde liste olduğu için, bir başkasının anahtarının aynısını üretiliyor, gerçek anahtar sahibi gibi giriş yapabiliyor. Birçok insan bu durumun farkında değil. Bu yüzden kimlerin saldırıya uğramış olabileceğini bilmek zor. Koç, şöyle devam etti:

“RSA yeni bir liste, yeni cihazlar yapar, herkese gönderir, tamam. Ama yine çaldırılmaması lazım. Bu alandaki diğer şirketler de aynı metodolojiyi kullanıyor. Yani bu, RSA Security'ye has bir problem değil. Bu yüzden genel olarak yedeklenmesi gerekmeyen çözümlere bakmalıyız.” Kaç şirketin bu sorunla karşılaştığını bilmek zor. Çünkü, Lockheed Martin'in yanında, daha az ciddi

saldırıya uğrayan, hatta saldırıya uğradıysa bile bunu fark etmemiş veya bilinmesini istemeyen şirketler de vardır. Türkiye'de SecureID çözümünü kullanan şirketle konuştuğunu belirten Koç, onların da yavaş yavaş sistemden çıkmaya başladığı bilgisini verdi. Bu tabloda RSA, yeni seri numaraları ile yeni kartlar üretecek.

handana@interpromedya.com.tr



ASAL FAKTÖRLER

RSA SecurID ve Lockheed Martin

ÇETİN KAYA KOÇ koc@sehir.edu.tr

Son birkaç aydır, casus romanlarına ait gibi gözükten olay ve haberler güvenlik dünyasını etkiledi. Önce Mart ayı ortalarında, RSA şirketinin yeni sahibi EMC şirketi ileri düzeyli bir siber saldırıya uğradıklarını ve saldırının RSA SecurID denilen iki-faktörlü donanım anahtarlarının (token) altyapısını hedeflediğini ve bazı bilgilerin çalındığını açıkladı. Türkiye'de de kullanılan bu anahtarlar, üzerindeki minik düğmeye basıldığında kullanıcı için 6-8 rakamlı bir sayı üretiliyor; kullanıcı da bu sayıyı şirket bilgisayarlarına veya internet bankacılık hesabına girerken parola olarak kullanıyor. Sunucu ile senkronize olan bu sayılar dizisi, böylece sunucunun bu anahtarın sizde olduğuna emin olmasını sağlayarak, size erişim hakkı vermesini sağlıyor. Üretilen sayılar, genellikle bir önceki kullanımdaki sayı veya anın zaman bilgisi (gün-saat-dakika) gibi bilgileri bir blok şifreleme algoritması ile şifreleyerek elde edilmekte. RSA şirketi bir bildiri yayınlayıp, müşterilerimiz bundan etkilenmedi, dedi. Ancak, böyle düşünmeyenler çok. Eğer, saldırıyı yapan kişiler ve kurum, SecurID şifreleme anahtarını elde etmişse, bundan en azından belirli bir grup SecurID kullanıcıları etkilenecektir. Bu olaylar, Mart ve Nisan aylarındaydı. Herkes hepsi bu kadarmış, diye düşünürken, 28 Mayıs günü, ABD'nin en prestijli savunma şirketlerinden Lockheed Martin, çok ciddi bir saldırıya uğradıklarını, ancak hızla hareket ederek, sistemlerinin güvenliğini sağladıklarını açıkladılar (herhalde, sistemleri devre dışı bıraktık demek istiyorlar). Gerçekten de ciddi bir saldırı olduğu belli ama, ABD'deki savunma şirketleri nerdeyse her hafta böyle şeylerle meşguller. Burada ilginç olan şey: adının yazılmasını istemeyen bir görevli, saldırının sahtesi yapılmış RSA SecurID anahtarlarıyla login olan (veya olmaya çalışan) kişiler tarafından yapıldığını belirtti. Lockheed Martin sistemlerinde, savunma bakanlığına ait çok değerli bilgiler olduğunu sanılıyor. Küçümsenecek bir olay, basit hacker saldırısı olmadığı belli. Gördüğünüz gibi, Mart ve Nisan aylarındaki EMC/RSA saldırısını alıp, Mayıs ve Haziran aylarındaki Lockheed Martin saldırısına iliştiirseniz, güzel bir John Le Carre romanı ortaya çıkabilir!