İstanbul'da Kevin Mitnick Konferansı

19-20 Mart 2002 tarihlerinde İstanbul'da gerçekleştirilen Bilişim Sistemlerinin Güvenlik, Denetim ve Kontrolü Konferans ve Fuarı (SACIS 2002), açılışında video konferans yoluyla Amerika'dan ilginç bir konuşmacıyı ağırladı: Kevin Mitnick. Mitnick, geçmişinde bilgisayar ve iletişim sistemlerinde tespit ettiği zayıf noktaları kullanarak çeşitli zararlara neden olmuş ve Pentagon dahil birçok bilgisayar sistemine sızmayı başarmış bir bilgisayar korsanı. Hatta bu aktiviteleri nedeniyle vaktinde FBI tarafından fotoğraflı afişi bile basılmış ve işlediği bilişim suçlarından ötürü de birkaç kez hüküm giyerek hapsin yolunu tutmuş. Mitnick'in geçtiğimiz yıllarda tamamladığı son hapis cezasını takip eden şu zamanlarda, mahkemece kararlaştırılmış gözetim ve rehabilitasyon programı çerçevesinde bilgisayar ve cep telefonu kullanması kanunen yasaktı. Dolayısıyla Mitnick, konferans sırasında elinde teknik ekipmanlarla bu işlerin nasıl yapıldığı üzerine somut örnekler vermek şansına sahip değildi. Ancak sorulan sorulara verdiği cevaplarla bilgisayar sistemlerinin güvenliği konusunda herkesin ilgisini çekebilecek detaylara değinerek, deneyimlerini bizimle paylaşmaktan geri durmadı.

Mitnick, iletişim ve bilgisayar ağlarına sızma girişimlerine ilk kez 1980'li yılların başlarında telefon operatörleriyle başlamış. Operatörlerin kodlarına erişerek otomatik santrallerin cevap metinlerini esprili ve kafa karıştırıcı ifadelerle değiştiren, istediği hatları ücretli veya ücretsiz hale getirebilen ve bu şekilde sistemdeki iletişim ağını kontrolü altına alan Mitnick, küçükken yalnız ve toplumunun dışında kalmış biri olarak bu tür şeylerle uğraşmanın kendisini güçlü hissetmesini sağladığını söylüyor. Ancak zaman içinde özellikle bilgisayar sistemlerine yapılan saldırıların getirdiği maddi ve manevi zararlar, insanların bu olguya bakış şeklini değişime uğratmış. "İlk zamanlarda bu tür işlerle uğraşabilecek yeteneği olanlara kahraman gözüyle bakılırdı" diyor Mitnick; "ancak bugün bunlar birer suçlu olarak nitelendiriliyor".

Bilgisayar Korsanı (Hacker) Nedir?

Bilgisayar korsanı, bilgisayarlar konusundaki bilgilerini sistemlerde güvenlik açıkları aramak için kullanan ve bu yolla bilgisayar sistemlerine sızarak içeriğini kontrol altına alan kişilere verilen genel bir isimdir. İçeriğin kontrol altına alınması sonucunda sistemin zarara uğratılması, sistemden habersiz bilgi aktarılması veya sistem yönetiminin ele geçirilmesi gibi aktivitelerden bir veya birkaçının korsanın niyetine ve sistemin özelliklerine bağlı olarak gerçekleştirilmesi mümkün olabilir. Bilgisayar korsanının yaptığı bu sisteme sızma işine ise hack adı verilir.

Mitnick'e göre bilgisayar korsanları ikiye ayrılıyor. Sistemlerde güvenlik açıkları bularak bunları sisteme zarar vermek amacıyla kullananlar, ve sistemlerdeki olası güvenlik açıklarını tespit ederek sistemi daha güvenli hale getirmeye çalışanlar. Bunlardan ilk gruba dahil olanlar bilgisayar korsanı (ya da hacker) olarak adlandırılırken, ikinci gruba dahil olanlar güvenlik danışmanı gibi isimler alıyorlar. Mitnick, ilk kategoriye dahil olanların, genellikle gündüz uğraşacak başka işleri olan ve gece vakti bilgisayarını açıp bu tarz işlerle vakit geçiren, yaşı küçük gençlerden olduğunu söylüyor. Tanımlarını da kabaca "bütün gün hayatın olağan işleriyle uğraştıktan sonra, akşam bilgisayar başında kendilerine ve başkalarına güçlü olduklarını ispatlamaya çalışan kişiler" olarak yapıyor.

Mitnick, günümüzde şirketlerin hızla Internet'e açılmasıyla beraber son derece değerli bilgilerin de bu ağın bir parçası haline geldiğini, dolayısıyla bunları korumak için güvenliğe ayrı bir önem verilmesi gerektiğini söylüyor. Mitnick'e göre sistem güvenliği çözümü bir ürün değil, üç aşamalı bir süreç: korunma, tespit ve reaksiyon. Bu üç sürecin birbiriyle bağlantılı olarak düzgün bir şekilde işletilmesinin sistem güvenliği için son derece faydalı olduğunu söylemekle birlikte, sistem güvenliğini etkileyen asıl unsurun insan olduğunun özellikle altını çiziyor. "Yaptığımız iş esasında bir aldatmacadan ibaret" diyor Mitnick; "siz istediğiniz kadar sistemlerinizi dışarıdan gelecek saldırılara karşı koruma altına alın, içeriden bir tanıdık sayesinde bütün koruma engelleriniz kolayca aşılabilir".

Peki cezası bittikten sonra Kevin Mitnick ne yapmayı planlıyor? Mitnick bu soruya "elbette ki yeteneklerimi bilgisayar sistemlerini korumak için kullanabileceğim bir işin arayışına gireceğim" diyor. Kısaca Mitnick'in şu andaki düşüncesi, bir zamanlar sistemlere sızmak ve zarar vermekle uğraşmış olup da, sonradan sistem güvenliği danışmanı sıfatıyla yeteneklerini güvenlik açıklarının bulunup kapatılmasına adamış "gri şapkalılardan" olmak. Bakalım Mitnick 2003 yılında cezasını tamamlamasının ardından verdiği bu sözü tutabilecek mi...

Levent Daşkıran

Devlet Eliyle "Korsanlık" Mantıklı mı?

SACIS 2002 fuarında eski bilgisayar korsanlarından bir isim daha vardı: John Draper, ya da bilinen takma adıyla Captain Crunch. John Draper, bir şekerlemenin içinden çıkan oyuncak düdüğün çıkardığı 2600 hertz'lik sinyalin, Amerika'daki eski telefon sistemlerinde ücretsiz telefon görüşmesi yapabilmek için gerekli onay koduna denk olduğunu bulan ve bu sayede bu işlerin temelini atan kişinin ta kendisi. Hatta Kevin Mitnick'in 1980'lerin başında telefon santrallerine sızmak için kurduğu ekibinin kullandığı takma isimlerden birinin John Draper olduğu biliniyor. SACIS 2002'ye konuşmacı olarak katılan Draper, şu ara ShopIP adıyla kurduğu firmasında kendi oluşturduğu güvenlik çözümlerini pazarlamakla meşgul.


John Draper

Konferans sırasında Draper, Mitnick'e FBI'ın Magic Lantern projesiyle ilgili ne düşündüğü şeklinde bir soru yöneltti. Magic Lantern projesi, FBI tarafından belli kurum ve kişilerin iletişimini kontrol altına almak için tasarlanmış bir tür casus programla ilişkili bir proje. Bu program, bilgisayar sisteminin içine koyulduğunda kullanıcının tuş vuruşlarını tek tek kaydediyor ve sistem dışına gönderiyor. Bu tuş vuruşları kullanıcının sadece ne yazdığıyla ilgili bilgileri değil, aynı zamanda erişim yaptığı sistemlere dair isim ve şifre bilgilerini de olduğu gibi kaydettiği için, bu bilgilerin gönderilmesi; kullanıcının her türlü şifresinin karşı tarafa iletilmesi anlamına geliyor. Kısaca buna bir bakıma devlet yararına casusluk da denebilir. Ancak Mitnick, soruya verdiği cevapta bu tür bir projenin oldukça tehlikeli olduğunu savunuyor ve bence de haklı. "Sonuçta bu tarz bir uygulama bir başkasının eline geçerek bambaşka amaçlar için kullanılabilir. Bunu kontrol altında tutamazsınız".

Açıkçası bu projenin varlığı ve FBI'ın da bunu onaylamış olması, devletlerin ellerindeki bilişim olanaklarını kendileri için avantaj sağlamaya yönelik kullanma potansiyeli olduğu yönünde ciddi bir gösterge. Ayrıca ortalıkta bu kadar meraklı varken eğer siz bir yerden açık gösterdiyseniz, bunun hangi amaçlar için kullanılacağını kestirmeniz oldukça zor. Bu konu aslında hem araştırmaya, hem de spekülasyona gayet açık bir konu. Sonuçta dünya çapında kullanılan bazı yazılımların, üretildiği ülke hükümetine yarar sağlamaya yönelik bilgileri aktaran bir takım bilinmeyen güvenlik açıklarıyla donatılıp donatılamayacakları konusunda ne Mitnick, ne de Draper kesin bir cevap verebiliyor. Konu aslında spekülasyona çok açık ve bilgisayar sistemlerinin güvenliği sözkonusu olduğunda, okunacak şeylerin haddi hesabı yok. Ancak dileyen meraklılar, yola Security Focus Web sitesinden başlayabilirler. (www.securityfocus.com).

Daha Fazla Bilgi İçin:

http://www.sacisexpo.com (SACIS Konferans ve Fuarı ana sayfası)
http://www.takedown.com/bio/#Kevin (Kevin Mitnick'in biyografisi)
http://www.discovery.com/area/technology/hackers (Mitnick ve Draper Discovery listesinde)
http://www.shopip.com/crunch_bio.html (John Draper'in biyografisi)
http://news.com.com/2102-1001-276976.html?legacy=cnet (FBI'ın Magic Lantern'i kabul ettiğine dair haber)
http://www.securityfocus.com (Sistem güvenliğine dair başlıklar)
http://www.shopip.com (John Draper'in güvenlik çözümleri şirketine ait Web sayfası)