13 - 19 Aralık 1999
Sayı: 247

Internet'in Yaramaz Çocukları; Hacker'lar

Internet dünyasının vazgeçilmez aktörleri "Her sisteme lazım" hacker'lar kendilerini iyi niyetli, meraklı, zeki, sürekli kendini aşman insanlar olarak tanımlıyorlar. "Kötü niyetli olanlara hacker değil doğrudan onlara **bilişim** veya **bilgisayar suçlusu** diyoruz. Sanayi casusluğu yapan bilgisayar uzmanları bunlara iyi bir örnek" diyen hacker'lar kendilerinin mevcut sistemlerin boşluklarından girip sistemin güçlenmesi için önerilerde bulundukları bazen de sistemlerin açıklarını bizzat kapattıklarını söyülyorlar.

Gamze GÖKER

Görüştüğümüz üç hacker da kendini tanıtmak istemediği için yazıda onların takma ad(nick name)larını kullanacağız. Önce hacker'ın tanımını hacker'ların kendisine soralım dedik ve yanıtı Wideman'den aldık: "**Hacker'lar** kendilerini asla deşifre etmeyen, sistemleri bir sistem yöneticisi kadar hatta daha da fazla bilen ve bu mevcut sistemlerin boşluklarını bulmaya çalışan kişiler. Bu sistemlerin boşluklarını ortaya koyan exploit dediğimiz minik programcıklar yazıyorlar. Bir de bu baba hacker'ların çıkartmış olduğu exploit'leri kullanarak sistemler üzerinde yıpratma çalışması yapan **cracker** dediğimiz kişiler var. Internet'ten önceki dönemde kullanılan yazılımların şifrelerini kırmaya da 'crack' deniyordu. Ama günümüzde cracker olarak nitelendirdiğimiz kişiler gerçek hacker'ların çıkarmış olduğu exploit'leri kullanarak sistemlerin boşluklarından yararlanarak sistemlere giren insanlar.

Genel anlamda hacker'ların amacı boşluk bulmak, yeni şeyler keşfetmek ve hedefledikleri işletim sistemini mümkün olduğunca güvenli hale getirmek."

Bir de herkesin çekindiği, zarar veren hacker'lardan söz edelim deyince Wideman düzeltti: "Kötü niyetli olanlara hacker değil doğrudan bilişim veya bilgisayar suçlusu diyoruz. Sanayi casusluğu yapan bilgisayar uzmanları bunlara iyi bir örnek. Bunlar da hacker olarak geçiyor. Bir biçimde bilgisayar sistemlerine sızarak yeni tasarlanan bir kayıt cihazının mikrofilmlerinin sayısal kopyalarını ele geçirip bunu pazarlamak da bir **bilişim** suçu sayılır. Yani mutlaka Internet üzerinden gitmek gerekmiyor. ABD'de, Rusya'da birçok örneği görüldüğü gibi bankaların sanal POS sistemlerine sızarak para çalmaya çalışanlar var. Bunlar hacker düzeyinde bilgi sahibi olan suçlular. Bunları ben hacker olarak nitelendirmiyorum."

Wideman, Türkiye'de hacker olarak nitelendirilebilecek insanların yüzde 90'ının halihazırda bu piyasada sistem yöneticisi olarak çalışan kişiler olduğunu söylüyor.

"Hacker deyince insanların aklına Matrix filmindeki Neo gibi biri geliyor Benim evimde bilgisayar bile yok. İşten saat 6-7'de çıkıyorum, geziyorum, dolaşıyorum, evime gidiyorum" diyen Baxter bu imajdan rahatsızlık duyduğunu da belirtiyor.

"En güvenli finans sektörü"

Hacker'lar, Türkiye'deki sektörlerin sistemlerini en güvenli ve en güvensiz olarak ayırıyorlar. Wideman en güvenli bulduğu finans sektörünü ve bu sektördeki ilk deneyimlerini şöyle anlattı: " Türkiye'de bankalar ilk Internet bankacılığı yapmaya başladıklarında "durumları nedir?" diye bir yokladım. Web sitesi tasarım hatalarından kaynaklanan güvenlik boşlukları vardı. Bir java applet'inin doğru çalışmaması ya da web sitesini ana sistemle entegre eden minik ara yazılımdaki minik programlama hatalarından dolayı komik suistimallerde(abuse) bulunabiliyordunuz. Bir keresinde 240 karakterli bir ad soyad doldurarak hesap açtım. Ben keşfettikten yaklaşık yarım saat sonra sistemi yamadılar."

Hacker'lara göre başında ilgilenen kimse olmadığından kamuda en güvensiz sistemler üniversitelerin sistemleri. Doğal olarak hacker'lar da kendi işlerini yapmak için rahatlıkla girip çıkıyorlar. Nemesis bir hobisini bu yolla sürdürüyor: " Ben müzikle ilgilendiğim için sürekli bir müzik arşivi oluşturuyorum. Bunun için hızlı bir hattı ve büyük bir diski olan bir sistem lazım. Bu sistem en iyi üniversitelerde olduğu için ODTÜ

Nemesis, özel sektörün sistemlerini daha güvenli hale getirmeye başladığını ancak kamu sektörünün çok kötü durumda olduğunu da söylüyor: " Onlara acıdığımız için sisteme girip düzeltip çıkıyoruz. Sistemden sorumlu olan kişi benim girip çıktığımı bile fark etmiyor. Benim düzelttiğim yerden bir daha kimse giremiyor çünkü düzeltip çıkıyoruz. Herkes kendi bilgisi dahilinde güvenliğini sağlayabilir."

"Bir finans kurumuna asla saldırmam"

Wideman bir sisteme girip problemlerini gördüğünde genellikle uyarıyor ama bazen de hızlı adımlarla bir anlamda hemen oradan uzaklaşıyor. "Örneğin. bir keresinde bir üniversitenin sitesine girecektim yanlışlıkla başka bir numara çevirip bir bankanın pos cihazlarının şehiriçi çevirdiği numaralardan birini düşürmüşüm. Sayısal bir santralden bağlı olduğumu anlayınca korkudan bilgisayarı şalterden kapatıp hemen oradan uzaklaştım. Karşınızdaki bir kamu kurumu veya üniversite olunca korkmak gerekiyor. İMKB, bir borsa aracı kurum veya banka sistemine yani bir finans kurumuna asla saldırmam."

Nemesis, sistemini kırdığı bir yerden daha sonra sistem yöneticiliği teklifi de almış: "İki yıl önce İzmir'de bir özel lisenin sistemini kırmıştım. Sonra sistem yöneticisi bana sistemlerini yönetmemi bunun karşılığında da hacking işini öğretmemi istedi. Anlaştık. Bir buçuk iki yıl onların sistemini yönettim. Ayrıca geçtiğimiz dönemlerde Askeri sitelere girip ana sunucunun adını Nemesis yapıp çıkmıştım. Altı ay boyunca bunu farketmediler. Fark ettikten sonra da bunu silemeyip Netmask'e yönlendirdiler. Sanırım o isim hala orada duruyor."

Baxter da Bilkent Üniversitesi'nin sistemine dışarıdan giremeyince atlayıp otobüse Bilkent'e gitmelerini ve orada yaptıklarını şöyle anlatıyor: "Kütüphane laboratuarında Internet yasak. Kitap arama programını kurcalarken bir şekilde shell yani komut satırına düştük. Oradan telnet çektik. Bilkent'i kendi içinden kırdık. Yani firewall'ı ayaklarımızla aşmış olduk."

Nerelere saldırmak eğlenceli? Bu sorunun ortak cevabı: Medya kuruluşları. Wideman'in anlattığına göre hepsi çok güvenliksiz. Milliyet gazetesinin sitesini birileri 'indirdikten' sonra Milliyet'in ISS'i DorukNet çok ciddi bir güvenlik yatırımı yapmış, ayrıca SCO sunucusu güncellenmiş. Şimdi artık amatörler giremiyormuş.

"En iyi güvenlikçi eski hırsızdır"

İyi bir hacker olmak için Unix'i iyi bilmek gerektiğini hatırlatan Wideman'e 'Sınır tanımaz' hacker olarak hangi sistemin güvenli olduğunu sorduk. " En iyi güvenlikçi eski hırsızdır" dedi ve başladı anlatmaya: "Kullanımı kolay olduğu için genellikle NT tercih ediliyor. Ben bir veritabanı kurup üzerine milyon dolarlık para akacak sistem kuracaksam NT de almam, Linux da. Eğer Internete bağlı değilseniz yani bir intranet ya da LAN iseniz ve PC sunucu kullanıyorsanız, risk işlemciler kullanmıyorsanız kesinlikle SCO kullanmanızı öneririm. En azından göçtüğü zaman karşınızda bir muhatabınız var. "Peki bir sistemin güvenli olması için neler yapılması gerekiyor?": "Bir sistem yöneticisinin öncelikle yapması gereken öncelikle sistemi dizayn etmektir. Bir aracı kurumun sistemini yönetiyor olsam işletim sisteminde SCO kullanırım. Onun üzerinde Oracle, SQL veya Informix veritabanı çalıştırırım. Eğer bir finans kurumunda PC tabanlı bir sunucu kullanıyorsam üzerinde Linux değil SCO çalıştırırım. Ve kesinlikle personelimi eğitirim. Son kullanıcı dahi sistemde bir arıza çıktığında anında müdahale edebilecek kadar o sistemi bilmeli. Aslında Türkiye'deki işletim sistemlerinde ya da ağlarda bir problem yok. Sistemler yanlış veya eksik dizayn edildikleri için güvensizler. Dünyanın en pahalı güvenlik yazılımı AltaVista firewall'u kullandığı halde yanlış kurulduğu için güvensiz olan sistemler gördüm. Ama öyle sistemler de gördüm ki iki bilgisayar, bir modem ve bir yönlendiriciyle bir hosting firması çalıştırıyor. Oraya aylarca uğraşsan giremezsin, çünkü sistemlerini optimize etmişler."

Nemesis bu dizayn hatasına örnek olarak TurNet'i gösteriyor. Sisteme çok rahat girip çıktıkları ve tekelciliğinden dolayı her zaman karşı oldukları TT'yle yaşadığı problemi şöyle anlatıyor: " Ben bir öğrenci olarak hem ISP'ye ayda 20 dolar hem de telefon faturasına10 milyon ödeyemem. Buna karşı çıkmak için kendime bir abonelik hesabı açtım. Diğer sistemdeki abonelikleri arkadaşlarıma dağıttım. Bunun hakkında bazı yazılar çıkıp bunu parayla sattığımı iddia ettiler. Oysa ben bunları arkadaşlarıma ücretsiz olarak dağıtmıştım. Sonra evime telefon açıp beni dava edeceklerini söylediler. Daha sonra ilişkiyi biraz düzelttik. Bana iş teklifinde bulundular. Okuldan dolayı kabul edemedim."

Wideman ise TT'yi şöyle değerlendiriyor: " Minik hatalarının dışında TTNet'in gerçekten güzel bir sistemi var. Kesinlikle iyi niyetle hazırlanmış. Bunun yanında Türk Telekom transmisyon açısından kendinden kaynaklanan problemleri bulunan bir sistem."

“Internet’i geliştiren partiye oy veririm”

Baxter “Internet’i hangi parti geliştirirse ona oy veririm” deyince Wideman bunun çok yaygın bir görüş olduğunu, Internet’i geliştiren partinin şu an 2/3’ü oy verme yaşında olan, Internet kullanan 250-300 bin kişinin oyunu alacağını söyledi ve bir öneride bulundu: “ Bence bir bakanlık kurulmalı ve Mahşerin Dört Atlısı: Mustafa Akgül, Ethem Derman, Atilla Özgit ve Ufuk Çağlayan’dan biri Bilişimden Sorumlu Devlet Bakanı olmalı.”

BT haber Online
e-posta:
bthaber@interpro.com.tr

13 - 19 Aralık 1999
Sayı: 247