ELEKTRONİK CASUSLUK

İleri elektronik çağı, sanayi casusluğunu zorlaştırıyor.

Kelly COSTIGAN

Poly Trancs Security Corporation adlı bir dedektif firmasının genel müdürü Doug Kelly, "1983 yılında büyük müteahhit firmalardan biri 200 milyon dolarlık bir ihaleyi, sadece birkaç bin dolar fark yüzünden kaybetmişti. Kazanan teklifin, kendi tekliflerine, rastlantının ötesinde çok yakın olması, şüphe uyandırmış ve bize başvurmuşlardı" diyor. Gerçekten de araştırma sonucu, toplantı odasının tavanına saklanan ve yöneticilerin konuşmalarını erkekler tuvaletine yerleştirilen teype aktaran bir mikrofon açığa çıkarılmıştır.

Olay, tümüyle tipik bir nitelik taşıyor: Sanayi casusluğu yeni bir olay değildir; ancak ortada milyonlarca dolar bulunması, casusluk teknolojisinin gittikçe daha karışık bir durum kazanmasına yol açıyor. Burada hedef, yalnızca iş hayatı değildir. Film yıldızları, antrenörler ve politikacılar da gizli dinleme hedeflerinin adaylarıdır. Elektronik casusluğuna karşı korunmada uzmanlaşmak da firmaların hedefi haline dönüşmüştür.

Elektronik dinlemenin birçok çeşiti vardır, fakat şimdiye kadar en çok rastlananı telefonla bağlantı kurarak dinleme olmuştur. New York CCS Communication Control Inc. firmasından Peter Savale, "Şüphesiz telefonla bağlantı, bir büroya dinleme cihazı yerleştirmekten çok daha kolaydır. Başında beyzbol şapkası, üzerinde tişörtle gelen bir adam, telefon hattını tamir etmeye geldiğini söyleyebilir. Birçok firma da bu oyuna gelir" demektedir.

Casuslar telefonları, ya doğrudan telefon hattına girerek, ya da dolaylı yoldan izleyebilir. Bunların ilki, telefon hattını fiziksel olarak keserek bağlantı kurma şeklinde olmaktadır. Savale, AT&T hatları, telefon ahizesi kapalı durumdayken 48—52 Volt, açık durumdayken 6—8 Volt taşıyor" demektedir. Eğer bir voltaj detektörü bu değerlerden sapma gösteriyorsa; bir şey, muhtemelen bir dinleme aygıtı enerji çekmektedir.

Dolaylı yoldan izleme yapan dinleme aygıtları indüksiyonla çalışırlar; bu nedenle enerji çekimi görülmez. Aygıtı yerleştiren, cihazı telefon hattının yakın bir yerine koyar. Hattan geçen elektrik sinyalleri hat etrafında bir manyetik alan yaratır, dolayısıyla aygıt içindeki bobinde bir elektrik akımı oluşur. Bobine bağlı bir minik radyo vericisi ise bu elektriksel bilgiyi, dinleyici ya da kaydediciye iletir.

Gerçekte dinleme aygıtlarının çoğu, ister telefon vasıtasıyla büroya yerleştirilmiş olsun, ister arabaya yerleştirilsin (son zamanlarda popüler olmaya başladı), iletimi, radyo frekansları yoluyla sağlamaktadır, onun için gizli dinleme aygıtı detektörleri daha çok spektrum analizörleri (frekans çözümleyici), AM, FM, kısa ve çok kısa dalga yayınlarını alabilen radyo alıcıları gibidirler.

Havada Gizlenenler

Böyle bir detektör kullanan araştırıcı, şüphe edilen telefona veya odaya referans bir ses gönderir; aynı anda analizör, algılama alanı çevresinde döner. Referans ses dalgası, elektromanyetik ses dalgası olarak çıkış yapıyorsa, cihaz onu yakalayacaktır.

Başka bir problem de bilgi ileten yayın uydularının kullanılmasından kaynaklanmaktadır. Özel bilgilerin korunması üzerinde çalışan Amerikan Sanayi Güvenlik Kurulu Başkanı Brian Hollenstein, "Uydudan verilen bir sinyal, bulunduğu noktadan gideceği yere doğru gittikçe yayılır. Sinyal yere ulaştığında Kaliforniya eyaleti kadar geniş bir alanı kaplar, herhangi bir anten bu sinyali kolaylıkla alabilir" demektedir. İşte burada, sinyali sayısal bir değere dönüştürüp, binlerce muhtemel formülden birine göre karıştıran şifre aygıtları devreye girer.

Gizli dinleme cihazının bulunması, geçici olarak ayrıcalık taşıyan bilginin akıp gitmesini önleyebilir; fakat o ana kadar çıkanları durduramaz. Bunun için firma yöneticileri, gizli bir dinleme cihazının varlığına karşı uyaran cihazlar satın almaktadırlar. Serbest piyasada satılan bu cihazlardan bazıları oldukça yaygın kullanılmaktadır.