Kendiliğinden şifreli cihazlar

ÇETİN KAYA
KOÇ

Şirket bilgilerinin güvenliği için yeni bir yöntem.

İki hafta kadar önce bir cihaz şirketinin dizüstü bilgisayarlarda kullanılmak üzere kendiliğinden (native, built-in) şifre yapan hafıza diskleri üretmeye başladığını okuduk. Böylece eğer bilgisayarınız çalınırsa, hırsızlar disk üzerinde sadece şifreli dokümanları bulacaklar ve şirket veya şahsi bilgilerinizin içerikleri başkalarının eline geçmemiş olacak.

Bu gerçekten de önemli ve adreslenmesi gereken bir sorun. Şimdiye kadar birkaç tane farklı çözüm mimarileri önerildi. Şifreleme motorunu disk içinde tutma nedeni, bilgisayar üzerinde yapılacak saldırılara karşı korunmak. Diske gönderdiğiniz her veri kümesi, disk üzerindeki gömülü küçük bir işlemci yardımıyla şifrelendikten sonra diske yazılıyor. Kullanılan anahtar, bilgisayarınız tarafından önceden diskin işlemcisine sağlanıyor ve işlemci bu anahtarı ya erişilemeyecek (tamper-resistant) bir şekilde tutuyor veya kullandıktan sonra siliyor. Tabii, ondan beklentimiz şifreli verileri bize açık bir şekilde sunması; yani bir veri kümesi bilgisayar tarafından istendiğinde, diskin gömülü işlemcisi bu anahtarı kullanıp, bilgisayara bu veri kümesini açık olarak sunmalı. İşlemcinin şifreleme hızı, diskin okuma yazma hızından yavaş olmamalı, çünkü bu dışarıdan izlenen okuma/yazma hızını belirler. Ancak hız sorunları artık aşılmışa benziyor, yani işlemci disk kadar hızlı.

Ancak anahtar yönetim problemleri var olmaya devam edecek. Anahtar disk üzerinde tutuluyorsa, onu yönetme derdimiz azalıyor ama disk üzerinde tutulan anahtarın başkaları tarafından ne kadar erişilemez olduğunun analizi gerekli. Anahtar diskte tutulmuyorsa, arka plandaki anahtar yönetim sistemini dikkatli bir şekilde inceleyip, şirket amaçlarına ve gizlilik politikalarına ne kadar uygun olduğuna bakmamız gerekecek. Anahtarların üretilmesi, dağıtılması ve erişilmesi her zaman şifreleme sistemlerinin en duyarlı ve saldırıya açık yanları olmuştur. Bunun bilinci içerisinde hareket etmemiz de fayda var.

koc@krip.to