ASAL FAKTÖRLER

Bulut güvenliğinde 6 nokta

ÇETİN KAYA KOÇ koc@sehir.edu.tr

Bir önceki yazımda bulut güvenliğinin teknik yanlarından bahsetmiştim. Bulut Güvenlik Konsorsiyumu (Cloud Security Alliance) bulut güvenliği şu 6 noktada inceliyor: 1) Verinin bulut içindeki depolardaki güvenliği, 2) Verinin transmisyon sırasındaki güvenliği, 3) Veriye ulaşan aktörlerin kimlik doğrulaması, 4) Farklı müşteri veri ve işlemlerinin ayrıklığı, 5) Bulut ile ilgili hukuki konular, 6) İhlal durumunda hızlı müdahale.

(1) Bilgiyi durduğu yerde (hard disk, file server) güvenli tutmak için şifreleme yapmamız gerekiyor. Sabit disk üreticileri TCG (Trusted Computing Group) standartlarında kendiliğinden şifreleme yapan (self-encrypting) diskler üretmesi işimizi kolaylaştırıyor. Yazılımla şifreleme de mümkün ancak bu daha yavaş bir teknoloji. Her iki durumda da, anahtar yönetimi dikkate alınması gereken bir konu. Bulut hizmet sağlayıcıları, kanun gereği şifreleme hizmeti sunuyor.

(2) Hareket halindeki bilginin güvenliğini sağlamak için çok iyi tasarlanmış ve yıllardır kullandığımız ve güvendiğimiz SSL/TLS protokolleri var. Ancak burada kimlik doğrulama çok önemli bir faktör.

(3) Kullanıcı (aktör) kimlik doğrulaması erişim kontrolünde ilk ve önemli adım. Gerçek kullanıcılara en az zahmetle erişim sağlarken, kötü kişileri dışarda tutmamız gerekiyor. Bulut hizmetleri tamamıyla Internet üzerinden olduğu için, erişim kontrolü çok daha önemli. TPM (Trusted Product Module) cihazları ile kuvvetli kimlik doğrulama sağlamamız söz konusu. Yine TCG standartlarından IF-MAP (Interface for Metadata Access Points) ile bulut hizmet sağlayıcısı ve müşteri şirket arasında erişim hakkı verilen kullanıcılar ile ilgili bilgiler gerçek zamanlı olarak paylaşılmakta ve erişim hakkı alınan kullanıcı birkaç saniye içinde sistem dışı kalmaktadır.

(4) Bulut hizmetleri hakkında belirgin tereddütlerinden biri de müşterilerin başkalarına ait duyarlı bilgilerine ulaşıp ulaşamadığıdır. Bulut müşterileri birbirlerinin ticari rakibi hatta bunların bazıları hacker da olabilir. Bulut hizmet sağlayıcıları virtual machine (VM) ve hypervisor teknolojileri ile bu ayrımı sağlarlar. Buna ilave olarak TPM ile donanım bazlı kimlik doğrulama ve VM bütünlüğü sağlanır.

(5) Müşteri çalıştığı bulut hizmet sağlayıcının uyması gereken kanun ve yönetmelikler konusunda ev ödevini yapmalıdır.

(6) Her ne kadar bulut hizmet sağlayıcılar bu konuda çok yetkin iseler, müşterinin bulut güvenliği güvenlik ihlalleri ve kullanıcı yanlış davranışları konusunda hazırlıklı olmasında fayda vardır.