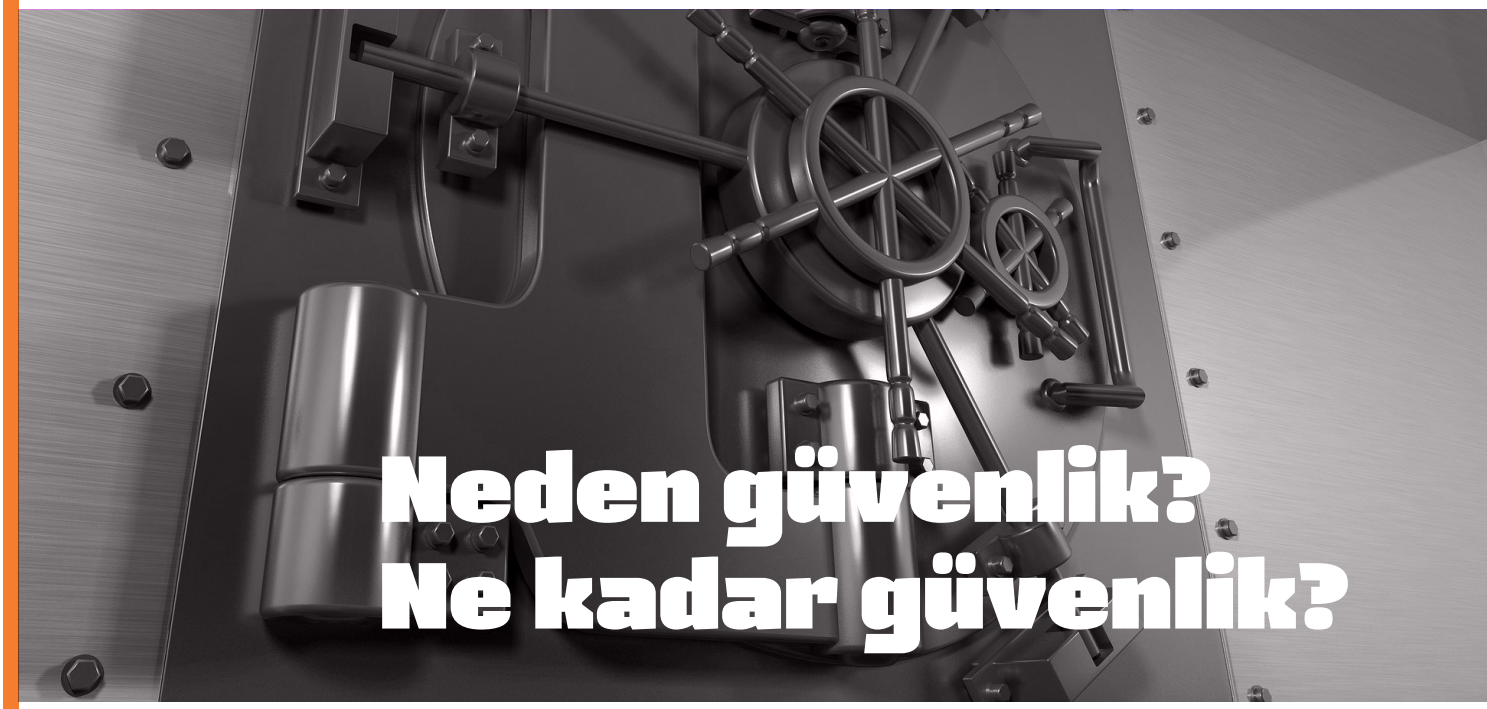
GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar.
Bültenlerin her ay size ulaşması için üye olunuz: http://eepurl.com/bP-tWn

MART 2016



Neden güvenlik? Ne kadar güvenlik?

BİLGİ GÜVENLİĞİ, SON YILLARIN EN GÜNDEMDEKİ KONULARINDAN BİRİ HALİNE GELDİ VE YALNIZCA FİNANS KURUMLARININ DEĞİL DEVLET KURUMLARININ VE ÜRETİM SEKTÖRÜNÜN DE GÜNDEMİNİN ÜST SIRALARINA YERLEŞTİ.

Buna yol açan ne oldu, neden güvenliği gittikçe daha fazla önemsemek zorunda kalıyoruz?

En önemlisi, kurum ve birey olarak ne kadar güvenliğe ihtiyacımız olduğunu biliyor muyuz?

Önce, ilk sorudan başlayalım. Pek çoğumuz bu sorunun cevabını "dijital dönüşüm" olarak vereceğiz ve büyük ölçüde doğru da söylemiş olacağız. Dijital dönüşümle birlikte tamamen "konekte" bir dünya haline dönüştük ve dönüşmeye devam ediyoruz. Ancak bu "konekte" dünyanın bir yerinde, sizin kullandığınız teknolojiyi sizden daha iyi bilen birileri mutlaka vardır, üstelik de bu kişiler her zaman pek iyi niyetli değillerdir. Teknolojik gelişmelerin çok hızlanmış olması da, güvenliğin bugün için karşısında olan konulardan biridir. Dün teknolojik olarak mümkün olmadığı için hayata geçirilemeyen pek çok konu bugün gerçekleştirilebilmektedi ama aynı zamanda bir güvenlik açığı olarak karşımıza çıkmaktadır. Fütüristlerin gelecek tahminlerine bakıldığında, konunun daha da ciddi hale geleceği beklenebilir. Uzaktan yönetilen sürücüsüz arabalar, uzaktan yönetilen üretim tesisleri gibi teknolojik gelişme beklentileri, kısa - orta vadede güvenliğin kazanacağı önemin ne derece büyük olacağı konusunda bir fikir vermektedir.

Bu durumda ikinci soru daha da fazla önem kazanmaktadır: **Kurum ve birey olarak ne kadar güvenliğe ihtiyacımız olduğunu biliyor muyuz?** Bunu bilebilmek için, öncelikle risk analizi yapmamız gerekir. "En kötüsü başıma geldiğinde ne kaybetmiş olurum? Karşılaşabileceğim tehditler ne? Karşılaşma ihtimalim ne kadar? Engel olmak için yapabileceklerim neler?" sorularının cevaplarını önceden oluşturmuş olmalıyız.

Peki, **risk analizi sonuçları nasıl okunmalı ve uygulanmalı?** Bilgi güvenliği uzmanı olarak kendi tecrübem şu yönde: Müşteriye değecek yerlerde, mevzuata uyumda bir sorun oluşturmaması kaydıyla, belirli esneklikler tanınabileceği düşüncesindeyim. Ancak, bu nedenle alınmakta olan risk, iş birimleri tarafından biliniyor ve kabul ediliyor olmalı; risk kabulünün formel ve yazılı yürütülmesi gereken ciddi bir iş olduğunu da hatırlatmak isterim. Öte yandan, risk analizi sonuçları o gün için gerekli-lik göstermese de, teknik güvenlik için yapılabilecek tüm güvenlik önlemlerini almayı öneririm. Alınan her fazla güvenlik önlemi, BT operasyonu tarafında yönetim maliyetini artıran bir unsur olarak karşımıza çıkar, ancak tehditlerin her gün arttığı bir dünyada güvenlik kalkanlarımız çok hızla incelebilmekte ve bugün gereksiz gördüğümüz ekstra güvenlik kontrolü kısa bir süre sonra saldırıyı göğüsleyen kalkan haline dönüşebilmektedir. Müşteriyle doğrudan temasın söz konusu olduğu durumlarda en yüksek güvenliği hedeflemek caydırıcı ve sevimsiz olabileceği için, riskler değerlendirilerek uygun güvenlik seviyesi oluşturulurken, doğrudan müşteri memnuniyetsizliği yaratmayacak bütün süreçlerde en yüksek güvenlik hedeflenmeli görüşündeyim.

Peki, **hangi güvenlik önlemleri mutlaka alınmalı?** Kendi gözlemim, çok etkili ve oldukça da kolay uygulanabilir bir yöntem olan IP kontrolünün yeterince uygulanmadığı yönünde. Daha önce de belirtmiş olduğum gibi, kullandığınız teknolojiyi sizden iyi bilen birilerinin mutlaka bulunduğunu hatırınızda tutup, uygulamanızı, erişmesi gerekmeyen hiç kimseye ağ üzerinden açmamanızı kesinlikle öneririm. Kullandığınız uygulamalarda da kullandırdığınız uygulamalarda da IP kontrolünü en etkili ve sınırlayıcı şekilde kullandığınızdan emin olun. Ağ seviyesinde önlem alabildiğiniz durumlarda çok şanslı olduğunuzu aklınızdan çıkarmayın ve bu şansınızı iyi değerlendirin. İkinci sırada ise, "müte-vazı olma" gerekliliği yer almaktadır. "Bizim ortam çok güvenli"diye başlayan sözler duyduğumda çok endişeleniyorum. **"Doğrulanmayan güven" büyük yanılsamalara ve risklere açık hale dönüşmenize yol açabiliyor.** Üçüncü önemli önlem ise, "yama ve konfigürasyon yönetimi" diye düşünüyorum. Asla kolay ve hızlı olmayan bu önlem, özellikle tüm dünyaya açmak zorunda kaldığınız uygulamalarda çok kritiktir. Hem çok hızlı hem de çok çalışkan olmanız gereken bir alandır. Son olarak da, tüm web ve mobil uygulamalarda HTTPS kullanılması sağlanmalıdır. Hattın üzerinden şifrelerin ve gizli bilgilerin ele geçirilmesi riskini hedeflemesinin yanı sıra, hatta taşınan bilgilerin değiştirilmemesinin sağlanması tarafında da HTTPS en kolay uygulanabilir güvenlik önlemi olma özelliğini korumaktadır.

Teknolojinin nimetlerinden yararlanmayı sevdiğimiz gibi, yarattığı yan etkilerle başa çıkmayı da öğrenmemiz gerekiyor. Gerek bireyler gerekse kurumlar olarak bunu doğal bir gelişim olarak görmeye başlayıp eksiklerimize odaklanırsak, hızlıca doğru noktaya geleceğimiz görüşündeyim.

YAZAR HAKKINDA

GÜLDEN YÜNCÜOĞLU, CISSP® İTÜ Kontrol ve Bilgisayar Mühendisliği Bölümü mezunu olup, 20 yılı aşkın süredir bilgi güvenliği alanında çalışmaktadır. Uzun yıllardır finans sektöründe, bilgi güvenliği, BT sürekliliği ve BT uyum yöneticiliği yapmakta olup, Türkiye'nin önde gelen sistem entegratörlerinden birinde bilgi güvenliği danışmanı olarak da görev yapmıştır.