NIZAMETTIN MERAL, TEKNOSER NETWORK VE GÜVENLİK ÇÖZÜMLERİ MUDURU

"Aslında güvenlik projelerinin bir sonu yok"

"Firmalara en önemli tavsiyem, güvenlik danışmanlığı alanında uzmanlaşmış sistem entegratörü firmalara bu hizmetin outsorce edilmesidir"

Teknoser, teknolojide ilklerin yaratıcısı Hitay Yatırım Holding bünyesinde, 65 hizmet noktası ve 700'den fazla çalışanı ile Türkiye bilgi ve iletişim teknolojileri pazarında önde gelen sistem entegrasyon ve saha hizmetleri firmalarından. Sistem entegratörlüğü alanındaki uzmanlığını yerinde kurulum, bakım ve destek hizmetleri yetkinlikleri ile birleştiren Teknoser, ülke genelindeki yaygın saha gücünü de kullanarak, tüm IT hizmetlerini yüksek müşteri memnuniyeti sağlayarak sunabilen bir organizasyona sahiptir.

"ÖNEMLİ OLAN HER ZAMAN, HER YERDEN, HER CİHAZLA AMA GÜVENLİ KAYNAĞA ERİŞİM"

Günümüzde kurumların network sistemleri, işletim sistemleri, kritik kurumsal verileri, yazılımları, veri tabanları eskiye oranla daha nitelikli saldırılara maruz kalmaktadır. Çünkü IT güvenliği konusunda 2-3 sene öncesi ile karşılaştırsak dahi teknolojik, yöntemsel ve donanımsal olarak devrim niteliğinde gelişmeler yaşanmıştır. Bu gelişmeler neticesinde sıradan saldırılar basit Firewall altyapıları, kullanıcı bazlı Antivirüs yazılımlan gibi temel bileşenler ile dahi bertaraf edilebilmektedir. Çünkü saldırı tipleri/ signature veri tabanları son derece gelişmiş ve tüm güvenlik üreticileri bu veri tabanlarını etkin olarak kullanabilmektedir. Aynca işletim sistemleri, kurumsal yazılımlar, veri tabanı uygulamaları konusunda üretim yapan ve destek veren firmalar, IT güvenliği konusunda eskisine göre daha hızlı cevap vermekte ve rekabetin yoğun yaşandığı sektörde pazarını kaybetmemek adına güvenlik tehditlerine karşı yama yazılımlan daha hızlı ve başanlı bir şekilde geliştirmekte ve yaymaktadır. Bunun bilincinde olan kötü niyetli kişiler de daha kompleks saldın yöntemleri geliştirmekte ve güvenlik üreticilerini kendilerini ve ürünlerini sürekli geliştirmeye zorlamaktadır. Bu anlamda ARP temelli saldınlar, belli servislere yoğun istek göndererek bloke etme amaçlı DoS saldırılar, MAC klonlama, MAC flooding/ spoofing, IP protokol açıklanna yönelik AET saldınlar, netvvork dinleme/ sniffing, SYN ataklar değişik türevleri ile sürekli IT Yöneticilerinin kabusu olmaya devam etmektedir.

Güvenlik terminolojisinde sürekli bahsi geçen bir konu da iç ve dış saldınlar ve bunlann kıyaslamalandır. Genel kabul gören tez, içeriden gelen saldırıların dış saldırılara göre yüzdesel anlamda ciddi ağırlıkta olduğudur. İçeriden gelen saldırıların aslında çok azı kötü niyetli ve bilinçli yapılmakta, büyük oranda bilinçsiz kullanıcı ve firmaların yetersiz güvenlik politika ve altyapı eksikliğinden kaynaklanmaktadır. İç saldırıları önlemek için kullanıcı bilgisayarlarındaki işletim sistemlerinin sürekli güncellenmesi, antivirüs yazılımlan, 802.1x ve üstü Network Access Control (NAC) çözümleri, kritik firma verilerinin dışarıya sızmasını önlemek amaçlı Data Loss Prevention (DLP) çözümleri, e-mail güvenlik ürünleri, network'te sürekli izleme, veri analizi ve trafik anormalliklerini raporlayan çözümler, kritik veri ve networklerin soft veya fiziki izolasyonu, sistemsel ve networksel verileri/ logları toparlayıp anlamlı yorumlar üreten yazılımlar, uygulama seviyesinde güvenlik sağlayan UTM ürünler ve bunlan anlamlı kılacak prosedürel süreç yönetim ve güvenlik politika sertifikasyon programları kaçınılmaz hale gelmiştir. Bu plan ve projeleri üretirken, net-ork'lerin artık sadece PC/ Notebook tan ibaret olmayıp, mobil tablet, akıllı telefon gibi her türlü cihazın ofis veya ev-ofis her yerden ve her zaman network'e dahil olabileceğini de hesaba katmak gerekir. Günümüzde yasaklayarak güvenlik sağlamak moda deyimi ile "Trend Topic" değildir, önemli olan her zaman, her yerden, her cihazla ama güvenli ve güvenlik politikaları kapsamında izin verilen kaynağa ve noktaya kadar network erişimidir.

GÜVENLİK ÇÖZÜMLERİ, BİLİŞİM SEKTÖRÜNDE SÜREKLİLİĞİN EN KRİTİK OLDUĞU ALAN

Bu konuda firmalara en önemli tavsiyem, güvenlik danışmanlığı alanında uzmanlaşmış sistem entegratörü firmalara bu hizmetin outsorce edilmesidir. Günümüzde pek çok sistem entegratörü firma bile, temel network ve sistemsel altyapılarda sağlıklı ve sürdürülebilir kalitede hizmet vermekte zorlanırken, firmalann bunu kendi bünyelerinde çözmeye çalışmaları aslında pek mümkün olan bir yöntem değildir. Düşünsenize 10 sene önce bir sistem admin biraz da network'den anlasa tek başına bir firma altyapısına destek verebilirken, bugün orta düzeyde bir firma bünyesinde Wireless, Firewall, NAC, IPS /IDS çözümleri, Database /Yazılım Güvenliği, İşletim Sistemi/ Sanal Güvenliği, Routing/ Switching uzmanı gibi ayrı ekipler oluşturması gerekmektedir. Bu segmentlerdeki farldı marka/ model çözümlere de aynı kişinin uzman seviyesinde destek olmasını beklemek çok gerçekçi değildir. Bu durumda firmalar 10 ve üstü sayıda elemanlardan oluşan IT kadroları ve yine kişilere bağımlı bir sistem açmazı ile karşı karşıya kalmaktalar.

Şunu unutmamak lazım ki cihazların üzerindeki servisler açıldıkça toplam kapasite düşmekte ve cihaz bir şeyi çok iyi yapan, bir güvenlik açığını çok iyi kapatan bir ürün durumundan herşeyi yapan ama biraz yapabilen yani "light versiyon" olarak çalışan bir ürün durumuna gelebilmektedir. Aslında güvenlik projelerinin bir sonu yok. Öyle olsa çok stratejik öneme sahip ve çok ciddi güvenlik yatırımları yapan global kurum ve kuruluşlann bu saldırılardan etkilenmemesi gerekirdi, maalesef realite böyle değil. Önemli olan konu şu: hangi datanız firma için ne kadar kritik önemde ve mutlak surette korunmalı, yedeklenmeli veya olağanüstü durum merkezlerinde yedeği korunmalı, hangi data daha az önemde riske edilebilir veya edilemez, yani firma kurumsal işleyişine göre güvenlik politikalan ve uygulamasının, sürecinin doğru tanımlanması ve doğru uygulanması. Burada firmalar için isabetli bir network ve güvenlik danışmanı partner seçimi ve konusunda uzman kişilerin yönlendirmeleri ile hareket edilmesi en doğru strateji olacaktır.

Güvenlik çözümleri, bilişim sektöründe sürekliliğin en kritik olduğu alandır. Bir LAN, Wireless sistemde konfigsel anlamda ilk kurulum anından sonra çok radikal değişimler olmaz. Bu sistemlerde sürekli güncellemeler çıkmaz, her çıkan güncelleme de sizin topolojiniz ve konfigürasyonunuz için kritik olmayabilir. Oysa ki güvenlik altyapısında ilk kurulum yapısı önemli olmakla birlikte, daha kritik olan sistemin sürekli güncellenerek canlı tutulması, dinamik bir yapı içerisinde güncellenen global saldırı imza tipleri/ signature veri tabanı ile entegre edilmesidir. Yoksa kurduğunuz sistem başlangıçta ne kadar sağlıklı çalışsa ve doğru bir topolojiye otursa da bir kaç ay sonra pek çok güvenlik açığı ile karşı karşıya gelmek kaçınılmazdır.

TEKNOSER

Önemli olan şu:" Hangi datanız firma için ne kadar kritik önemde ve mutlak surette korunmalı, yedeklenmeli veya olağanüstü durum merkezlerinde yedeği korunmalı?"