

Bilgi Güvenliğinde Vizyon

Şüphesiz vizyon sahibi kişiler ve kurumların başarıya ulaşma ihtimalleri diğerlerine göre daha yüksektir. Ancak vizyon tanımı farklı mecralarda farklı anlamlar taşıyabiliyor. Örneğin üniversitelerin işletme derslerinin çoğunda vizyonun bireysel bir görüş bütünü olduğu, şirketlerin ya da organizasyonların vizyonu olamayacağı söylenir. Oysa iş danışmanları Kurumsal Vizyon geliştirme hizmetleri vermektedir. Kurumsal danışmanlar vizyonu genelde ikiye ayırır: şimdiki vizyon ve gelecek vizyonu. Ben en iyisi "vizyon sahibi" kavramı üzerinde durayım, kavramın da Türk Dil Kurumu sözlüğünde nasıl geçtiğini yazayım.

Vizyon Sahibi: Geniş görüşlü, ileri görüşlü, ufku geniş kimse.

Vizyon ile bilgi güvenliği arasındaki bağlantıyı 3 temel adımda ortaya koyabiliriz.

Üretici Vizyonu

Üreticiler bilgi güvenliğinde gelecek zamanlarda ortaya çıkacak tehditleri düşünür ve ürünlerini bu yönde geliştirir. Ancak bu sayede müşterilerine katma değerli hizmetler üretebilirler. Pazar araştırmaları ile yatırım kararı desteklenir ve ürünler piyasaya sürülür.

İş Ortağı Vizyonu

Biz hem üreticilerin hem de müşterilerimizin iş ortağıyız. Bizim gibi bilişim sektörünün hizmet tarafında bulunan şirketlerin belki de tek hedefi müşteri memnuniyetidir (en azından bence öyle olmalıdır). Ancak müşteri memnuniyeti bir sonuçtur, müşteriye gelecek teknolojilere hazırlamak ve bu konuda donanımlı olmak ön şarttır.

Son Kullanıcı Vizyonu

Türkiye'de en zayıf halka olarak gördüğüm konu, son kullanıcı vizyonu. Ticaret şekli ve yasal düzenlemeler (ihale kanunları, satın alma prosedürleri vs.), çoğu zaman şirketlerin teknoloji alımlarındaki vizyonunu arka plana itiyor. 10 yılı aşkın bilişim sektörü tecrübemde mevcut kurallar sebebi ile son kullanıcılarıdaki teknik uzmanların istemedikleri ürün, teknoloji veya hizmetleri satın almak zorunda kaldığını defalarca gördüm.

Benim sorumluluğum elbette daha çok iş ortaklarının vizyonu çerçevesinde. Bugünkü vizyonumuz için Network IPS, Host IPS, SSLVPN, Security Management, 2 Factor Authentication, Vulnerability Assessment ve Risk Management gibi oldukça yüklü bir teknoloji yatırımı yaptık ve bu ürünlerin tamamını kullanıyoruz. Tek amacımız teknik ekibimizin bilgi ve tecrübesini maksimum seviyede tutmak. Gelecek vizyonumuz ise yarın talep edilecek ürün ve hizmetleri tespit etmek, gerekli yatırımları yapmak ve yarınla şimdiden hazır olmak üzerine kurulu.

Bu yazıda "Bilgi Güvenliği" konusunda gelecek vizyonuna nasıl baktığımı anlatmaya çalışayım dedim ama biraz uzun bir önsöz oldu. Gelecek zamanlarda karşımıza çıkacak olan tehditleri ve bu tehditlerle nasıl mücadele edeceğimizi düşünmek, bu alanlara yatırım yaparak müşterilerimize doğru çözümler sunmak zorundayım. Hepimiz bu konuda düşünmeliyiz, çünkü şirketimizin yarınlarını ancak bu sayede güvende tutabiliriz. 2007 yılının bu ilk günlerinde bizce güvenlik teknolojilerinin nasıl bir geleceğe sahip olduğunu ve Türkiye pazarının mevcut teknolojilere adaptasyon sürecini bir beyin fırtınası yaparak ortaya koymaya çalışalım.

Beyaz Şapka'nın önceki sayılarında da yer aldığı gibi, ataklar ağ ve uygulama seviyesine doğru kaydı. Yani güvenliğimizin bu tarafına biraz daha öncelik vermeliyiz. Ağ seviyesinde Network IPS projeleri hızla yürümeye devam ediyor ama uygulama güvenliği tarafında güvenli kod geliştirme, Application Firewall ve uygulama güvenlik taraması hizmetlerinde önemli artışlar bekliyorum. Network IPS ürünleri biraz daha küçük sistemlerde projelendirilecek diye umarken Application Firewall teknolojilerinin büyük şirketlere hızla gireceğini sanıyorum. Sektörün üretici tarafında ise önemli güvenlik üreticilerinin Application Firewall ürünleri geliştirmesi ya da var olan başka şirketleri satın alması beni şaşırtmayacak. Hatta birkaç sene sonra Network IPS teknolojisi ile Application Firewall teknolojisinin ya da Network Firewall ile Application Firewall ürünlerinin aynı donanımlar üzerinde birlikte çalıştığını görürsek şaşırmayalım.

Klasik Network Firewall ürünleri güvenlik sağlamakta çok yeterli değildir. Yıllardır bunu söyleyip dururken, Unified Threat Management (UTM) ürünleri hızla yayılıp beni haklı çıkardı. UTM cihazları tek kutu üzerinde Firewall, IPS, Antivirus ve Antispam gibi teknolojileri çalıştırabiliyor. Ancak her zaman söylediğim gibi, UTM cihazlarının her bir özelliği kısıtlandırılmıştır. Dolayısı ile UTM cihazları daha ziyade küçük sistemlere yayılacak, büyük sistemlerde her bir güvenlik teknolojisi ayrı ürünler olarak çalışacak.

Secure Content Management (SCM) adına henüz Türkiye alışmadı. Hala birçoğumuz bu ürünlere 'gateway antivirus' gözüyle bakıyoruz. Ancak bilgi güvenliği sektöründe SCM artık bir ürün grubu haline geldi. Hatta global araştırma şirketleri SCM ürün grubu için pazar araştırmaları yapar oldu.

SCM ağımda önemli bir güvenlik noktası oluşturuyor. Elektronik posta sunucularımızın yükünü %70 oranında azaltıyor. HTTP, FTP ve POP3 gibi protokollerden doğan atakları engelleyebilir. Önümüzdeki aylarda SCM ürünlerine basit atak engelleme imzaları eklenebilir. Hatta önümüzdeki yıllarda SCM ürünleri büyük sistemler için spesifik protokollerde çalışmak üzere



88485416562234006653490
1198849822121987546015792
1456158213621223549
8549872161599
316848992216548911
57546216654547778



tasarlanabilir. Örneğin sadece SMTP için çok daha gelişmiş SCM, sadece HTTP için çok daha gelişmiş SCM gibi...

Spam postalar hepimizin ortak derdi. Bağımsız Antispam ürünleri de var, SCM ürünlerine entegre ürünler de. Spam mücadelesinde Karantina Yönetimi ağırlık kazanacak. Her ne kadar spam tanımlama başarısı günden güne artsa da, bu işe internet otoritelerinin kesin bir çözüm getirmesi gerektiğini ve getireceğini düşünüyorum. Microsoft, Sender Policy Framework (SPF) ile bu konuda bir adım attı ancak bilişim sektörü bunu çok halletmiş gibi görünmüyor. Ben daha ziyade dijital imza temelli bir kesin çözüm ortaya konacağına inanıyorum. Ancak bu çok yakın bir gelecekte olmayacaktır.

Google'dan bilgi güvenliği harcamaları ile ilgili bir araştırma yaptım. Özellikle kuzey Amerika'da kimlik doğrulama teknolojilerinin satış rakamları şaşırtıcı derecede yüksek. Nedeni ise çok basit: güvenlik ihlallerinin çok büyük bölümü zayıf şifre politikası, zayıf kimlik denetimi nedeniyle ortaya çıkıyor. Sadece kimlik doğrulama olarak baksak bile ürünler çok ucuz yazılmaz. Kullanıcı başına 50-100\$ gibi maliyetler söz konusu olabiliyor. Ancak sisteme erişim bilgilerimiz bu rakamdan daha düşük bir öneme sahip değil ki? Single Sign-On (SSO) çözümlerini düşünürsek maliyet daha da artabilir. Yine de Türkiye'de pek değerini bulmamış olan kimlik doğrulama çözümlerinin 2007 yılı içerisinde önemli derecede artacağını düşünüyorum.

ADSL hizmetinin yayılması ile internet kullanıcı sayısı önemli derecede arttı. Eskiden sadece bir web sunucusu ile yürütülen hizmetler artık dört-beş sunucu ile yapılıyor. Metro Ethernet altyapısı bant genişliklerini önemli derecede arttırmaya başladı. Load Balancing ve SSL Acceleration tarafında yapılan projeler zaten 2006 yılında artmaya başladı. 2007 yılında Application Acceleration çözümlerinin de hızla artarak yayılacağını düşünüyorum.

Dünyanın en büyük kurumsal danışmanlık şirketlerinden birinin çalışanı, dünyanın en büyük bilişim üreticilerinden birinin çalışanlarına ait önemli bilgiler taşıyan CD'yi çaldırdı. Türkiye'de bu hırsızlığın önemi çok anlaşılabilir. Fakat Amerikan kanunlarına göre bu bilgilerin çalınması, satılması ve kullanılması çok büyük bir suç. Benzer durumlar Türk şirketlerinde de oluyor. Bugüne kadar proje dokümanlarını çaldırılmış, önemli dokümanların bir köstebek tarafından sızdırıldığını düşünen, dizüstü bilgisayarını çaldırılmış ve içerisinde önemli bilgiler olduğunu söyleyen yüzlerce müşteri gördüm. Bu gibi sıkıntılara bilgi güvenliği üreticileri çözüm getirmiş durumda. 2007 yılından itibaren hayatımıza yeni bir güvenlik teknolojisi girecek, Data Loss Prevention (DLP). DLP ürünleri bilgisayarlarda bulunan gizli ve kritik bilgilerin dış ortamlara taşınmasını engelliyor. DLP ile korunan bilgileri CD'ye ya da USB belleklere kopyalamak, e-posta eki

olarak başkalarına göndermek, anında mesajlaşma yazılımları ile başka sistemlere transfer etmek, yazdırılmasını ya da fakslanması engellemek mümkün.

NAC teknolojisi sürekli kafamda soru işareti uyandırıyor. Managed ve unmanaged sistemlerde NAC teknolojisini yürütmek çok zor. Ben en başından beri NAC teknolojisini çok yayılamayacağını düşündüm. Microsoft bu işe elini attığında işin çehresi bir miktar değişecek gibi. Longhorn ile gelecek olan Microsoft NAP sektörde bir standart haline gelebilir. Yine de NAC ürünlerinin, harcanan işletim emeğine karşılık gelebilecek bir fayda yarattığını düşünmüyorum ve her müşteride söylediğim lafımı bu sayfada sizlerle paylaşmak istiyorum: Prevention First!

Türkiye'de ne kadar pazara sahip olacağını kestiremediğim bir tek ürün grubu var, o da Policy Management (Policy Auditing ve Compliance Analysis gibi isimleri de bu kategoriye dahil ediyorum). Güvenlik ve kural denetimi yapan bu ürünler geniş bir bandada denetim ve raporlama yapabiliyor. Ancak nedendir bilinmez, Türkiye pazarı bu tarz ürünlere pek sıcak bakmıyor. Özellikle Amerikan şirketleri pek gönüllü olmasalar da bu ürünleri kullanmak zorunda kalıyor. Nitekim HIPAA, SOX, PCI gibi onlarca uyulması gereken ve sıkı denetimi yapılan standart var ve bu ürünler standartların tamamına uyum sağlayan denetimler yapabiliyor, raporlar üretebiliyor. Türkiye'de özellikle Finans gibi sektörel denetim sistemi gelişmiş pazarlarda bu gibi yazılımlar kullanılacaktır diye düşünüyorum.

Ne kadar çok üründen ve teknolojiden bahsettik değil mi? Kim yönetecek bunca ürünü, kim raporlayacak? Güvenlik sistemleri geliştikçe ve kullanılan ürün sayısı arttıkça mecburen Enterprise Security Management (ESM) ürünlerine yöneleceğiz, başka çaremiz yok. ESM ürünleri farklı iş yapan birçok bilişim ve güvenlik sisteminden bilgi toplayıp yorumluyor ve bize anlamlı raporlar üretebiliyor. ESM sayesinde tek merkezden risk haritasını görüp acil önlemler üretebiliyoruz.

Bu yazıma sığdıramadığım Automated Remediation, Risk Management, Mobile Device Security, Encryption gibi konular da var. Ancak temelde anlatmaya çalıştığım şey şu ki; her birimiz çalıştığımız kurumun güvenliğini sağlamakla yükümlüyük. Sorumluluklar paylaştırılabilir ancak devredilemez. Yarın risklerini bugünden düşünmek, sistemimizin ve şirketimizin geleceğini garanti altına alacaktır. Bu sayede kolay kazanılmayan para, daha mantıklı yatırımlara kaydırılabilir ve yatırım geri dönüş hızı artırılabilir. Bilişim güvenliğini sağlamanın rahatlığı bir köşede dursun, güvenilir sistemlerimiz sayesinde müşterilerimizin memnuniyetini arttırabilir, çetin rekabet koşullarında rakiplerimizden bir adım ileride olabiliriz. Yarınlarınız güvenli olsun.