BThaber

Yayın Adı	: BT Haber	Yayın Tarihi	: 24.08.2015	Küpür Sayfa	: 17
Referans No	: 50256206	Etki	: Etkisiz	Tiraj	: 7500
Renk	: Renkli	STxCM	: 286,388888	Sayfa	: 17

Olmaz olmaz demeyin, çok fena olabilir

Handan Aybars

Son birkaç yıldır, dünyanın önde gelen şirketlerinin yaşadığı siber saldırı haberlerini okuyoruz. Her ölçekte şirket kendince önlemler almaya çalışıyor, ama saldırı amaçları, taktikler ve kullanılan yöntemler gün be gün çeşitlendikçe, bu önlem anlayışı da değişiyor, en azından değişmek zorunda. Eskidendi bir masaüstü bilgisayara virüs koruma programı yükleyip ertesi yıl bunu güncellemek. Şimdi kullanılan cihazlar çok çeşitli, bireysel bazda da kurumsal bazda da cihaz çeşitliliği, dolayısıyla her biri için en uygun koruma yöntemleri bir gereklilik.

Ama bu kadar da değil. Bu risk çeşitliliğine uygun yapıyı kurdunuz, ama yine bunlara ayda yılda bir bakma lüksünüz yok. Tehditlerden daha hızlı olabilmenin her sektörde bir gereklilik olduğunu unutmadan, güvenliği an be an takip bu devirde şart.

Her şirket bu konuda bir şeyler yapma çabasında, ama konu hele de Türkiye'de her ölçekte şirketin güvenlik algısı olduğunda, dosyamıza yanıt veren sektör temsilcilerinin serzenişinden de anlayacağınız gibi, bu konuda pek de başarılı sayılmayız. Küresel saldırılara hedef olan şirket sayımız çok, herkes riskin farkında, ama hala güçlü bir 'güvenliğe bakış açısı değişimi' yok. Bu nedenle bir saldırıyı bertaraf edenin ikinci adımda kurban olması maalesef imkansız değil.

Dosyamızda göreceksiniz, kamunun adımları, sektörel düzenlemeler tamam, ama her şirketin kendine, ölçeğine, ihtiyacına, önceliklerine göre güvenlik adımları atması şart. Aksi halde, kapıyı kapatıp kilitlemeye gerek görmeden odadan çıkmaktan ötesi değil yapılanlar...

Doğru güvenlik politikasını belirleyip buna uygun yapılan yatırımın geri dönüşünün çok hızlı olduğunu da belirtelim. En azından bir saldırı sonrası kurumsal BT yapısını ve çalışanların cihazlarını toparlamak, daha da önemlisi bozulan karizmayı düzeltmek imkansız.

BTHaber

Yayın Adı	: BT Haber	Yayın Tarihi	: 24.08.2015	Küpür Sayfa	: 20
Referans No	: 50256206	Etki	: Etkisiz	Tiraj	: 7500
Renk	: Renkli	STxCM	: 286,388888	Sayfa	: 17

CSC Türkiye Genel Müdürü Alev Alp Esen

GÜVENLİK POLİTİKASI SÜREKLİ GÖZDEN GEÇİRİLMELİ

Siber güvenliğe yönelik çalışmalarında farklı bir bakış açısına ihtiyaç duyan ve riski azaltmak isteyen kurumlara öncelikle tehdit modellemesi geliştirmelerini öneriyoruz. Kurumun verilerinin ve BT sistemlerinin ne tip saldırganlar tarafından hedef alındığını bilmek kritik. Bu şekilde, kurumsal BT sistemleri ve veriler içinde hangi varlıkların, kimin, niçin hedefi olacağına yönelik modeller geliştirilebilir; zayıf kısımlar güçlendirilebilir. Ek olarak, kurumlar kendi ihtiyaçları doğrultusunda kendi siber güvenlik uzmanlarını yetiştirmeye de yönelebilirler. Güvenlik durumundaki değişimlerin ya da performans göstergelerinin ölçümlenmesine yönelik güvenlik metriklerinin dikkate alınması, güvenliğe ve iş hedeflerine yönelik stratejilerin etkin bir biçimde bir araya getirilmesi, tehditlere hazırlıklı olunması ve kısa sürede tepki verilmesi de olmazsa olmazlar arasında yer alıyor.

Siber güvenlik son dönemde kurumların ilk sırada gelen teknoloji yatırımı konumunda. Tehditlerin artmasının ve saldırıların çeşitlenmesinin, kurumların bu alandaki yatırımlarına hız vermelerinde önemli rol oynadığı düşüncesindeyiz. Elbette bir kurumun siber güvenlik konusunda olumsuz deneyim yaşamış olması, kurum yöneticilerinin konuyu çok daha ciddiye almalarına neden olabiliyor. Biz güvenliğe yönelik gerçekleştirdiğimiz çalışmalarda, gerçekleşmiş ya da gerçekleşmesi muhtemel münferit olaylar yerine, öncelikle altyapının güçlendirilmesine ve kullanıcıların bilinçlendirilmesine odaklanıyoruz.

Etkin bir siber güvenlik politikası için dikkate alınması gereken altı unsur var. İlki, siber güvenliği iş süreçlerinin bir parçası haline getirerek bunu kurum için bir standart kılmak. Diğer bir unsur ise mevcut siber güvenlik konumunun dikkatli bir şekilde değerlendirilmesi. Veri ihlallerinin yüzde 17'sinin sosyal mühendislikten geldiği göz önünde bulundurulduğunda, bir şirketin siber güvenlik açısından neye sahip olduğuna tam anlamıyla hakim olması kritik önemde. Üçüncü parti yönetilebilir servis kullanımını sağlamak; hızlı bir kurtarmanın işi sürdürmenin anahtarı olduğunu unutmadan hazırlıklı olarak, olası aksaklık ve felaketlere karşı plan yapmak da önemli. Sistem üzerinde hangi kullanıcının hangi işlemler için yetki sahibi olduğunu düzenli kontrol etmek ve veri kaybı ya da saldırılara karşı hazırlıklı olmak da diğer unsurlar. Saldırıların zaman içinde çeşitlendiği ve boyut değiştirdiği düşünüldüğünde, güvenlik politikasının da uzmanların uygun göreceği aralıklarla gözden geçirilmesi faydalı olacaktır.

Proline Network Çözümleri Uzmanı Mehmet Emin Yağcı

SİBER GÜVENLİĞE BAKIŞTA İKİ TEMEL HATA VAR

Hayatın her alanında olduğu gibi bilişim dünyasında da "Bir musibet bin nasihatten iyidir." kuralı her daim geçerli. Küresel ölçekteki saldırı ve tehdit haberleri, farkındalığın artmasına olumlu katkıda bulunuyor. Yalnız unutulmaması gereken nokta; tehditler başa geldikten sonra geri dönüşü olmayan sonuçlar da bırakabiliyor. Bu sonuçlardan sadece bireysel değil, ticari olarak işletmeler de ciddi para ve itibar kaybına uğrayabiliyor.

Türkiye'de genel olarak olmasa da teknolojiyi iş süreçlerine dahil eden ve bulut bilişim çözümlerini kullanan kurumların artık güvenlik çözümleri konusunda farkındalık seviyelerini arttırdığını gözlemliyoruz. Mevcut verilerin ve iş süreçlerinin çevrimiçi hale gelmesi, taşınan verinin işletmeler için kritikliği, devletin uyguladığı yasal zorunluluklar ve yaşanan kötü tecrübeler işletmelerin bu alandaki stratejilerini gözden geçirmelerine neden olmakta.

Siber güvenliğe bakış açısında iki temel yanlışlık bulunmakta. Bunlardan ilki; yıllardır süre gelen alışkanlığın sonucu olarak siber güvenliğin tek bir cihaz yahut yazılım ile sağlandığının zannedilmesi. Günümüzde tehdit tiplerinin kaynakları o kadar farklılık göstermekte ki, bir gün DDoS atağı ile hizmet verme işlemi engellenebilirken, bir başka gün e-posta ile ulaşan bir dosya ile içeriden dışarıya bilgi sızıntısı gerçekleşebilmekte.

İkinci ve daha köklü bir yanlışlık ise siber güvenliği bir 'kapı görevlisi' olarak görmek. Günümüzde iş modelleri ve güvenlik araştırmaları gösteriyor ki, işletmelerin siber güvenlik konusunda başlı başına bir strateji ve politika geliştirilmesi gerek. Ancak bu sayede işletmeler güvenli ve sürdürülebilir BT modelleri oluşturabilirler. Proline bu noktada kurumlara kendi çalışma modellerine uygun siber güvenlik stratejilerini belirlemeleri ve bu stratejiyi uygulayabilecekleri çözümler bütününü sağlayabilmeleri noktasında danışmanlık sağlamakta. Siber güvenlik alanında temel güvenlik ihtiyaçlarının yanı sıra BYOD, MDM, Advanced Malware Protection, SIEM ve korelasyon çözümleri gibi konularda da çözümler sunulabilmekte.

Eset Türkiye Genel Müdür Yardımcısı Alev Akkoyunlu

BİR SALDIRI OLMASINI BEKLEMEYİN, ÖNLEM ALIN

Fiziksel yollardan işlenen suçların pek çoğu bugün küresel anlamda sayısal şekle evriliyor. Siber saldırılar, kısa süre içinde tüm ülkelerde astronomik düzeyde artmış durumda. Sadece 2014 yılı içerisinde 550 milyon adet siber saldırı gerçekleşti. Rakam giderek artıyor.

Sürekli yeni saldırı teknikleri geliştiren siber saldırganlar, son iki yıldır 'phishing', yani oltalama saldırılarını hızlandırmış durumda. Bu konuda fidye yazılımı Cryptolocker, açık ara önde gidiyor. Şifre-fidye yazılımları, kötü amaçlı yazılım geliştiricileri için ana işlerden biri haline geldi. Cryptolocker, e-posta kutusuna gelen sahte telefon faturası veya kredi kartı ekstresi görünümünde eklenti dosyalı bir e-posta ile bulaşıyor. Kişi merak ederek, eklentiyi açıyor ve böylece virüsü bulaştırıyor.

Burada ilginç olan şu: Bu e-postalar bireysel olarak kişilere geliyor. Ancak kişi, çalıştığı işyerinde bu e-postayı görmek üzere eklentiyi açtığında, virüsü kurumdaki bilgisayara, dolayısıyla da tüm sisteme bulaştırıyor. Yani saldırı bireysel görünüyor, ancak bulaşma kurumlarda gerçekleşiyor.

Son dönemde hem küresel düzeyde hem de Türkiye'de bu tarz siber saldırılar adeta zirve yapmış durumda. Örneğin 2014'ün Kasım ve Aralık aylarında gerçekleşen Crytolocker saldırısında Türkiye, 11 bin 700 adet etkilenen sistemle, en fazla saldırıya uğrayan ülke oldu

Özellikle KOBİ'lerde bu tarz saldırıların çok yoğun gerçekleştiğini görüyoruz. Ne yazık ki, firmalar, saldırılar gerçekleştikten sonra harekete geçiyor ve önlem almaya çalışıyor. Yani farkındalık ne yazık ki zarardan sonra oluşuyor. Oysa tüm zarar oluşmadan, üstelik çok daha makul maliyetlerle önlem alınabilir. Burada "önlem" kelimesini de biraz açmak gerekiyor. Öyle veya böyle, artık tüm şirketler ve bireyler, bir biçimde güvenlik yazılımı kullanıyor. Ama maalesef bunların pek çoğu güncel değil, crack ürün veya yeterli güvenlik seviyesine sahip değil. Durum böyle olunca, güncel saldırılara karşı esasen sistemler savunmasız kalıyor.

Kurumların, sayısal güvenlik konusunu bir şirket politikası olarak benimseyip, bu yönde yatırım yapması gerekiyor. Güncel işletim sistemleri, proaktif antivirüs, yedekleme gibi güvenlik ve iş sürekliliği çözümleri mutlaka uygulanmalı. Bunları yapmamak, yapmaktan daha maliyetli.

Labris Networks İş Geliştirme Yöneticisi Hakan Sarıkaya

RİSKLER KARŞISINDA ÖNLEMLERİN ÖNEMİ AÇIKCA ORTADA

BT sistemlerinde güvenliği sağlamanın yöntemi bu güvenliğin sürekli olması. Bu sürekliliği sağlayabilmenin en önemli aracı; şirketin düzenli olarak teknolojinin gereklerine ve değişimine göre güncellenen bir güvenlik politikası olması. Özellikle şirketleri maddi anlamda etkileyen olaylar yaşandığı zaman veya denetleme mekanizmaları geliştikçe, siber güvenliğin ne kadar önemli olduğu daha fazla anlaşılıyor. Kültür olarak işine, kullandığı altyapılara, iş verimliliği ve güvenliğine önem veren kurumlar için bilişim güvenliği de önemli bir kalem. Eğer bir siber korsan en önemli verilerinizi ele geçirirse, o an verilerinizi geri almak için nasıl bir meblağı gözden çıkarabileceğinizi düşünün. İşte bilişim güvenliği çözümleri, bu meblağın çok çok küçük bir parçasına mal oluyor ve sizi belki de şirketinizin faaliyetlerini durdurmanıza yol açacak bir süreçten sakınıyor. Olası bir felaketin boyutları göz önüne alındığında bilişim güvenliğinin önemi açık seçik gün yüzüne çıkıyor. Tüm dünyada bilişim suçlarının ekonomiye etkisi 400 milyar doların üzerinde.

Kamu kurumlarında da güvenlik, milli çözümlerle birlikte anılır olmuştur. Kamuda son yıllarda oluşan bilincin, ürün açıklarının veri sızdırmada kullanılıyor olduğuyla ilgili kanıtların ortaya çıkması ve yurtdışı veri merkezlerinin güvensizliğinin anlaşılması ile daha da şekillendiği ve hızlı aksiyonlara dönüştüğü görülmekte. Alınan tedbirlerde Almanya, Kore gibi ülkeler öne çıkmakta. Türkiye yayınlanan eylem planı ve devamında gelen aksiyonlarla duruşunu belirlemiş, fakat ürün ve bilgi birikimi çıkarmakta, oluşması gereken rol ve birimlerin içini doldurmakta zorluk çekmekte. Üretici olmayan, sürdürülebilir bilgi birikimine sahip olmayan ülkelerin bu başlıkta gerçekten dik ve içi dolu bir duruş sergileyebilmeleri zor.

Kurmuş olduğumuz Labris SOC'de (Security Operations Center), Türkiye ve dünyadaki siber tehditler ve yayılımlar takip ediliyor. Olası güvenlik açıkları, CWL (Cyber Warfare Labs) ilgililerinin de bulunduğu ekiplerce değerlendiriliyor. DDoS saldırılarına karşı geliştirdiğimiz Harpp DDoS Mitigator ürün ailemiz bu laboratuvardan çıktı. Siber güvenlik dediğimiz konu, özellikle yetkin ekiplerle merkezi mekanizmalar ile korunmanın sağlanması gerekliliğini ve bunu destekleyen süreçlerin ve prosedürlerin "bilgi güvenliği" disiplinine uygun şekilde tüm firmaya yaygınlaştırılıp uygulanması ile sağlanabilir. Burada yazanlara bakarsak çok az firmada veya kurumda bu tarz bir yapılanma olduğunu görebilirsiniz.