TREND MICRO

A Brave

Bulutta Güvenlik Kimin Kontrolünde?

Trend Micro Görüşü

Şubat 2011

Yazan: Dave Asprey,
Bulut Güvenliği Bölümü
Başkan Yardımcısı

BULUTTA GÜVENLIK KIMIN KONTROLÜNDE?

I. BULUTTA GÜVENLIK KIMIN KONTROLÜNDE?

Bulut bilgi işlem bugün için teknoloji dünyasında en moda sözcüktür. Talep üzerine verilen BT yazılım ve altyapı hizmetlerinin internet üzerinden sunulması, BT ekiplerine eşi benzeri görülmemiş verimlilik, maliyet tasarrufu ve ölçeklendirilebilirlik olanakları sağlayabilir. Bununla birlikte, oyunun kurallarını değiştiren bu avantajlarla beraber yepyeni zorluklar da baş göstermekte ve bu zorluklar güvenliğe yönelik en geleneksel yaklaşımları geçersiz kılmaktadır. Bu yeni bilgi işlem paradigmasının kalbinde yer alan çelişki, bulutun bir anlamda ağır işlerin büyük bir bölümünün dış kaynaklarla karşılandığı basitleştirilmiş ve kullandıkça ödenen BT sunmasına karşın, aynı zamanda çok sayıda karmaşık sorun ve olası veri güvenliği riskine yol açmasıdır.

İster kendi inisiyatiflerine dayalı olarak, ister işlerin neden olduğu bir zorlamaya bağlı olarak olsun, BT yöneticileri 21. yüzyıldaki bu bilgi işlem ortamında sahip oldukları seçenekleri yeniden değerlendirmektedir. Söz konusu riskleri ve güvenlik sorumluluklarının nereye kadar uzandığını bilmek istiyorlar.

Burada Hizmet Olarak Altyapı (IaaS) (BT yöneticilerinin ağ, depolama, sunucu ve diğer operasyonel öğeleri kiralamasını sağlayan altyapı) bağlamında bu sorunları ele almaya çalışıyoruz. Bu aynı zamanda, SaaS gibi modellerde olduğundan daha fazla sayıda güvenlik kontrolü kullanma konusunda şirketlere daha fazla özerklik de sağlamaktadır.

II. NEDEN BULUT?

İşin genel bulut tarafında, her şey ölçeklendirme ve capex (Yatırım Harcamaları) yerine opex'in (İşletim Harcamaları) kullanılabilmesi ile ilgilidir. Bulut bilgi işlem müşterileri, bir fayda modeli içinde hizmet sağlayıcılarına sadece kullandıkları şeyler için para ödeyerek donanım, yazılım ve diğer altyapı hizmetleri ile ilgili yatırım harcamaları yapmaktan kurtulurlar. Kaynakların talep üzerine sağlanması da, firmaların bilgi işlem gereksinimlerine göre dinamik olarak ölçeklendirme yapabilmelerini sağlar ve bu da şirketlerin daha atak olmalarını mümkün kılar.

Özel bulut cephesinde, her şey daha fazla esneklik ve dahili müşterilerin gereksinimlerine daha kısa sürede tepki verilmesi ile ilgilidir.

Bu tür avantajlar sunduğu için, yeni bilgi işlem paradigmasının bu kadar ilgi görmesi şaşırtıcı değildir. Örneğin, Aralık ayında Cisco tarafından yapılan araştırma, tüm dünyadaki BT uzmanlarının yüzde 52'sinin bulut bilgi işlem teknolojisini zaten kullandığını ya da önümüzdeki üç yıl içinde kullanmayı planladığını ortaya çıkarmıştır. Güvenlik organı ISACA tarafından yapılan benzer bir ankette (Mart 2010) Avrupa'daki organizasyonların üçte birinin zaten bulut bilgi işlem sistemlerini kullandığı anlaşılmış ve küresel danışmanlık şirketi Accentura (Temmuz 2010) müşterilerinin yarısının görev açısından önem taşıyan uygulamalardan bazılarını bulutta çalıştırdığını açıklamıştır.

III. ÇEVRE GÜVENLIĞI ÖLMEDI — BULUTU KORUMAYA YÖNELIK IKI YAKLAŞIM

Söz konusu olan genel bulut modeli olduğunda, geleneksel kurumsal güvenlik çevresinin artık var olmadığı gerçeği konusunda çok şey söylenmiştir. Tartışma sürmektedir ama güvenlik duvarları, izinsiz giriş önleme sistemleri ve diğer güvenlik işlevleri buluta kadar uzanmamaktadır. Bunun yerine, firmalar bulut sağlayıcıları tarafından sunulan temel düzeydeki çevre güvenliğine güvenmek zorunda kalmaktadır.

Ama başka bir açıdan bakıldığında, çevre tabanlı güvenlik modeli aslında ölmemiştir; çalışan bir güvenlik mimarisinin faydalı bir parçası (ama tek parçası değil) haline gelmiştir. Bulut konusuyla ilgilenirken, kuruluşlarda hâlâ çevre güvenliği eğilimi vardır. Burada firmaların yapacağı seçim, çevre güvenliğini buluta ya da bulutu çevre güvenliğine (ya da her ikisi) genişletip genişletmeyecekleridir. Her iki durumda da, dahili kurumsal güvenlik ortamlarında oldukları için, ek güvenlik katmanları gereklidir. Ancak, buluttaki dış kaynak kullanımından kaynaklanan olası görülebilirlik ve kontrol kaybı ile ilgili olarak, her iki senaryonun da benzer dezavantajları vardır. CISO'ların tetikte olmaları, durum tespiti yapmaları ve söz konusu risklerin farkında olmaları gerekir.

1) İlk senaryo (çevre güvenliğinizin buluta genişletilmesi) genel bulut hizmeti sağlayıcınızın sunucularına IPSec VPN tüneli kurulması ve genellikle güvenlik yazılımı ve sanal araçlar biçiminde, genel bulut sunucusuna kurumsal düzeyde güvenlik çözümü yerleştirilmesini kapsar.

Bu düzenlemenin **avantajı** Active Directory'yi yeniden yapılandırmak zorunda olmamanız ve bulut sunucularınız "çevre güvenliğinizin" içinde olduğu için, diğer mevcut yönetim araçlarının da bulut düzenlemenizle çalışacak olmasıdır.

Ancak, **dezavantajlar** açısından bakıldığında, bulut sunucunuzu ne kadar iyi koruduğunuza bağlı olarak, mimarinizi bulutla ilgili risklere maruz bırakmış olabilirsiniz [aşağıda ana hatlarıyla açıklanmaktadır]. Bu risklerin hafifletilmesine yardımcı olmak için, bulutta olsun ya da olmasın, önemli sunuculara yönelik tüm bağlantılarda da olduğu gibi, bulut ile şirket içi sunucular arasındaki bağlantının, şüpheli trafiğe karşı takip edilmesi önemlidir. Bu, korunması gereken bir başka çevre daha yaratsa da, bir diğer seçenek de, ekstra bir DMZ ve güvenlik duvarı eklemektir.

Özellikle bu güvenlik bariyerlerini tasarlamak için zamanı ve BT kaynakları olmayan küçük organizasyonlar başta olmak üzere, bulut telaşı içindeki birçok firma bu adımı unutmakta ya da göz ardı etmektedir.

Bulut sunucularına güvenebilmeniz için bu bulut sunucularına IDS/IPS çift yönlü güvenlik duvarı, vb. yeterince güvenlik çözümü eklemek de gereklidir.

RİSKLER

CIO'lar bulut sunucularının dahili olarak hafifletmeye alıştıklarından farklı tehditlere maruz kalacağını unutmamalıdır.

- Kaygı duyulan önemli konulardan biri de, firmalara bulut sağlayıcılarının fiziksel ya da yönetimsel erişim kayıtlarının büyük olasılıkla verilmeyecek olmasıdır. Örneğin, firmalar genel bulut sağlayıcıları için çalışan bir BT yöneticisinin verilerine erişip erişmediğini nasıl bilecekler? İçeriden kaynaklanan tehdit, erişim kayıtları tutularak şirket içinde hafifletilebilir ama buluttaki bu görülebilirlik kaybı, standart olarak veri şifrelemesinin yaygın bir biçimde benimsenmesine yol açacaktır.

  [*Aralık ayında, Microsoft tarafından barındırılan kurumsal set BPOS müşterilerine ait kurumsal verilere, bir yapılandırma hatası sonrasında, yazılımın diğer kullanıcıları tarafından erişildiği ve indirildiği ortaya çıkmıştır. Sorun kısa bir sürede giderilse de, bu nelerin yanlış gidebileceğini ve sizin düzenleme organlarınızın standartlarını karşıladıklarından emin olmanız için bulut sağlayıcınızın sistemlerinde görülebilirlik olanağına sahip olmanın önemini göstermektedir*.]

- Ortak depolama da, verilerinin bulutta aynı disk içinde rakip bir şirketin verileri ile birlikte olması halinde, verilerinin güvende olmayacağı konusunda endişeleri olan firmalar açısından risk taşıyan bir diğer noktadır.

- Bazı genel bulut sağlayıcıları güvenlik konusunda yeterince istekli ya da yaptıkları şeyler konusunda olmaları gerektiği kadar saydam değildir. Başlangıç noktası olarak, görev açısından önem taşıyan verileri buluta yerleştiriyorsanız, en azından ISO 27001 ve SAS70 II gibi en iyi güvenlik uygulamalarına uyulup uyulmadığına bakmanız ve sağlayıcınızın SLA'larını ve güvenlik ilkesini dikkatle incelemeniz gerekir.

- Önceki nokta ile ilgili konuşmak gerekirse, birçok bulut sağlayıcı bir ihlalin söz konusu olduğu durumlarda, ödeyecekleri tazminatı verdikleri hizmet bedeli ile sınırlandırmaktadır (hata onlara ait olsa bile). Bir veri ihlalinin neden olacağı itibar kaybı, cezalar ve milyonlarla ifade edilebilecek finansal kayıpların, müşteri tarafından karşılanması gerekecektir.

2) İkinci senaryo (bulutun çevre güvenliğinize genişletilmesi) bulutun etkili bir şekilde çevre güvenliğinize genişletilmesine olanak sağlar ve bir IaaS genel bulut sağlayıcısı ya da bulut tabanlı MSSP ile tesis içinde bir bulut düğümü kurulması konusunda anlaşma sağlanmasını gerektirir.

Büyük kuruluşlar arasında her geçen gün biraz daha yaygınlaşan bu düzenlemenin **avantajı**, nispeten daha iyi anlaşılan bir model olmasıdır. Örneğin Akamai benzeri bir çalışmayı on yılı aşkın bir süredir yapmaktadır. Akamai uzun yıllardır müşterinin güvenlik çevresi dahilinde bulunan bir sunucuyu yönetmekte ve Integralis gibi MSSP'ler de "buluttan" uzak güvenlik

duvarı yönetim hizmetlerini sağlamaktadır. Diğer örnekler arasında, bir kurumsal ağ içindeki güvenlik sunucularını, buluttaki binlerce sunucudan oluşan güvenlik ağına bağlayan Trend Micro Smart Protection Network yer almaktadır.

Ancak, veri merkezinizde ya da şubenizde bulunan ve bulut sağlayıcısı tarafından merkezi olarak yönetilen ya da güncellenen bu kutulardan birine sahip olmanın kolaylığına karşın, asıl **dezavantajlar** bunun özünde hâlâ bir bulut hizmet olması ve bu nedenle de, BT yöneticisi açısından ilk kurumla ilgili çok sayıda risk teşkil etmesidir.

- Fiziksel ve/veya yönetimsel erişim kayıtlarda görülebilirlik kaybının neden olduğu riskler devam etmektedir.

- Görev açısından önem taşıyan verilerin kaybedilmesine yol açacak ihmallerde sorumluluk, hâlâ hizmet bedeli ile sınırlı olarak kalacaktır.

- Bu özelliğin açılması ve kapatılması mümkün olmasına karşın, açık olduğunda, bulut sağlayıcı ağınıza ve uygulama verilerinize erişecektir ve bu nedenle de bulut sağlayıcısına güvenilmesi gerekir. O sağlayıcı güvenlik konusuna odaklanıyor ve SLA'ları konusunda şeffafsa, endişelenecek pek bir şey yok demektir. Ancak, daha önce de üzerinde tartışıldığı gibi, en kapsamlı hizmetleri sunan bulut sağlayıcıların değer tekliflerinin merkezinde güvenlik yoktur.

  Bu ‘yeterince iyi’ güvenlik ile ‘en uygun düzeyde’ güvenlik arasındaki farkın ortaya konulması meselesidir. Örneğin, yönetilen bir güvenlik hizmeti sağlayıcısı tarafından güvenlik çevrenizde yapılan bulut tabanlı bir e-posta hizmeti kurulumu, büyük olasılıkla tipik bir genel bulut satıcısının sağladığı kurulumdan daha güvenilir olacaktır.

IV. ÖYLEYSE BULUTTA GÜVENLIK KIMIN KONTROLÜNDE VE NEREDE BOŞLUKLAR VAR?

Buradaki tatsız gerçek şu ki, bulut sağlayıcısından yardım almanın yollarını arıyorsanız, büyük olasılıkla hayal kırıklığına uğrayacaksınız. Aslına bakılırsa, erişim kayıtlarındaki görülebilirlik kaybı ya da güvenlik ilkelerinin rahatsız edici derecede belirsiz şekilde yazılmış olması nedeniyle, işinizin daha da zorlaştığını fark edebilirsiniz.

- Bulut sunucularınızı aynı dahili sunucularınızı olduğu gibi koruma altına almalısınız. Buna IDS/IPS, DLP araçları, çift yönlü güvenlik duvarı ve şifreleme dahildir.

- Çok az sayıda genel bulut sağlayıcı ağ trafiğini sizin istediğiniz kadar yakından izlemenize izin vereceği için, bulut ortamında ağ güvenliği cephesinde sorunlar yaşayabilirsiniz. Kendi ağınızda, tüm yönlendirici/anahtar yapılandırmaları ve kayıtları serbesttir ve ağ trafiğini istediğiniz gibi takip edebilirsiniz. Ama bulutta bunların hiçbiri söz konusu değildir. Uyum açısından bakıldığında, bu durum bulut teknolojisinin kabul edilmemesine neden olabilir; bu nedenle sağlayıcınızın ağ takibine ve erişimine ne kadar izin verdiğini öğrenmeniz hayati önem taşır.

- Ağ trafiğinde ve sağlayıcınızın erişim kayıtlarında görülebilirlik kaybı nedeniyle, sabit ve hareket halindeki verilerin şifrelenmesi fazlasıyla önemli bir hal almaktadır.

- Bununla birlikte, birçok bulut sağlayıcısı yönetim düzeyinde endişe verici derecede fazla rol tabanlı erişim kontrolü de sunmaktadır. Örneğin Amazon EC2 ile, bir hesap tüm kutulara sahiptir ve böylelikle, organizasyonun hesap erişimine sahip bir üyesi istediği zaman kutu ekleme ve çıkarma olanağı sayesinde, krallığın tüm anahtarlarını elinde tutabilir.

- Özel bulutta, BT departmanının güvenliği elinde bulundurmasına, sunucuların yaratılabileceği hız ile meydan okunmaktadır. BT'nin sunucular sunabilme becerisi ile şirketlerin sunucu gereksinimi arasındaki doğal denge, bu süreç hızlandıkça bozulmaktadır. Şirketlerin bugün ihtiyacı olan şey, bir lisansın maliyetini karşılayıp karşılamayacaklarını bilmektir ve özel bir bulut ortamında, bir iş birimi bir sunucuyu 6 hafta yerine 1 ya da 2 gün içinde kurup çalışır duruma getirebilir.

  Bununla birlikte, her bir yeni sunucu talebi düzgün şekilde yönetilmelidir; çünkü yönetilmesi gereken kutuların sayısı arttıkça, güvenlik riskleri de artar. BT yöneticilerinin işletmelerden gelecek taleplerin önce BT'den geçmesini sağlayacak, merkezi bir yetkilendirme süreci tahsis etmeleri büyük önem taşımaktadır.

V. EYLEM ÇAĞRISI

Şirketler

Sabit ve hareket halindeki verileri şifreleyin ve şifreleme anahtarlarını verilerden ayrı bir yerde (örneğin bulut sağlayıcının kolayca erişemeyeceği bir yerde) muhafaza etmeye özen gösterin.

Fiziksel sunucularınızda kullandığınız tüm güvenlik araçlarını bulutta da kullanın; çünkü tüm bulut sağlayıcılarının size vereceği şey, yeterli güvenlik önlemlerinin olmadığı çıplak bir İS'dir.

Bulut sağlayıcılar

Güvenlik ilkeleriniz ve erişim kontrolleri ve ağ trafiği ile ilgili prosedürleriniz konusunda daha açık ve şeffaf olun. Müşterilerin kimin, ne zaman ve ne yaptığını bilmeleri ve kayıtları görmelerine izin verilmesi gerekir.

Müşterilerinizin sunduğunuz güvenlik özelliklerini ve verilerini kendi ve düzenleme organlarının standartlarına uygun olarak koruma altına almak için neler yapmaları gerektiğini anlamaları için, SLA'larınızı anlaşılır hale getirin.

BULUTTA GÜVENLIK KIMIN KONTROLÜNDE?

Özel bulut ortamları

Şirketten gelen tüm yeni bulut sunucu talepleri için merkezi bir yetkilendirme süreci yaratın (mevcut bir süreç yoksa). Neden bir sunucuya ihtiyaçları olduğunu, sunucuda hangi uygulamaların çalıştırılacağını, bu sunucunun ne kadar süre var olacağını ve sunucudan ne kadar akış geçeceğini bilmeniz ve bu gereksinimlerle ilgili düzenli kontroller yapmanız gerekir.

Hazır olun....BT çalışma hızını artırmaya zorlanmaktadır. Şirketin iyiliği adına, güvenlikten ödün vermeden, bu gereksinimleri zamanında desteklemeye hazır olmanız gerekir.