Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Bulutu Güvenle Kullanmak

Giriş

"Bulut" farklı insanlara farklı şeyler ifade edebilir ancak genellikle internette yazılımlarınızı ve/ve ya verilerinizi sizin için saklayan ve yöneten bir servis sağlayıcı anlamına gelir. Bulut'un bir avantajı, kolayca verilerinize erişebilmeniz, dünyanın herhangi bir yerinden çeşitli cihazlardan gelen bilgiler ile senkronize edebilmeniz ve ayrıca bilgilerinizi istediğiniz herhangi biri ile paylaşabilmenizdir. Bu tür servislere "Bulut" diyoruz çünkü verilerinizin fiziksel olarak nerede olduklarını çoğunlukla bilemezsiniz. Google Docs'da doküman yaratmak, Dropbox ile dosya paylaşmak, Amazon Cloud'da kendi sunucunuzu kurmak, Salesforce'da müşteri verilerini tutmak ya da Apple'ın iCloud servisinde müziklerinizi veya resimlerinizi arşivlemek Bulut Bilişimin örneklerindendir. Bu çevrim-içi servisler sizi daha fazla üretken yapabilirler ancak kendilerine özgü riskleri de beraberlerinde getirirler. Bu sayıda Bulut'u nasıl güvenli hale getirebileceğinizi ele alacağız.

Konuk Yazar

Dave Shackleford (**@daveshackleford**), Voodoo Güvenlik'in sahibi ve SANS Güvenlik 579: Sanallaştırma ve Özel Bulut Güvenliği ve Güvenlik 524: Bulut Güvenlik Temelleri dahil olmak üzere birçok SANS eğitim kursunun yazarı olan profesyonel bir danışmandır.

Bir Bulut Sağlayıcısı Seçme

Bulut ne iyi ne de kötüdür, hem evde hem de işte işleri yapmak için kullanılan bir araçtır. Ancak, bu servisleri kullandığınızda, özel verilerinizi başkalarına teslim etmiş olursunuz ve bu servislerden hem bu verileri güvende tutmasını hem de bu verilere ulaşılabilirliği sağlamasını beklersiniz. Durum böyle olunca Bulut sağlayıcınızı akıllıca seçtiğinizden emin olmak istersiniz. İş bilgisayarlarınız ve iş ile ilgili bilgiler için şirketinizin Bulut servisleri kullanmanıza izin verip vermediğini yöneticiniz ile kontrol edin. Eğer Bulut'u kullanmaya izniniz var ise hangi Bulut servisini kullanacağınızı ve bu servisleri nasıl kullanacağınız ile ilgili politikaları teyit edin. Kişisel kullanım için Bulut servisi üzerinde düşünüyorsanız, aşağıdakileri dikkate alın.

1. **Destek**. Yardım alma ya da soruların cevaplanması ne kadar kolay? Bağlantıya geçebileiceğiniz bir e-posta adresi var mı, sorularınızı gönderebileceğiniz bir açık forum ya da web sitelerinde Sıkça Sorulan Sorular bölümü?
2. **Basitlik**: Servisi kullanmak ne kadar kolay? Servis ne kadar karmaşık ise sizin hata yapma ve yanlışlıkla bilgilerinizi açık etme olasılığınız o kadar yüksektir. Kolay anlaşılabilir, konfigüre edilebilir ve kullanılabilir olduğunu düşündüğünüz bir Bulut sağlayıcı seçin.

Bulutu Güvenle Kullanmak

3. **Güvenlik**. Sizin hakkınızda ne gibi bilgiler toplanıyor, eğer tutuluyorsa? Bilgisayarınızdan Bulut'a bilgiler nasıl aktarılacak ve Bulut'ta nasıl tutulacak - şifrelenecek mi ve eğer öyleyse kim sizin verilerinizin şifresini çözecek?
4. **Kullanım Koşulları**: Bir dakikanızı ayırın ve kullanım koşullarını gözden geçirin (Şaşırtıcı bir şekilde çoğunlukla okuması kolaydır). Kimin verilerinize ulaşacağını ve yasal haklarının ve sağlayıcı tarafından ya da sizden beklenen herhangi bir güvenlik sorumluluğu var ise neler olduğunu teyit edin.

Bulut sizin bilgilerinizi data ulaşılabilir ve üretken yapabilir ancak verilerinize nasıl eriştiğinize ve bu bilgileri nasıl paylaştığınıza dikkat edin.

Verilerinizi Koruma

Bulut sağlayıcıyı seçtikten sonra bir sonraki adımınız Bulut servisini uygun bir şekilde kullandığınızdan emin olmaktır. Dosyalarınızın güvenliği açısından bilgilerinize nasıl ulaştığınızın ve paylaştığınızın başka herhangi bir şeyden daha büyük bir etkisi vardır. Kilit önemlerden bazıları:

1. **Kimlik Doğrulama**: Bulut hesabınız ile kimliğinizi doğrularken eşsiz ve güçlü bir şifre kullanın. Eğer Bulut sağlayıcınız iki-adımlı doğrulama sunuyorsa bunu etkinleştirmenizi kuvvetle tavsiye ederiz. Hesabınızı korumak adına bu, alınabilecek en önemli önlemlerden biridir.
2. **Dosya/Klasör Paylaşma**: Bulut paylaşmayı çok kolaylaştırır, bazen çok basittir. En kötü senaryoda dosyalarınızı belirli bir kişiyle paylaşıyor olduğunuzu düşünürsünüz ancak yanlışlıkla internette herkesin ulaşabileceği şekilde dosyalarınızı ve dahası tüm klasörlerinizi herkese açabilirsiniz. Kendinizi korumanın en iyi yolu varsayılan olarak kimse ile hiçbir dosyanızı paylaşmamanızdır. Daha sonra belirli kişilerin (ya da grupların) belirli dosyalara veya klasörlere gerektiğinde erişimine izin verirsiniz. Eğer birinin sizin dosyalarınıza erişmesine gerek kalmadıysa, onları kaldırın. Bulut sağlayıcınız size, dosya ve klasörlerinize kimin erişimi olduğunu takip etmenizi sağlayan kolay bir yol sağlamalıdır.
3. **Bağlantılar ile Dosya/Klasör Paylaşma**: Bazı Bulut servislerinin ortak bir özelliği, dosya ya da klasörlerinizi işaret eden bir web bağlantısı yaratabilmeleridir. Bu özellik sizin basitçe bir web bağlantısı temin ederek dosyalarınızı istediğiniz herhangi biri ile paylaşmanıza müsade eder. Ancak bu yaklaşımın güvenliği azdır, bu bağlantıya sahip herhangi biri sizin kişisel dosya ya da klasörlerinize ulaşabilir. Eğer bu bağlantıyı sadece bir kişiye gönderirseniz, bu kişi bu bağlantıyı başkalarıyla paylaşabilir ya da arama motorlarında bu bağlantı görünebilir. Eğer veriyi bir bağlantı ile paylaşacaksanız, son kullanım zamanı belirleyerek ya da mümkünse bağlantıyı bir şifre ile koruyarak ihtiyaç kalmadığında bağlantıyı etkisizleştirdiğinizden emin olun.

Bulutu Güvenle Kullanmak

4. **Ayarlar**: Bulut sağlayıcınız tarafından size sunulan güvenlik ayarlarını bilin. Örneğin, eğer bir dosyayı biri ile paylaşırsanız, sizin bilginiz olmadan başkaları ile bu verileri paylaşacaklar mı? Ayrıca ne zaman ve kimin paylaştığınız içeriği görüntülediğini görme yolları olup olmadığına bakın. kişilerin dosyaları değiştirebildiği "okuma+yazma" hakkı vermek yerine paylaşımı "Salt okunur" ile sınırlandırabiliyor musunuz?
5. **Antivirüs**: En güncel versiyon antivirüs programının bilgisayarınıza ya da bilgileriniz paylaştığınız diğer bilgisayarlarda yüklü olduğundan emin olun. Eğer paylaştığınız bir dosyaya virüs bulaşırsa, aynı dosyaya ulaşan diğer bilgisayarlara da bulaşır.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Kaynaklar

İki-Aşamalı Doğrulama:	https://securingthehuman.sans.org/ouch/2015#september2015
Şifreler:	https://securingthehuman.sans.org/ouch/2015#april2015
Şifre Yöneticileri:	https://securingthehuman.sans.org/ouch/2015#october2015
Kötü Amaçlı Yazılım Nedir?:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Bulut Güvenlik Temelleri:	https://sans.org/sec524