OUCH! | Eylül 2014

Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Bulut Bilişim Hizmetlerini Güvenle Kullanmak

Özet

"Bulut Bilişim" bireylerin ve organizasyonların hızlı bir şekilde geçiş yaptıkları güçlü bir teknoloji. "Bulut" farklı bireyler için farklı anlamlara geliyor olabilir ancak genel olarak sizin verilerinizin internet üzerinden yönetilmesi ve saklanması için bir hizmet sağlayıcının kullanılması anlamına gelir. Bulutun tek avantajı kolaylıkla ve farklı cihazlardan dünyanın herhangi bir yerinden verilerine erişmeniz ve senkronize etmeniz değildir, aynı zamanda dilediğiniz kişiyle dilediğiniz bilgilerinizi paylaşabilirsiniz. Bu hizmetleri "Bulut" olarak adlandırmamızın nedeni, verilerin fiziksel olarak nerede saklandığının genellikle bilinmemesidir. Bulut bilişime verilebilecek örnekler; Google Docs kullanılarak dokümanların yaratılması, Dropbox kullanılarak dosya paylaşımı, Amazon Cloud üzerinde kendi sunucunuzu kurmak, Apple iCloud üzerinde müzik ya da resim dosyalarını barındırmak olabilir. Bu çevrimiçi hizmetler sizin daha üretken olmanızı sağladığı gibi, kendilerine özgü riskleri de beraberinde getirirler. Bu sayıda, "Bulut"dannasıl güvenli bir şekilde yararlanabileceğinizi anlatacağız.

Konuk Yazar

James ve Kelli Tarala (**@isaudit** / **@kellitarala**) Enclave Güvenlik'in baş danışmanları ve aralarında "SANS Audit 566 : 20 Kritik Güvenlik Kontrolünün Uyarlanması ve Denetimi" ile "MGT 415 : Risk Değerlendirmelere Uygulamalı Giriş" gibi eğitimlerin de olduğu birçok SANS eğitim içeriklerinin yazarlarıdır.

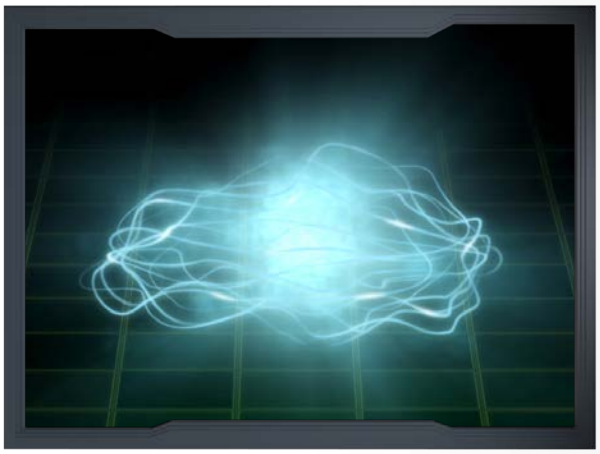
Bir Bulut Hizmet Sağlayıcısı Seçmek

Bulut ne iyi ne de kötüdür, o hem işyerinde hem de evde kullanabileceğiniz bir araçtır. Ancak, bu hizmetleri kullandığınızda, kişisel verilerinizi yabancılara teslim ediyor ve onlardan bu verileri hem güvenli hem de erişilebilir tutmalarını bekliyorsunuz. Hal böyle olunca da seçiminizi akıllıca yaptığınızdan emin olmak istersiniz. İş bilgisayarlarınız ve iş ile ilgili bilgileriniz için, Bulut bilişim hizmetlerini kullanıp kullanamayacağınızı, yöneticinizle görüşmelisiniz. Eğer izniniz varsa, lütfen hangi Bulut bilişim hizmetlerini kullanabileceğinizi ve bunları nasıl kullanacağınızı anlatan politikaların hangileri olduğunu doğrulayın. Eğer kişisel olarak Bulut bilişim hizmeti kullanmayı düşünüyorsanız, aşağıdakileri göz önüne alın.

1. **Destek**: Yardım almanız ya da bir sorunuzun cevaplanması ne kadar kolay ? Arayabileceğiniz bir telefon numarası ya da iletişime geçebileceğiniz bir e-posta adresi var mı? Destek için halka açık forumlar ya da internet sitelerinde Sıkça Sorulan Sorular sayfası gibi başka seçenekler var mı ?
2. **Basitlik**: Bu hizmeti kullanmak ne kadar kolay? Daha karmaşık hizmet, sizin hata yapmanızı ve yanlışlıkla bilgilerinizi açığa çıkarmak ya da kaybetmenizi kolaylaştırır. Anlaması, yapılandırması ve kullanımı kolay bir Bulut hizmet sağlayıcısı seçin.

Bulut Bilişim Hizmetlerini Güvenle Kullanmak

3. **Güvenlik**: Bilgisayarınızdan Bulut ortamına veriniz nasıl iletiliyor, bağlantı şifreleme yöntemleri ile güvenli mi? Verileriniz nasıl saklanıyor, şifrelenerek mi ve eğer evet ise, kimler verilerinizin şifrelerini çözebilir ?
4. **Hizmet Koşulları**: Bir dakikanızı ayırın ve Hizmet Koşulları bölümünü okuyun (genellikle okunması oldukça kolaydır). Verilerinize kimlerin erişebileceğini ve kanuni haklarınızın neler olduğunu öğrenin.



Bulut bilgilerinizin daha erişilebilir olmasını ve sizin daha üretken olmanızı sağlar, ancak, bilgilerinizi nasıl sakladığınıza ve paylaştığınıza dikkat etmelisiniz.

Verinizi Güvenli Hale Getirmek

Bulut hizmetini seçtikten sonraki adım, bu hizmeti uygun şekilde kullanıyor olduğunuzdan emin olmaktır. Verinizi nasıl eriştiğiniz, verinizi nasıl paylaştığınız, dosyalarınızın güvenliği üzerinde, diğer her türlü şeyden daha büyük bir etkiye sahiptir. Uygulayabileceğiniz önemli adımlardan bazıları:

1. **Kimlik Doğrulama**: Bulut hesaplarınız için güçlü, benzersiz birer parola kullanın. Eğer hizmet sağlayıcınız iki aşamalı doğrulama (2FA) destekliyorsa, aktif hale getirmenizi kesinlikle tavsiye ediyoruz.
2. **Dosya / Dizin Paylaşımı**: Bulut, paylaşımı gayet basit hatta bazen fazla basit hale getirir. Olumsuz bir senaryoda, siz yanlışlıkla dosyalarınızı hatta tüm dizinlerinizi, internet üzerinden halka açık hale getirebilirsiniz. Kendinizi korumak için en iyi yöntem, varsayılan olarak hiçbir dosya/dizin paylaşmayıp, ihtiyaç oldukça belirli kişi ya da grouplara yetkilendirme yapabilirsiniz. Erişim ihtiyacı ortadan kalktığında, yetkilerini kaldırın. Bulut hizmet sağlayıcınız dosya ve dizinlerinize kimlerin erişim izni olduğunu kolayca izleyebileceğiniz bir yöntem sağlıyor olmalıdır.
3. **Bağlantılar kullanarak dosya ve dizin paylaşımı**: Bulut hizmetlerinin ortak bir özelliği de dosya/dizinlerinizi gösteren bir web bağlantısı oluşturmalarıdır. Bu özellik, basitçe bu bağlantıyı paylaşarak herhangi biriyle bu dosyaları paylaşmanızı sağlar. Az da olsa güvenli görünen bu yaklaşım ile, bağlantıyı bilen herkesin kişisel dosya ya da dizinlerinize erişebilir. Siz bağlantıyı tek bir kişiye gönderseniz de, o kişi bu bağlantıyı başka birine gönderebilir, o da başkaları ile paylaşabilir ya da arama motorlarında görünebilir. Eğer bu şekilde paylaşım yapıyorsanız, ihtiyaç kalmadığında bağlantıları pasif hale getirin, ya da eğer mümkünse, bağlantıyı bir parola ile koruyun.
4. **Ayarlar**: Bulut hizmet sağlayıcınız tarafından sunulan güvenlik ayarlarını inceleyin. Örneğin, eğer bir başkası ile bir dizin paylaşıyorsanız, sizin bilginiz dışında onlar da başkaları ile verilerinizi paylaşabiliyorlar mı?
5. **Antivirüs**: Bilgisayarınızdaki ya da verilerinizi paylaştığınız herhangi bir bilgisayardaki antivirus uygulamasının en güncel sürümünün kurulu olduğundan emin olun. Paylaştığınız bir dosyaya virus bulaştığında, aynı dosyaya eriştiğiniz diğer bilgisayarlara da bulaşacaktır.

Bulut Bilişim Hizmetlerini Güvenle Kullanmak

6. **Yedekleme**: Bulut hizmet sağlayıcınız verilerinizi yedekliyor olsa bile, kendiniz düzenli olarak yedeklerinizi alma seçeneğini değerlendirin. Bu, sadece hizmet sağlayıcınızın iflası, kapanması ya da herhangi bir sebeple erişilemez olması durumunda verilerinizi korumakla kalmaz, aynı zamanda büyük miktardaki verilerde Bulut üzerinden yedekten dönmeye kıyasla çok daha kolay bir geri dönüş sağlar. Bir de, Bulut hizmet sağlayıcınızın dosyalarınızı ne kadar sıklıkla yedeklediğini, dosyalarınızın önceki sürümlerine geri dönme imkanı verip vermediklerini ve yedeklerinizi ne kadar sure ile erişilebilir tuttuklarını kontrol edin.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve http://www.securingthehuman.org 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

Güçlü Parolalar:	http://www.securingthehuman.org/ouch/2013#may2013
Parola Yöneticileri:	http://www.securingthehuman.org/ouch/2013#october2013
Yedeklemeler:	http://www.securingthehuman.org/ouch/2013#september2013
Güvenlik Terimleri:	http://www.securingthehuman.org/resources/security-terms

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis