

Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

- Yedekleme: Ne, Ne Zaman ve Nasıl ?
- Kurtarma
- Önemli Noktalar

Yedekleme ve Kurtarma

Giriş

Eğer yeterince uzun süredir bir bilgisayar ya da mobil cihaz kullanıcısı iseniz, er ya da geç, kişisel dosyalarınızı, dokümanlarınızı ya da fotoğraflarınızı kaybetmekle sonuçlanacak şekilde birşeyler ters gidecektir. Örneğin yanlış dosyaları silecek, donanım problemleri yaşayacak, cihazınızı kaybedecek ya da bilgisayarınıza fidye yazılımları gibi kötü amaçlı bir yazılım bulaşacaktır. Böyle zamanlarda yedeklemeler çoğunlukla sizin dijital hayatınızı yeniden kurabilmeniz için tek yoldur. Bu sayıda yedeklemelerin ne olduğunu, verilerinizin nasıl yedeklenmesini yapacağınızı ve sizin için en uygun stratejiyi nasıl geliştirebileceğinizi anlatacağız.

Konuk Yazar

Keith Palmgren BT güvenlik alanında 30 yılı aşkın deneyimi olan bir siber güvenlik uzmanıdır. SANS Kıdemli eğitmeni ve SANS SEC 301: "Bilgi Güvenliğine Giriş" in yazarıdır. Keith başarılı bir güvenlik danışmanlığı yürütmekte olup Twitter'da [@kpalmgren](https://twitter.com/kpalmgren) hesabı ile aktiftir.

Yedekleme: Ne, Ne Zaman ve Nasıl ?

Yedeklemeler verilerinizin bilgisayarınız ya da mobil cihazınız dışındaki herhangi bir yerdeki kopyalarıdır. Önemli bir veriyi kaybettiğinizde, yedeklerinizden verilerinizi kurtarabilirsiniz. Maalesef basit ve ucuz olmasına rağmen çoğu insan düzenli yedekleme yapmamaktadır. İlk adım neyi yedeklemek istediğinize karar vermektir. Bunun için iki yaklaşım vardır: (1) sizin için önemli olan belirli verilerin yedeklenmesi, (2) işletim sisteminiz de dahil herşeyin yedeklenmesi. Birçok yedekleme çözümü varsayılan yaklaşım olarak birinci yaklaşımı benimser ve en çok kullanılan dizinlerdeki tüm verileri yedekler. Çoğu zaman bu sizin için yeterli olabilir. Ancak neyi yedek alacağınız konusunda emin değilseniz ya da daha korumacı olmak isterseniz, herşey yedeklemenizi öneririz.

Bir sonraki kararınız ise ne kadar sıklıkla verilerinizi yedekleyeceğinizdir. Apple Time Machine ya da Microsoft Windows Yedekleme ve Geri Kurtarma gibi yedekleme uygulamaları, size otomatik "ayarla ve unut" yedekleme çizelgesi sunar. Yaygın seçenekler arasında saatlik, günlük, haftalık gibi seçenekler vardır. Bu çözümler siz çalışırken ya da bilgisayarınızdan uzakta iken gün içinde sessizce verilerinizi yedeğini alır. Diğer çözümler, yeni veya değiştirilmiş dosyaların kapatıldıktan sonra hemen yedeklerinin alındığı "sürekli korumayı" sunabilir. En azından otomatik olarak günlük yedek almanızı tavsiye ederiz.

Son olarak, nasıl yedekleme yapacağınıza karar vermelisiniz. Verilerinizi yedeklemek için iki yolunuz var: Fiziksel ortamlar ya da bulut tabanlı depolama. Herbir yaklaşımın avantaj ve dezavantajları bulunmaktadır. Eğer hangi yaklaşımı seçeceğinizden emin değilseniz, ikisini de eş zamanlı olarak kullanın. Fiziksel ortamlar, harici USB sürücüler ya da Wi-Fi erişimi olan ağ cihazları gibi sizin kontrolünüzde olan herhangi bir donanım olabilir. Kendi fiziksel ortamınızı kullanmanın avantajı, büyük miktardaki veriyi çok hızlı yedekleyebilme ve gerektiğinde kurtarabilmenizdir. Dezavantajı ise eğer bilgisayar ya da cihazınıza fidye yazılımı gibi bir kötü amaçlı yazılım bulaştıysa, yedeklemelerinize de bulaşmış olma ihtimali olmasıdır. Ayrıca

Yedekleme ve Kurtarma

yangın veya hırsızlık gibi felaketler yaşarsanız, sadece bilgisayarınızı kaybetmekle kalmayıp yedeklerinizi de kaybetme ihtimaliniz vardır. Durum bu olunca yedeklerinizin kopyalarını dışarıda güvenli bir yerde saklamalı ve uygun şekilde etiketlediğinizden emin olmalısınız.

Bulut tabanlı yedekleme çözümleri, dosyalarınızın internette çevrimiçi olarak herhangi bir yerde tutulduğu çözümlerdir. Genellikle bilgisayarınıza bir uygulama kurarak başlarsınız. Sonra bu uygulama, verilerinizi ya tanımladığınız aralıklarla ya da siz değiştirdikçe yedekler. Bulut tabanlı çözümlerin avantajı basitlikleridir, yedeklemeler çoğunlukla otomatiktir ve dosyalarınıza her yerden erişebilirsiniz. Ayrıca yedekleriniz bulut ortamında olduğundan yangın ya da hırsızlık gibi felaketlerle karşılaşsanız bile yedeklemeleriniz etkilenmeyecektir. Son olarak, bulut tabanlı yedeklemeler fidye yazılımları gibi kötü amaçlı yazılımların bulaşması sonrasında, verilerinizin etkilenmemiş sürümlerine dönmenizi sağlayabilir. Dezavantajları ise, özellikle büyük miktarlarda veriniz varsa yedekleme ve kurtarmaların yavaş olmasıdır.

Ayrıca mahremiyet ve güvenlik de önemlidir. Acaba hizmet sağlayıcınız verilerinizi şifrelemek ya da iki adımlı doğrulama çözümleri gibi güçlü güvenlik kontrolleri sağlıyor mu?

Son olarak mobil cihazlarınızı unutmayın. Mobil cihazların avantajı, e-postalarınız, takviminizdeki etkinlikleriniz, iletişim kurduğunuz kişiler gibi verilerinizin büyük bir çoğunluğunun halihazırda bulutta saklanmasıdır. Ancak, mobil uygulama konfigürasyonları, yakın zamanda çekilmiş fotoğraflarınız ve sistem tercihleriniz gibi bulutta saklanmayan bilgileriniz olabilir. Mobil cihazınızın yedeğini alarak sadece bu bilgileri korumakla kalmaz, örneğin yeni bir modele geçmek istemeniz gibi durumlarda cihazınızı tekrar yapılandırmayı da kolaylaştırırsınız. iPhone/iPad otomatik olarak Apple'in iCloud'ına yedekleme alabilir. Android ya da başka bir işletim sistemine sahip mobil cihazlar ise üretici ve ya servis sağlayıcıya bağlıdır. Bazı durumlarda özellikle yedekleme için tasarlanmış mobil uygulamalar da alabilirsiniz.

Kurtarma

Verilerinizi yedeklemek için yarıdır, verilerinizi kurtarabileceğinizden de emin olmalısınız. Yedeklemelerinizin çalışıp çalışmadığını düzenli olarak, bir dosyayı kurtarıp ve içeriğini doğrulayarak kontrol edin. Bunun yanında, büyük bir güncelleme yapmadan önce (yeni bir bilgisayara veya mobil cihaza geçmek gibi) ya da kapsamlı bir tamirden önce (sabit sürücünün çıkarılması gibi) tüm sistemin yedeğinin alındığından emin olun ve bu yedekten kurtarma yapılabildiğini doğrulayın.

Önemli Noktalar

- Verilerinizi yedeklemek için hangi çözümü kullandığınızdan bağımsız olarak Yedeklemelerinizi olabildiğince otomatik hale getirin ve düzenli olarak kontrol edin.



Yedekleme ve Kurtarma

- Sisteminizi yedeğini kullanarak baştan kurduğunuzda tekrar kullanmadan önce en son güvenlik yamalarının ve güncellemelerin uygulandığından emin olun.
- Süresi geçmiş ya da artık ihtiyacınız olmayan yedeklemeler size yükümlülük oluşturabilir, yetkisi olmayan kişilerin ulaşmasını engellemek için imha edin.
- Eğer bulut tabanlı bir çözüm kullanıyorsanız, sağlayıcınızın politikalarını ve itibarını araştırın ve sizin isteklerinizle eşleştiğinden emin olun. Örneğin, verilerinizi şifreliyorlar mı? İki adımlı doğrulama gibi güçlü kimlik doğrulama yaklaşımlarını destekliyorlar mı?

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives adresini ziyaret ederek SxANS 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 (<https://tr.linkedin.com/in/semayuice>), Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yapmış olup, Nisan 2016 itibarıyla Trust ISC (www.trustisc.com) adıyla uzmanlık alanlarında hizmet vermekte olduğu kendi danışmanlık şirketini kurmuştur.

Kaynaklar

Parolalar:	https://securingthehuman.sans.org/ouch/2017#april2017
İki Adımlı Doğrulama:	https://securingthehuman.sans.org/ouch/2015#september2015
Bulut Güvenle Kullanmak:	https://securingthehuman.sans.org/ouch/2016#november2016
Şifreleme:	https://securingthehuman.sans.org/ouch/2016#june2016
Fidye Yazılımlar:	https://securingthehuman.sans.org/ouch/2016#august2016

OUCH!, SANS Securing The Human Programı tarafından yayınlanır ve [Creative Commons BY-NC-ND 4.0 lisansı](https://creativecommons.org/licenses/by-nc-nd/4.0/) altında dağıtılır. Bülteni değiştirmedığınız sürece, bu bülteni dağıtabilir ya da kendi farkındalık programlarınızda kullanabilirsiniz. Çeviri ya da daha fazla bilgi için, lütfen ouch@securingthehuman.org e-posta adresini kullanarak iletişime geçiniz.

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus