ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- از چه چیز پشتیبان بگیریم و چه زمان؟
- چگونه پشتیبان بگیریم
- بازیابی
- نکات کلیدی

پشتیبان گیری و بازیابی

مقدمه

دیر یا زود با اتفاق ناخواسته به احتمال زیاد فایل های شخصی، مدارك یا عکس هایتان را از دست خواهید داد. مثال ها شامل پاك کردن تصادفی و ناخواسته فایلی، خرابی سخت افزار، گم کردن لپ تاپ یا آلوده شدن به ویروس کامپیوتری می باشند. در چنین مواقعی، پشتیبان ها اغلب تنها راه بازیابی زندگی دیجیتالی شماست. در این خبر نامه ما توضیح خواهیم داد پشتیبان چیست و چگونه از داده هایمان پشتیبان بگیریم و چگونه استراتژی ای را که برایمان مناسب است را طرح ریزی کنیم.

سردبیر مهمان

Heather Mahalik متخصص تحقیقات دیجیتال امور قضایی شناخته شده است، و تمرکزش بر امور قضایی مربوط به تلفن های هوشمند است. او یکی از نویسندگان کتاب تحقیق امور قضایی روی موبایلهای و نویسنده مشترک کتاب آموزش امور قضایی آندروید و یکی از نویسندگان FOR585 امور قضایی پیشرفته تلفن هوشمند و FOR518 امور قضایی مکینتاش برای موسسه SANS است. او را در **smarterforensics.com** و Twitter:**@heathermahalik** تعقیب کنید.

از چه چیز پشتیبان بگیریم و چه زمان؟

پشتیبان ها کپی اطلاعات شما هستند که جای دیگری ذخیره شده اند، وقتی شما اطلاعات مهمی از دست می دهید، می توانید آن اطلاعات را از پشتیبان ها بازیابی کنید. مشکل اینست که متاسفانه بیشتر مردم پشتیبان تهیه نمی کنند گرچه پشتیبان گیری کاری ساده و ارزان است. دو روش در زمینه انتخاب اینکه از چه فایلی پشتیبان بگیریم وجود دارد. ۱- داده خاصی که برایتان خیلی مهم است. ۲- همه چیز! شامل همه سیستم عامل. روش اول پشتیبان گیری را آسان می کند و در فضای دیسك سخت صرفه جویی می کند. دومین روش ساده تر و قابل فهم تر است. اگر شك دارید از چه چیزی پشتیبان گیری کنید، ما توصیه می کنیم از همه چیز پشتیبان گیری کنید.

در مرحله بعد باید تصمیم بگیرید که هر چند وقت یکبار از داده هایتان پشتیبان گیری کنید. گزینه های معمول ساعتی، روزانه، هفتگی و غیره هستند. برای استفاده در منزل، برنامه های پشتیبان گیری شخصی مثل Time Machine شرکت اپل یا Restore and Backup Windows شرکت مایکروسافت به شما امکان ایجاد پشتیبان گیری بصورت خودکار برنامه زمانی « تنظیمش کن و دیگر بهش فکر نکن» می دهند. این راه حل ها در طول روز و هنگام کار با کامپیوترتان یا حتی وقتی با آن کار نمی کنید، بی سر و صدا از داده هایتان پشتیبان گیری می کنند. راه حل های دیگر «حفاظت مستمر» است که در آن از فایل های جدید و فایل های تغییر یافته به محض اینکه بسته شدند پشتیبان گیری می کند. ما پیشنهاد می کنیم حداقل روزانه پشتیبان گیری کنید. در نهایت سوالی که از خود می پرسید اینست « چقدر اطلاعات ممکن است از دست بدهم اگر مجبور شوم از نسخه پشتیبان اطلاعات را برگردانم؟»

چگونه پشتیبان بگیریم

دو راه برای پشتیبان گیری از داده ها وجود دارد. رسانه فیزیکی و ذخیره سازی ابری. رسانه فیزیکی به انواع سخت افزار، مثل دی وی دی، یو اس بی درایو یا درایور های سخت خارجی گفته می شود. از هر رسانه ای که انتخاب می کنید، هرگز فایل های پشتیبان را همانجایی که فایل های اصلی را ذخیره کرده

پشتیبان گیری و بازیابی

پشتیبان گیری های خودکار و قابل اعتماد اغلب آخرین خط دفاعی شما برای حفاظت از داده هایتان هستند.

اید، ذخیره نکنید. مشکلی که رسانه فیزیکی دارد اینست که اگر در محل شما فاجعه ای رخ دهد مثل آتش سوزی یا دزدی، نه تنها ممکن است کامپیوترتان را از دست بدهید، بلکه ممکن است پشتیبان را هم از دست بدهید. به همین دلایل، شما باید نسخه هایی از پشتیبانتان را در مکان مطمئن دیگری نگه دارید. اگر پشتیبان ها را جای دیگری بردید، حتما یادداشت کنید که از چه چیزی و کی پشتیبان گرفته اید. برای امنیت بیشتر، پشتیبان ها را رمز گذاری کنید.

راه حل های ابری متفاوتند، آنها خدماتی هستند که فایل های شما جایی در اینترنت ذخیره شده نگهداری می شوند. بسته به حجم داده ای که می خواهید از آن پشتیبان بگیرید ممکن است پولی باشند. طریقه کارکردش بدین صورت است برنامه ای بر روی کامپیوترتان نصب می شود که بطور خودکار از فایل هایتان پشتیبان می گیرد. برتری این روش اینست که چون پشتیبان های شما در اینترنت هستند، اگر فاجعه ای در خانه تان اتفاق بیفتد، پشتیبان ها در امنیت هستند. بعلاوه، می توانید به پشتیبان هایتان دسترسی داشته باشید، اغلب حتی فقط فایلی منحصر بفرد، از هر کجا حتی هنگام مسافرت. اشکال این روش اینست که پشتیبان گیری و بازیابی بر اساس سیتم ابری ممکن است آهسته تر باشند، بخصوص اگر حجم دیتا زیاد باشد. اگر نمی دانید کدام روش پشتیبان گیری برای شما مناسب تر است (رسانه فیزیکی یا ابری) در ذهن داشته باشید که همیشه می توانید از هر دو روش استفاده کنید.

در پایان، دستگاه های موبایلتان را فراموش نکنید. مزیت دستگاههای موبایل اینست که بیشتر داده ها قبلا در ابر ذخیره شده اند، مثل ایمیل، رویدادهای تقویم یا تماس ها. اما ممکن است اطلاعاتی داشته باشید که که در ابر ذخیره نشده باشد، مثل موقعیت اپلیکشن های موبایل، عکس های جدید و تنظیمات سیستم. با پشتیبان گیری از دستگاه موبایلتان، نه تنها از این اطلاعات حفاظت می کنید، بلکه بازیابی دستگاه هم آسانتر است. مثلا هنگامی که به دستگاه جدید ارتقاء می دهید (یا دستگاه جدید تر می خرید)، یك آیفون/ آیپد بطور خودکار با ابر شرکت اپل پشتیبان گیری می شود. آندروید یا دستگاههای دیگر بسته به سازنده یا ارائه دهنده خدمات پشتیبان گیری می شوند. در بعضی موارد، ممکن است اپلیکشن موبایلی بخرید که مخصوصا برای پشتیبان گیری طراحی شده باشد.

بازیابی

پشتیبان گیری از داده فقط نیمی از چالش است؛ شما باید اطمینان حاصل کنید که می توانید داده ها را بازیابی کنید. هر ماه با بازیابی یك فایل و معتبر کردن محتویات بررسی کنید که پشتیبان ها درست کار کنند. بعلاوه، حتما قبل از ارتقای اساسی، از کل سیستم پشتیبان بگیرید (مثل تعویض هارد درایو) و بررسی کنید که قابل بازگرداندن باشد.

پشتیبان گیری و بازیابی

نکات کلیدی

- پشتیبان گیری را تا جای ممکن خودکار کنید و آنرا بطور مرتب چك کنید.
- هنگام بازیابی کل سیستم با استفاده از پشتیبان، حتما از آخرین و جدید ترین روش های امنیتی بروز رسانی شده استفاده کنید.
- پشتیبان های قدیمی ممکن است باعث زحمت شوند، و باید از بین برده شوند تا اشخاص غیر مجاز به آن ها دسترسی پیدا نکنند.
- اگر از راه حل ابری استفاده می کنید، در مورد سیاست ها و شهرت ارائه دهنده آن تحقیق کنید و اطمینان حاصل کنید آنها نیاز های شما را برآورده می کنند. برای مثال، آیا آنها داده ها را رمز گذاری می کنند؟ چه کسی به پشتیبان ها دسترسی دارد؟ آیا آنها strong authentication مثل تایید دو-مرحله ای را پشتیبانی می کنند؟

بیشتر بدانید

با مراجعه به آدرس زیر، مشترک ماهنامه OUCH! شوید و به آرشیو خبرنامه آگاهی از امنیت OUCH! دسترسی داشته باشید، و در مورد راه حل‌های افزایش آگاهی‌های امنیتی موسسهSANS بیشتر بدانید.

آدرس: http://www.securingthehuman.org

یادداشت مترجم

سایت www.sycurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

رمزعبارتگونه (Passphrases):	http://www.securingthehuman.org/ouch/2015#april2015
تایید هویت دو مرحله ای:	http://www.securingthehuman.org/ouch/2013#august2013
امنیت سیستم های ابری:	http://www.securingthehuman.org/ouch/2014#september2014
رمزنگاری:	http://www.securingthehuman.org/ouch/2014#august2014
نکته روزانه:	http://www.sans.org/tip_of_the_day.php

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
ترجمه شده توسط : سعید میرجلیلی