ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

استفاده امن از خدمات ابری

مقدمه

سردبیر مهمان

جیمز و کلی (@isaudit / @kellitarala) James and Kelli Tarala مشاوران ارشد شرکت Enclave Security می باشند و مطالب درسی دوره های آموزشی متعدد، از جمله دوره ممیزی SANS 566، پیاده سازی و ممیزی بیست کنترل امنیتی حیاتی MGT 415 ، مقدمه عملی بر ارزیابی ریسک را تالیف کرده اند.

«سیستم ابری» تکنولوژی قدرتمندی است که سازمان ها و اشخاص به سرعت در حال بکارگیری آن هستند. «سیستم ابری» برای افراد مختلف معنای متفاوتی دارد، ولی به طور کلی منظور استفاده از یک ارائه دهنده خدمات در اینترنت برای ذخیره و مدیریت داده های کاربر است. مزیت استفاده آن این است که نه تنها می توان به راحتی به داده ها از چند دستگاه مختلف در هر نقطه از جهان دسترسی داشته باشید و اطلاعات را همگام سازی کرد، همچنین می توان اطلاعات را با هر کسی که بخواهیم به اشتراک گذاشت. دلیلی که این خدمات را «ابری» مینامند آن است که اغلب نمی دانید داده های شما به صورت فیزیکی در کجا ذخیره می شوند. نمونه هایی از سیستم ابری عبارتند از ایجاد اسناد در Google Docs، به اشتراک گذاری فایل ها از طریقDropbox ، راه اندازی سرور اختصاصی در سیستم ابری آمازون، و یا ذخیره سازی موسیقی و یا تصاویر در iCloud اپل است. این خدمات ابری کارایی را به مراتب افزایش میدهند، ولی با خطراتی هم همراه هستند. در این خبرنامه توضیح میدهیم چگونه با حفظ امنیت از توانایی سیستم ابری بهره ببرید.

انتخاب یک ارائه دهنده خدمات ابری

خدمات ابری نه خوب است و نه بد، تنها ابزاری است برای انجام کارها، در محل کار و در خانه. با این حال، هنگامی که شما از این خدمات استفاده میکنید شما اطلاعات خصوصی خود را دو دستی به غریبه ها واگذار میکنید و انتظار می رود که آنها داده ها را امن و در دسترس نگهدارند. به این ترتیب، شما می خواهید مطمئن شوید که انتخاب عاقلانه ای کرده اید. برای رایانه محل کار و یا اطلاعات مربوط به کار، با سرپرست خود هماهنگ کنید که آیا می توانید از خدمات ابری استفاده کنید یا خیر. اگر مجاز به استفاده از خدمات ابری هستید، مطمئن شوید که از کدام خدمات ابری می توانید استفاده کنید و سیاست استفاده از آنها چه هستند. اگر از خدمات ابری برای استفاده شخصی میخواهید استفاده کنید، موارد زیر را در نظر داشته باشید.

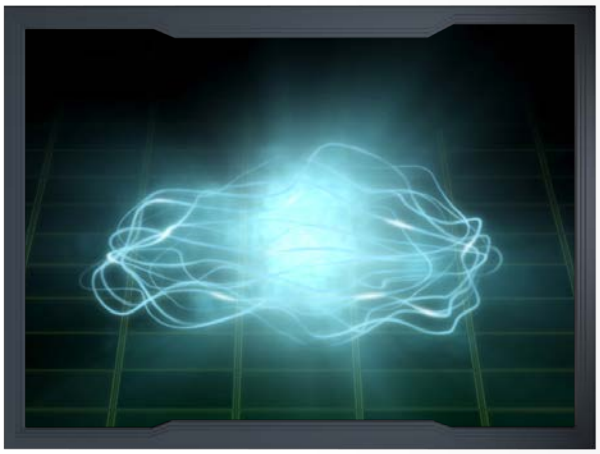
۱. **پشتیبانی:** پاسخ به سوالاتان و کمک گرفتن برای رفع مشکلات چگونه است؟ آیا شماره تلفنی یا آدرس ایمیلی دارند که شما بتوانید با آنها تماس بگیرید؟ گزینه های دیگری برای پشتیبانی، مانند انجمن های عمومی و یا پرسش و پاسخهای متداول در وب سایت شان وجود دارد؟
۲. **سادگی:** استفاده از خدمات چقدر ساده و آسان است؟ هر چه خدمات پیچیده تر باشد، احتمال اشتباه و اینکه به طور تصادفی اطلاعات خود را افشا یا از دست بدهید بیشتر است. از ارائه دهنده خدمات ابری استفاده کنید که کار با آن، پیکربندی و استفاده آسان باشد.

© The SANS Institute 2014

استفاده امن از خدمات ابری

۳. **امنیت:** چگونه اطلاعات از کامپیوتر شما به سیستم ابری ارسال میشود؟ آیا ارتباط امن و رمزشده است؟ چگونه داده ها شما در سیستم ابری ذخیره شده است؟ آیا رمزگذاری شده است و اگر چنین است چه کسی می تواند اطلاعات شما را رمز گشایی کند؟

۴. **شرایط و ضوابط سرویس:** حتما نگاهی به قوانین و مقررات خدمات دهنده بیاندازید (اغلب خیلی آسان و ساده نوشته شده اند). کنترل کنید که چه کسی می تواند به اطلاعات شما دسترسی داشته باشد و حقوق قانونی خود را بدانید.



سیستم ابری می تواند دسترسی به اطلاعاتتان را آسانتر کند و کارآیی شما را افزایش دهد، اما مراقب باشید که چگونه اطلاعات را ذخیره و به اشتراک میگذارید.

امن کردن اطلاعات

هنگامی که یک ارائه دهنده خدمات ابری را انتخاب کردید، گام بعدی این است که مطمئن شوید که از خدمات ابری به درستی استفاده میکنید. اینکه چگونه شما به اطلاعات خود دسترسی پیدا میکنید یا به اشتراک میگذارید، اغلب بیشترین تاثیر بر روی امنیت فایل های شما نسبت به هر چیز دیگری دارد. برخی از گام های کلیدی که شما می توانید بردارید، عبارتند از:

۱. **احراز هویت:** از یک رمز عبور بسیار قوی و منحصر به فرد برای احراز هویت به حساب ابری خود استفاده کنید. اگر ارائه دهنده خدمات ابری تأیید هویت دو مرحله ارائه می دهد توصیه میشود که آن را فعال کنید.

۲. **به اشتراک گذاری فایل / پوشه:** سیستم ابری امکان به اشتراک گذاشتن را خیلی ساده کرده است، گاهی اوقات بیش از حد ساده است. در بدترین حالت، شما ممکن است تصادفا فایل های خود را و یا حتی تمام پوشه ها را در دسترس عموم در تمام اینترنت قرار دهید. بهترین راه برای محافظت از خود این است که به طور پیش فرض هیچ یک از فایل های خود را با کسی به اشتراک نگذارید. بلکه تنها به افراد خاص (یا گروهی از افراد) اجازه دسترسی به فایل ها و یا پوشه های خاص بر اساس نیاز آنها بدهید و وقتی آنها دیگر نیازی به دسترسی به فایل های شما ندارند، آنها را حذف کنید. ارائه دهنده خدمات ابری شما باید یک راه آسان برای ردیابی دسترسی به فایل ها و پوشه های شما را داشته باشد.

۳. **به اشتراک گذاری فایل / پوشه ها با استفاده از لینک ها:** یکی از ویژگی های مشترک برخی ارائه دهنده های خدمات ابری توانایی ایجاد یک لینک وب است که به فایل ها و یا پوشه های شما اشاره دارد. این قابلیت به شما اجازه می دهد تا این فایل ها را با هر کسی که می خواهید به سادگی با ارائه یک لینک وب به اشتراک بگذارید. ولی این روش امنیت بسیار کمی دارد، هر کسی که این لینک را داشته باشد ممکن است به فایل ها و یا پوشه های شخصی شما دسترسی داشته باشد. اگر شما لینک را فقط به یک نفر ارسال کنید، آن شخص می تواند این لینک را با دیگران به اشتراک بگذارد و یا آن را می تواند به موتورهای جستجو بدهد که در جستجوها آورده شود. اگر شما داده هایی را با استفاده از یک لینک به اشتراک گذاشته اید، حتما وقتی دیگر مورد نیاز نیست لینک را غیر فعال کنید و یا در صورت امکان، برای لینک رمز عبور بگذارید.

© The SANS Institute 2014

استفاده امن از خدمات ابری

۴. **تنظیمات:** تنظیمات امنیتی ارائه شده توسط ارائه دهنده ابری خود را مطالعه کنید. به عنوان مثال، اگر شما یک پوشه را با شخص دیگری به اشتراک گذاشته اید، آیا او می تواند آنها را بدون اطلاع شما با دیگران به اشتراک بگذارد؟

۵. **آنتی ویروس:** حتما آخرین نسخه نرم افزار آنتی ویروس بر روی کامپیوتر شما و بر روی هر کامپیوتر دیگری که استفاده می کنید که اطلاعات به اشتراک میگذارید نصب کنید. اگر فایلی که به اشتراک گذاشتید آلوده باشد، کامپیوتر های دیگری که دسترسی به آن فایل دارند نیز می توانند آلوده شوند.

۶. **پشتیبان گیری:** حتی اگر ارائه دهنده خدمات ابری شما از داده های شما پشتیبان گیری میکند، شما نیز از داده ها بطور منظم پشتیبان گیری کنید. اگر ارائه دهند خدمات ورشکست شد یا به هر دلیلی خدمات خود را متوقف کرد، با داشتن پشتیبان اطلاعات محافظت شده است. همچنین شما خیلی آسانتر میتوانید داده های خود را از نسخه پشتیبان تهیه شده محلی خود بازیابی کنید به جای اینکه از روی سیستم ابری دانلود کنید. همچنین، بررسی کنید که ارائه دهنده خدمات ابری چند وقت یکبار از فایل های شما پشتیبانی میگیرد؟ و آیا به شما اجازه بازیابی نسخه های قبلی را میدهند؟ و چه مدت نسخه های پشتیبان را در دسترس نگه میدارند؟

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

رمز عبور قوی :	http://www.securingthehuman.org/ouch/2013#may2013
برنامه های مدیریت رمز عبور :	http://www.securingthehuman.org/ouch/2013#october2013
پشتیبان گیری :	http://www.securingthehuman.org/ouch/2013#september2013
اصطلاحات امنیت اطلاعات :	http://www.securingthehuman.org/resources/security-terms

OUCH! توسط برنامه «زندگی امن» موسسه SANS تحت مجوز Creative Commons BY-NC-ND ۴.۰ منتشر و توزیع شده است. اجازه توزیع این خبرنامه به شرط ذکر منبع، بدون تغییر محتوا و نداشتن مقاصد تجاری داده میشود. برای اطلاعات بیشتر، لطفا با ouch@securingthehuman.org تماس بگیرید.

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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus