OUCH! آگست 2021

SANS SECURITY AWARENESS

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

استفاده ایمن از فضای ابری

مقدمه

ممکن است مفهومی به نام "فضای ابری" را شنیده باشید. فضای ابری به معنای استفاده از ارائه دهنده خدمات در اینترنت برای ذخیره و مدیریت داده های شما است. به عنوان مثال می توان به ایجاد اسناد در Google Docs، دسترسی به ایمیل در Microsoft O365، به اشتراک گذاری پرونده ها از طریق Dropbox یا ذخیره عکس ها در iCloud اپل اشاره کرد. وقتی که از چندین دستگاه در هر جای دنیا به داده های خود دسترسی پیدا کرده و آنها را همسان سازی(Sync) می کنید و اطلاعات خود را با هر کسی که می خواهید به اشتراک می گذارید، اغلب نمی دانید و نمی توانید کنترل کنید که داده های شما به صورت فیزیکی کجا ذخیره میشوند.

انتخاب یک ارائه دهنده فضای ابری

سرویسهای ابری صرفا نه خوب هستند و نه بد. بلکه آنها ابزاری برای انجام کارهای ما هستند. با این حال، هنگام استفاده از این خدمات، اساسا داده های خصوصی خود را به افرادی غریبه تحویل میدهید و انتظار دارید آنها اطلاعات شما را هم به صورت ایمن و هم در دسترس نگاه دارند. به همین ترتیب، شما باید مطمئن شوید که ارائه دهنده خدمات خود را هوشمندانه انتخاب میکنید. برای اطلاعات مربوط به کار، با سرپرست خود مشورت کنید تا ببینید اجازه استفاده از سرویسهای ابری را به شما میدهد و کدام یک از آنها مجاز میباشند. اگر می خواهید از سرویس های ابری برای استفاده شخصی استفاده کنید، موارد زیر را در نظر بگیرید:

1. **اعتماد**: آیا میتوانید به ارائه دهنده سرویس ابری اعتماد کنید؟ آیا یک شرکت عمومی شناخته شده است که میلیون ها نفر قبلاً از آن استفاده کرده اند، یا یک شرکت کوچک و ناشناخته است که در خارج از کشور مستقر شده و هرگز نام آن را نشنیده اید؟
2. **پشتیبانی**: کمک گرفتن و یا پاسخ به سوالات برای شما چقدرآسان است؟ آیا شماره تلفنی وجود دارد که با آن تماس بگیرید یا آدرس ایمیلی دارند که با آن در ارتباط باشید؟ آیا گزینه های دیگری برای پشتیبانی مانند تالارهای گفتمان عمومی (Public Forums) یا بخش سوالات متداول در وبسایت آنها وجود دارد ؟
3. **سادگی**: استفاده از این سرویس چقدر آسان است ؟ هر چقدر خدمات پیچیده تر باشند، احتمال اشتباه شما بیشتر شده و به طور تصادفی اطلاعات خود را فاش کرده یا آنها را از دست میدهید. از ارائه دهنده سرویس ابری که درک، پیکربندی و استفاده از آن ساده تر است استفاده کنید.
4. **امنیت**: داده های شما چگونه از رایانه تان به سرویس ابری میرسند؟ آیا این اتصال با رمزگذاری امن شده است؟ اطلاعات شما چگونه ذخیره شده اند؟ آیا رمزگذاری شده اند واگر اینطور است، چه کسی میتواند اطلاعات شما را رمزگشایی کند؟ هنگام انتقال داده های خود، این موضوع را به خاطر داشته باشید که امنیت، یک مسئولیت مشترک بین شما و فروشنده است.
5. **سازگاری**: آیا ارائه دهنده خدمات از تمامی دستگاهها و سیستم عاملهایی که استفاده کرده یا قصد استفاده از آنها را دارید پشتیبانی میکند؟

6. **شرایط استفاده از خدمات**: چند لحظه وقت بگذارید و شرایط استفاده از خدمات را مرور کنید(اغلب خواندن آنها بسیار آسان است). ارائه دهنده خدمات طبق قوانین کدام کشور فعالیت میکند؟ به حقوق که به ارائه دهنده خدمات خود واگذار میکنید توجه ویژه ای داشته باشید.

امنیت داده های شما

قدم بعدی این است که مطمئن شوید از خدمات ابری خود به درستی استفاده میکنید. چگونگی دسترسی و به اشتراک گذاری اطلاعات توسط شما اغلب میتواند بیش از هر مورد دیگری در امنیت داده های شما تاثیرگذار باشد. برخی از مراحل کلیدی که میتوانید انجام دهید عبارتند از:

1. **احراز هویت**: برای محافظت از حساب ابری خود از یک رمز عبور قدرتمند و منحصر به فرد استفاده کنید. اگر ارائه دهنده سرویس ابری شما تائید دو مرحله ای (**two-step Verification**) را ارائه میدهد، اکیدا توصیه میکنیم آن را فعال کنید.
2. **به اشتراک گذاری پرونده ها / پوشه ها**: ارائه دهندگان سرویس ابری، اشتراک گذاری داده ها را بسیار ساده (گاهی اوقات بیش از اندازه ساده) میکنند. به آسانی ممکن است اطلاعات خود را تصادفی و به صورت عمومی به اشتراک بگذارید. با محدود کردن اجازه دسترسی به پوشه ها و فایلهای خاص توسط افراد مشخص (یا گروهی از افراد) از خودتان محافظت کنید. زمانیکه فردی دیگر نیازی به دسترسی ندارد، حذفشان کنید. ارائه دهنده سرویس ابری شما باید یک روش آسان برای ردیابی اینکه چه افرادی به پرونده ها و پوشه ها دسترسی دارند، ارائه نماید.
3. **تنظیمات**: تنظیمات امنیتی ارائه شده توسط ارائه دهنده ابری خود را بررسی کنید. به عنوان مثال، اگر تصاویر، پرونده ها یا پوشه ای را با شخص دیگری به اشتراک گذاشتید، بررسی کنید که آیا او میتواند داده های شما را بدون اطلاع تان با دیگران به اشتراک بگذارد؟
4. **تمدید**: تمدید اشتراک خود را فراموش نکنید در غیر اینصورت دسترسی به داده های خود را از دست خواهید داد.

سردبیر مهمان

Tameika Reed (@womeninlinux)، بنیانگذار زنان در لینوکس. او ابتکاراتی را با تمرکز بر کشف مشاغل در زیرساخت ها، امنیت سایبری و DevSecOps هدایت می کند. او جلسات هفتگی ای را با موضوعات مختلف از زیرساخت تا Blockchain برگزار می کند. او در OSCon، LISA، Seagl، HashiConf EU صحبت کرده است.

منابع

حملات مهندسی اجتماعی: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
آسان کردن رمزهای عبور: https://www.sans.org/newsletters/ouch/making-passwords-simple
مدیریت رمزهای عبور: https://www.sans.org/newsletters/ouch/password-managers/
قدرت به روز رسانی: https://www.sans.org/newsletters/ouch/the-power-of-updating/

ترجمه شده برای عموم توسط: سعید میرجلیلی، مجید هدایتی