وای! اوت 2017

SafeNet Network & Security Services
شبکه امن اندیشه فردا

ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- چگونه پشتیبان بگیریم
- بازیابی
- نکات کلیدی

پشتیبان ها: از چه؟ کی و چگونه؟

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 بازسازی 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 توسعه دهیم.

سردبیر مهمان
کیت پامگرن متخصص حرفه ای امنیت سایبری با بیش از ۳۰ سال تجربه در زمینه امنیت تکنولوژی اطلاعات می باشد. او مدرس ارشد SANS می باشد و نویسنده SANS SEC301 «مقدمه ای بر امنیت اطلاعات» است. کیت جلسات آموزشی مشاوره امنیتی موفقی را اداره می کند و با **@kpalmgren** در توییتر فعالیت می کند.

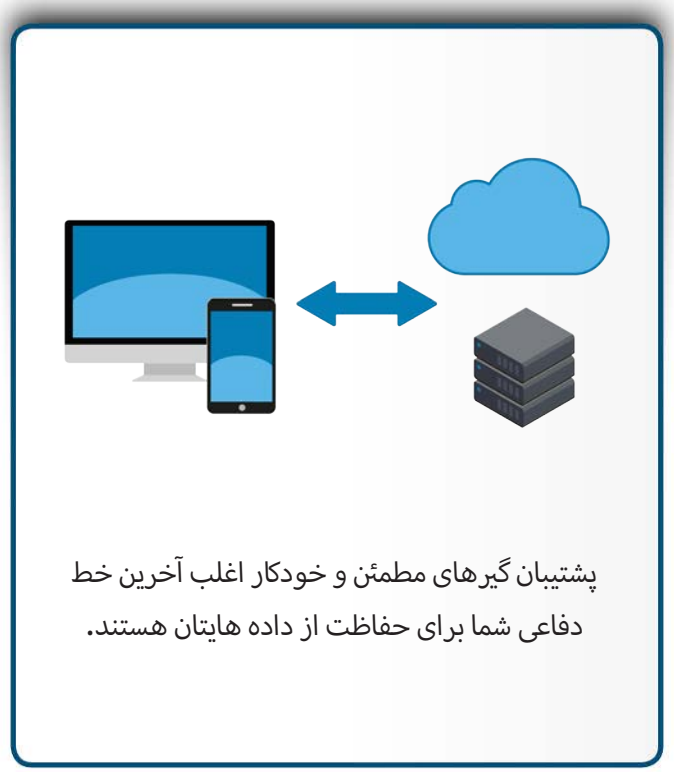
پشتیبان ها: از چه؟ کی و چگونه؟

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 بیشتر مردم پشتیبان تهیه نمی کنند که جای تعجب است است چون 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 تمام فایلهای 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 Windows Backup and Restore شرکت مایکروسافت به شما امکان ایجاد پشتیبان گیری بصورت خودکار برنامه زمانی « تنظیمش کن و ولش کن» 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 باید تصمیم بگیرید چگونه می خواهید پشتیبان بگیرید. دو روش برای پشتیبان گیری وجود دارند. رسانه فیزیکی یا ذخیره سازی

پشتیبان ها: از چه؟ کی و چگونه؟



پشتیبان گیرهای مطمئن و خودکار اغلب آخرین خط دفاعی شما برای حفاظت از داده هایتان هستند.

روی اینترنت. هر روش مزایا و معایبی دارد. اگر نمی دانید از کدام روش استفاده کنید از هر دوی این روشها استفاده کنید. رسانه فیزیکی دستگاهی است که کنترلش می کنید مثل یو اس بی درایو خارجی یا دستگاههای دسترسی به شبکه وای فای. مزیت استفاده از رسانه فیزیکی شخصی اینست که قادرید حجم زیادی از داده را با سرعت بالا ذخیره و بازیابی کنید. عیبش اینست که اگر آلوده به بد افزاری مثل باج افزار شدید ممکن است بدافزار در پشتیبان شما منتشر شود. همچنین اگر حادثه ای مثل آتش سوزی یا دزدی اتفاق بیفتد ممکن است نه تنها کامپیوتر از دست بدهید بلکه ممکن است پشتیبان ها هم از دست بروند. به همین دلیل اگر از رسانه خارجی برای پشتیبان گیری استفاده می کنید باید نسخه ای از پشتیبان را در جای امن دیگری نگه دارید. آنها را برچسب گذاری کنید.

راه حل های بر اساس سیستم های ابری خدمات آنلاینی هستند که فایل ها را روی اینترنت ذخیره می کنند. معمولا، اپلیکیشنی روی کامپیوتر نصب می کنید. اپلیکیشن بطور خودکار فایلها را یا بصورت برنامه زمان بندی شده یا طوری که شما اصلاح کرده اید پشتیبان می گیرد. سادگی، پشتیبان گیری اغلب خودکار، و دسترسی به فایل ها از هر جا که باشید از مزایای راه حل ابری است. همچنین چون داده روی اینترنت است حوادث خانگی مانند دزدی و آتش سوزی به پشتیبان ها آسیب نمی زند. نهایتا با پشتیبان های ابری می توان فایل ها بدون اینکه به بدافزار هایی مثل باج افزار آلوده شده باشند بازیابی کرد. معایب آن شامل زمان طولانی برای پشتیبان گیری و بازیافت حجم بالای داده می باشد. همچنین امنیت و حریم خصوصی مهم هستند. آیا خدمات پشتیبان گیری کنترل های امنیتی قوی ای مانند کدگذاری داده ها و تأیید هویت دو مرحله ای ارائه می دهد؟

در پایان، دستگاه های موبایلتان را فراموش نکنید. مزیت دستگاههای موبایل اینست که بیشتر داده ها قبلا در ابر ذخیره شده اند، مثل ایمیل، رویداد های 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 بازسازی دستگاه هم آسانتر است. مثلا هنگامی که دستگاه جدید تر می خرید یک 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 راه حل است؛ شما باید اطمینان حاصل کنید که می توانید داده ها را بازیابی کنید. هر ماه با بازیابی یک

پشتیبان ها: از چه؟ کی و چگونه؟

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.

نکات کلیدی

- پشتیبان گیری را تا جای ممکن خودکار کنید و آنرا بطور مرتب چك کنید
- هنگام بازسازی 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-گام 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: securingthehuman.sans.org/ouch/archives

شرکت شبکه امن، پیشرو در ارائه راهکارهای امنیت شبکه و اطلاعات، خدمات مشاره، آموزش و تست نفوذ. اطلاعات بیشتر در: www.safenet-co.net

منابع

رمز عبارتگونه:	https://securingthehuman.sans.org/ouch/2017#april2017
تایید هویت دو مرحله ای:	https://securingthehuman.sans.org/ouch/2015#september2015
امنیت سیستم های ابری:	https://securingthehuman.sans.org/ouch/2016#november2016
رمزنگاری:	https://securingthehuman.sans.org/ouch/2016#june2016
نکته روزانه:	https://securingthehuman.sans.org/ouch/2016#august2016

هیأت تحریریه : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
ترجمه شده توسط : سعید میرجلیلی، مجید هدایتی