禪

بیگانهای پرسه میزند !

مراقب کلیدهای رمزنگاری در ویندوز 10 باشید

اگر از یک کامپیوتر شخصی مجهز به ویندوز 10 استفاده میکنید یا سیستمعامل خود را به ویندوز 10 ارتقا دادهاید، احتمال ذخیرهسازی کلید رمزنگاری دیسک شما روی سرورهای مایکروسافت زیاد است . بهعبارتدیگر ممکن است کنترل کاملی روی حریم خصوصی و دادههای شخصیتان نداشته باشید .

اگر از آن گروه کاربرانی هستید که برای ورود به ویندوز 10 بهجای استفاده از حساب محلی از حساب مایکروسافت استفاده میکنید، بهاحتمالزیاد کلیدهای رمزنگاری مورداستفاده شما روی سرورهای مایکروسافت ذخیره شده است. این ویژگی زمانی کاربردی و مفید است که گذرواژه مربوط به دادههای خود را ازدستداده باشید، در این صورت با استفاده از حساب ابری بهراحتی قادر به بازیابی آن خواهید بود . اما این سکه روی دیگری نیز دارد، این روزها هکرها بهشدت به سرورهای ابری علاقهمند شدهاند و برای این منظور از ابزارها و فناوریهای قدرتمندی استفاده میکنند، درنتیجه اگر هکری شانس نفوذ به سرورهای مایکروسافت را پیدا کند به حسابهای کاربران دسترسی پیداکرده و بهموازات آن به جزییات رمزگشایی دادهها نیز دسترسی پیدا خواهد کرد . با توجه به این تحلیل، ممکن است این سؤال برای شما پیشآمده باشد که اولاً کلید رمزنگاری را باید چگونه ایجاد کنیم و دوم اینکه بهترین مکان برای نگهداری کلید ساختهشده کجاست؟ مایکروسافت در سیستمعامل ویندوز از ابزار قدرتمندی در این زمینه استفاده میکند که BitLocker نام دارد؛ یک مؤلفه مستقل که برای رمزنگاری دادهها در ویندوز در نظر گرفتهشده است.

این ابزار به کاربران این توانایی را میدهد تا کلید رمزنگاری خود را به سه روش ذخیرهسازی کنند؛ ذخیره روی فلش، چاپ روی کاغذ و بارگذاری در سرورهای ابری، سه راهکاری است که مایکروسافت در

اختیار کاربران قرار میدهد . BitLocker ابزار قدرتمند و ایدهآلی است، اما ویندوز 10 از راهکار مجتمع و یکپارچهای برای این منظور استفاده میکند . ویندوز 10 بهطور خودکار کلیدهای رمزنگاری را مستقیم روی سرورهای ابری ذخیره میکند . به نظر میرسد مایکروسافت تمام توان خود را به کار گرفته است تا به هر شیوه ممکن کاربران را به سمت رایانش ابری و خدمات آنلاینی سوق دهد که روی بستر اینترنت ارائه میکند .

کاربرانی که از اشتراک مایکروسافت یا ویندوز 10 استفاده میکنند، باید بدانند کلید رمزنگاری مورداستفاده آنها بهطور مستقیم روی سرور ابری مایکروسافت ذخیرهسازی میشود، درنتیجه کار چندان خاصی در این زمینه از دست کاربر ساخته نیست . اگر مسائل مربوط به حریم خصوصی برای شما اهمیت خاصی دارد و تمایل دارید بدانید کلیدهای رمزنگاری شما روی سرورهای مایکروسافت ذخیرهسازی شدهاند یا خیر، میتوانید از این آدرس استفاده کنید . برای این منظور لازم است با حساب کاربری خود به این سرویس وارد شوید. کاربرانی که در نظر دارند کلیدهای رمزنگاری خود را از فضای ابری مایکروسافت پاک کنند، حتماً به این موضوع توجه داشته باشند که یک نسخه پشتیبان از این کلیدها تهیه کنند . به دلیل اینکه مایکروسافت اعلام کرده اگر کلیدهای خود را از روی سرورهای این شرکت پاک کنید نهتنها دسترسی به آنها دیگر امکانپذیر نخواهد بود، بلکه بعد از گذشت چند ساعت نسخههای پشتیبان این کلیدها نیز از سرورهای مایکروسافت پاک خواهند شد . اگر هیچ کلیدی را در این آدرس مشاهده نکردید به این معناست که هیچگونه داده رمزنگاریشده روی کامپیوتر شما وجود ندارد یا کلیدهای مربوطه روی سرورهای مایکروسافت ذخیرهسازی نشدهاند.

اما نکتهای درباره ابزار BitLocker وجود دارد . این ابزار تنها در اختیار کاربرانی قرار دارد که تراشه TPM روی مادربرد آنها نصبشده باشد . اگر به ابزار BitLocker دسترسی ندارید توصیه میکنیم از ابزار BestCrypt که در این زمینه قابلیتهای قدرتمندی ارائه میکند استفاده کنید . BestCrypt ابزاری است که امکان پیادهسازی رمزنگاری قدرتمندی را در اختیار کاربران قرار میدهد . ازجمله قابلیتهای این نرمافزار میتوان به این نکات اشاره کرد : پشتیبانی از بوت ایمن توسط UEFI، رمزنگاری RAID و انواع مختلف ولومها، مکانیسم احراز هویت پیش از بوت، احراز هویت دوعاملی، رابط کاربری دوستانه و پشتیبانی از TPM. این ابزار با طیف گستردهای از سیستمعاملهای خانواده ویندوز، ازجمله ویندوز 10 سازگار است. برای اطلاع بیشتر درباره این نرمافزار به این آدرس مراجعه کنید

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
01:50 - 19/12/1394
برچسب:
رمزنگاری - کلیدهای رمزنگاری - ویندوز 10 - امنیت ویندوز 10

□□□□□ منبع :https://www.shabakeh-mag.com/security/3054