ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- رمزگذاری چیست؟
- رمزگذاری داده های ذخیره شده
- رمزگذاری داده های در حال انتقال

رمزگذاری

رمزگذاری چیست؟

شاید اصطلاح «رمزگذاری» را شنیده باشید و اینکه چگونه باید از آن برای محافظت از خود و اطلاعاتتان استفاده کنید. با این حال، مفهوم رمزگذاری می تواند به نظر گیج کننده باشد. علاوه بر این، رمزگذاری شما را در مقابل همه خطرات محافظت نمی کند، و محدودیت هایی دارد. در این خبرنامه با عباراتی بسیار ساده توضیح خواهیم داد که رمزگذاری چیست، چرا باید از آن استفاده کرد و نحوه پیاده سازی درست آن چگونه است.

سردبیر مهمان

کریستوفر کراولی (@CCrowMontance; +ChrisCrowley) در منطقه واشنگتن دی سی کار می کند. او سرمربی دوره آموزشی امنیت دستگاه تلفن همراه و هک اخلاق (SEC575) و مولف دوره مدیریت گروه واکنش سریع (MGT535) در موسسه SANS است.

شما ممکن است مقدار بسیار زیادی اطلاعات حساس بر روی دستگاه های خود داشته باشید، از جمله اسناد مالی، عکس های شخصی و خانوادگی، ایمیل، و یا سوابق پزشکی. اگر یکی از دستگاه های خود را گم کنید و یا به سرقت بروند، تمام آن اطلاعات بسیار حساس توسط هر کسی که دستگاه را در اختیار دارد قابل دسترسی است. علاوه بر این، ممکن است عملیات حساس آنلاین مانند بانکداری و یا خرید آنلاین انجام دهید. اگر یک هکر سایبری فعالیت های آنلاین شما زیر نظر بگیرد، او می تواند تمام اطلاعات شما مانند حساب مالی یا شماره کارت اعتباری شما را سرقت کند. رمزگذاری تضمین می کند که افراد غیر مجاز نمی توانند به اطلاعات و عملیات آنلاین شما دسترسی داشته باشند و یا آن را تغییر دهند.

وقتی اطلاعات رمزگذاری نشده اند، آنها را متن ساده (plain-text) مینامند. این به این معنی است که هر کسی براحتی می تواند آنرا بخواند و یا به آن دسترسی داشته باشد. رمزگذاری این اطلاعات را به یک شکل غیر قابل خواندنی به نام متن رمزشده تبدیل می کند. رمزگذاری با استفاده از عملیات ریاضی پیچیده و یک کلید منحصر به فرد متن ساده را به متن رمزشده تبدیل میکند. این کلید منحصربفرد دسترسی به اطلاعات را قفل و یا باز میکند، درست مثل یک کلید که درب را قفل و یا باز میکند. یک مثال معمول از این کلید، همان رمز عبور است، تنها افرادی که رمز عبور دارند می توانند اطلاعات را رمزگشایی و به اطلاعات دسترسی پیدا کنند. برای محافظت از اطلاعات رمزگذاری شده، شما نیاز به حفاظت از کلید خود دارید. بطور کلی، رمزگذاری به دو منظور انجام میشود، رمزگذاری داده های ذخیره شده (مانند داده های ذخیره شده در لپ تاپ شما) و رمزگذاری داده های در حال انتقال (مانند انتقال اطلاعات آنلاین).

رمزنگاری داده های ذخیره شده

هدف اصلی از رمزنگاری داده های ذخیره شده محافظت از اطلاعات است چه کامپیوتر و یا دستگاه تلفن همراه تان را از دست بدهید و یا به سرقت برود. پانزده سال پیش، این مشکلی نبود، چون بیشتر رایانه ها بزرگ و سنگین بودند که جابجایی آنها بسیار دشوار بود. اما امروزه بسیاری از لپ تاپ

رمزگذاری

رمزگذاری یک روش قدرتمند برای امنیت اطلاعات شما است، اما قدرت آن بستگی به قدرت کلید شما دارد.

ها فقط چند کیلو وزن دارند، در حالی که دستگاه تلفن همراه می تواند چند صد گرم باشد. این دستگاه ها بسیار قدرتمند و مقدار بسیار زیادی از اطلاعات را نگه میدارند، که از دست دادن آنها بسیار آسان است. علاوه بر این، حافظه های قابل حمل مانند درایوهای فلش USB و یا CD ROM می توانند اطلاعات حساس نگه دارند. روش معمول برای رمزنگاری اطلاعات ذخیره شده روی این حافظه ها رمزگذاری کامل دیسک (Full Disk Encryption =FDE) است. این به این معنی است که همه چیز بر روی سیستم به طور خودکار رمزنگاری میشود و لازم نیست تصمیم بگیرید چه چیزی رمز شود و چه چیزی رمز نشود. اکثر سیستم های عامل امروزی قابلیت رمزگذاری کامل دیسک در آنها وجود دارد، که بهتر است آن را فعال کنید. به عنوان مثال، سیستم عامل مک X نرم افزار FileVault را برای اینکار دارد و برخی از نسخه های ویندوز نیز شامل نرم افزار Bitlocker هستند. اگر کامپیوتر شما از رمزگذاری کامل دیسک پشتیبانی میکند، ما به شدت توصیه میکنیم آن را فعال کنید. علاوه بر این، بسیاری از تلفن های همراه از رمزگذاری کامل دیسک برای حافظه های داخلی خود استفاده میکنند. به عنوان مثال iOS، سیستم عامل iPhones و iPads، وقتی رمز عبور برای دستگاه میگذارید رمزگذاری کامل دیسک را به طور خودکار فعال میکند. برای کسب اطلاع از اینکه آیا کامپیوتر و یا دستگاه تلفن همراه شما در محل کار از رمزگذاری کامل دیسک پشتیبانی میکند، از مرکز رایانه و یا سرپرست خود سوال کنید. برای رایانه های شخصی، با تولید کننده کامپیوتر خود تماس بگیرید یا اسناد آنلاین را مطالعه کنید.

رمزنگاری اطلاعات در حال انتقال

اطلاعات در حال انتقال هم آسیب پذیر هستند. اگر داده ها رمزگذاری نشده باشد، آنها را میتوان خواند و به محتوای آنها دسترسی پیدا کرد. به همین علت است که باید هر گونه ارتباطات حساس آنلاین مانند بانکداری آنلاین، ایمیل ارسال و یا شاید حتی دسترسی به سایت های رسانه های اجتماعی نیز رمز شده باشند. رایج ترین نوع رمز گذاری آنلاین HTTPS است. این به این معنی است که همه ترافیک بین مرورگر شما و وب سایتی که به آن وصل شده اید رمزگذاری شده است. وجود https:// در URL، یا یک شکلک قفل در صفحه مرورگر، و یا رنگ سبز نوار URL این ها همه نشانه هایی است که ارتباط رمزگذاری شده است. بسته به مرورگر شما و وب سایت، ممکن است هر سه نشانه را همزمان ببینید. علاوه بر این، هر زمان که شما به یک شبکه Wi-Fi عمومی متصل می شوید، اگر امکان پذیر است حتما از رمزگذاری استفاده کنید. در نهایت، هنگام ارسال یا دریافت ایمیل مطمئن شوید نرم افزار ایمیل تان طوری تنظیم شده است که ایمیل ها را رمز شده دریافت یا ارسال میکند. اکثر برنامه های ایمیل امکان رمزگذاری دارند، علاوه بر این، شرکت فراهم کننده خدمات اینترنت (ISP) شما میتواند به شما برای تنظیم رمزگذاری بر روی نرم افزار ایمیل شما کمک کند.

رمزگذاری

طرز پیاده سازی صحیح رمزنگاری

صرف نظر از این که از چه نوع رمز نگاری و یا چگونه استفاده میکنید، تقریبا تمام اشکال رمزگذاری برخی گام های مشترک برای استفاده صحیح از آن دارند.

- قدرت رمز نگاری به قدرت کلیدی که استفاده کرده اید دارد. اگر کسی کلید را حدس بزند و یا به آن دسترسی بیابد، آنها میتوانند به داده های شما دسترسی داشته باشند. از کلید باید به خوبی حفاظت شود.
- اگر از رمز عبور عددی و یا کلمه ای برای کلید خود استفاده میکنید، حتما رمزی طولانی و امن انتخاب کنید و مواظب باشید که آن را گم و یا فراموش نکنید. اگر آن را فراموش کنید، دیگر به داده های خود دسترسی نخواهید داشت.
- رمزنگاری شما به اندازه ای امن است که کامپیوتر شما امن است. اگر کامپیوتر شما به خطر افتاده یا ویروسی شده باشد، هکرهای سایبری می توانند رمزگذاری را دور بزنند. به این ترتیب، مطمئن شوید که کامپیوتر و یا دستگاه تلفن همراه امن است.
- اگر گزینه های مختلف برای رمزنگاری ارائه شده، همیشه قوی ترین روش را انتخاب کنید.

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 syscurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

Mac OS X FileVault : http://support.apple.com/kb/ht4790

رمزگذاری در iOS : http://support.apple.com/kb/ht4175

رمزگذاری آندروید : /http://www.androidauthority.com/how-to-encrypt-android-device-326700

رمزگذاری در ویندوز : http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7

تضمین امنیت رایانه شما : http://www.securingthehuman.org/ouch/2012#december2012

نرم افزارهای مدیریت رمز عبور : http://www.securingthehuman.org/ouch/2013#october2013

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

ترجمه شده توسط : سعید میرجلیلی