ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

- رمز نگاری چیست؟
- چه چیزی را می توانید رمز نگاری کرد؟
- رمز نگاری را درست انجام دهید

رمزنگاری

رمز نگاری چیست؟

ممکن است از مردم واژه «رمزنگاری» را بشنوید و اینکه چگونه از آن برای محافظت از خودتان و اطلاعاتتان استفاده کنید. اما، رمزنگاری ممکن است گیج کننده باشد و باید محدودیت هایش را هم بدانید. در این شماره با کلمات ساده توضیح خواهیم داد رمزنگاری چیست، چگونه شما را محافظت می کند وچگونه آنرا بطور مناسب پیاده سازی کنید.

سردبیر مهمان

فرانچسکا بوسکو(**@francibosco**) محقق و مدیر پروژه است که پروژه های مربوط به جرم سایبری، امنیت سایبری و سوء استفاده از تکنولوژی را مدیریت می کند. او در موسسه تحقیقات عدالت و جرم بین منطقه ای ملل متحد کار می کند. او همچنین یکی از موسسان مرکز تکنولوژی و حقوق (Tech and Law Center) است.

شما مقدار بسیار زیادی اطلاعات حساس از قبیل مدارك شخصی، عکس ها، و ایمیل ها روی دستگاه هایتان دارید. اگر یکی از دستگاههایتان گم شود یا دزدیده شود، همه اطلاعات حساس شما ممکن است توسط شخصی که دستگاهها را در اختیار دارد قابل دسترسی باشد. بعلاوه ممکن است معاملات حساسی مانند عملیات بانکی یا خرید را آنلاین انجام دهید. اگر شخصی این فعالیت ها را زیر نظر بگیرد ممکن است بتواند اطلاعات شما مانند حساب های مالی یا شماره کارت اعتباری تان را بدزدد. رمزنگاری شما را در این موقعیت ها با اجازه ندادن به افراد غیر مجاز به دسترسی داشتن و یا تغییر دادن اطلاعات، محافظت می کند.

هزاران سال است که رمزنگاری مورد استفاده قرار می گیرد. امروزه، رمزنگاری خیلی پیچیده شده است، اما مورد استفاده اش همان فرستادن پیامی سری از مکانی به مکانی دیگر و اطمینان از اینکه فقط اشخاص مجاز بتوانند آنرا بخوانند و به آن دسترسی داشته باشند است. وقتی اطلاعات رمزنگاری نشده باشد به آن متن ساده می گویند. معنی آن اینست که هر کسی به آسانی می تواند آنرا بخواند و به آن دسترسی داشته باشد. رمزنگاری این اطلاعات را به فرمت غیرخوانا که متن رمز نگاری شده نامیده می شود تبدیل می کند. رمزنگاری امروزه، با عملیات پیچیده ریاضی و کلیدی منحصر بفرد کار می کند که اطلاعاتتان را به متن رمزنگاری شده تبدیل می کند. کلید چیزی است که اطلاعاتتان را قفل می کند یا قفلش را باز می کند. در بیشتر موارد، کلید رمز عبور یا کد عبور است.

چه چیزی را می توان رمزنگاری کرد؟

عموما دو نوع داده را می توان رمزنگاری کرد. داده ساکن (مثل داده ذخیره شده روی دستگاه موبایل) و داده متحرك (مثل ایمیل یا پیام ارسالی به دوست).

رمزنگاری داده متحرك جهت حفاظت از اطلاعاتتان اگر کامپیوتر یا موبایلتان گم یا دزدیده شد بسیار حیاتی است. دستگاههای امروزی بسیار قوی هستند و مقدار بسیار زیادی اطلاعات را روی خود ذخیره می کنند، اما این دستگاهها براحتی ممکن است گم شوند. بعلاوه، انواع دیگر وسایل سیار مانند فلاش

رمزنگاری

یو اس بی یا حافظه های جانبی خارجی هم می توانند حاوی اطلاعات حساسی باشند. رمزنگاری کامل دیسك (FDE) تکنیك رمزنگاری ای است که بطور وسیعی برای رمزنگاری کل درایو روی سیستم بکار می رود. یعنی همه چیز روی سیستم بطور خودکار رمزنگاری می شود، شما نباید تصمیم بگیرید چه چیزی رمزنگاری بشود و چه چیزی رمزنگاری نشود. امروزه بیشتر کامپیوتر ها با FDE تولید می شوند، اما ممکن است که بطور دستی آنرا بکار بیاندازید یا از کار بیندازید. در کامپیوتر های مك FileVault نامیده می شود در حالیکه در کامپیوتر های ویندوز بسته به نسخه، می توانید از Bitlocker یا Device Encryption استفاده کنید. بیشتر دستگاههای موبایل هم FDE را پشتیبانی می کنند iOS در آیفون و آیپد FDE را بطور خودکار بعد از اینکه کد عبور تنظیم شد فعال می سازند. با شروع Android 6.0 (مارشملو) گوگل خواسته است FDE بطور پیش فرض بکار بیفتند، در صورتیکه سخت افزار مینیمم استاندارد های بخصوصی داشته باشد.

رمزنگاری راه قوی برای کمك به امنیت اطلاعات شماست. اما قدرتش به اندازه قدرت کلیدرمز شماست.

اطلاعات همچنین هنگام انتقال آسیب پذیر هستند. اگر داده رمزنگاری نشده باشد، ممکن است دیده شوند، تغییر داده شوند و بطور آنلاین ربوده شوند. این دلیلی است که می خواهید مطمئن باشید هر معامله حساس آنلاین و ارتباط حساس رمزنگاری شده است. راه رایج رمزنگاری آنلاین HTTPS است. یعنی همه آمد و شد ها بین مرورگر و وبسایت رمزنگاری شده است. در URL دنبال https:// بگردید، آیکن قفل در مرورگر باشد، یا خط URL سبز شود. مثال دیگر اینست که وقتی که ایمیلی می فرستید یا می گیرید. بیشتر نرم افزارهای ایمیل قابلیت رمزنگاری فراهم می کنند که ممکن باشد خودتان مجبور باشید آنرا فعال کنید. مثال سوم رمزنگاری داده در نقل و انتقال بین دو کاربر که در حال چت با یکدیگر هستند، مثلا در iMessage, Wicker, Signal, WhatsApp یا Telegram است. اپلیکیشن هایی مثل اینها، از رمزنگاری ابتدا تا پایان استفاده می کنند که از اینکه نفر سومی بتواند به داده در حال انتقال از یك سیستم پایانی یا دستگاه به دستگاه دیگر دسترسی پیدا کند جلوگیری می کند. این یعنی فقط شما و شخصی که با او در حال گفتگو هستید می توانید چیزی که فرستاده شده را بخوانید.

رمزنگاری را درست انجام دهید

برای اطمینان از اینکه با استفاده از رمزنگاری واقعا محافظت شده اید، باید از آن درست استفاده کنید.

- قدرت رمزنگاری به اندازه قدرت کلیدرمز شماست. اگر کسی کلیدرمز شما را حدس بزند یا به آن دسترسی پیدا کند، آنها به داده شما دسترسی خواهند داشت. از کلیدتان محافظت کنید. اگر از کد عبور یا رمز عبور برای کلیدتان استفاده می کنید، حتما باید کلمه عبور

رمزنگاری

قوی و منحصر بفرد باشد. هر چه کلمه عبور طولانی تر باشد برای حمله کننده سخت تر است که آنرا حدس بزند. کلمه عبورتان را فراموش نکنید، بدون کلید شما دیگر نمی توانید اطلاعات را رمزگشایی کنید. اگر نمی توانید همه کلمات عبور را به خاطر بسپارید، توصیه می کنیم از نرم افزار مدیریت رمز عبور استفاده کنید.

- قدرت رمزنگاری به اندازه امنیت دستگاهتان است. اگر دستگاهتان با بدافزارها آلوده شده باشد، حمله کنندگان سایبری می توانند رمزنگاری تان را دور بزنند. به همین دلیل مهم است که قدم دیگری جهت امنیت دستگاهتان بردارید، مثلا استفاده از آنتی-ویروس، استفاده از رمز عبور قوی و بروز نگه داشتنش.
- برای محافظت از داده ها و ارتباطاتتان بسیاری از اپلیکیشن های موبایل و کامپیوتر رمزنگارهای قوی ارائه می دهند. اگر اپلیکیشنی که مدنظرتان است رمزنگاری را حمایت نمی کند، به جایگزین فکر 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: securingthehuman.sans.org/ouch/archives

یادداشت مترجم

سایت www.sycurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

توضیح رمزنگاری: http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

عبارت عبور: https://securingthehuman.sans.org/ouch/2015#april2015

مدیریت رمز عبور: https://securingthehuman.sans.org/ouch/2015#october2015

بدافزار چیست؟: https://securingthehuman.sans.org/ouch/2016#march2016

تبلت جدیدتان را امن کنید: https://securingthehuman.sans.org/ouch/2016#january2016

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

ترجمه شده توسط : سعید میرجلیلی