رمزگذاری کلید آسایش سازمانی و فراسازمانی

نقص‌های داده‌ای عامل سرقت اطلاعات مالی و شخصی

در سال 2015، نقص‌های داده‌ای باعث به سرقت رفتن حجم گسترده‌ای از داده‌های کاربران شد. در حالی که در خلال سال‌های 2013 و 2014 مجرمان سایبری سرفصل‌های مشخصی در خصوص سرقت اطلاعات کارت‌های اعتباری و اطلاعات مالی برای خود ترسیم کرده بودند، اما در سال 2015 این سرفصل‌ها منحصراً به سرقت اطلاعات شخصی کاربران معطوف شد. جالب آنکه تا اواسط سال جاری میلادی نیز همچنان مشاهده می‌کنیم که این سرفصل پابرجا بوده و اطلاعات شخصی کاربران در سایت‌های لینکدین و توتیتر به سرقت می‌روند.

آمارها نشان می‌دهند که در 53 درصد موارد، سرقت داده‌ها بر مبنای نقص‌های داده‌ای صورت گرفته است. آمارهای جهانی به صراحت اعلام می‌کنند که بزرگ‌ترین حملاتی که منجر به سرقت داده‌ها در مقیاس میلیاردها رکورد شده‌اند، به فقدان مفهومی به نام رمزگذاری اطلاعات (encryption) بازمی‌گردد. جالب آنکه حتی خود این مفهوم نیز به‌آرامی در حال تغییر است. در آینده‌ای نه‌چندان‌دور، رمزگذاری تحت‌الشعاع فناوری قدرتمند اما در عین حال ترسناکی به نام «رایانش کوانتومی» قرار خواهد گرفت.

مطلب پیشنهادی

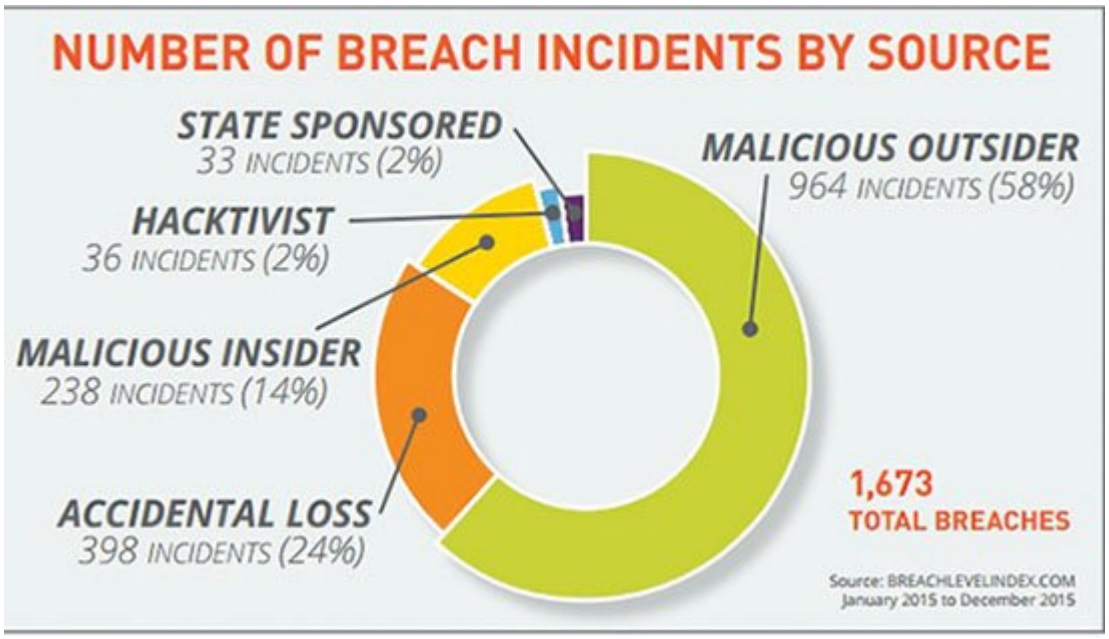
جدال بر سر آینده

گوگل به مبارزه با هکرهای کوانتومی آینده برخواسته است

آمارهای جهانی هشدار می‌دهند

بدون تردید، سال 2015 میلادی کابوس بزرگ مدیران اجرایی فناوری اطلاعات و کارشناسان امنیتی در سراسر جهان بود. جالب آنکه این کابوس همچنان نیز ادامه دارد. اگر به مقالات و سرمقاله‌های امنیت اطلاعات در سال میلادی گذشته نگاهی بیندازید، متوجه می‌شوید که نیمی از آن‌ها بر ضرورت توجه به مبحث امنیت در شبکه‌های ارتباطی و سامانه‌های دولتی و لزوم توجه بیشتر به مفهوم رمزگذاری (encryption) تأکید کرده‌اند. با استناد به داده‌های جمع‌آوری‌شده از سوی BLI، سرنام Breach Level Index، در سال گذشته میلادی 1673 مورد نقص داده‌ای در مقیاس کلان به ثبت رسیده (شکل 1) و نزدیک به 707.5 میلیون رکورد حساس و نیمه‌حساس از شهروندان

کشورهای مختلف را تهدید کرده است. (شکل 2) در 58 درصد موارد، دسترسی به این نقص‌های داده‌ای از سوی ابزارهای مخرب ناشناس صورت گرفته است. هکرها نیز بیش از هر زمان دیگری به سرقت اطلاعات شخصی و هویت فردی مردم توجه نشان داده‌اند و 53 درصد داده‌های به‌سرقت‌رفته درباره هویت فردی و اطلاعات کاربری مردم بوده است. صنعت بهداشت و درمان در بخش‌های مختلف شاهد سرقتی 22 درصدی بوده است. با این حال نقص داده‌ای و سرقت داده‌ها با ضریب 43 درصد، همچنان در اختیار سوابق کارمندان دولتی قرار دارد. هکرها و مجرمان سایبری به این بخش بیش از سایر بخش‌ها توجه کرده‌اند. نکته جالب توجه دیگری که در این گزارش‌ها وجود دارد، این است که همه این نقص‌ها به یک شکل و اندازه نیستند.



□□□ 1: □□□□□□ □□□□□□ □□ □□□□□□ □□ □□□□□□□ □□□□□ □□□□□ □□□□

آیا رمزگذاری مترادف با پیچیدگی است؟

خیر؛ رمزگذاری بسیار ساده است. هیچ دلیل قانع‌کننده‌ای وجود ندارد که سازمانی در سال 2016، هنوز از مکانیزم رمزگذاری استفاده نکرده باشد. این فناوری اکنون به ساده‌ترین شکل وجود دارد. یک دلیل منطقی برای استفاده از این راهکار امنیتی وجود دارد؛ اگر به دنبال آن هستید تا از سرقت اطلاعات که بر پایه نقص‌های داده‌ای رخ می‌دهد ممانعت کنید، راه‌حل شما رمزگذاری داده‌ها است. هکرها منتظر فرصت هستند تا به داده‌های شخصی و کسب‌وکار ما دسترسی پیدا کنند، در نتیجه باید در مرحله اول طرز تفکر هکرها و مکانیزمی را که استفاده می‌کنند بررسی کرده و در ادامه راهکاری برای محافظت از اطلاعات حیاتی خود پیدا کنیم.

هکرها در فکر نفوذ و به سرقت بردن چه اطلاعاتی هستند؟

گزارش‌های سال 2015 به‌خوبی نشان می‌دهند که هکرها به دنبال کردن و دسترسی به اطلاعاتی که از ارزش و دوام بیشتری برخوردار هستند، علاقه بیشتری پیدا کرده‌اند. در حالی که در سال‌های پیش مجرمان سایبری مترصد فرصتی بودند که به داده‌های مالی دسترسی پیدا کنند، گزارش‌ها نشان می‌دهد که آن‌ها اکنون تمرکزشان بر اطلاعات زمان‌دار است. اگر کمی به این مسئله فکر کنید، متوجه خواهید شد که سیاست جدید آن‌ها تا چه اندازه می‌تواند خطرناک باشد. دسترسی به اطلاعات و هویت شخصی افراد این ظرفیت را در اختیار هکرها قرار می‌دهد تا طیف متنوع و گسترده‌تری از حملات را پایه‌ریزی کنند. کافی است کمی به اطلاعات پزشکی خود یا اطلاعاتی که در بانک‌های اطلاعاتی دولتی ذخیره شده‌اند، توجه کنید. این حجم از اطلاعات به‌راحتی زمینه‌ساز حملات خطرناکی همچون اخاذی‌های آنلاین یا حملات فیشینگ می‌شوند.

□□□ 2: □□□□□
□□□□□□□□□
□□□□□□□□□□□ □□ □□□
2015

هکرها آگاه شده‌اند که امکان تغییر شماره تأمین اجتماعی در کوتاه‌مدت بسیار دشوارتر از باطل کردن شماره کارت‌های اعتباری است. جالب آنکه در سوابق پزشکی افراد امکان تغییر اطلاعات به هیچ وجه امکان‌پذیر نیست. هکرها اکنون به ماندگاری این چنین اطلاعاتی به‌خوبی آگاه شده‌اند. در سطح یک مصرف‌کننده، اگر هکری توانایی ضبط اطلاعات کلیدی شخصی را در اختیار داشته باشد، نه تنها می‌تواند حمله‌ای را منحصر به یک قربانی ترتیب دهد، بلکه می‌تواند سازمانی را که او در آن مشغول به کار است یا حتی سازمان‌هایی که با سازمان متبوع کاربر یا خود کاربر در ارتباط هستند، به صورت آنلاین در معرض خطر قرار دهد. کافی است یک مقایسه ساده انجام دهید؛ زمانی که مهاجمی دیجیتالی اطلاعات کارت اعتباری شما را به سرقت می‌برد، به‌سادگی می‌توانید تراکنش‌های مالی خود را متوقف و باطل کرده و در نهایت از کارت جدیدی استفاده خواهید کنید. حال این چنین وضعیتی را در خصوص یک شرکت متصور شوید. در قرن 21 داده‌های علمی، قلب تپنده کسب‌وکارهای بزرگ هستند. این داده‌ها تمامی استراتژی‌های حال و آینده شرکت را خط‌دهی می‌کنند. در هیچ مقطع زمانی داده‌ها تا این اندازه ارزشمند نبوده‌اند. حالا فکر کنید یک هکر دیجیتالی باهوش به سراغ چه گروهی از داده‌ها می‌رود؟ در عصر یکپارچگی اطلاعات سازمانی، کمتر هکری به سراغ اهداف کم‌اهمیت‌تر می‌رود.

نقص‌های داده‌ای همیشه منتهی به سرقت اطلاعات نمی‌شوند

هر زمان درباره نقص‌های امنیتی و نفوذ به سازمان‌ها صحبت می‌کنیم، در انتظار شنیدن آمارها و ارقامی هستیم که بیانگر رکوردهای به‌سرقت‌رفته از یک سازمان هستند. اما باید بدانید همیشه حمله با این هدف انجام نمی‌شود. نقص‌های داده‌ای باعث به وجود آمدن حملات بسیار ظریف و مینیاتوری می‌شوند. شرکتی در زمینه تولید ویجت‌ها فعالیت دارد. چنین شرکتی کم‌وبیش با داده‌های بزرگی که بر مبنای رویکردهای تحلیلی تولید می‌شوند، سروکار دارد. حال اگر هکر دیجیتالی فقط یک نفوذ کوچک انجام دهد و تغییر مختصری در داده‌ها به وجود آورد، باعث می‌شود ماهیت استراتژی‌های آن سازمان دستخوش تغییر شود. در این حالت هکر نیازی ندارد که حتی یک بیت مجزا از اطلاعات سازمان رقیب را به سرقت ببرد، بلکه تنها باید تغییر کوچکی به وجود آورد. شرکت بی‌اطلاع از این پیشامد، تصمیمات خود را بر مبنای تحلیل‌های انجام‌گرفته عملیاتی می‌کند و ماه‌های متوالی کسب‌وکار خود را بر اساس این داده‌ها پیش می‌برد. در طول این مدت، شرکت تصمیمات خطرناکی می‌گیرد، به دلیل اینکه داده‌های اصلی تغییر پیدا کرده‌اند. شرکت ماه‌ها بر پایه این رویکرد اشتباه به حرکت خود ادامه می‌دهد و بدتر آنکه بازیابی داده‌های درست به دلیل اینکه به بانک اطلاعاتی پشتیبان نیز حمله شده است، سودی ندارد. در نهایت، شرکت با هزینه‌های غیرمتعارف و سرسام‌آور روبه‌رو می‌شود، سهام و دارایی‌های خود را از دست می‌دهد و سرانجام اعتبارش از بین می‌رود.

چگونه می‌توانیم از بروز این حملات جلوگیری کنیم؟

در ظاهر این‌گونه به نظر می‌رسد که پیاده‌سازی راهکاری برای پیشگیری از بروز این چنین حملاتی، برای یک شبکه سازمانی کار چندان ساده‌ای نخواهد بود. حال این پرسش پیش می‌آید که آیا ما باید این باور باشیم که به دلیل اینکه خود را به دانش پیشگیری از حملات تجهیز کرده‌ایم، این نقص برای ما رخ نخواهد داد، یا بدتر از آن، گمان کنیم داده‌های ما آن اندازه ارزشمند نیستند که در معرض تهدید قرار گیرند؟ با توجه به 1600 نقص داده‌ای در سال 2015 که در سراسر جهان داده‌ها را در معرض تهدید قرار داده، عاقلانه است که جانب احتیاط را در پیش بگیریم. اما این کار در چند مرحله به‌سادگی انجام می‌شود.

گام اول: ارتباطات را کنترل کنید

بهتر است به ارتباطات بیش از اندازه‌ای که در آینده برقرار خواهید کرد، خوب فکر کنید. از هم‌اکنون در فکر استراتژی مدونی برای تجهیزات اینترنت اشیا باشید. اینترنت اشیا در حال حاضر مفهومی نیست که خارج از مرزهای کشور باشد، شما نیز به‌آرامی شاهد حضور این گجت‌ها در زندگی و محیط کاری خود خواهید بود. حتی یک ابزار دیجیتالی مستقل، حداقل از سوی پنج گروه تهدید خواهد شد: سازنده محصول، مصرف‌کننده، ارائه‌دهنده خدمات ابری که داده‌ها روی آن میزبانی می‌شوند، سازنده تلفن هوشمند، نرم‌افزاری که کاربر آن را روی تلفن خود نصب کرده و با استفاده از آن گجت خود را کنترل می‌کند و حداقل یک گجت دیگر که به صورت دیجیتالی به این دستگاه اینترنت اشیا متصل خواهد شد. زمانی که خانه یا ماشین مملو از اتصال‌های مختلف است، در عمل تعداد ارتباطات ممکن است فراتر از پنج موردی شود که به آن اشاره شد.

گام دوم: نظارت بر زنجیره ارتباطات

در هر نقطه‌ای از زنجیره انتقال، هکرها می‌توانند نواقص دفاعی را شناسایی کرده و مسیر اطلاعات را منحرف کنند. اگر هر یک از بخش‌های تولیدی وب تهدید شوند، با مشکلی جدی روبه‌رو خواهیم شد. جای تعجب نیست که امروزه شاهد هستیم امنیت ارتباطات مرتبط با وب تا این اندازه پیچیده شده است. اکنون سازمان عظیمی را با هزاران دستگاه در نظر بگیرید که وظیفه برقراری ارتباط همراه در سراسر جهان را بر عهده دارد. طبیعی است این چنین سازمانی با طیف گسترده و پیچیده‌ای از حملات دیجیتالی که به‌طور فزاینده‌ای پیچیده‌اند و برای پیدا کردن حتی یک شکاف کوچک در ارتباط‌های دیجیتالی به فعالیت مشغول هستند، روبه‌رو باشد. طبیعی است این سازمان از ابزارهای دقیق و پیشرفته‌ای برای نظارت بر ارتباطات وارد و خارج‌شونده استفاده کند. در نتیجه، همواره سعی کنید بر فرایند نقل و انتقال اطلاعات درون‌شبکه‌ای خود کنترل داشته باشید.

گام سوم: نظارت دوچندانی بر دارایی‌های حساس داشته باشید

لازم است که بر محافظت از دارایی‌هایی که هکرها واقعاً به آن‌ها علاقه‌مند هستند، تمرکز بیشتری کنیم. این دارایی‌ها همان داده‌ها هستند. داده‌ها سبب می‌شوند که نه تنها رمزگذاری، بلکه نقص‌های احتمالی داده‌ها نیز بررسی شوند. در نتیجه تنها محافظت از داده‌ها، ما را در مقابل هکرها ایمن نمی‌سازند. رهبران امنیتی در سازمان‌های بزرگ و کوچک باید نقص‌های کشف‌شده در سازمان متبوع خود را اعلام کنند و پس از کشف آن‌ها، به دنبال راه علاجی برای حل مشکل خود باشند. چه داده‌ای بیش از سایر داده‌ها در معرض تهدید قرار گرفته است؟ چه داده‌هایی در طول این حمله یکپارچگی خود را از دست داده‌اند؟ آیا نقص اطلاعاتی باعث نابودی کسب‌وکار سازمان خواهد شد؟ این رهبران همچنین باید به این نکته توجه کنند که به کارگیری راهکارهای عجیب و گران‌قیمت هرچند به حفظ دارایی‌های حیاتی یک سازمان کمک می‌کنند، اما همواره هکر سخت‌کوشی وجود دارد که بتواند رخنه‌ای پیدا کند. در نتیجه رهبران امنیتی سازمان‌ها باید همواره در فکر راهکارهای متفاوتی برای محافظت از داده‌ها باشند. آن‌ها باید به ارزیابی مخاطرات و اعمال کنترل بر اطلاعات حیاتی و امنیتی بپردازند و از مکانیزم‌های رمزگذاری، مدیریت کلید و احراز هویت - گاهی احراز هویت دوعاملی- استفاده کنند. به‌کارگیری این راهکارها باعث بهبود امنیت می‌شود. در چنین شرایطی اگر حمله‌ای رخ دهد، شرایط تقریباً تحت کنترل خواهد بود. کارشناسان امنیتی به این پیشامد نقص ایمن (secure breach) می‌گویند. در این حالت حتی اگر هکری موفق شود از مکانیزم‌های تعبیه‌شده عبور کند و در جعبه را بگشاید، داده‌های چندان باارزش و مفیدی را پیدا نخواهد کرد، به دلیل اینکه داده‌ها تکه‌تکه شده‌اند، همگی آن‌ها قفل شده و رمزگذاری شده‌اند.

رمزگذاری؛ کلید حل مشکل سرقت اطلاعات است

در حالی که رمزگذاری یکی از بارزترین استراتژی‌های مؤثر در رویارویی با نقص‌ها به شمار می‌رود؛ اما تنها 48 مورد از نقص‌های داده‌ای سال 2015 که در مجموع چهار درصد رخنه‌ها را شکل می‌دادند، از درجات مختلفی از رمزگذاری استفاده کرده بودند. باید این حقیقت را قبول کنیم که نقص‌ها همواره رخ می‌دهند و برای اینکه به شکل ایمنی با آن‌ها روبه‌رو شویم، باید از سلاح قدرتمندی استفاده کنیم؛ این سلاح قدرتمند همان رمزگذاری (encryption) است.

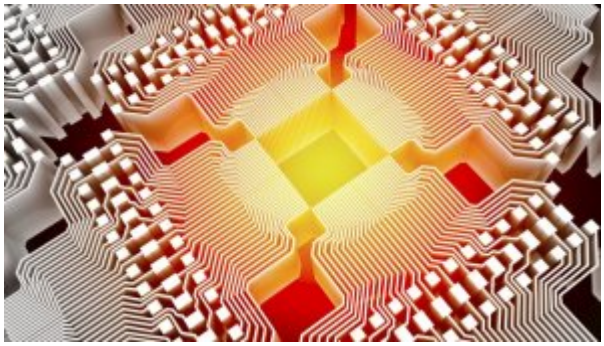
==========

شاید به این مقالات هم علاقمند باشید:

شبیه‌سازی فرآیند ساخت پادماده با یک کامپیوتر کوانتومی

مجرمان سایبری حملات فیشینگ را سازمان‌دهی می‌کنند!

هک گسترده مسافران المپیک ریو با وای‌فای و اپلیکیشن‌های جعلی



سرمایه‌گذاری یک میلیارد یورویی اتحادیه اروپا در حوزه رایانش کوانتومی

حمله سایبری که «احراز هویت دو مرحله‌ای» را هم دور می‌زند!

هک خودروها با یک میکروکامپیوتر سوار بر دِرون

حملات فیزیکی برای استخراج کلیدهای رمزنگاری

نرم‌افزار مدیریت گذرواژه‌ای که گذرواژه‌ها را لو می‌دهد!

تاریخ انتشار:

25 مرداد 1395

نشانی منبع: https://www.shabakeh-mag.com/security/4056