چه کسی از ایمیل‌های شما جاسوسی می‌کند

برای داشتن یك درگاه ایمیل امن، باید دنبال چه چیزهایی بود؟

تقریباً تمامی ایمیل‌ها در اینترنت به‌صورت رمزنگاری‌شده و به‌صورت متن ساده پراکنده هستند. این مانند ارسال یک کارت‌پستال از طریق پست است. هرکسی که اتفاقی یا عمدی به آن برخورد کند می‌تواند محتوای آن را بخواهند، بدون اینکه شما خبردار شوید.

ایمیل‌های شما یک کتاب باز است

شاید برایتان جالب باشد بدانید که چه کسی تمایل دارد ایمیل‌های شما را بخواند. نظرتان در مورد ISP یا ارائه‌دهنده‌ی خدمات ایمیلتان چیست؟ گوگل که قطعاً تمایل دارد. در یک پرونده‌ی اخیر حقوقی، گوگل اعلام کرد که کاربرانش نباید انتظار رعایت حریم خصوصی خود را داشته باشند.

در خلال پرونده‌ی حقوقی بزرگی که در ماه مه ۲۰۱۳ علیه گوگل عنوان شد، آن‌ها در جوابیه‌ی خود برای درخواست ابطال آن عنوان کردند که:

«تمام کاربران ایمیل باید انتظار داشته باشند که تمام ایمیل‌های آن‌ها به‌صورت خودکار پردازش خواهد شد. درست مانند وقتی‌که فرستنده‌ی یک نامه از باز شدن نامه‌اش توسط منشی گیرنده تعجب نمی‌کند، مردمی که از ایمیل‌های مبتنی بر وب استفاده می‌کنند نباید تعجب کنند اگر ایمیل‌هایشان توسط ارائه‌کنندگان خدمات ایمیل گیرنده پردازش شود. درواقع هیچ فردی در مورد اطلاعاتی که به‌صورت تعمدی به طرف سومی ارسال می‌کند، نباید انتظار حفظ حریم خصوصی را داشته باشد.»

به گفته‌ی شرکت وکالت Consumer Watchdog این یک اعتراف بسیار جالب‌توجه است. وی به تمام کسانی که نگران حریم خصوصی خود در ایمیل‌ها هستند توصیه می‌کند که از جیمیل استفاده نکنند. ولی متأسفانه این راهکار مناسبی نیست و به‌نوعی مانند این است که به مردم توصیه کنید اصلاً از ایمیل استفاده نکنند. حتی اگر خود شما از جیمیل استفاده نکنید، بی‌شک مجبور خواهید با مشتریان، شرکا یا دیگر ذینفعانی کارکنید که از آن استفاده می‌کنند.

همچنین ممکن است اسم PRISM را شنیده باشید. یک برنامه‌ی داده‌کاوی جمعی که برای جاسوسی الکترونیک توسط آژانس امنیت ملی ایالات‌متحده مورداستفاده قرار می‌گیرد. درواقع NSA مقادیر فاش نشده‌ای از ترافیک ایمیل ISP، Googleها، و دیگر ارائه‌دهندگان خدمات ایمیل مانند Yahoo و Hotmail را جمع‌آوری و ذخیره‌سازی می‌کرده است.

ولی ریسک مربوط به ایمیل‌ها به جاسوسی تعمدی توسط امسال گوگل و NSA محدود نمی‌شود. چند بار تابه‌حال اشتباهی برای پاسخ دادن به یک نفر، اشتباهی گزینه‌ی «پاسخ دادن به همه» را انتخاب کرده‌اید؟ یا اینکه به‌واسطه‌ی فناوری کامل کردن خودکار اسم گیرنده، ایمیلتان را اشتباهی به فرد دیگری ارسال کرده باشید؟ این اتفاق همیشه می‌افتد. و عواقب ارسال اطلاعات حساس به یک فرد اشتباهی می‌تواند ویران‌کننده باشد، از عمومی کردن خبر مربوط به نشت داده گرفته تا جریمه‌ها، ضرر و زیان‌ها، ضربه به اعتبار شرکت و حتی بدتر.

جعل، فیشینگ هدفمند و هرزنامه‌ی کفش برفی

و بعد به آخرین نوع حملات ایمیلی، مانند فیشینگ، اشاره می‌کنیم که در حال تکامل هستند. فیشینگ تلاشی است برای کسب اطلاعاتی مانند گذرواژه‌ها، نام‌های کاربری یا اطلاعات مربوط به کارت‌های اعتباری از ایمیل‌های جعلی و مبدل که گویی از فرستنده‌های معتبر ارسال‌شده‌اند.

فیشینگ معمولاً موفق است و دلیل آن تکنیکی است به نام جعل آدرس ایمیل، که در آن مهاجمان در قسمت «از:» از آدرسی استفاده می‌کنند که شبیه به آدرس بانک معتبر یا شرکتی است که در آن کار می‌کنید.

جدیدترین روش متداول این است که مهاجمان افراد یا گروه‌های خاصی را در یک سازمان هدف قرار گیرند و به روش‌های کاملاً شخصی و فریبنده به آن‌ها نزدیک شوند – که امروزه به آن فیشینگ هدفمند می‌گویند. فیشینگ هدفمند یکی از تاکتیک‌های متداول کمپین‌های پیشرفته‌ی پایا است، که هدف آن دستیابی به شبکه‌های سازمان هدف و سرقت اطلاعات محرمانه است.

و لازم به ذکر است که هرزنامه‌های قدیمی و خوب هنوز هم وجود دارند. به‌واسطه‌ی فیلتر ضد هرزنامه‌ای که روی ایمیل شما نصب‌شده است، احتمالاً بسیاری از آن‌ها را نمی‌بینید، و به‌راحتی می‌توانید ایمیل‌های عجیبی که از شاهزاده‌ی نیجریه دریافت می‌کنید را شناسایی کنید.

ولی هنوز هم مردم در معرض این‌گونه فریبکاری‌ها قرار دارند و ممکن است ترغیب شوند و پیوست‌های بدخواهانه را باز کنند. محققان دریافته‌اند که هرزنامه‌هایی که از یک سایت شبکه اجتماعی مانند فیس‌بوک ارسال می‌شوند تأثیر بیشتری دارند.

هرزنامه نویس‌ها هر روز نوآورتر می‌شوند، و از تکنیک‌هایی مانند هرزنامه‌ی کفش برفی استفاده می‌کنند تا فیلترهای ضد هرزنامه را دور بزنند. هرزنامه‌های کفش برفی، همان‌طور که از نام آن برمی‌آید، حجم بار را میان IPهای متعددی پخش می‌کند. این امر شناسایی هرزنامه‌ها توسط فیلترها را با مشکل مواجه می‌کند و احتمال اینکه یکی از ایمیل‌ها وارد اینباکس کاربر شود را افزایش می‌دهد.

تطابق با قوانین دولتی

امن کـــردن اطلاعات حســـاس برای مشـــتریان، شـــرکا و کارمنـــدان تنهـــا یـــک «بهتریـــن رویه» نیســـت، بلکه اغلب اوقات یک قانون اســـت. تطابق با قوانیـــن یکـــی از اولویت‌هـــای شـــرکت‌های فعـــال در حـــوزه‌ی ســـلامت، خدمـــات مالـــی و نهادهای دولتی اســـت. حتی اگر جزئی از این نوع شـــرکت‌ها نباشـــید، باید قوانین مربوط به حفاظت از داده‌ها که ممکن است روی مشتریان شما تأثیر بگذارد را رعایت کنید.

تقریباً در هر جایـــی قوانینی وجود دارد که تطابق و همچنین الزامات افشـــای اطلاعات در حین نشـــت داده‌ها را تأکیـــد می‌کند. در ایالات‌متحده این GLBA اســـت که روی موسســـه‌های مالی حکومت می‌کند، PCI DSS که برای امنیت کارت‌های اعتباری اســـت، و HIPAA و HITECH برای بخش پزشـــکی و سلامت، و بســـیاری از قوانین دیگر که مربـــوط به ایالت‌های مختلف است.

همه‌ی آن‌ها در یک چیز مشترک هستند و آن الزام بـــه رمزنگاری داده‌های ذخیره‌شـــده و یا داده‌های در حال ارسال (از طریق کانال‌های الکترونیکی) هستند. این قوانین، در صورت بروز نشت اطلاعات، جرائمی را برای عدم تطابق با قوانین و الزامات افشـــای اطلاعات تعیین می‌کند.

سه گام ساده برای تطابق

۱. با تدوین یک خط‌مشی و آموزش کارمندان شروع کنید

یک خط‌مشی تدوین کنید که در آن عناصر کلیدی استراتژی جلوگیری از نشت داده‌هایتان مشخص‌شده باشد. آن را در اختیار تمام کارمندان و ذی‌نفعان قرار دهید. روی انواع داده‌هایـــی که می‌خواهید محافظت کنید، انگیزه‌های شـــما برای حفاظت از آن‌ها، عواقب محافظت نکـــردن از آن‌ها، و روال‌هایی که باید دنبال کرد تا از آن‌ها محافظت کرد، متمرکز شوید.

۲. از فنّـــاوری حفاظـــت از داده‌های ایمیل استفاده کنید

کاربران و خط‌مشی شـــما باید توسط یک فناوری شـــفاف و مؤثر پشـــتیبانی شود. شـــما به یک راهکار برای حفاظت از داده‌ها در مقابل گم‌شـــدگی تصادفی آن‌ها نیاز دارید تا تضمین کند که داده‌های ارســـالی امـــن خواهند بود. یـــک دروازه‌ی ایمیل امن همراه با رمزنـــگاری مبتنی بر خط‌مشـــی از عناصر کلیدی هر راهکار مؤثر حفاظت از داده‌ها است.

۳. با ضروریات شروع کنید، به مرور گسترش دهید

حفاظـــت از داده‌هـــا خیلـــی زود به امـــری بزرگ و ترســـناک تبدیل می‌شـــود، برای همین اســـت که توصیه می‌شـــود نیازهای حفاظت از داده‌های خود را

اولویت‌بندی کنید.

با منبعی شروع کنید که احتمال نشت آن بیشتر است: ایمیل‌ها. اطمینان حاصل کنید که خط‌مشی‌های لازم را برای حفاظت از حساس‌ترین داده‌های مشتریان، کارمندان و شرکای خود را دارید. زمانی که این خط‌مشی‌ها به‌آرامی و بدون مشکل به کار خود ادامه دهد، زمان آن فرامی‌رسد که پیاده‌سازی را وسیع‌تر کنید.

چه چیزی جلوی راه شماست؟

باوجود تمام این انگیزه‌ها برای ایمن ساختن ایمیل و داشتن یک راهکار رمزنگاری، چه چیزی سر راه شما قرارگرفته است؟

پیچیدگی: بسیاری از راهکارهای رمزنگاری ایمیل را به‌سختی می‌توان پیاده‌سازی، و مدیریت کرد. شما نیاز به سرمایه‌گذاری وسیعی دارید تا زیرساخت لازم برای این تأثیر گسترده روی تمام شرکت را ارزیابی و پیاده‌سازی کنید. خیلی همه‌چیز ساده‌تر می‌شد اگر بتوان راهکار را از عرضه‌کننده‌ی کنونی خود دریافت کرد و آن را به‌راحتی سرجایش نصب کرد، یک راهکار که نیازمند پروژه‌ی بزرگ پیاده‌سازی و کارمندان متخصص برای مدیریت آن نباشد.

هزینه: بیشتر راهکارهای رمزنگاری بسیار گران‌قیمت هستند، همچنین هزینه‌های مربوط به مدیریت تو نگهداری آن هم باید در نظر گرفت. شاید بسیار عالی می‌شد اگر یک راهکار امنیت ایمیل وجود داشت که رمزنگاری و DLP را با بودجه‌ی کنونی شما برایتان به ارمغان می‌آورد.

تجربه‌ی کاربر: بیشتر راهکارهای رمزنگاری ایمیل جریان کاری کاربران نهایی را مختل می‌کنند. آن‌ها نیازمند کارهای خاصی از جانب کاربران هستند تا اطلاعات حساس را رمزنگاری کنند، و این امر دعوت به اشتباه است. یا اینکه کاربران نیاز دارند تا ایمیل‌ها را خارج از جریان کاری خود رمزنگاری کنند، که این امر بازدهی را کاهش داده و مقاومت در برابر فناوری جدید را افزایش می‌دهد. یک راهکار خوب به‌صورت نامرئی در پس‌زمینه فعالیت می‌کند و به‌صورت خودکار ایمیل‌ها را بر اساس خط‌مشی‌های DLP رمزنگاری می‌کند، بدون تأثیرگذاری روی کاربران یا نیاز به نرم‌افزار دیگری برای انجام این کار.

در یک دروازه‌ی ایمیل امن به دنبال چه چیزی بود؟

این‌ها ویژگی‌های یک راهکار دروازه ایمیل امن است که برای حفاظت از داده‌ها لازم است.

سادگی و سهولت مدیریت

به دنبال یک راهکار دروازه‌ی ایمیل باشید که ضد هرزنامه DLP و رمزنگاری ایمیل مبتنی بر خط‌مشی را با هم ترکیب کرده و از یک کنسول واحد مدیریت می‌شوند.

راهکار منتخب شما باید شامل انواع داده‌های حساس از پیش تعریف‌شده باشد تا بتوان به‌سادگی خط‌مشی‌های DLP توسعه داد.

اطمینان حاصل کنید که خط‌مشی‌های رمزنگاری ایمیل شما آن‌قدر ساده هستند که هرکدام از کارمندان بتوانند به‌سادگی خط‌مشی جدیدی ایجاد کرده یا خط‌مشی‌هایی کنونی را اصلاح کنند، بدون اینکه آموزش یا مستندسازی نیاز باشد.

راهکاری را انتخاب کنید که مدیریت آن زمان‌بر و پیچیده نباشد.

تجربه‌ی کاربری عالی

یک راهکار مؤثر رمزنگاری ایمیل باید به‌صورت خودکار ایمیل و پیوست‌های آن را اسکن کرده و قبل از اینکه ایمیل سازمان را ترک کند آن را رمزنگاری کند، به‌صورت خودکار و نامرئی، بدون اینکه کاربر مجبور باشد ایمیل را برای رمزنگاری علامت بزند (شاید فراموش کنند.)

راهکاری را انتخاب کنید که در کار کاربر اختلالی ایجاد نمی‌کند. باید کاربران را قادر سازد تا همانند قبل، از ایمیل کلاینت خود استفاده کنند، چه از طریق کامپیوتر رومیزی، لپ‌تاپ، دستگاه‌های موبایل یا از طریق آنلاین.

راهکار منتخب شما نباید نیازمند یک نرم‌افزار خاص یا یک پرتال وب برای گیرنده باشد تا بتواند ایمیل رمزنگاری‌شده را باز کند.

ارزان

راهکاری را انتخاب کنید که DLP و رمزنگاری ایمیل را در ظرف بودجه‌ی ضد هرزنامه‌ی شما فراهم کند.

راهکاری را انتخاب کنید که ارزیابی و پیاده‌سازی آن آسان باشد، بدون نیاز به سخت‌افزار، نرم‌افزار یا آموزش‌های خاص.