توضیحات یک مدیر برای سایر مدیران

آنچه هر مدیر باید درباره امنیت فناوری اطلاعات بداند

چگونه مدیران را در حفظ امنیت اطلاعات سازمانی با خود همراه کنیم

نویسنده: راب پگورارو

روزنامه‌نگار و ستون‌نویس در روزنامه واشنگتن پست

ترجمه، آماده سازی و گرافیک: ماهنامه دیده‌بان فناوری

پیش‌گفتـــار:

برای یک مؤسسه تجاری، چه چیزی می‌تواند مهم‌تر از داده‌ها باشد؟ صرف نظر از اینکه این داده‌ها اطلاعات مشتری باشند یا حقوق مالکیت معنوی، یا هر داده با ارزش دیگر به هرترتیب‌برای‌سازمان‌ها حیاتی هستند. اما متاسفانه اکثر مدیران عامل نمی‌دانند که باید این مسئله را در اولویت کاری خود قرار دهند.

در حقیقت، بر اسـاس نتـایج نظرسنجی‌هـای انجـام شده از کاربران (که توسط مؤسسه Ponemon انجـام شد)، تقریباً نیمی از تصمیم گیرنده‌هـای پاسخ‌دهنده در حـوزه فنـاوری معتقد بودند نمی‌توانند مشکلات امنیتی خود را برطرف کنند؛ زیرا این مسئله توجه مدیران عامل را به قدر کافی جلب نمی‌کند.

اکنون، به عنوان یک مدیر عامل درک می‌کنم که امنیت از نظر شما چطور ممکن است نسبت به مسائل تجاری دیگر اولویت ثانوی پیدا کند. می‌دانم که شما باید یک سازمان را با سودآوری مناسب و به طور موفقیت‌آمیز، بدون درگیر شدن با جزئیات فنی اداره کنید. اما به عنوان یک فرد باسابقه در حوزه امنیت، همچنین شاهد بوده‌ام که نادیده گرفتن خطرات امنیتی می‌تواند هزینه‌های سنگینی را برای یک شرکت به بار آورد.شما نمی‌توانید همه مشکلات مربوط به امنیت داده را برطرف کنید، اما می‌توانید آنها را اولویت‌بندی نمایید. همان‌طور که درباره همه مسائل دیگر هم همینطور است، محافظت از داده‌های حیاتی اقدامی است که باید با هزینه و بهره‌وری سازمانی متعادل شود.

در مورد احتمال بروز اشکال در داده‌ها به گفته‌های من اعتماد کنید؛ همیشه و در هر حال، نه فقط در صورت بروز اشکال داده‌های شما نسبت به حمله آسیب‌پذیر هستند، زیرا داده‌های همه سازمان‌ها نسبت به حمله آسیب‌پذیر هستند و من قصد دارم شما را دراین‌باره راهنمایی کنم. با توجه به ماهیت دوگانه تجربیات من، که از یک طرف مدیر عاملی با گرایش سودآوری هستم و از طرف دیگر یک متخصص امنیت، درموقعیت منحصر به فردی قرار دارم‌تا با همکاران مدیـر خـود درباره امنیت داده‌هـا صادقـانه سخـن بگویم.می‌خواهم اصطلاحات فنی پیچیده و سخنان نامفهوم بازاریابی را کنار بگذارم و با صراحت با شما صحبت کنم.

آنچه اکنون به شما ارائه می‌دهم، توضیح «مدیر به مدیر» درباره لزوم اهمیت دادن به امنیت فناوری اطلاعات و شیوه استفاده از نقش مدیریتی برای ایجاد فرهنگ امنیت در سازمان است.

فهـرست مطالـب

۱. امنیت فناوری اطلاعات موضوعی برای طرح در جلسه هیأت مدیره است

لحظه‌ای درباره داده‌هایی که کسب و کار شما را به پیش می‌برند فکر کنید: پیشرفت طرح‌های پژوهش و توسعه (R&D) که به زودی شما را در صحنه رقابت یاری می‌کند، طرح کلی برای جدیدترین محصول شما، داده‌هایی که از آن برای انعقاد قراردادها استفاده می‌کنید، برنامه‌های بازاریابی که فروش شما را به اوج می‌رسانند، فهرست جامع مشتریان که ارتباط شما با خریداران را حفظ می‌کند. همه این اطلاعات برای بهبود عملکرد سازمان شما ضروری هستند. کارکنان شما چگونه از این داده‌ها محافظت می‌کنند؟ آیا می‌دانید؟ نباید بدانید؟

بر خلاف آنچه برخی مدیر عامل‌ها ممکن است تصور کنند، امنیت اطلاعات به طور مطلق موضوعی برای طرح در جلسه هیأت مدیره است.

وقتی می‌شنوید که مسئول ارشد اطلاعات (CIO) یا مسئول ارشد امنیت اطلاعات (CISO) شما از اصطلاحات بیگانه‌ای چون دیواره‌های آتش برنامه وب، امضاهای ضد ویروس یا ایجاد فهرست سفید استفاده می‌کند، به آسانی می‌توانید اکثر این اصطلاحات را به عنوان جزئیات فنی که ارزش تلف کردن وقت مدیریتی شما را ندارند، نادیده بگیرید.

اگر امنیت فناوری اطلاعات را نادیده بگیرید، با مسیر دشواری روبرو خواهید شد. مانند خیلی از افرادی که می‌شناسید، اگر به این موضوع در جلسه هیأت مدیره نپردازید، با یک بروز یک اشکال در امور مالی یا حتی بدتر در روزنامه‌ها مواجه خواهید شد.اگر یک شرکت سیاست‌های امنیتی خود را تعیین نکند یا آنها را آنچنان کلی تعیین کند که با یک حمله فوق‌العاده عمومی مواجه شود، ممکن است بزرگترین مشتریان، شرکا یا حتی دولت از کار کردن با آن اجتناب کنند. فقط کافیست در این باره از سیتی گروپ یا بانک ملی آمریکا بپرسید. یا حتی بهتر، از شرکت سونی سؤال کنید. بر اساس برآوردها، اشتباهات اخیر این شرکت به بهای میلیون‌ها دلار زیان و از بین رفتن حسن نیت تعداد بی‌شماری از مشتریان تمام شد. این‌ها مسایل فناورانه نیستند؛ بلکه موضوعات اصلی تجاری هستند.

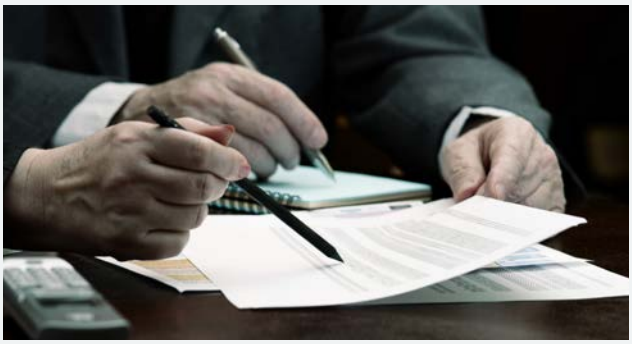
امنیت داده‌ها دیگر صرفاً دغدغه‌ای برای بانکداری، مراقبت از سلامت و سازمان‌های دولتی نیست. بنابراین، چگونه آن را به یک موضوع برای طرح در جلسه هیأت مدیره محدود کنید؟ موظف هستید از متخصصان فناوری خود بپرسید که سازمان چگونه امنیت داده‌های خود را حفظ می‌کند، چه نوع ارزیابی‌هایی برای پیگیری اقدامات حفاظتی و حمله‌ها وجود دارد، و سیاست‌ها چگونه به اجرا گذاشته می‌شوند. شما به طور معتمدانه مسئول هستید که بدانید چه داده‌هایی را در اختیار دارید، بزرگترین خطر در چه جاهایی وجود دارد و چه اقداماتی را برای محافظت از داده‌ها انجام می‌دهید.

اگر یک اردوگاه برای تعلیم مدیر عامل‌ها داشتم، قطعاً به آنان می‌گفتم: «مطمئن شوید که همه گزارش‌دهنده‌های مستقیم شما امنیت را در درجه اول اولویت قرار می‌دهند: مسئول ارشد امور مالی، مسئول ارشد اطلاعات، کارکنان منابع انسانی، مسئولان فروش و غیره.» امروزه برای اکثر شرکت‌ها، محصول، اطلاعات است و امنیت یک عامل کلیدی است. بنابراین باید مطمئن شوید که گزارش‌دهنده‌های ارشد شما درک می‌کنند که امنیت بخشی از ارزیابی فعالیت آنها محسوب می‌شود. این امر صرفاً وظیفه مسئول ارشد اطلاعات نیست؛ بلکه بخشی از زندگی تک تک گزارش‌دهنده‌های مستقیم شما را تشکیل می‌دهد.

جان پِسکاتور – گارتنِر

۲. نادیده گرفتن امنیت فناوری اطلاعات برای شما هزینه خواهد داشت

بروزاشکال در داده‌ها هر ساله میلیون‌ها دلار زیان در قالب بازرسی های قانونی، جریمه‌های کنترلی و هزینه‌های جبرانی برای شرکت‌ها به بار می‌آورد، اما سنجش بزرگترین هزینه ناشی از نادیده گرفتن امنیت ممکن است بسیار دشوارتر باشد. برند (Brand) بستری است که اکثر شرکت‌های بزرگ بر آن مستقر هستند. از دست دادن اعتبار برند که از اقدامات امنیتی سهل‌انگارانه ناشی می‌شود، شاید بزرگترین خطر ممکن باشد.



مدیران اجرایی که امنیت را نادیده می‌گیرند نه تنها برند و شهرت خوب شرکت خود را به خطر می‌اندازند، بلکه فرصت متمایز ساختن خود از بقیه گروه را از دست می‌دهند.

البته خسارت‌های فراوان ناشی از نقض داده‌ها را می‌توان تعیین کرد. آمار صنعتی نشان می‌دهد که نقض داده‌ها در سال ۲۰۱۰ به طور میانگین حدود ۲/۷ میلیون دلار به ازای هر رویداد یا ۲۱۴ دلار به ازای هر داده‌ای که در معرض خطر قرار می‌گیرد برای سازمان‌ها هزینه دارد. در این آمار، تخمین‌های مربوط به موارد زیر نیز شامل شده است:

- از دست دادن مشتریان
- بازرسی های قانونی
- هزینه‌های ناشی از اصلاح مواردی که با قوانین مطابقت ندارند و جریمه‌های مربوطه
- مطلع ساختن قربانیان نقض و مقامات دولتی

رسوایی کامل زمانی روی می‌دهد که این پول خرج شده و مشکلات نیز روی داده است. بازرسی جدیدی که بعد از بروز نقض صورت می گیرد، شرکت شما را وادار می‌کند برای اجرای برنامه امنیتی که از ابتدا باید اجرا می‌کردید هزینه کنید. پس چرا این پول را از ابتدا خرج نکنید و از همه هزینه‌های ناشی از آن اجتناب نکنید؟ در حالی که راه حل معجزه‌آمیزی وجود ندارد، می‌توانید با درک خطرات مهم، حفره‌های امنیتی را کاهش دهید.

نمونه‌هایی از شدیدترین حمله‌ها

نقض بزرگ امنیتی شرکت سونی.

نقض داده‌های شرکت سونی باید درس آموزنده‌ای برای همه باشد تا بدانیم در صورت از دست رفتن داده‌ها چه خساراتی ممکن است به بار آید. طبق گزارش، بیش از ۱۰۰ میلیون حساب کاربران سونی در معرض خطر قرار گرفت که بیش از ۱۷۰ میلیون دلار برای این شرکت هزینه داشت. متاسفانه سونی از ابتدا با به کارگیری اقدامات امنیتی یا ارتباطاتی به این بحران واکنش مناسب نشان نداد.

قدم اشتباه شماره ۱.

هیأت مدیره شرکت سونی مسئله مدیریت ریسک را نادیده گرفت. این امکان وجود داشت که اثرات بسیاری از مشکلات به آسانی کاهش یابند و از بروز این نقض بزرگ در وهله اول جلوگیری شود. در حالی که هر شرکتی ممکن است یک مشکل امنیتی داشته باشد، شرکتی که اقدامات اساسی مدیریت ریسک را دنبال نکرده باشد، آسان‌تر در دام خواهد افتاد و بیشتر ضربه خواهد خورد.

قدم اشتباه شماره ۲.

شرکت سونی اقدامات مؤثر مدیریت بحران را دنبال نکرد تا اوضاع بدتر شد. شاید آنچه مشتریان سونی را بیش از همه چیز عصبانی کرد این بود که شرکت بعد از اینکه متوجه بروز نقض شد تا زمانی که به مشتریان اطلاع دهد، یک هفته یا بیشتر تأخیر داشت.

از آنجا که مشکلات داده‌ای می‌تواند برای همه اتفاق بیفتد، باید از خود بپرسید چه اقداماتی را انجام می‌دهید تا مطمئن شوید شرکت شما مرتکب اشتباهات مشابهی نخواهد شد؟

درباره نقض امنیتی شرکت سونی و آنچه باید انجام می‌شد در وبلاگ ما تحت عنوان Optimal Security (امنیت بهینه) بیشتر بخوانید.

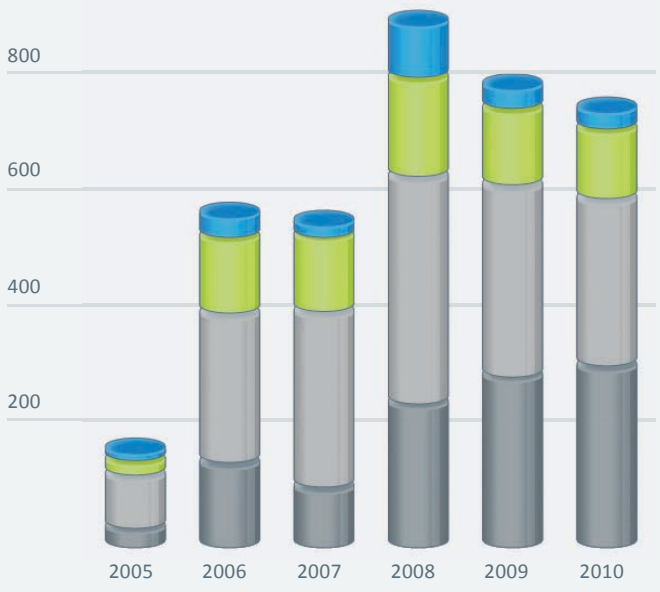
۳. هکرها به شکل‌های مختلف و با انگیزه‌های مختلف ظاهر می‌شوند

خیلی از مدیران عامل معتقدند که «هکرهای مخفی» که تیم‌های فناوری اطلاعات در مورد آنها هشدار می‌دهند صرفاً موجودات خیالی ترسناکی هستند که این تیم‌ها برای متقاعد کردن مدیریت به تخصیص بودجه، از آنها استفاده می‌کنند. حقیقت این است که این مهاجمان کاملاً واقعی هستند و سازمان‌هایی را انتخاب می‌کنند که مدیران آن ها برای امنیت اولویت قائل نمی‌شوند.

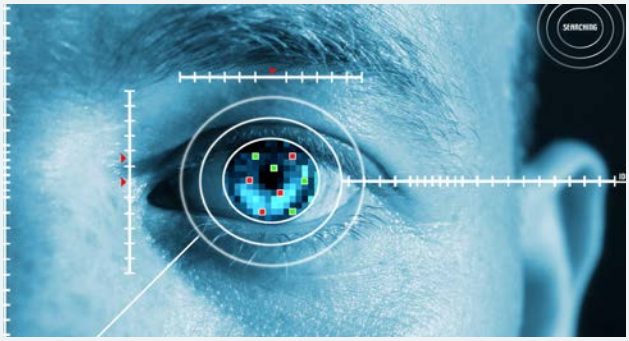
در سال ۲۰۱۱، انجمن 3765Digital Forensics رویداد نقض عمومی داده را در ۳۳ کشور بین سال‌های ۲۰۰۵ تا ۲۰۱۰ بررسی کرد که شامل بیش از ۸۰۶ میلیون لورفته می‌شد.

همان طور که می‌بینید، هکرهای خارجی پس از هکرهای داخلی بیشترین تعداد حمله‌ها را به خود اختصاص می‌دهند. عاملان از دست رفتن این حجم زیاد داده چه کسانی هستند؟ تبهکاران زرنگ بسیاری وجود دارند که به دنبال سود بردن از فروش داده‌های مشتری و اطلاعات مربوط به دارایی‌های شما هستند.

افـزایش حملات(۲۰۱۰-۲۰۰۵)



مهاجمان برای کسب درآمد قادرند تقریباً هر نوع داده را به پول نقد تبدیل کنند. آنها این کار را از طریق بازار سیاه انجام می‌دهند که به



افراد تبهکار به خاطر غارت دیجیتال پاداش می‌دهد. شبکه‌های جنایی پیچیده اکنون بیش از ۶/۵ میلیارد دلار را بابت اطلاعات شخصی و شرکتی که از طریق نقض‌های امنیتی شناخته شده به سرقت رفته‌اند، به این بازار تزریق می‌کنند. سرقت داده همیشه یک اقدام مستقیم برای سرقت پول نقد نیست. هکرهای دیگر به انتفاع از مبادلات مالی سازمان شما کمتر متمایلند و بیشتر به سرقت ذخایر مالکیت معنوی شما علاقه دارند. جاسوسی شرکتی در عصر دیجیتال، زنده و پابرجاست؛ به طوری که هکرها روی طرح‌های جدید محصول، برنامه‌های زمانی تولید و حتی قیمت‌های فروش پیش‌بینی شده تمرکز می‌کنند؛ زیرا این اطلاعات البته برای بسیاری از رقبای شما بسیار ارزشمند است. هکرها آن را به سرعت می‌ربایند و به شخصی که حاضر است بیشترین مبلغ پیشنهادی را پرداخت کند عرضه می‌کنند.

اخیراً شاهد ظهور نوع جدیدی از هکرها تحت عنوان هکتیویست‌ها نیز بوده‌ایم. این هکرها به جای تلاش برای کسب سود، به دنبال انجام اقدام ویژه‌ای هستند و از شرکت شما برای این کار استفاده می‌کنند. گروه های هکر مانند Lulzsec و Anonymous به شرکت‌های بسیاری، در اعتراض به اقدامات آنها، حمله کرده‌اند.

این امر در مورد شرکت سونی نیز اتفاق افتاد؛ آن هم بعد از اینکه این شرکت یک نفر را که سعی داشت سخت‌افزار سونی را دستکاری کند تحت پیگرد قانونی قرار داد.

هکتیویست‌ها تمام ادارات دولتی را نیز مورد حمله قرار داده‌اند؛ مانند اداره ایمنی عمومی آریزونا در اعتراض به سیاست‌های مهاجرتی دولت و وبگاه شهر اورلاندو در اعتراض به دستگیری شهروندانی که بدون مجوز به افراد بی‌خانمان در یکی از پارک‌های شهر غذا داده بودند.

هکرها تنها افرادی نیستند که باید در مورد آنها نگران بود: تهدیدهای کارکنان داخلی

تنها افراد پولدار و شرور خارج از شرکت نیستند که باید در مورد آنها نگران باشید. تهدیدهای فراوانی نیز خیلی نزدیکتر به شما یعنی در داخل شرکت وجود دارد.

خطراتی که کارکنان و شرکای امین مطرح می‌کنند، ممکن است از کلاهبرداری کامل گرفته تا خطای ساده کاربر را در بر گیرند. به طور معمول، هر دوی آنها از عدم کنترل و نظارت ضعیف بر فعالیت‌های رایانه‌ای کارکنان ناشی می‌شوند و از طریق ابزارهای همراهی که در بین نیروی کار شما نفوذ کرده‌اند تشدید می‌شوند.

تعداد زیادی از شرکت‌ها روی ارتباط کارمندان با مالکیت معنوی و داده‌های حساس نظارتی ندارند و در نتیجه هزینه گزافی را به این خاطر می‌پردازند.

آیا سازمان شما روشی را برای ردیابی شیوه‌های کپی و انتقال اطلاعات در اختیار دارد؟ آیا راهکاری را برای محافظت از داده‌های غیر فعال، فعال و در حال استفاده پیدا کرده است؟ به عنوان یک مدیر عامل باید دست کم پاسخ این پرسش‌ها را بدانید.

۴. حملات همچنان انجام می گیرد

امروزه موضوع وحشتناک در مورد خطرات سایبری، شرکت‌هایی هستند که امنیت را کاملاً نادیده می‌گیرند. آنها ممکن است هم اکنون هم در معرض حمله قرار گرفته باشند، اما حتی از آن آگاه نباشند. انگیزه هکرهای جدید این نیست که توجه شما را جلب کنند و به زیرساخت شما حمله کنند، بلکه بیشتر علاقمندند که به آرامی در سیستم شما نفوذ کنند و داده‌ها را تا بیشترین حد ممکن و بدون اطلاع شما سرقت کنند.

آنها با اجرای مداوم اسکن‌های خودکار اینترنت شروع می‌کنند و به دنبال آسیب‌پذیری‌های رایج برای سوء استفاده مخفیانه هستند؛ تفاوتی نمی‌کند شرکتی که این مشکلات را دارد چقدر بزرگ یا کوچک باشد.

سپس با بدافزار مخربی که برای ایجاد اختلال، انکار، سرقت و غیره ایجاد شده است، به سراغ شما می‌آیند. تعداد بدافزارها به سرعت بالا رفته است و پیچیدگی آنها برای برآورده ساختن خواسته‌های مالی این تبهکاران افزایش یافته است؛ به طوری که آنها قلمروی غیرقانونی خود را به سرعت ایجاد کرده‌اند.

امروزه بدافزارهای مختلف بسیاری وجود دارد. برخی از آنها برای انداختن دام‌های بزرگ طراحی شده‌اند و اینترنت را برای یافتن آسیب پذیری‌ها جستجو می‌کنند. برخی دیگر بسیار هدفمند هستند. قطع نظر از نوع بدافزار، تبهکاران می‌توانند بدون اینکه شناسایی شوند در داخل و خارج از شبکه شما وجود داشته باشند.

آنها صرفاً سیستم عامل مایکروسافتی شما را مورد حمله قرار نمی‌دهند. در یک مقیاس بزرگتر، آنان تقریباً به دنبال هر گونه برنامه مبتنی بر وب هستند که برای کارتان از آن استفاده می‌کنید. بر اساس یک گزارش جدید، تعداد آسیب‌پذیری‌ها در سال ۲۰۱۰ در میان ۵۰ برنامه برتر که روی رایانه معمولی کاربر نهایی نصب می‌شوند، ۷۱ درصد افزایش یافت. این وضعیت در این روزگار و در عصر برنامه‌های مجازی سازی، ابری و همراه، حتی بدتر هم می‌شود.

احتمالاً استفاده از فناوری‌های مجازی‌سازی، ابری و همراه، شیوه‌ای که بخش فناوری اطلاعات شما به واحدهای تجاری خدمات ارائه می‌دهد را دگرگون ساخته است. همه این فناوری‌ها مطمئناً فرصت‌های فراوانی را برای کاهش هزینه‌های عمده و هزینه‌های عملیاتی به شرکت ها ارائه می‌دهند.

در حالی که مجازی‌سازی امکان به‌کارگیری مقرون به صرفه نیروی محاسباتی بیشتر را در ازای هزینه کمتر فراهم می‌کند، با فراهم شدن

فرصت‌های بزرگ، خطرات بزرگ نیز توأم می‌شود. فناوری‌های مجازی‌سازی و ابری مشکلات عملیاتی و امنیتی بسیاری را مطرح می کنند که خیلی از مدیران عامل شرکت‌ها و حتی مسئولان ارشد اطلاعات قبل از اینکه با عجله به آن ها بپردازند، آن ها را به نحو لازم مد نظر قرار نمی‌دهند.

رایانه‌های رومیزی مجازی

برای مثال، کاربردهای مجازی‌سازی رایانه رومیزی خانگی خود را در نظر بگیرید. برای اولین بار در تاریخ پردازش، می‌توانیم یک رایانه رومیزی مجازی را در اختیار افراد قرار دهیم و امکان کار کردن بدون نگهداری از سخت‌افزار رایانه‌ای را برای آنها فراهم کنیم. مسئله این است که این رایانه‌های رومیزی مجازی در معرض هر گونه آلودگی هستند که ممکن است روی سیستم عامل میزبان نشسته باشد و بالعکس. بدون بهره‌گیری از فناوری تخصصی برای محافظت از این دستگاه های مجازی و جلوگیری از انتقال ویروس‌های خطرناک بین میزبان‌های مجازی، ممکن است ویروس‌هایی را داشته باشید که رایانه های دیگر را آلوده کنند. اوضاع خیلی زود آشفته می‌شود. مسئله این است که جذابیت صرفه‌جویی در هزینه اکثر سازمان‌ها را به استفاده از مجازی‌سازی جذب کرده است؛ آن هم قبل از اینکه فناوری امنیت فرصتی داشته باشد تا همگام با بقیه نوآوری ها پیش رود.

نمی‌توانید به دلیل این مشکلات، مجازی‌سازی را کنار بگذارید. مدیر عامل‌ها و مدیران اجرایی دیگر باید خطرات امنیتی را در معادلات صرفه‌جویی در هزینه خود محاسبه نمایند.

خطرات پردازش ابری

مسائل پیرامون محاسبه ابری حتی پیچیده‌تر هم هستند. زیرا این محیط‌ها نه تنها در برابر همه خطراتی که از طریق مجازی‌سازی مطرح می‌شوند آسیب‌پذیر هستند، بلکه داده‌های وابسته به ابر نیز خارج از حوزه نفوذ شما هستند.

امروزه ارائه‌دهندگان فضای پردازش ابری، حفاظت‌ها یا تضمین‌های کمتری را در مورد داده‌های شما عرضه می‌کنند؛ زیرا برای انجام این کار تحت فشار نبوده‌اند. خیلی از مدیران عامل و مسئولان ارشد اطلاعات آنچنان تحت تأثیر صرفه‌جویی‌های ناشی از فناوری ابر قرار گرفته‌اند که خطرات را نادیده گرفته‌اند و با دانش ناچیزی درباره اینکه ارائه‌دهندگان این فناوری چگونه از داده‌های بسیار مهم محافظت می‌کنند وارد این سیستم‌ها شده‌اند.

هر زمانی که داده‌های شما از محدوده شرکت خارج شوند، شما و کارکنان‌تان باید از خود بپرسید که آیا با شریک تجاری‌تان در یک زنجیره اعتماد هستید. چرا که او اساساً ضعیف‌ترین حلقه در زنجیره اعتماد است. اگر این طور نیست، می‌توانید مطمئن باشید که خطر برای به دام انداختن شما باز خواهد گشت درست همان طور که برای ده‌ها علامت تجاری بزرگ که در Epsilon، ارائه‌دهنده خدمات پست الکترونیکی، تحت تأثیر نشت داده قرار گرفتند، اتفاق افتاد.

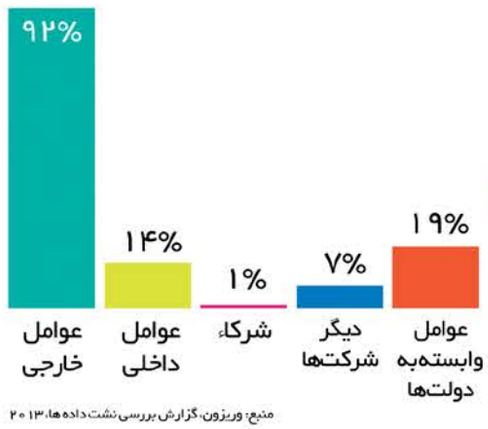
در بهار سال ۲۰۱۱، این شرکت حلقه ضعیفی در زنجیره امنیتی شرکت‌های بزرگی مانند JPMorgan Chase، Disney، Hilton و غیره محسوب می‌شد. هکرها از روی حماقت پول به دست نمی‌آورند. در مورد Epsilon، آنها می‌دانستند که بهترین روش به دام انداختن هفت شرکت از فهرست فورچون ۱۰، حمله به ساختارهای داده مستحکم این شرکت‌ها نیست. تنها کاری که آنها باید انجام می‌دادند، به دام انداختن یک شرکت بازاریابی بود که به طور ضعیفی از آن محافظت شده بود.

دیدهبان
ماهنامه اقتصاد و مدیریت فناوری اطلاعات

خودی‌های نفوذی

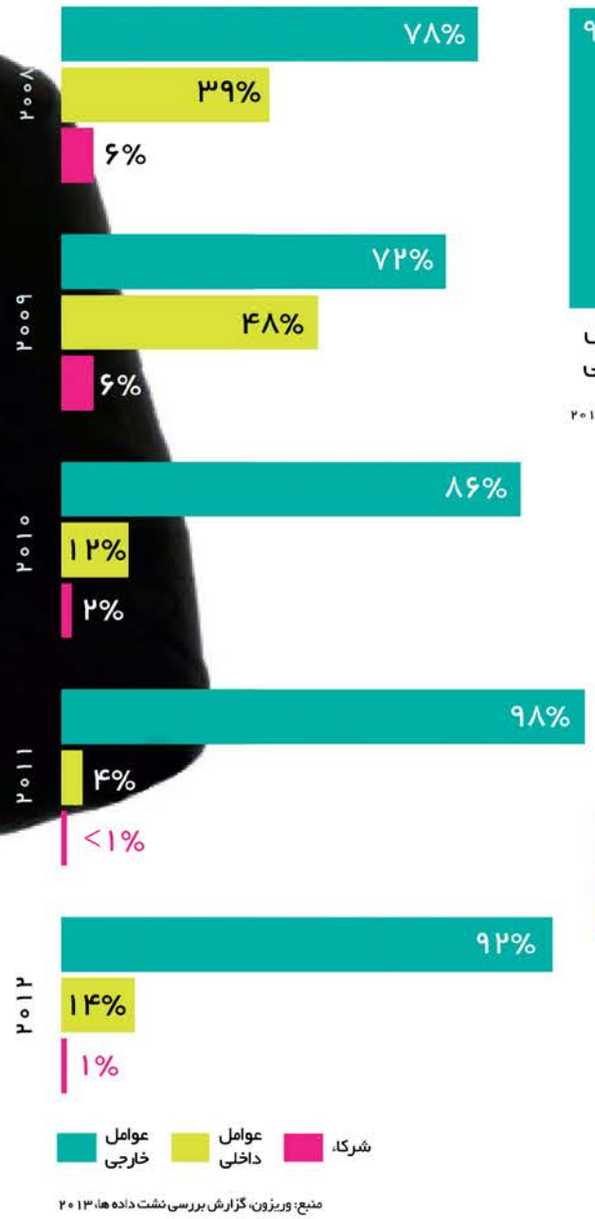
برای دریافت نسخه با کیفیت اینفوگرافی اینجا کلیک کنید.

چه کسی مرتکب نفوذها می‌شود؟



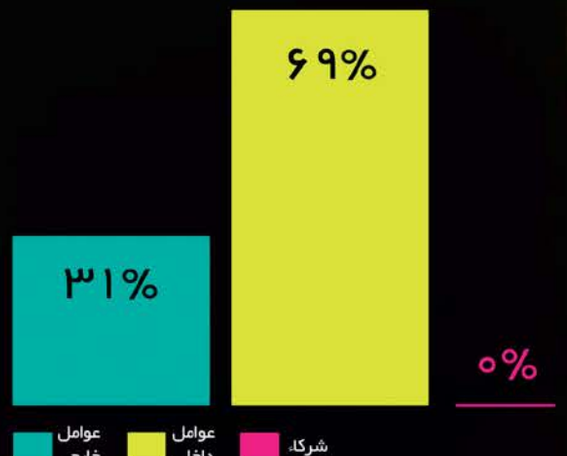
منبع: وریزون، گزارش بررسی نشت داده‌ها، ۲۰۱۳

نقش عوامل تهدیدکننده در طول زمان

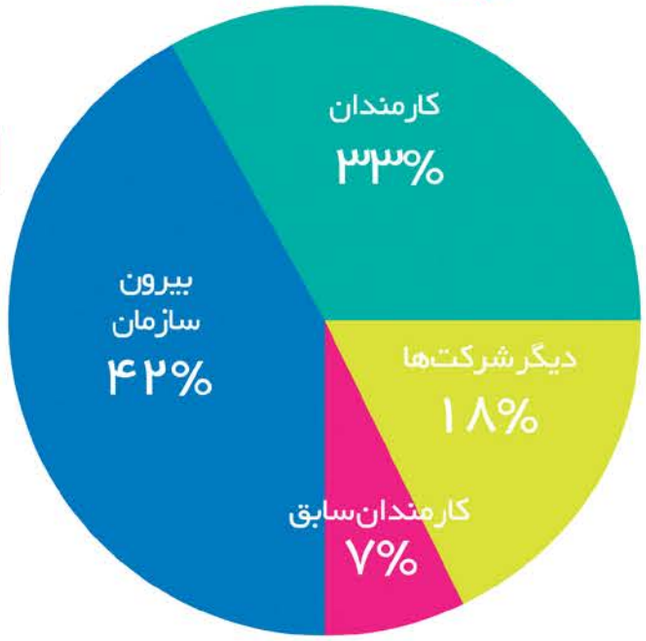


منبع: وریزون، گزارش بررسی نشت داده‌ها، ۲۰۱۳

تقسیم‌بندی عوامل تهدیدکننده در بیش از ۴۷۰۰۰ رویداد امنیتی



تهدیدات از کجا می‌آیند؟



۵۸% از نفوذها ناشی از بزرگ شدن سازمان ها هستند(کارمندان، کارمندان سابق، شرکای مورد اعتماد)

۸۲% از پاسخ‌دهندگان ورود ویروس از دستگاه‌های شخصی کارمندان به شبکه سازمان را یکی از منابع داخلی و اصلی تهدیدات می‌دانند.

۸۲% از پاسخ‌دهندگان عدم آگاهی و درک از مسائل و تهدیدات IT را یکی از منابع داخلی و اصلی تهدیدات می‌دانند.

۸۷% از پاسخ‌دهندگان خطای غیرعمدی انسانی را یکی از منابع داخلی و اصلی تهدیدات می‌دانند.

۲۶% از پاسخ‌دهندگان کاملاً اطمینان دارند که می‌توانند دقیقاً منبع تهدید را شناسایی کنند.

۳۴% از پاسخ‌دهندگان کاملاً اطمینان دارند که می‌توانند دقیقاً نوع رویداد امنیتی را تعیین کنند.

۳۷% از پاسخ‌دهندگان کاملاً اطمینان دارند که می‌توانند دقیقاً تعداد رویدادهای امنیتی IT سال گذشته را برآورد کنند.

۵.تطابق لزاما با امنیت یکسان نیست

متاسفانه، تصور اکثر مدیران اجرایی از امنیت، از مطابقت با مقررات امنیتی مانند Sarbanes-Oxley، HIPAA، استانداردهای امنیت داده PCI DSS و قانـون حریم خصوصی داده‌های ماسـاچوست (برای هر کسی که مایل به انجـام تجارت درماسـاچوست است) فراتر نمـی‌رود. هرچقدر روی این موضوع تأکید کنم، کم گفته‌ام: ایجاد تطابق با ایجاد امنیت یکسان نیست. داستان تکان‌دهنده پردازنده کارت اعتباری سیستم‌های پرداخت Heartland را با حساسیت در نظر بگیرید. در سال ۲۰۰۹، Heartland از یک نقض که هنوز هم بزرگترین نقض ثبت شده است، زیان دید. مهاجمان بیش از ۱۳۰ میلیون شماره کارت اعتباری را به سرقت بردند که خسارتی بیش از ۱۲ میلیون دلار به شرکت وارد کرد. در زمان بروز نقض، تصور می‌شد که شرکت مقررات PCI DSS را رعایت کرده است.

البته نمی‌توانید مطابقت با استانداردها را نادیده بگیرید. سازمان‌هایی که برنامه‌های مطابقت یکپارچه‌ای را طرح‌ریزی نمی‌کنند، در معرض خطر جریمه و بازرسی‌های کامل قرار می‌گیرند. بر اساس یک نظرسنجی جدید، بسیاری از شرکت‌ها حتی نمی‌توانند حداقل استانداردهای امنیتی تعیین شده توسط ناظران را رعایت کنند.

بیش از نیمی از سازمان‌ها می‌گویند که اخیراً در بازرسی‌های مطابقت کنترلی موفق نبوده‌اند و ۹ درصد دیگر هم اکنون در بازرسی مردود شده‌اند که به صدور جریمه منجر شده است.

واضح است که همکاران شما می‌ایستند و گوش می‌دهند، زیرا از سوی ناظـران تحت فشـار قرار گرفته‌انـد. حـدود نیمی از سازمان‌هـا می‌گویند قصد دارند در سال ۲۰۱۱ برای رعایت الزامات مطابقت پول اضافی خرج کنند؛ به طوری که پیش‌بینی می‌شود هزینه آنها ۲۱ درصد افزایش یابد.

از جهاتی این کار می‌تواند مفید باشد.

امـا مطابقت بـه عنـوان محـرک امنیت یک شمشیر دولبه است. مطابقت قطعاً در آشکـار شدن مشکلات امنیتی در بین مدیران ارشد اجرایی مؤثر بوده است.

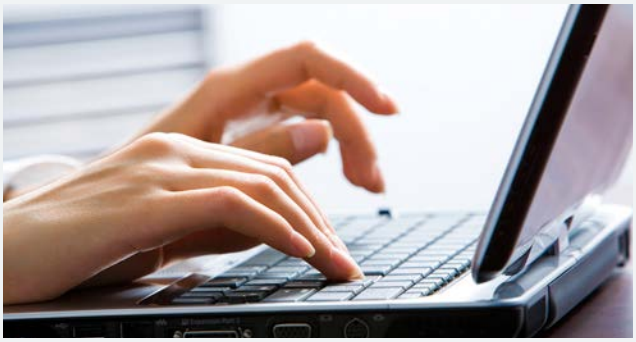
اما همزمان موجب شده است که بسیاری از مدیران اجرایی قوانین مطابقت را با امنیت جامع واقعی یکسان بپندارند. در عوض، موضوعات مطابقت و امنیت را در ذهن خود و برای کارکنان خود از هم متمـایز کنید. مطمئـن شـوید که از دسـتورالعمل‌هـای مطابقت

پیروی می‌کنید - این یک موضوع است. همچنین به طور جداگانه، از وجود امنیت مناسب اطمینان حاصل کنید.

۶. متعادل کردن نیاز به امنیت با نیاز به بهره‌وری

دوران کارمندان پشت میزی گذشته است. افزایش دستگاه‌ها و برنامه‌های همراه در شرکت‌ها در طول چند سال گذشته بی‌سابقه است و برای همیشه شیوه کار ما را تغییر داده است.

اما تحرک و انتقال، امنیت را چنان غیر قابل پیش‌بینی کرده است که شرکت‌ها صرفاً تلاش می‌کنند خود را حفظ کنند. فقط کافیست همه کارکنان خود به همراه آی‌پدها، آندروییدها، بلک‌بری‌ها و دستگاه‌های USB در نظر بگیرید.

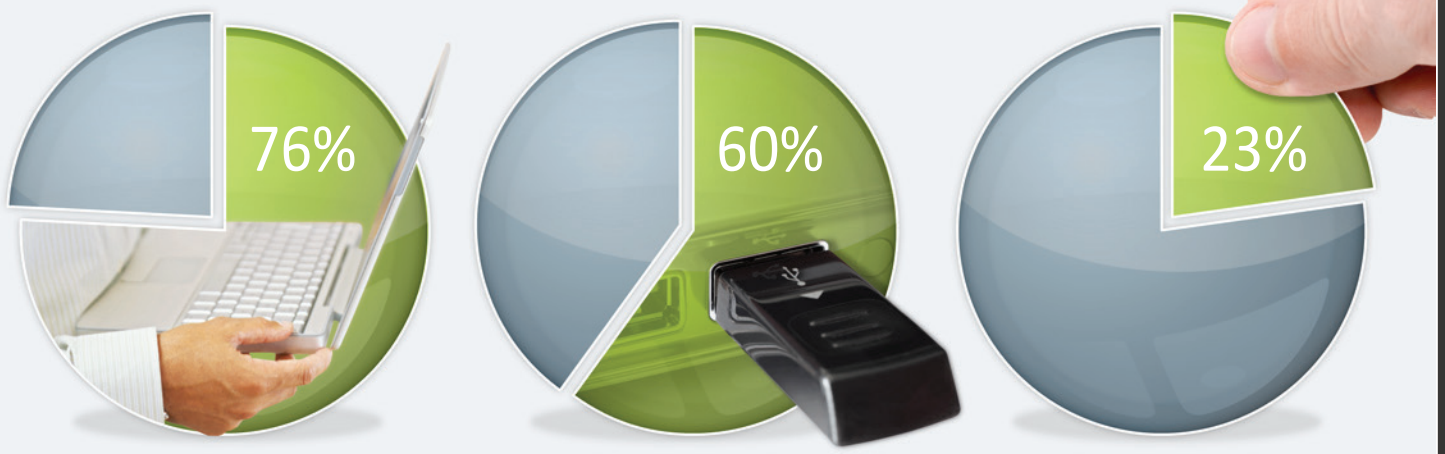


خیلی از این دستگاه‌ها حتی متعلق به شرکت شما نیستند، و با این وجود کارکنان شما هزاران داده ارزشمند شرکت را با استفاده از آنها دانلود می‌کنند. این موضوع به تنهایی گویاست که داده‌های ارزشمند شما ایمنی شبکه شرکت را به صورت کاملاً محافظت‌نشده رها می‌کنند. این داده‌ها در معرض خطر هستند، مدیریت نشده‌اند و بدون نظارت در دستگاه‌های کارکنان فعلی و سابق شما وجود دارند.

در حالی که کارکنان بخش فناوری خود را راهنمایی می‌کنید، مواقع خاصی را در نظر بگیرید که انعطاف‌پذیری کارکنان از دغدغه‌های امنیتی پیشی می‌گیرند و بالعکس. این امر مستلزم طبقه‌بندی یکپارچه داده‌ها و دستگاه‌ها و تعیین سیاست‌های دسترسی مبتنی بر نقش و ابزارهای صحیح برای اجرای این سیاست‌هاست.

به طور ایده‌آل، سازمان شما باید نسبت به اینکه چه کسانی و با چه دستگاه‌های همراهی به شبکه وصل می‌شوند، چگونه و چه وقت به داده‌ها دسترسی می‌یابند و چقدر از این داده‌ها بر اساس سیاست های محافظت از داده‌های شرکت به بیرون منتقل می‌شوند، قابلیت دید بهتری پیدا کند. به عنوان یک مدیر عامل ممکن است لازم نباشد با ویژگی‌های شیوه کسب این قابلیت آشنایی داشته باشید، اما این قابلیت باید در دسترس شما باشد. بدون آن هرگز نخواهید توانست درباره سیاست‌هایی که شما و مدیران اجرایی شما در مورد استفاده مناسب از دستگاه‌های همراه در سازمان اتخاذ می‌کنند، به طور هوشمندانه تصمیم‌گیری کنید.

User Habits and Influence



۲۳ درصد از سازمان‌ها با یک رویداد یا نقض امنیتی جدی به دلیل اتصال یک دستگاه شخصی روی شبکه مواجه شده‌اند.

اکثر مدیران فناوری اطلاعات می‌گویند شرکت‌های آنها سیاست‌هایی را برای اتصال دستگاه‌های شخصی روی شبکه دارند، اما تقریباً ۶۰ درصد از آنها گزارش کرده‌اند که اتصال‌های غیر مجاز هنوز هم روی می‌دهد.

۷۶ درصد از مدیران امنیت و فناوری اطلاعات معتقدند که نفوذ کاربران روی تصمیم‌گیری‌های مربوط به خرید دستگاه‌ها و برنامه‌ها در حال افزایش است.

۷.امنیت صرفاً یک مسئله در حوزه فناوری نیست

همه مدیران عامل خیلی زود به این نتیجه می‌رسند که برای موفقیت در کارها، باید به کارکنان خود اجازه دهند امور تخصصی را انجام دهند. نمی‌توانید در انجام همه کارهایی که در شرکت انجام می‌دهید مهارت داشته باشید. به همین دلیل، گروهی از کارکنان متخصص را به خدمت گرفته‌اید. اما باید پیشرفت آنها را با دقت زیر نظر داشته باشید و تصمیم‌های آنها را هدایت کنید تا مطمئن شوید که نسبت به دیدگاه شما درباره اولویت‌های تجاری متعهد هستند. این امر به همان اندازه که در مورد تصمیم‌گیری‌های مالی صادق است در مورد تصمیم‌گیری‌های امنیت فناوری اطلاعات نیز صدق می‌کند.

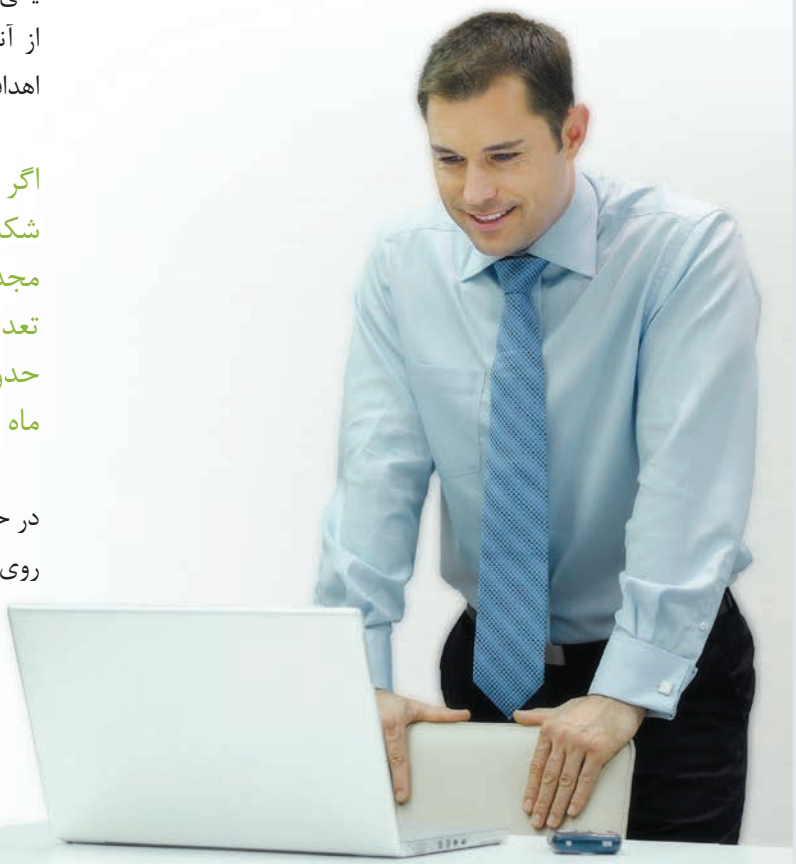
اگر قرار است سازمان شما بر خطرات نظارت داشته باشد و یک فرهنگ امنیتی ایجاد نماید، شما و تیم ارشد مدیریت شما باید از کارکنان فناوری بخواهید که یک تصویر واقعی از وضعیت امنیت در شرکت را به شما ارائه دهند. اولویت‌های مهم خود را بازنگری کنید.

سپس با حسن نیت از آنها بخواهید واقعیت را درباره کیفیت خوب یا بد محافظت از داده‌های مهم از جمله گزارش‌های منظم درباره محل استقرار داده‌ها، انواع خطراتی که داده‌ها با آنها مواجه می شوند، شیوه فعلی محافظت از داده‌ها و ارزیابی این محافظت به شما ارائه دهند.

یکی از خطرات واقعی کار با مدیران اجرایی فنی این است که برخی از آنها ممکن است آنچنان مجذوب برخی از فناوری‌ها شوند که اهداف اصلی خود را فراموش کنند.

اگر تصور می‌کنید نصب نرم‌افزار ضدویروس یک طلسم شکست‌ناپذیر در برابر تهدیدهای امنیتی امروز است، مجددا در این مورد فکر کنید. از سال ۲۰۰۷ تاکنون، تعداد تهدیدهای امنیتی جدید که شناسایی شده اند، از حدود ۲۵۰هزار مورد در ماه به بیش از ۲ میلیون مورد در ماه افزایش یافته است.

در حوزه امنیت، خیلی‌ها دچار این تصور نادرست هستند و متاسفانه روی خرید و استفـاده از ابزارهـایی که آنها را علاج همه دردهـا می دانند تمرکز می‌کنند.



به عنوان یک مدیر عامل احتمالاً می‌دانید که هیچ محصولی در دنیا وجود ندارد که بتواند یک مسئله پیچیده تجاری را به طور کامل حل و فصل کند. این امر در مورد امنیت اطلاعات نسبت به موضوعات دیگر تجاری شدیدتر است. ابزارهای فناوری همان طور که در مورد خیلی دیگر از جنبه‌های تجارت صادق است، از اساس محکمی که از طریق تعیین سیاست‌ها و فرایندهای مؤثر نهاده شده است، پشتیبانی می‌کنند. وظیفه شما به عنوان مدیر عامل این است که مسئول ارشد اطلاعات و مسئول ارشد امنیت اطلاعات خود را راهنمایی کنید تا مطمئن شوید که آن ها از فناوری به عنوان یک تکیه‌گاه غیرمؤثر استفاده نمی‌کنند.

«موضوعات دیگر» باید شامل این موارد باشند: ارزیابی ریسک، رویه‌های استاندارد شده، تعیین مرز برای آنچه کارکنان باید و نباید با سیستم‌ها و داده‌ها انجام دهند و همچنین تعیین خطوط مبنا در مورد شیوه پیکربندی سیستم‌ها. از این طریق، فناوری می تواند همه این سیاست‌ها و رویه‌ها را کنترل و اجرا کند و برای اثبات اینکه همه چیز به درستی کار می‌کند به بازرسان گزارش ارائه دهد.

به منظور انجام بهبودها، با متخصصان فناوری درباره کارهایی که آن ها در صورت داشتن «عصای جادوگری» انجام می‌دادند و شیوه رفع مشکلات در صورتی که بودجه مسئله نباشد، به طور منظم گفتگو داشته باشید. از این طریق می‌توانید درباره شیوه یافتن یک راه حل مقرون به صرفه که با نوع برخورد سازمان شما با خطر سازگار است و از اتفاقات پرخرج جلوگیری می‌کند، بحث‌های معناداری داشته باشید.

بنابراین هر زمان اگر مشکلی وجود داشت و تنها راه حلی که مسئول ارشد امنیت اطلاعات شما پیشنهاد می‌داد فناوری بود، باید از آن ها بخواهید تا مشکل را توضیح دهند. باید بگویید: «یک لحظه صبر کنید، تغییر فرایند یا چیزهای دیگری که همیشه باید با فناوری همراه شوند تا آن را به کار بیندازند، کجا هستند.» جان پسکارتور – گارتنر

برای اینکه مسئول ارشد امنیت اطلاعات سیاست‌ها را به خوبی تعیین کند، مؤسسه SANS پیشنهاد می‌کند که:

- همه دارایی‌های که سعی می‌شود از آنها محافظت شود را شناسایی کند.
- همه آسیب‌پذیری‌ها و تهدیدها و احتمال وقوع تهدیدها را شناسایی کند.
- یافته‌ها و نتایج را به طرف‌های ذی‌ربط اطلاع دهد (یعنی شما و هیأت مدیره)
- فرایند بهبود را در طول مسیر کنترل و بازبینی کند.

از چیزهایی که به اشتراک می‌گذارید آگاه باشید

از آنجا که بزرگترین خطر برای یک سازمان اغلب رفتار افرادی است که در آن کار می‌کنند، Lumension یک مجموعه ویدیویی را برای کاربران فناوری تهیه کرده است. این راهکارهای اساسی را برای محافظت از اطلاعات شخصی و داده‌های سازمانی با کارکنان شرکت خود در میان بگذارید. ویدیوهای دیگر در مرکز مرجع Lumension موضوعاتی مانند سرقت هویت، وب‌گاه‌های امن، رمزهای عبور امن و تعریف ویروس رایانه‌ای را در بر می‌گیرند.

lumension.com/be-aware

نتیجه‌گیـــری: نقش امنیتی مدیـــر عامـــل

از آنجا که امنیت می‌تواند تأثیر چشمگیری روی سودآوری یک سازمان داشته باشد، موظف هستید در این زمینه مدیر مقتدری باشید. به نظر خیلی از مسئولان ارشد امنیت اطلاعات که با آنها در Lumension صحبت کردیم، تنها راه برای مشارکت دادن کاربران در اجرای طرح‌های اصلی امنیت اطلاعات، ایجاد اطمینان نسبت به پشتیبانی از سوی رأس هرم است. به عنوان مدیر عامل، شما اولین فردی هستید که باید فرهنگ امنیت را ارتقا دهید. بدون انجام این کار، شانسی برای برخورداری از یک امنیت خوب در سراسر بخش ها و دفاتر منطقه ای و شعب نخواهید داشت.

همان طور که یکی از مشتریان ما مطرح می‌کند: «موضوع وقتی از طرف مدیر عامل مطرح شود، نسبت به زمانی که از طرف مسئول امنیت مطرح شود، مهم‌تر است. همکاران خواهند گفت: "اُه! مدیر عامل!" آن ها به من به عنوان مسئول، توجه نمی‌کنند، اما به مدیر عامل گوش می‌دهند.»

برای بهبود امنیت خود، همین امروز شروع کنید

بنابراین از کجا شروع می‌کنید؟ به یاد داشته باشید، آدم‌های بد، واقعی هستند – آن ها می‌دانند چطور از حفره‌های موجود در شبکه سوء استفاده کنند و از کاربران نهایی و سیستم‌های آفلاین به منظور کسب دسترسی به داده‌های شما سود ببرند.

با اجرای برخی از بهترین اقدامات اساسی امنیتی، قادر خواهید بود خود را با تاکتیک‌های جدید تبهکاران سایبری وفق دهید و در برابر آنها از خود محافظت کنید:

۱. طرز تفکر خود را تغییر دهید

امنیت صرفاً حوزه کاری متخصصان فناوری اطلاعات در مرکز داده ها نیست. شما و هیأت مدیره شما در هنگام بروز نقض پاسخگو خواهید بود، بنابراین اکنون تصمیم‌گیری را شروع کنید.

۲. برنامه داشته باشید

شرکت‌ها به طور اتفاقی ایمن نمی‌شوند و رعایت مقررات به تنهایی برای تضمین موفقیت کافی نیست. با علم به اینکه نمی‌توانید همه مشکلات را حل کنید، دیدگاه خود را ساده سازید. سپس به مدیران اجرایی شرکت مأموریت دهید که با متخصصان فناوری (و خودتان) برای ترسیم دقیق مسائل همکاری کنند.

۳. دفاع کامل

نصب یک دیواره آتش و یک ضدویروس در محیط تهدید امروز کارساز نخواهد بود. این برنامه باید شامل دفاع چند لایه باشد تا تضمین کند که حمله‌ها نادیده گرفته نمی‌شوند.

هفت چیزی که کارکنان به شما نخواهند گفت

راب پگورارو

کارکنان شما مطمئناً به بخش فناوری اطلاعات شما نمی‌گویند چه کارهایی را از طریق رایانه‌های خود برای سرگرمی انجام می‌دهند. همچنین احتمالاً اطلاعات مربوط به شیوه کار خود از منزل را نیز با شما در میان نمی گذارند. و اگر تجربه من و ماجراهایی که از همکاران و خوانندگان شاغل در این پست شنیده‌ام نوعی راهنمایی در نظر گرفته شود، بخش فناوری اطلاعات از شنیدن حقیقت خوشحال نخواهد شد.

۱) کارکنان از رمزهای عبور همسان در چندین وب‌سایت استفاده می‌کنند (۳۱ تا ۴۳ درصد در مطالعه اخیر پژوهشگران دانشگاه کمبریج و ۱۰ تا ۲۰ درصد در پژوهش‌های قدیمی‌تر). این موضوع جای تعجبی ندارد: وقتی تعداد بسیاری از وب‌سایت ها برای کاربردهای کم‌ارزشی مانند خواندن یک داستان، رمز عبور می‌خواهند، کاربران خلاقیت خود را برای چیزهای دیگر حفظ می‌کنند. بخش فناوری اطلاعات شما موظف است به آنها یادآوری کند که نباید از رمز عبور یکسانی برای شبکه سازمانی و هر گونه وب سایت دیگر استفاده‌نمایند.

۲) آنها رمزهای عبور را یادداشت می‌کنند. هیچ کس نباید از این مسئله نیز تعجب کند. سیاست‌های انقضای رمز عبور، به خصوص آنهایی که دارای «الزامات حداقل پیچیدگی» در اندازه رمز هستند، تقریباً همگی از کاربران دعوت می‌کنند که هر رمز عبور جدید را بعد از ایجاد آن یادداشت کنند، تا مبادا زمانی که به منزل بازگشتند آن را فراموش کرده باشند. مسئله این است که یادداشت کردن رمز عبور می‌تواند آن امن نگه دارد، در صورتی که مطمئن باشید در کیف پولتان جای آن امن است.

۳) آنها احتمالاً موضوع قوی بودن رمز عبور را درک نمی‌کنند. اگر به جدولی نگاه کنند که نشان می‌دهد افزودن یک کاراکتر دیگر به یک رمز عبور هفت حرفی، مدت زمان لازم برای شکستن آن را از روزها به ماه‌ها (یا در بدترین حالت از دقیقه‌ها به ساعت‌ها) تغییر می‌دهد، شاید متوجه شوند که این الزامات پیچیدگی نفرت‌انگیز از کجا می‌آیند و ممکن است به انتخاب رمزهای عبور قوی‌تر ترغیب شوند.

۴) آنها کارهای شرکت را از طریق ایمیل های شخصی انجام می‌دهند. سهولت دسترسی از راه دور که مثلاً از طریق نصب برنامه قدیمی Lotus Notes فراهم می‌شود را با برنامه Gmail مقایسه کنید. کارکنان پرمشغله اغلب از آسان‌ترین راه‌های ارتباطی موجود استفاده می‌کنند، حتی اگر این کار آنها را در معرض خطر حمله‌های سرقت هویت قرار دهد. البته درنظر دارید که آن ها برای میزان دشواری کار کردن از راه دور پاداش دریافت نمی کنند

۵) آن ها درایوهای فلش حاوی اسناد کاری را گم می‌کنند. به آخرین جمله پاراگراف قبلی رجوع کنید. این مشکل تا حدی یکی از عیوب اجتناب‌ناپذیر ابعاد فشرده درایوهای فلش است. اگر خوش شانس باشید، این درایوها تا زمانی که در ته کیف لپتاپ یا جیب ژاکت قرار داده شوند، گم نخواهند شد.

۶) آنها اغلب نرم‌افزار نصب شده روی رایانه‌های خود را به قدر کافی روزآمد نمی‌کنند. مطمئناً ویندوز، اینترنت اکسپلورر یا فایرفاکس را بروز نگه می دارند. اما آیا پلاگین‌های این مرورگرها که به طور روزافزون مورد حمله بدافزارها قرار می‌گیرند را نیز بهنگام می‌کنند؟ آمار، دلسردکننده است. در سال ۲۰۰۸، Secunia تخمین زد که ۱/۲۵ درصد از رایانه‌های دارای ویندوز، از فایل‌های بهنگام‌سازی ضروری برای شش تا ۱۰ برنامه آسیب‌پذیر استفاده نمی کنند.

۷) اگر هکرها به آنها حمله کنند، نمی‌دانند این اتفاق چطور افتاده است. دشوارترین گفتگوهایی که با خواننده‌ها داشته‌ام، زمانی بوده است که آنها درباره حمله‌های بدافزاری سؤال کرده‌اند. هیچ کدام از آنها نتوانست به من بگوید رایانه یا حساب او چگونه در معرض خطر قرار گرفته است، که تشخیص اینکه چه کاری باید طور دیگری انجام شود را دشوار می‌ساخت.

اگر وسوسه شده‌اید که کارکنان خود را به خاطر همه این اشتباهات سرزنش کنید، این کار را انجام ندهید. مثال مبارزه صنعت ضبط موسیقی در برابر وب سایت‌های اشتراک‌گذاری فایل را در نظر بگیرید: سرزنش مردم مؤثر واقع نشد، اما ارائه گزینه‌های آسان و ساده مانند آی‌تونز شرکت اپل و دستگاه ذخیره‌سازی MP3 شرکت آمازون مؤثر واقع شد. امنیت خوب نباید دشوار باشد؛ نباید جلوی بهره‌وری را بگیرد. در عوض، با هم همکاری کنید تا راه حلی را پیدا کنید که برای همه مناسب باشد.

این کتاب کوچک توسط واحد ترجمه ماهنامه دیده‌بان فناوری آماده‌سازی شده و توسط تیم گرافیک آن صفحه‌آرایی شده است. لطفا در صورت تمایل به دریافت عناوین دیگر، انجام همکاری‌های بیشتر و یا کسب اطلاعات تکمیلی، با ایمیل info@dfe.ir در تماس باشید و یا به سایت www.dfe.ir مراجعه فرمایید.
لازم به‌ذکر است این ماهنامه توسط هلدینگ رسانه‌ای دیده‌بان منتشر می‌شود.