کد خبر: ۱۰۲۸۸۲۲
دوشنبه ۲۷ آبان ۱۳۹۸ ۸:۰۴

ایسکانیوز گزارش می دهد؛

زنجیر امنیت اطلاعات را محکم‌تر ببندیم

در سال‌های اخیر با گسترش بانک‌های داده و ذخیره اطلاعات، بحث‌های زیادی در مورد مشکلات امنیتی داده‌ها به‌ویژه در شبکه های اجتماعی شکل گرفته است. از آنجایی که این پایگاه‌های داده منبعی استراتژیک برای هر سازمانی است، در این میان آنهایی موفق‌ترند که بتوانند امنیت این گنج‌های مدرن را بیشتر تامین کنند.

استفاده ایمن از رایانه در محل کار و خانه، همیشه در اولویت کسانی است که دائم با آن سروکار دارند. در این گزارش عادات مهم برای ایمن ماندن، امنیت آنلاین داده ها و همچنین جلوگیری از نقض امنیت در محل کار برای کاربران مطرح شده است.

به گزارش گروه علم و فناوری ایسکانیوز، هر زمان که خبری مبنی بر رخنه اطلاعات منتشر می شود، ممکن است حملات پیچیده هک شدن یا سرقت داده های غیرقانونی توسط کارمندان بدذات را تصور کنید؛ اما در این میان آنچه که ممکن است متوجه نشوید این است که در بسیاری از موارد این لو رفتن داده ها تنها به دلیل اتفاق و تصادف رخ می دهد.

گزارش سال ۲۰۱۹ نشان می دهد که کارمندان می توانند تا چند بار سهوی باعث رخنه اطلاعات شده باشند. در بیش از ۶۰ درصد موارد نقض داده ها، فردی از شرکت آسیب دیده مقصر بوده است؛ بنابراین برای این که اتفاقات مشابه برای شما در هنگام استفاده از دستگاه در دفتر کارتان رخ ندهد، راهکارهایی داریم.

در هنگام ارسال داده‌های حساس، گیرندگان را دو بار بررسی کنید

گزارشی که اخیراً توسط شرکت امنیتی انجام شده است، نشان می دهد که کارمندان می توانند سهواً باعث انتشار اطلاعات محرمانه و نقض داده شوند؛ اما غالباً به جای شرارت های عمدی، تنها اشتباهات ساده باعث رخ دادن آنها شده است. به عنوان مثال، ممکن است هنگام نوشتن ایمیل فوری یا ارسال یک سند مهم، به طور تصادفی آن را به مقصد اشتباه ارسال کنید.

گزارش بیان می کند که ۴۳درصد نشت داده ها به دلیل افشای نادرست صورت پذیرفته است. این فقط به معنای ارسال پرونده برای شخص اشتباه است. این شامل قرار دادن آدرس ایمیل اشتباه در قسمت گیرنده یا فکس کردن اطلاعات به شماره اشتباه است. خطای متداول دیگر استفاده تصادفی از به جای است که آدرس کلیه گیرندگان را در معرض دید شما قرار می دهد.

نکته مهم در اینجا این است که دو برابر، گیرندگان داده های حساس را بررسی کنید. این که از طریق پست الکترونیکی، فکس یا پست اطلاعات را ارسال می کنید، مهم نیست مسئله اینجاست که تنها یک دقیقه طول می کشد تا دوباره اطمینان حاصل شود که اطلاعات را فقط برای افرادی ارسال می کنید که باید آنها را داشته باشند. برای امنیت بیشتر بهتر است که از یک همکار دیگر خود هم خواهش کنید تا برای شما دوباره اطلاعات را چک و تایید کند.

هرگز کلمات عبور خود را با همکاران به اشتراک نگذارید

همه شنیده اند که شما نباید رمزهای عبور خود را به اشتراک بگذارید؛ اما به راحتی می توان فهمید که چرا هنوز هم اتفاق می افتد. شاید بیمار شده و مجبور به ماندن در خانه باشید و یک همکار دیگر به رایانه و یا اطلاعات شما نیاز دارد. یا شاید رئیس شما بخواهد در زمان تعطیل بودن به ایمیل شما دسترسی پیدا کند. روش همیشگی این است که رمزهای عبور را روی یادداشت های – بنویسید و آنها را به صفحه رایانه خود بچسبانید.

مشکل این است که وقتی یک گذرواژه به اشتراک می گذارید، از ایمنی آن کم می کنید. اگر رمزعبور خود را به رئیس خود ایمیل بزنید و ایمیل آنها هک شود، هکرها به دستگاه شما نیز دسترسی خواهند داشت. اگر یک همکار با استفاده از گذرواژه شما وارد شود و داده هایی را که نباید، ببیند؛ مسئولیت آن به عهده شما خواهد بود زیرا این حساب شماست.

هرچند همیشه راهی برای حل این مسئله وجود دارد. اگر در به خاطر سپردن رمزهای عبور خود مشکل دارید، بهترین راه برای حل این مسئله استفاده از یک مدیر رمز عبور( ) است. به این ترتیب، شما فقط باید یک رمز عبور را به خاطر بسپارید و با همان رمز عبور می توانید از هرجایی به همه حساب های خود دسترسی پیدا کنید.

از رمزهای عبور واضح مانند ۱۲۳۴۵ یا رمز عبور مخوف استفاده نکنید؛ زیرا حدس زدن آنها برای هکرها بسیار آسان است.

اگر می خواهید دسترسی به اطلاعات را با همکاران خود به اشتراک بگذارید، تنظیم یک ایمیل گروهی یا یک فایل اشتراک گذاری با استفاده از خدماتی مانند می تواند راه بهتری باشد.

درباره اخلاق داده‌ها مطالعه کنید

چیزی که بسیاری از کارمندان درک نمی کنند این است، داده هایی که آنها به عنوان بخشی از مشاغل خود با آنها سروکار دارند، منحصراً به شرکتی تعلق دارد که برای آن کار می کنند و متعلق به آنها یا بخش آنها نیست. اگر داده های زیر دست شما یک لیست از مشتریانی است که شما در کنار هم قرار داده اید یا داده های ترجیحی مربوط به مشتری هایی است که جمع آوری کرده اید، باز هم چندان تفاوتی در اصل موضوع نخواهد داشت و اطلاعات کاملاً متعلق به شرکت خواهد بود.

این مهم است که شما به دلایل کارمندان برای به اشتراک گذاشتن عمدی داده ها توجه کنید. یکی از پنج نفری که عمداً داده ها را به اشتراک می گذاشتند گفت این کار را انجام داده؛ زیرا فکر می کرده که اطلاعات مربوط به خودش بوده و حق هرگونه استفاده از آنها را دارد. ۵۵ درصد دیگر اما گفتند که اگر داده ها را به صورت ناامن به اشتراک می گذاشته اند به این دلیل بوده که نمی دانستند چگونه به طور ایمن آن را به اشتراک بگذارند.

متأسفانه شما نمی توانید لزوماً روی رئیس یا مسئول بخش خود حساب کنید تا هر آنچه را که باید درباره امنیت داده بدانید به شما یاد دهد. اگر داده های امن را به عنوان بخشی از کار خود اداره می کنید ، باید خودتان وقتی را اختصاص دهید تا در مورد الزامات قانونی و بهترین شیوه های کار با داده ها آگاهی کسب کنید.

نسبت به فیشینگ و سایر حملات هوشیار باشید

احتمالاً از تهدید فیشینگ ( )اطلاع دارید. وقتی ایمیلی را می بینید که ادعا می کند از سمت بانک ارسال شده و از شما می خواهد رمز عبور خود را وارد کنید، می دانید که این ماجرا مشکوک است؛ اما فیشینگ روزبه‌روز بسیار پیشرفته تر می شود و شما باید برای آن آماده باشید.

بررسی ها نشان داد که تنها ۵درصد نشت داده ها مربوط به فیشینگ است. با این حال، این روش از نشت داده ها جدی تر از سایر روش ها به نظر می رسد. تکنیک های جدید مانند نیزه فیشینگ یک فرد خاص و دارای اطلاعات بسیار خاص را هدف قرار می دهد. به‌ویژه اگر در کار می کنید یا مدیر اجرایی بالایی هستید، باید در مورد این حملات مواظب باشید.

حمله سایبری پیشرفته شبیه یک نهنگ است. این جاست که هکرها حساب یک مدیر ارشد را به خطر می‌اندازند و از این کار برای کلاهبرداری کارکنانی که زیردست آنها هستند، استفاده می کنند.

اگر درخواست الکترونیکی عجیب و غریبی را مشاهده کردید، تلفن را بردارید؛ زیرا برقراری تماس با فرستنده، بهترین راه برای تعیین واقعی بودن یا مجازی بودن فرستنده است.

نرم افزارهای پاک کننده از راه دور را روی دستگاه‌های خود نصب کنید

حوادث رخ می دهد و ممکن است که در پایان یک روز طولانی، لپ تاپ یا تلفن خود را در قطار جا بگذارید. بدیهی است که سعی خواهید کرد دستگاه های کاری خود را گم نکنید؛ اما همیشه این احتمال وجود دارد که چنین اتفاقی رخ دهد.

علاوه بر داشتن گذرواژه در تمام دستگاه های کاری خود، باید نرم افزار پاک کردن از راه دور را نیز نصب کنید. این نرم افزارها را می توانید با استفاده از ابزارها و برنامه هایی مانند برای یا با قرار دادن موقعیت مکانی در ستینگ روی گزینه راه دور و پاک کردن تنظیمات دستگاه خود، داده های مهم و از پیش تعیین شده را پاکسازی کنید. وقتی این ویژگی ها را فعال کردید، می توانید دستگاه خود را از راه دور و از طریق یک رایانه دیگر مدیریت کنید.

می توانید به حساب کاربری خود وارد شوید و سپس از موجود در دستگاه گم شده خود، برای یافتن آن استفاده یا محتویات هارد را از راه

دور پاک کنید.

مطمئناً مجبور خواهید شد تا همه داده ها را حذف کرده و به بخش فناوری اطلاعات سازمان خود توضیح دهید که یک دستگاه را گم کرده اید. این توضیح بسیار بهتر از آن است که مسئول خوراک دادن به هکرها برای سرقت اطلاعات با ارزش یا خصوصی از شرکت شما باشید.

برای امنیت بیشتر اطلاعات خود در محل کار اطلاعات بیشتری کسب کنید. اگر چه بسیاری از مسائل امنیتی دیگر در مورد استفاده از رایانه شخصی شما نیز باید در نظر گرفته شود؛ اما این شیوه های امنیتی خاص که در بالا ذکر شدند، به شما کمک می کنند تا داده هایی را که با آنها کار می کنید ایمن کنید.

انتهای پیام/