علاقه‌مندید در محل کار با شبکه‌های اجتماعی کار کنید، پس امنیت را فراموش نکنید!

نزدیک به یک ماه پیش (در زمان نگارش این مقاله) روز جهانی رسانه‌های/ شبکه‌های اجتماعی بود. امروزه شرکت‌های تجاری به‌خوبی به این موضوع واقف شده‌اند که برای گسترش کسب و کار خود باید توجه بیشتری به رسانه‌های اجتماعی داشته باشند. مقوله‌ای به‌نام رسانه‌های اجتماعی تأثیری به‌مراتب فراتر از آن چیزی دارد که بسیاری از کاربران یا حتی مدیران آن را تصور می‌کنند. این تأثیرگذاری به اندازه‌ای محسوس بوده است که بسیاری از کسب و کارها برای موفقیت در حوزه کاری خود روی رسانه‌های اجتماعی حساب ویژه‌ای باز کرده‌اند.

ما در عصری زندگی می‌کنیم که بسیاری از سازمان‌ها به رسانه‌های اجتماعی به مانند پلی برای دستیابی به موفقیت، دستیابی به مشتریان جدید و ثابت، راهکاری برای تقویت و گسترش نام تجاری و مناسبات تجاری خود نگاه می‌کنند. کاملاً روشن است که این دیدگاه دوسویه بوده است و رسانه‌های اجتماعی نیز برای حفظ محبوبیت و جایگاه خود سعی خواهند کرد ارتباطات تنگاتنگی با کسب و کارها برقرار کنند. اما هر زمان درباره رسانه‌های اجتماعی سخنی به زبان می‌آوریم، نباید از نقش امنیت اطلاعات ساده بگذریم. امنیت اطلاعات در هیچ برهه‌ای از زمان تا به این اندازه اهمیت نداشته است. اما با ورود رسانه‌های اجتماعی به محیط‌های شخصی و کاری پرسش‌های ناگفته یا بدون جواب جدیدی در ارتباط با امنیت خود را پدیدار می‌سازند.
اولین پرسشی که به ذهن خطور پیدا می‌کند این است که اساساً رسانه‌های اجتماعی یک تهدید بزرگ برای امنیت به شمار می‌روند؟ پاسخ این پرسش تا حدودی مثبت است. اما این موضوع پدیده جدیدی نیست. سیسکو در گزارشی تحلیلی که سال 2013 میلادی آن را منتشر کرد، مدعی شد سایت‌هایی با کاربران زیاد همچون رسانه‌های اجتماعی یک تهدید جدی برای امنیت اطلاعات به شمار می‌روند. به‌واسطه آنکه این امکان وجود دارد تا خط جداسازی اطلاعات شخصی از اطلاعات تقریباً محرمانه سازمانی و شرکتی از میان برود. این اتفاق زمانی رخ می‌دهد که کارمند شرکتی تصمیم می‌گیرد از یک حساب رسانه اجتماعی هم برای اهداف شخصی و هم برای اهداف کاری استفاده کند که این پدیده مشکلات بالقوه‌ای را به وجود می‌آورد. در حالی که بسیاری از کارکنان یک سازمان این موضوع را کم‌اهمیت تفسیر می‌کنند و بر این باورند که حساب‌های کاربری آن‌ها در رسانه‌های اجتماعی به هیچ عنوان مورد علاقه هکرها قرار ندارند؛ با وجود این، حساب‌ها شانس به خطر افتادن زیرساخت‌ها و شبکه‌های ارتباطی یک شبکه را دوچندان می‌کنند. به طوری که هکرها ممکن است از این حساب‌ها به‌عنوان نقطه‌ای برای ورود به شبکه‌ها استفاده کنند.

مطلب پیشنهادی

الزام شبکه های اجتماعی خارجی به دریافت مجوز

پرسش مهم دیگری که در این زمینه وجود دارد این است که به‌راستی رسانه‌های اجتماعی نقطه ضعفی به شمار می‌روند؟ پاسخ این پرسش نیز تا حدودی مثبت است. امروزه نشانی‌های ایمیلی متعلق به افراد سرشناس و بانفوذ در معرض تهدید جدی حملات فیشینگ قرار دارند، حال اگر این نشانی‌ها با رسانه‌های اجتماعی ترکیب شوند، تهدید دوچندان می‌شود. به طور مثال، اگر هکرها موفق شوند به یک حساب کاربری ساخته شده در شبکه‌ای همچون فیسبوک یا لینکدین نفوذ کنند، به‌راحتی قادرند افرادی که در شبکه قربانی قرار دارند را فریب دهند، به طوری که همکاران قربانی تصور کنند پیام‌ها از جانب همکارشان ارسال شده و به این شکل اطلاعات حساس را در اختیار هکر قرار دهند.
نکته‌ای که ضروری است در همین جا به آن اشاره داشته باشیم این است که خروجی نهایی شبکه‌های اجتماعی برآیندی از تصویر کلی یک برند یا بهتر بگوییم نام تجاری است. اگر هکری موفق شود یکی از کانال‌های موجود در شبکه‌ای را هک و به آن دست پیدا کند، صدماتی که در این زمینه ممکن است وارد کند سنگین خواهد بود. درست همانند اتفاقی که در سال 2013 میلادی رخ داد و هکری موفق شد به حساب کاربری توییتر متعلق به شرکت برگر کینگ نفوذ کند. این هکر در ادامه از حساب توییتری این شرکت به‌منظور نشان دادن نماد تجاری مک دونالد همراه با تصویر نامناسبی استفاده کرد.
با این تفاسیر، به سؤال بدیهی‌تری می‌رسیم که برای بهبود اوضاع چه کاری می‌توانیم انجام دهیم؟ بهترین راهکاری که در این زمینه پیش روی ما قرار دارد این است که سیاست‌های سخت‌گیرانه‌ای را در ارتباط با شبکه‌های اجتماعی و محافظت از حساب‌های شرکت به مرحله اجرا درآوریم. این استراتژی در اغلب موارد خوب جواب می‌دهد. در ادامه کارکنان را در قالب یک برنامه سایبری جامع مقید سازیم که از گذرواژه قدرتمندی استفاده کنند. سپس، آموزش‌های لازم در زمینه کشف برنامه‌های مخرب، پیاده‌سازی احراز هویت دوعاملی و حصول اطمینان از به‌اشتراک‌گذاری محتوای تأیید شده با نام تجاری را به مرحله اجرا درآوریم. این استراتژی به‌ویژه در ارتباط با شرکت‌هایی حائز اهمیت است که در شبکه‌های اجتماعی بیش از یک حساب کاربری دارند. درنهایت مدیران نباید از نقش خود در زمینه حفظ امنیت حساب‌های متعلق به شبکه‌های اجتماعی غافل شوند. در این زمینه نیز مدیران باید همواره به تشریح تهدیدات بالقوه‌ای بپردازند که از سوی شبکه‌های اجتماعی ممکن است کاربران را در معرض خطر قرار دهد. به طور مثال، کارمندان نباید روی لینک‌هایی که درون ایمیل‌های ناشناس قرار دارند کلیک کنند. همچنین، کارکنان یک سازمان نباید هیچ‌گاه اطلاعات حساس خود و سازمانشان را از طریق شبکه‌های اجتماعی انتقال دهند. همان گونه که مشاهده کردید، به‌کارگیری شبکه‌های اجتماعی در محیط کار با پیش‌زمینه‌های امنیتی بسیاری همراه است که اگر به آن‌ها کم‌توجهی کنید، ممکن است شغل خود را از دست بدهید.

تاریخ انتشار:

11 شهریور 1396

نشانی منبع:
https://www.shabakeh-mag.com/opinion/9356/%D8%B9%D9%84%D8%A7%D9%82%D9%87%E2%80%8C%D9%85%D9%86%D8%AF%DB%8C%D8%AF-%D8%AF%D8%B1-%D9%85%D8%AD%D9%84-%DA%A9%D8%A7%D8%B1-%D8%A8%D8%A7-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%DB%8C-%DA%A9%D8%A7%D8%B1-

%DA%A9%D9%86%DB%8C%D8%AF%D8%8C-%D9%BE%D8%B3-
%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%B1%D8%A7-
%D9%81%D8%B1%D8%A7%D9%85%D9%88%D8%B4-
%D9%86%DA%A9%D9%86%DB%8C%D8%AF