۱۰راهکار حفاظت از داده ها

برای خیل عظیمی از سازمان ها، داده ها و اطلاعات سازمانی بسیار اهمیت حیاتی و ضروری داشته و همین میزان اهمیت، بر رواج نقض اطلاعات با شیوه نفوذ و هک در سیستم‌ها افزوده است.

حال ۱۰ راهکار فردی و سازمانی ساده و کارآمد برای حفاظت از داده‌ها و اطلاعات مالی و خصوصی وجود دارد که به شرح زیر است:

۱. آپدیت بودن

این روشی است که بارها و بارها توسط متخصصان امنیت اطلاعات خواهید شنید و تنها صرف آپدیت‌های بحرانی امنیتی و پچ‌های ضروری نمی‌شود بلکه در همه حال، نرم‌افزار از منظر سیستمی هم باید بروز نگاه داشته شود.

بهترین راهکار برای آپدیت بودن همیشگی، استفاده از امکان آپدیت اتوماتیک نرم‌افزار است.

۲. رمزگذاری بر روی داده ها و اطلاعات حساس

رمزگذاری داده‌ای برخلاف تصور همگان تنها شامل شرکت‌های بزرگ نمی‌شود؛ ابزارهای بسیاری اکنون برای رمزگذاری اطلاعات شخصی و سازمانی وجود دارد.

با استفاده از رمزگذاری می‌توان خاطر جمع بود که اگر حتی اطلاعات به دست هکر بیفتد، خواندن آنها غیرممکن است. کسانیکه به دنبال امنیت بیشتر اطلاعات خود هستند باید پیش از انتقال داده ها به دستگاه های قابل حمل مانند فلش یا هارد اکسترنال، اطلاعات را رمزگذاری کنند.(در صورت لزوم برای مشاوره در انتخاب نرم افزار از کارشناسان سپکو کمک بگیرید)

۳. استفاده از نرم‌افزار ضدویروس

تقریبا بر کسی پوشیده نیست که نرم‌افزارهای ضدویروس قادر به شناسایی تمامی رفتارهای مشکوک نیستند و تنها به عنوان امنیت پایه از آنها یاد می‌شود ولی اثر بسار مفید و حیاتی در امنیت شما خواهند داشت.

پیشنهاد ما استفاده از آنتی ویروس های معتبر مانند کسپراسکی و ... می باشد.استفاده از آنتی ویروس رایگان مایکروسافت همیشه پیشنهاد می شود.

۴.استفاده از گذرواژه‌های منحصر به فرد و پیچیده برای حساب های کاربری کارمندان

استفاده مجدد از پسوردها در اکانت های مختلف از جمله بزرگترین نگرانی‌ها در برابر حملات هکری است؛ هکرها در این مواقع با دسترسی به گذرواژه های اکانت اصلی قادر به دستیابی به دیگر حساب‌ها از سوی یک کاربر خاص خواهند بود.

۵. بایگانی یا پاک کردن اطلاعات و داده‌هایی که مدت طولانی به کار نیامده‌اند.

به حداقل رساندن میزان داده های سازمانی راهکار خوبی برای حفظ امنیت نیست اما راهکار خوبی برای کوتاه کردن دست هکرها از اطلاعات مازاد که به درد تحلیل می‌خورد است.

باید همواره یادمان باشد که اطلاعات ماهیت ارزشمندی در جامعه اطلاعاتی دارد؛ بنابراین اگر اطلاعاتی در سیستم های اداری موجود است که مدت طولانی به کار نیامده است یا باید به دستگاه ذخیره‌سازی آفلاین انتقال داده شود یا رمزگذاری شود یا از بین برود.

اسناد کاری، وقایع سلامت، قراردادها، صورتحساب ها، اظهارات بانکی قدیمی و مسائلی از این دست در این رده جای می‌گیرند.

۶. نظارت مرتب روی فعالیت حساب‌های آنلاین

بهترین راهکار برای مقابله با خطر افتادن حساب یا تقلب این است که به شکل مرتب و دوره‌ای حساب‌های آنلاین مورد نظارت قرار گیرد.

اگر فعالیت مشکوکی شناسایی شود باید اطلاع رسانی فوری به تمامی بخش ها صورت گیرد. نظارت هوشیارانه سریع‌ترین راه برای شناسایی اعمال خرابکارانه است.

۷. تغییر تمامی گذرواژه‌ها در هنگام هک شدن

متأسفانه عملیات نقض داده ممکن است در تمامی موارد شنیده شود اما اگر سازمان شما در خطر بیفتد چه کاری باید در وهله اول انجام داد؟ در گام اول باید تمامی گذرواژه ها تغییر کند تا از این طریق مطمئن شوید که اعتبار شما حتی در صورت سرقت ناکارا خواهد بود.

۸. مدیریت تنظیمات خصوصی برای اپلیکیشن‌های موبایل و حساب‌های آنلاین

تنظیمات خصوصی‌سازی اکانت‌های دستگاه‌های مختلف که اطلاعات حساس و ضروری بر روی آن وجود دارد، اقدامی ضروری برای ایمن‌سازی است. این امکان شما را در برابر عدم دسترسی به اطلاعات خصوصی مطئمن می‌کند.

۹. نگران شبکه‌های رایگان وای‌فای باشید.

هکرها و سارقان آنلاین معمولا از شبکه های وای‌فای محافظت نشده استفاده می‌کنند یا از الگوی سرقتی man-in-the-middle (شنود)استفاده می‌کنند. شیوه هک به این شکل است که اطلاعات شما بعد از ارسال به مودم وای‌فای جهت ارسال به مقصد توسط هکری که به درگاه

مودم دسترسی دارد، شنود می‌شود و از این طریق گذرواژه های شما و اعتبارتان کاملا در اختیار هکر قرار می‌گیرد بدون اینکه در جریان قرار گیرید.

پس بهتر است در اینگونه موارد حساب های کاربری مهم و دارای حساسیت خود را چک نکنید.

۱۰. کارمندان خود را با حملات فیشینگ آشنا کنید

یکی از تاکتیک‌های مهم مهندسی اجتماعی، شناخت فیشینگ است؛ این دست از حملات رواج بسیاری یافته و به این گونه است که دامنه اینترنتی در تطابق با مقصد مورد نظر نیست و در یک یا دو کاراکتر متفاوت است و همین موجب می‌شود که کاربر گمان کند به صفحه اصلی رفته در حالیکه سایت جعلی است.