



شرکت برق منطقه ای باختر

راهنمای حفاظت از اطلاعات سازمانی در شرایط استفاده از سرویس های آنلاین

تاریخ تهیه: مهر ماه ۹۹

تهیه کننده: دختر مدیریت بهران و پدراخند غیرعامل



نمونه‌هایی از ریسک‌های امنیتی دورکاری

- در شرایط دورکاری، کارمندان از شبکه‌های خانگی و معمولاً از رایانه‌های منزل خود برای کار استفاده می‌کنند. این سیستم‌ها اغلب محافظت نشده و در برابر حملات سایبری آسیب‌پذیرترند.
- داده‌های حساس احتمالاً به خارج از شبکه سازمان انتقال پیدا می‌کند. در صورت عدم آموزش کافی، ممکن است کارمندان داده‌ها را در رایانه‌های شخصی خود ذخیره کنند، جایی که توسط سیستم‌های امنیتی سازمان محافظت نمی‌شود.
- در زمان دورکاری از کارکنان خواسته می‌شود که از ابزارهای جدید برای جایگزینی جلسات چهره به چهره استفاده کنند. این سیستم‌های جدید معمولاً عجلانه انتخاب و تنظیم می‌شوند و از همین رو ممکن است ریسک‌هایی را به همراه داشته باشند.
- هرج و مرج عمومی که در پی «روش متفاوت انجام کارها» به وجود می‌آید راه‌های جدیدی را برای حملات مجازی می‌گشاید. طبیعتاً شانس موفقیت ترفندهایی مانند دریافت یک ایمیل جعلی از طرف مدیر، هنگامی که کارمند نتواند به‌طور حضوری تأیید صحت ایمیل را از مدیر خود دریافت کند افزایش می‌یابد!

دقت و آگاهی شما

اولین و مهم‌ترین مورد این است که فناوری به‌تنهایی نمی‌تواند از شما محافظت کند؛ بلکه این خود شما هستید که در خط مقدمید! مهاجمان سایبری آموخته‌اند که آسان‌ترین راه برای به دست‌آوردن آنچه می‌خواهند، هدف قرار دادن خود شما است نه کامپیوتر یا دستگاه‌های دیگر. اگر آن‌ها رمز عبور، داده‌های کاری و ... را بخواهند، معمولاً سعی می‌کنند با ایجاد یک فوریت، شما را فریب دهند تا این اطلاعات را به آن‌ها بدهید. به‌عنوان مثال، ممکن است به‌عنوان پشتیبان فنی سازمان با شما تماس بگیرند و ادعا کنند که رایانه شما آلوده شده است. یا شاید یک ایمیل ارسال کنند و شما را فریب دهند تا روی یک لینک مخرب کلیک کنید. شایع‌ترین شاخص‌های این نوع حملات که «مهندسی اجتماعی» نامیده می‌شود شامل موارد زیر است:



- **فوریت:** در این حالت مهاجم اغلب از طریق ایجاد ترس، القای بحران یا مهلت زمانی مهم، احساس اضطراب فوق‌العاده‌ای را برای مخاطب خود به‌وجود می‌آورد. مهاجمان سایبری در ایجاد پیام‌های قانع‌کننده‌ای که به نظر می‌رسد از سازمان‌های معتبر مانند بانک‌ها، دولت و ... ارسال شده‌اند، خبره‌اند.
- **مخاطبین:** پیامی که در ظاهر از یک دوست یا همکار دریافت شده اما بررسی دقیق‌تر نشان می‌دهد این تنها یک ظاهرسازی به منظور فریب بوده است.
- **دسترسی سخت‌افزاری:** یک حافظه جانبی یا Flash Memory آلوده، همچنان یکی از مهم‌ترین خطراتی است که می‌تواند امنیت اطلاعات شما را تهدید کند!

بهترین دفاع در برابر این‌گونه تهدیدات امنیتی، افزایش آگاهی و دقت «شما»ست.

۲ شبکه اینترنت خانگی

تقریباً هر شبکه خانگی شامل یک شبکه بی‌سیم Wi-Fi است که همه دستگاه‌های شما از طریق آن به اینترنت متصل می‌شوند. این بدان معنی است که امنیت شبکه بی‌سیم بخش مهمی از امنیت سایبری خانه را تشکیل می‌دهد. مراحل زیر برای حفظ امنیت شبکه خانگی شما توصیه می‌شود:



- **تغییر گذرواژه پیش فرض کاربر ادمین مودم:** از طریق دسترسی به کاربر ادمین مودم می توان کلیه تنظیمات شبکه بی سیم را پیکربندی کرد. یک مهاجم به راحتی می تواند رمز عبور پیش فرض شرکت تولیدکننده مودم را پیدا کند و از این رو تغییر آن ضروری است.
- **اجازه اتصال فقط به افراد و دستگاه های مورد اطمینان:** با فعال کردن گذرواژه مودم خود، تنها به افرادی که مورد اعتمادتان هستند اجازه دهید به شبکه بی سیم تان متصل شوند. در این حالت برای اتصال هر فرد به شبکه بی سیم رمز عبور درخواست می شود و به محض اتصال، فعالیت وی رمزگذاری می شود. توجه کنید که حتما از گذرواژه ای قوی و متفاوت با رمز عبور ادمین مودم استفاده کنید. همچنین بهتر است هر چند وقت یکبار، آن را تغییر دهید.
- **تنظیمات صحیح مودم:** برای امنیت مودم، تنظیمات رمزنگاری آن را روی حالت WPA2 تنظیم و از به کارگیری حالت WEP اکیداً بپرهیزید. همچنین در صورتی که از حالت WPS مودم استفاده نمی کنید، پیشنهاد می شود آن را غیرفعال کنید.
- **به روزرسانی نرم افزار مودم:** در صورتی که سیستم مدیریت مودم شما اجازه به روزرسانی نرم افزار (Firmware) آن را می دهد، انجام این کار می تواند به بهبود امنیت تان کمک کند.

مطمئن نیستید که چگونه باید مراحل فوق را انجام داد؟

شیوه تنظیمات برای هر مودم متفاوت است. برای دریافت راهنمایی بیشتر می توانید با ارائه دهنده خدمات اینترنت (ISP) خود تماس بگیرید یا مستندات راهنمای مودم تان را مطالعه کنید.

۳ گذرواژه‌ها

برای حساب‌های کاربری خود مانند ایمیل، فضای ذخیره‌سازی ابری، حساب‌های کاربری سامانه‌های شرکت همچون سامانه ارتباط با مشتریان و ...، گذرواژه یا رمزعبوری قوی انتخاب کنید. این یکی از مهمترین مواردی است که به حفاظت از امنیت اطلاعات شما و سازمان‌تان در فضای مجازی کمک می‌کند.



ویژگی‌های انتخاب یک گذرواژه قوی

- تا حد امکان از گذرواژه‌های طولانی که ترکیبی از اعداد، حروف و نمادها باشند، استفاده کنید.
- از کاربرد اطلاعات خام شخصی و شرکتی بپرهیزید و ترکیب‌های تصادفی و بی‌معنی را به‌کار ببرید.
- برای هر حساب کاربری آنلاین و دستگاه، از گذرواژه‌ای منحصر به فرد استفاده کنید. به این ترتیب اگر یک گذرواژه به خطر بیفتد، حساب‌ها و دستگاه‌های دیگر شما همچنان ایمن هستند.
- در اولین زمان ممکن، احراز هویت دومرحله‌ای را (Two-Step Verification) بر روی کلیه حساب‌های کاربری خود فعال کنید. با احراز هویت دومرحله‌ای علاوه بر استفاده از رمز عبور، مرحله دومی مانند ارسال پیامک کد تأیید نیز اضافه می‌شود.
- هیچ‌گاه گذرواژه‌ی حساب‌های کاربری شرکت را به صورت متن عادی و غیر رمز شده (PlainText) نگهداری نکرده و برای دیگران نیز ارسال نکنید.

انتخاب و نگهداری از چنین گذرواژه‌های سخت است؛ راه حل چیست؟

نرم‌افزارهای تخصصی ساخت و مدیریت رمز عبور روشی است که امروزه به‌طور گسترده مورد استفاده افراد و شرکت‌ها قرار می‌گیرد. البته معماری مورد استفاده در این زمینه، باید با هماهنگی و تایید مدیران امنیت IT سازمان باشد.

۴ به روزرسانی نرم افزارها

اطمینان حاصل کنید تمامی رایانه‌ها، گوشی‌های تلفن همراه و ... شما آخرین نسخه از سیستم عامل و نرم افزار خود را اجرا می کنند.

مهاجمان سایبری دائماً به دنبال آسیب پذیری های جدید در نرم افزار دستگاه های شما هستند. هنگامی که مهاجمان آسیب پذیری ها را کشف می کنند، برنامه های ویژه ای را برای سوء استفاده از آن ها و هک کردن دستگاه ها به کار می برند. در همین حال، شرکت های تولید کننده نرم افزار، با انتشار به روزرسانی ها در تلاش هستند تا نقاط ضعف آن ها را به صورت مداوم تعمیر کنند. با اطمینان از اینکه رایانه و گوشی های تلفن همراه شما، از آخرین به روزرسانی ها استفاده می کنند، کار را برای مهاجمین سخت تر خواهید کرد. برای این کار، به سادگی در اولین زمان ممکن، به روزرسانی خودکار برنامه ها را فعال کنید.

در این میان به روزرسانی دائمی نرم افزارهای آنتی ویروس و فایروال (Antivirus & Firewall) اهمیتی دوچندان دارد. اگر روی رایانه های خود از چنین نرم افزارهایی استفاده نمی کنید، حتما نصب و راه اندازی آن ها را در برنامه خود قرار دهید.