Linkap
راهبران اینترنت اشیا

راهنمای حفاظت از امنیت اطلاعات در شرایط دورکاری

نسخه ۱/۱ - ۹۹۰۱۰۸

مقدمه

اگرچه پیش‌تر نیز شیوه دورکاری در برخی مجموعه‌ها (از جمله لینکپ) به صورت محدود مورد استفاده قرار می‌گرفت، اما این روزها بیشتر شرکت‌ها و سازمان‌ها برای حفظ سلامتی همکاران خود در مقابل ویروس کرونا (COVID-19) روش دورکاری را انتخاب کرده‌اند. از سوی دیگر ضرورت دورکاری در این ایام نباید ما را از لحاظ‌کردن چارچوب‌های امنیت IT متناسب با شرایط جدید غافل کند.

در این مستند که ساختار کلی آن بر مبنای فایل راهنمای شرکت امنیتی SANS با عنوان "Top 5 Steps to Securely Work from Home" و همچنین به‌کارگیری برخی مطالب دیگر از جمله توصیه‌هایی از رمزنگار شهیر، Bruce Schneier آماده شده، برخی نکات مهم امنیتی که لازم است در این شرایط مورد توجه قرار گیرد مرور شده است.

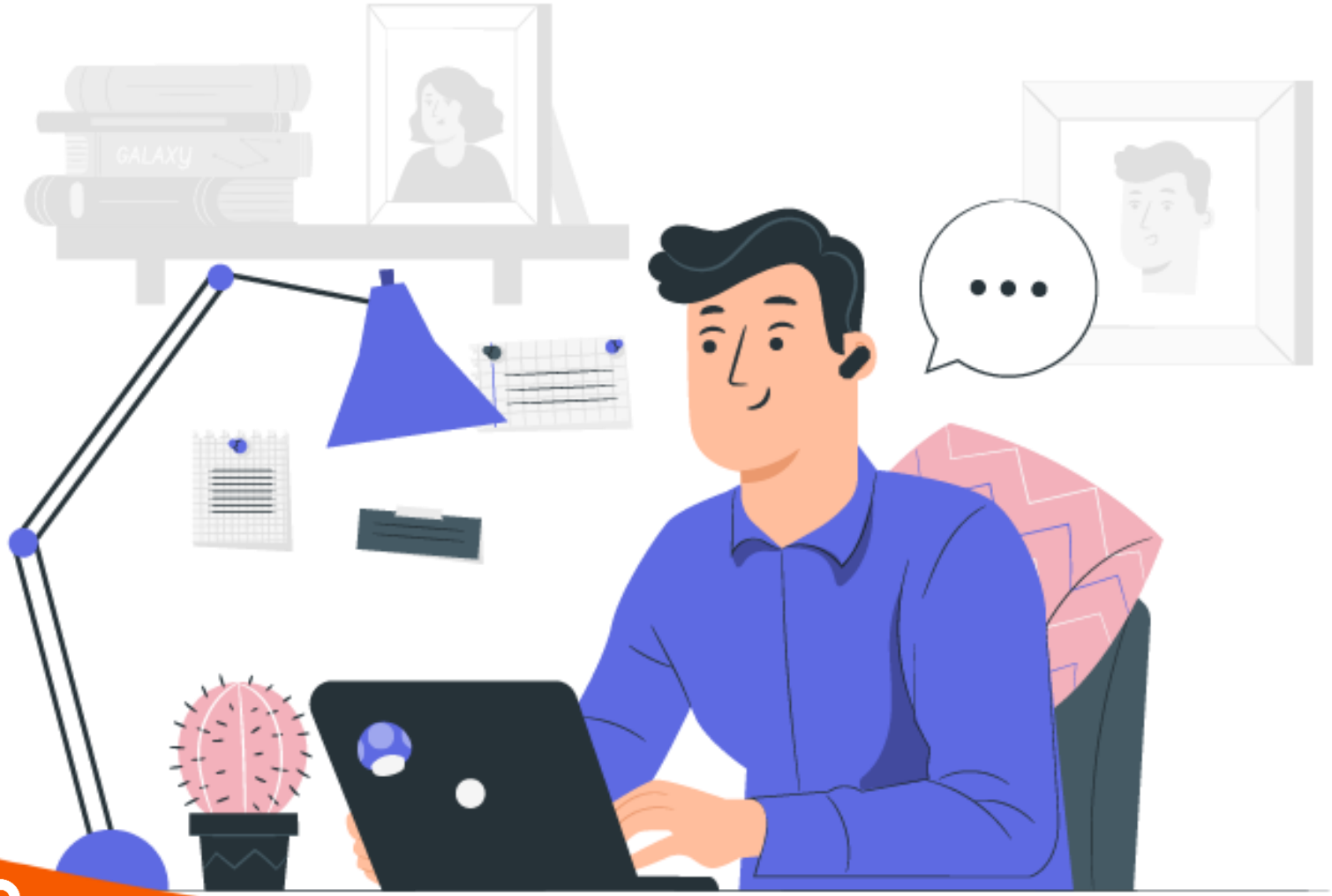
همچنین از آنجاکه رعایت این نکات در شرایط کنونی مورد نیاز همکاران سایر سازمان‌ها و شرکت‌ها نیز هست، تصمیم گرفتیم آن را به صورت عمومی منتشر کنیم.

در پایان خواهشمند است هرگونه نظر و پیشنهاد خود را از طریق آدرس hi@linkap.net برای ما ارسال کنید.

به امید فرارسیدن روزهای روشن‌تر، در کنار هم ...

چند نکته در مورد استفاده از این راهنما

- این مستند جایگزینی برای چارچوب‌های امنیتی شرکت و سازمان نیست، بلکه چک‌لیستی از برخی موارد ساده و مهم‌تر است که در شرایط کنونی باید مورد توجه قرار گیرد. از این رو، راهنمای حاضر را به‌عنوان یک نقطه شروع در نظر بگیرید و اگر مضامین دیگری برای مجموعه شما وجود دارد که رعایتشان در شرایط کنونی اهمیت دارد، آن‌ها را نیز در کنار این راهنما لحاظ کنید (مسائلی همچون استفاده از شبکه خصوصی مجازی یا VPN برای دسترسی از راه دور به شبکه سازمانی و ...).
- توصیه می‌شود در صورت ابهام درباره هر یک از فرآیندهای معرفی‌شده در این راهنما، ابتدا از طریق جستجو، آشنایی بیشتری با مفهوم یاد شده پیدا کنید و بسته به میزان اهمیت، برای به‌کارگیری فوری یا تدریجی آن برنامه‌ریزی نمایید.
- در این شرایط روی مهم‌ترین خطراتی که بیشترین تأثیر را بر روی مجموعه شما خواهند گذاشت، تمرکز کنید. در نظر داشته باشید که هرچه رفتارها، فرایندها یا فناوری‌های بیشتری را از همکاران خود بخواهید، احتمال اینکه آن‌ها بتوانند همه آن‌ها را پیاده‌سازی کنند، کمتر می‌شود.
- حفاظت فیزیکی از تجهیزاتی که هم‌اکنون برای کار در خانه استفاده می‌شوند و توضیح شفاف این مساله برای اعضای خانواده، نکته مهمی است که در شرایط دورکاری باید مورد توجه همکاران قرار گیرد.


GALAXY

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 عجولانه انتخاب و تنظیم می‌شوند و از همین رو ممکن است ریسک‌هایی را به همراه داشته باشند.
- هرج‌ومرج عمومی که در پی «روش متفاوت انجام کارها» به وجود می‌آید راه‌های جدیدی را برای حملات مجازی می‌گشاید. طبیعتا 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!

کار کردن از خانه ممکن است برای برخی از ما جدید و تاحدی غافلگیرکننده باشد. از این رو در ادامه راهکارهایی ساده برای حفظ امنیت اطلاعات هنگام کار در خانه، مرور شده است.

بهترین بخش رعایت‌کردن راهنمای حاضر این است که نه‌تنها برای امنیت اطلاعات کاری شما مناسب است، بلکه رعایت آن‌ها امنیت شما و خانواده‌تان را نیز در فضای سایبری به‌مراتب بیشتر خواهد کرد :)

۱ 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. به‌عنوان‌مثال، 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 ... ارسال‌شده‌اند، 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 پیش‌فرض کاربر ادمین مودم:** از طریق دسترسی به کاربر ادمین مودم می‌توان کلیه تنظیمات شبکه بی‌سیم را پیکربندی کرد. یک مهاجم به‌راحتی می‌تواند رمز عبور پیش‌فرض شرکت تولیدکننده مودم را پیدا کند و از این رو تغییر آن ضروری است.
- **اجازه اتصال فقط به افراد و دستگاه‌های مورد اطمینان:** با فعال کردن گذرواژه مودم خود، تنها به افرادی که مورد اعتمادتان هستند اجازه دهید به شبکه بی‌سیم‌تان متصل شوند. در این حالت برای اتصال هر فرد به شبکه بی‌سیم رمزعبور درخواست می‌شود و به‌محض اتصال، فعالیت وی رمزگذاری می‌شود. توجه کنید که حتما از گذرواژه‌ای 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 به‌کارگیری حالت WEP اکیداً بپرهیزید. همچنین در صورتی که از حالت WPS مودم استفاده نمی‌کنید، پیشنهاد می‌شود آن را غیرفعال کنید.
- **به‌روزرسانی نرم‌افزار مودم:** در صورتی که سیستم مدیریت مودم شما اجازه به‌روزرسانی نرم‌افزار (Firmware) آن را می‌دهد، انجام این کار می‌تواند به بهبود امنیت‌تان کمک کند.

مطمئن نیستید که چگونه باید مراحل فوق را انجام داد؟

شیوه تنظیمات برای هر مودم متفاوت است. برای دریافت راهنمایی بیشتر می‌توانید با ارائه‌دهنده خدمات اینترنت (ISP) خود تماس بگیرید یا مستندات راهنمای مودم‌تان 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 منحصربه‌فرد استفاده کنید. به‌این‌ترتیب 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 تائید نیز اضافه می‌شود.
- هیچ‌گاه گذرواژه‌ی حساب‌های کاربری شرکت را به صورت متن عادی و غیر رمزشده (PlainText) نگهداری نکرده و برای دیگران نیز ارسال نکنید.

انتخاب و نگهداری از چنین گذرواژه‌های سخت است؛ راه‌حل 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 به‌روزرسانی نرم‌افزارها

اطمینان حاصل کنید تمامی رایانه‌ها، گوشی‌های تلفن همراه و ... شما آخرین نسخه از سیستم‌عامل و نرم‌افزار خود را اجرا می‌کنند.
مهاجمان سایبری دائماً به دنبال آسیب‌پذیری‌های جدید در نرم‌افزار دستگاه‌های شما هستند. هنگامی‌که مهاجمان آسیب‌پذیری‌ها را کشف می‌کنند، برنامه‌های ویژه‌ای را برای سوءاستفاده از آن‌ها و هک‌کردن دستگاه‌ها به‌کار می‌برند. در همین حال، شرکت‌های تولیدکننده نرم‌افزار، با انتشار به‌روزرسانی‌ها در تلاش هستند تا نقاط ضعف آن‌ها را به صورت مداوم تعمیر کنند. با اطمینان از اینکه رایانه و گوشی‌های تلفن همراه شما، از آخرین به‌روزرسانی‌ها استفاده می‌کنند، کار را برای مهاجمین سخت‌تر خواهید کرد. برای این کار، به‌سادگی در اولین زمان ممکن، به‌روزرسانی خودکار برنامه‌ها را فعال کنید.

در این میان به‌روزرسانی دائمی نرم‌افزارهای آنتی‌ویروس و فایروال (Antivirus & Firewall) اهمیتی دوچندان دارد. اگر روی رایانه‌های خود از چنین نرم‌افزارهایی استفاده نمی‌کنید، حتما نصب و راه‌اندازی آن‌ها را در برنامه خود قرار دهید.

Website: www.linkap.net
Email: hi@linkap.net
Tel: +98(21) 41087280
Fax: +98(21) 89778403