امنیت فیزیکی

هرگاه در یک مبحث مربوط به کامپیوتر صحبت از امنیت به میان می‌آید، بسیاری به فکر جلوگیری از نفوذ ویروس‌ها و تروجان‌ها، مقابله با حملات فیشینگ و محافظت‌های نرم افزاری می‌افتند. اما هر مقدار که برای داشتن آنتی ویروس قوی و به روز، فایروال قدرتمند، رمزهای عبور قرص و محکم و برنامه‌های نرم‌افزاری هزینه کنید، باز هم یک سارق می‌تواند در اتاق کامپیوتر و یا شرکت‌تان را باز کرده و از اطلاعات شما کپی برداری کرده و یا سیستم‌های شما را بدزدد! بنابراین آخرین درس این دوره به امنیت فیزیکی اختصاص یافته است تا هیچ وقت این بخش کار را فراموش نکنید. شاید به جرات بتوان گفت که پایه‌ی هر برنامه و طرح حفاظتی، امنیت فیزیکی است. اگر در شرکت قفل و بند درستی نداشته باشد و یا کلید آن در اختیار همه باشد، خرید برنامه‌های امنیتی چند صد هزار تومانی هم دردی را دوا نخواهد کرد.

در این مطلب به برخی نکات ضروری در خصوص امنیت فیزیکی می پردازیم:

۱. از قفل‌های مطمئن داخلی برای درهای ورودی اصلی استفاده کنید

اول از همه باید به فکر زمانی باشیم که در خانه یا محل کار نیستیم. مطمئن هستید که درهای ورودی به اندازه‌ی کافی ایمن هستند و به خوبی بسته می‌شوند؟ بهتر است که در ورودی شرکت یا خانه فلزی باشد. علاوه بر قفل‌های آویز معمولی، آن را به قفل داخلی هم مجهز کنید. این قفل‌ها که به قفل‌های گاوصندوقی هم مشهور هستند، درون در نصب می‌شوند و معمولا دو یا چهار زبانه بلند دارند که داخل لنگه مقابل در چفت می‌شود. حتی اگر بخش آی‌تی و محل قرارگیری کامپیوترهای شما در قسمت مجزایی از محل کارتان است، در ورودی آن را هم به چنین قفلی مجهز کنید تا امکان نفوذ هنگام عدم حضور شما بسیار کاهش یابد.

۲. در اتاق کامپیوتر همیشه قفل باشد

هنگام انتخاب اتاقی برای نگهداری کامپیوتر و تجهیزات شبکه، قبل از توجه به زیبایی و شیک بودن اتاق، ابتدا به در آن توجه کنید. آیا محکم و قابل اطمینان است؟ آیا دارای قفل و بند درست و حسابی است و به خوبی قفل می‌شود؟ حال به عنوان یک قانون برای همه‌ی افرادی که از این اتاق استفاده می‌کنند، همیشه در باید قفل باشد. عادت کنید که حتی هنگام ترک اتاق برای چند دقیقه، در را قفل کنید. شاید سختگیرانه و مشکل به نظر برسد، اما برای یک دزد اطلاعات حرفه‌ای تنها چند دقیقه زمان برای

سرقت یک هارد یا کپی‌برداری از اطلاعات بر روی کول دیسک کافی است. برای اضافه کردن ابزاری به روتر، برای استفاده بعدی و یا نصب کی‌لاگرهای سخت افزاری هم که حتی یک دقیقه زمان زیادی به نظر می رسد.

اتاق کامپیوتر قلب فیزیکی شبکه‌ی کامپیوتری سازمان شما است. یک بدخواه با دست یابی به این اتاق، به راحتی با دستکاری سوییچ ها، روترها، کابل ها و دیگر ابزارها می تواند صدمات سختی را وارد آورد.

۳. یک سیستم نظارت و مراقبت دائمی داشته باشید.

درست است که قفل کردن در، راه کار بسیار مناسبی است اما اگر فردی که اجازه ی ورود و امکان دسترسی داشته باشد و بخواهد دست به خرابکاری بزند، یا فردی با شکستن در و تخریب قفل آن وارد شود، چگونه وی را شناسایی می‌کنید. بهترین راه داشتن یک سیستم کنترل تردد به اتاق است. این سیستم می تواند یک قفل با کارت مغناطیسی یا رمز و شاید یک دستگاه شناسایی هویت بیومتریک باشد. در هر صورت تمامی ورود و خروج ها با درج زمان دقیق ثبت و نگه داری می شوند. اگر امکان چنین هزینه هایی ندارید، یک دوربین ویدیویی نیز می تواند نیاز شما را برطرف کند. یک دوربین کوچک ویدیویی را در محلی که به راحتی قابل دیدن و از کار انداختن نباشد، به گونه ای نصب کنید که تصویر کاملی از ورودی اتاق یا ساختمان ضبط کند. حال شما در موقع لزوم می توانید ورود و خروج های صورت گرفته را کنترل کنید. حتی با کمی هزینه ی بیشتر می توانید از دوربین هایی استفاده کنید که علاوه بر ضبط تصاویر، از طریق ایمیل یا پیام کوتاه شما را خبر کنند.

٤. تمامی ابزارهای در معرض خطر، در محل امنی قرار داشته باشند

ممکن است کامپیوتر مرکزی شرکت خود را در اتاق امنی گذاشته و با رمز عبور قوی و نرم افزارهای لازم از آن مراقبت کنید. اما روتر، هاب، یا سوییچ های شبکه تان در کجا قرار دارند؟ یک هکر به راحتی با یک لپ تاپ و دسترسی به هاب قادر است خسارات شدیدی را به شما وارد کند. تا حد ممکن تمامی ابزارهای شبکه تان را در اتاق های مطمئن و قفل شده قرار دهید. اگر هم امکان چنین کاری را ندارید، حداقل آنها را درون جعبه های محکم و قفل داری قرار دهید که هر کسی نتواند به آنها دسترسی داشته باشد. محیط کاری را فراموش نکنید هکر می تواند از هر ابزار و دستگاه ناامن موجود در محیط کارتان برای نفوذ به شبکه و تخریب و سرقت اطلاعات استفاده کند. اتاق و میز کارمندی که به مرخصی رفته یا اخراج شده و کسی به آنجا سر نمی زند، بهترین طعمه برای یک هکر خبره است. دسترسی کامپیوتر و ابزارهای بلا استفاده به شبکه را قطع کنید و یا آنها را به انباری منتقل کنید. در اتاق های خالی را قفل کنید.

از کارکنان بخواهید حتی وقتی برای نهار بیرون می روند، درها را قفل کنند. اگر در خانه جشن یا برنامه ای دارید که همه ی شرکت کنندگان آن را نمی‌شناسید، حتما در اتاق کامپیوتر قفل شده باشد. استفاده از قفل های سخت افزاری از قبیل قفل پورت USB و شبکه هم فکر خوبی است.

۵. کیس کامپیوترتان را قفل کنید.

وضعیتی را در نظر بگیرید که جناب دزد به هر شکلی که شده به کامپیوتر شما دست پیدا می کند. حال باید به راحتی پیچ های پشت کیس را باز کند و هارد دیسک را بردارد و برود؟ یا اینکه هر بار از اتاق بیرون می روید هارد دیسک را درون جیب تان می گذارید و با خودتان می برید؟ امروزه در پشت همه کیس‌ها جایی برای استفاده از قفل تعبیه شده است. پس با کمی هزینه حتما کیس‌های تان را قفل کنید، تا برای سرقت هارد دیسک به چیزی بیش از یک پیچ گوشتی نیاز باشد.

٦. مراقب ابزارهای پرتابل باشید.

لپ تاپ ها و تبلت ها می تواند خطری بالقوه برای اطلاعات شما باشند. تا حدامکان هیچگونه اطلاعات مهم و حیاتی را بر روی ابزارهای اینچنینی نگهداری نکنید، زیرا حداقل رمز عبور شبکه بی سیم تان بر روی همه ی این ابزارها ذخیره شده است. پس برای لپ تاپ ها حتما کابل های قفل تهیه کنید یا اینکه آنها را درکشو یا کمدی امن نگه دارید یا حتی به عنوان یک روال کاری همه موظف باشند که همیشه ابزارهای شان را به همراه داشته باشند.

۷. نگهداری امن نسخه های پشتیبان

یکی از مهمترین کارهای هر فرد یا شرکتی تهیه ی نسخه های پشتیبان از اطلاعات است. اما محل نگهداری نسخه های پشتیبان هم از اهمیت بالایی برخوردار است. اگر آنها را در همان اتاق کامپیوتر بگذارید که ممکن است به راحتی دزدیده شوند و یا در اتفاقاتی مانند آتش سوزی از بین بروند، کل برنامه ی پشتیبان گیری شما بی مصرف خواهد بود. بهتر است که نسخه ای از بک آپ ها را به صورت رمزگذاری شده و در جای مطمئنی خارج از محل کارتان نگهداری کنید. اگر کارمندان تان هم به بک آپ گیری اطلاعات روی سی دی، کول دیسک یا هارد های اکسترنال عادت دارند، حتما آنها را به گونه ای آموزش دهید که اطلاعات را همیشه به صورت رمزگذاری شده و امن نگه داری کنند.

۸. مراقب دستگاه های کپی و پرینتر باشید.

در نگاه اول یک دستگاه کپی یا پرینتر نمی تواند خطری برای امنیت اطلاعات محسوب شود، اما متاسفانه دستگاه های کپی و پرینت امروزی، نسخه ای از اطلاعات چاپ شده را درون هارد و یا حافظه داخلی خود نگه می دارند. کافی است که فردی این دستگاه را بدزدد و با کمی تلاش به اطلاعات موجود در آن دست یابد تا نسخه ای از مطالب چاپی شما را در دست داشته باشد. بهتر است که این دستگاه ها را تا حد ممکن در اتاق های امن نگه داری کنید و یا آنها را به شکلی نصب کنید که به راحتی قابل حمل و سرقت نباشند. علاوه بر این برگه های چاپ شده توسط این دستگاه ها هم خطر بالقوه دیگری هستند، همیشه نسخه های چاپی هستند که به درد نمی خورند و راهی سطل زباله می شوند. این کپی ها به راحتی قابل سرقت و سوء استفاده هستند. به عنوان یک سیاست کاری حتی کاغذهای معمولی و بی اهمیت را هم به جای سطل زباله، راهی دستگاه کاغذ خرد کن کنید. این باعث می شود که همه به این کار عادت کنند و هیچ کپیِ مهم بی مصرفی به دست افراد سوءاستفاده گر نیافتد.

۹. از سیستم های هشداردهنده استفاده کنید.

قفل های مطمئن و در و پنجره های محکم جلوی ورود سارقان را می گیرند. اما استفاده از یک سیستم هشدار دهنده برای امنیت بیشتر امری ضروری است. اولین کاربرد یک سیستم هشدار دهنده ترساندن و فراری دادن دزدها است. علاوه بر این شما را با خبر می کند که اتفاقی افتاده است. یک سیستم دزدگیر معمولا از تعدادی سنسور حساس به حرکت، سنسور شکست شیشه و یک سیستم کنترل مرکزی تشکیل شده است. پس از اینکه حرکت غیر مجازی تشخیص داده شود، علاوه بر به صدا در آمدن آژیر، دستگاه با شما و پلیس تماس تلفنی برقرار خواهد کرد.

۱۰. مراقب کلیدهایتان باشید

امروزه ابزارهای امنیتی و حفاظتی بسیار پیشرفته ای در اختیار کاربران قرار دارد، ولی با این وجود هنوز همین کلیدهای فلزی کوچک، حفره ی امنیتی بزرگی محسوب می شوند. خانه یا محل کار شما تعداد زیادی در و قفل دارد و همه ی آنها برای باز شدن به کلید نیاز دارند. آیا همه ی افرادی را که این کلیدها را در اختیار دارند می شناسید؟ آیا می دانید که آنها چند کپی از کلیدهای شان دارند؟ کپی کردن یک کلید، کار چندان سختی نیست و تنها کافی است دارنده ی کلید به یک قفل ساز مراجعه کند. حتی یک سارق متبحر می تواند با یک تکه موم یا خمیر بازی طرح کلید را دزدیده و نمونه ای از آن بسازد. استفاده از کلیدهای چهار پهلو

و کلیدهای موسوم به کامپیوتری (که به جای دندانه سوراخ هایی بر روی خود دارند) هم ایده ی خوبی به نظر می رسد. به هر حال کلیدسازانِ کمی قادر به کپی کردن آنها هستند و دزدیدن طرح آنها با خمیر بازی اگر نگوییم غیر ممکن، حداقل خیلی سخت است. پس همیشه مراقب باشید که کلیدها دست چه کسانی هستند و هیچ گاه موضوع یک کلید گم شده را ساده نگیرید. با کم شدن هر کلید هم بهتر است به فکر استفاده از قفل جدید برای آن محل بود.