آشنایی با امنیت اینترنتی و عوامل تهدید کننده آن

تعریف حملات دسترسی: حملاتی هستند که در آنها سعی می شود به منابع و اطلاعات دسترسی غیر مجاز شود. هدف این نوع حملات نقص محرمانگی است. به یاد داشته باشیم کسی که تدارک یک حمله بزرگ را می بیند همیشه نیاز به اطلاعات دارد. پس این نوع حملات می توانند شروع حملات آینده باشند. برای بدست آوردن این اطلاعات لزوما نیازی به عملیات پیچیده جاسوسی و هک سیستم های کامپیوتری نیست. برخی از این حملات به قدری ساده هستند که به راحتی با رعایت موارد ساده امنیتی می توانیم از نشتی اطلاعات جلوگیری کنیم.

آشغالگردی: اولین و آسانترین راه بدست آوردن اطلاعات یک شخص یا یک سازمان گشتن به دنبال کاغذهای پاره، دیسکت و یا سی دی هایی است که به عنوان زباله در آخر وقت اداری بیرون می گذارند. به همین راحتی! یک مثال بانکی بزنیم شاید بهتر پی ببرید. کاغذهایی که پنج شنبه ها بعد از پایان کار شعبه به عنوان زباله بیرون از شعبه می گذاریم حاوی اطلاعات ارزشمندی است: شماره حساب مشتریان، نام آنها، گردش کار آنها، دریافت و پرداختهای آنها و ... . فاش شدن این اطلاعات برای افرادی که نیت سوء دارند می تواند بسیار خطر ساز باشد. اتفاقات بسیاری با دسترسی به این اطلاعات در بانک رخ داده که شاید همکاران با آن آشنا باشند. برای کاهش این خطر بهتر است کاغذ، سی دی و یا دیسکت هایی را که قرار است به عنوان زباله بیرون بگذاریم، حتما به وسیله دستگاه خرد کن و یا بصورت دستی به قطعات ریز تبدیل کنیم. مراقب زباله هایتان این طلای کثیف باشید.

مهندسی اجتماعی: در یک سازمان ممکن است بهترین تجهیزات برای دفاع در برابر نفوذ به شبکه سازمان و کسب اطلاعات خریداری شود، بهترین آنتی ویروس روی سیستم ها نصب شود و هزینه بسیار زیادی برای پشتیبانی امنیتی شبکه پرداخت شود. به طوری که ورود به شبکه بسیار مشکل باشد. حال تصور کنید شخص مهاجم با ایجاد یک رابطه دوستانه و عاطفی با یکی از کارکنان سازمان اقدام به کسب اطلاعات کند. او با این کار عملا توانسته تمام مراقبتهای امنیتی و تجهیزات امنیتی گران قیمت را دور بزند. مهندسی اجتماعی عبارتست از روشهایی که در آن یک فرد با بکار بردن حیله و فریب کارکنان سازمان به کسب اطلاعات سازمان اقدام کند بدون آنکه نیازی به نفوذ در شبکه سازمان داشته باشد.

بهترین روش برای مقابله با این نوع حملات و جلوگیری از افشاء اطلاعات، آموزش همه کارکنان، یاد آوری آن از طریق تکرار هشدارها، ارائه بروشورهایی جذاب در این خصوص و فرهنگ سازی می باشد. علاوه بر آن کنترل حق دسترسی کارکنان به اطلاعات سازمان و همچنین ایجاد روالی در سازمان که بر اساس آن اطلاعات تنها در قبال احراز هویت فرد مقابل داده شود، می تواند در جلوگیری از این نوع حملات موثر باشد.

شنود یا استراق سمع: همه ما با این اصطلاح آشنا هستیم. قدیمی ترین نوع آن همان فالگوش ایستادن است. این حمله در مکالمات تلفنی و تبادل اطلاعات در شبکه های کامپیوتری نیز رخ می دهد. مانند حمله Middle the In Man که در آن یک کامپیوتر سر راه کامپیوترهای فرستنده و گیرنده قرار می گیرد و به کپی برداری از اطلاعات تبادل شده می پردازد. استراق سمع یک نوع حمله غیر فعال است بدین معنی که شخص شنونده به هیچ عنوان سعی در تغییر مکالمه و یا قطع آن نمی کند و تمام تلاش خود را می کند تا طرفین در تبادل اطلاعات از وجودش باخبر نشوند.

بهترین روش برای مقابله و کاهش اثر این نوع حملات، انجام رمزنگاری اطلاعات است. نمونه بسیار ساده رمزنگاری که برای شما ملموس می باشد زبان زرگری است. همان زبانی است که مردم یک آبادی یا یک شهر با آن صحبت می‌کنند ولی کلمات را طوری دستکاری می‌کنند که غیر از خود آن گروه آن را نمی‌فهمند (به نقل از سایت ویکی پدیای فارسی). در امنیت شبکه های کامپیوتری نیز چیزی شبیه به این وجود دارد با این تفاوت که در آنجا از الگوریتمهای رمز مبتنی بر عملیات پیچیده ریاضی استفاده می شود که شکستن رمز و کشف پیام مبادله شده را برای کسی که مشغول شنود اطلاعات است بسیار مشکل و یا حتی غیر ممکن می سازد. راه حل ساده تری نیز وجود دارد: از تبادل اطلاعات محرمانه از طریق کانالهای غیر امن (مانند تلفن و یا اینترنت) پرهیز کنید.

جستجوی مخفیانه کامپیوتری: در این حمله فرد مهاجم فقط در کامپیوتر شما می گردد و هر فایل جالبی که نظرش را جلب کند باز کرده و یک کپی برای خودش بر می دارد. او با جستجو در فایلهایتان ممکن است بداند شغلتان چیست، به چه چیزی علاقه دارید، از طریق مطالعه نامه های شما بفهمد دوستانتان چه کسانی هستند، شماره حساب و رمز حساب بانکی تان را پیدا کند ، اسناد شغلیتان را بدست آورد، و یا به عکسها و فیلمهای خانوادگی شما دست پیدا کند.

برای مقابله با این حمله که امروزه به دلیل گسترش کامپیوترهای شخصی و لپ تاپ ها از پرشمارترین حملات می باشد نکات بیشتری را باید رعایت کنیم. رعایت تمهیدات زیر به شما برای ناکام گذاردن مهاجم کمک زیادی خواهد کرد:

از رمز عبور قوی برای کامپیوترتان استفاده کنید. مهاجمان از حمله ای موسوم به حدس زدن پسورد (Guessing Password) برای دسترسی به اطلاعات کامپیوترتان استفاده می کنند. پس سعی کنید رمزی که انتخاب می کنید ترکیبی از حروف کوچک و بزرگ و اعداد و علائم باشد. در ضمن کلمه عبور بهتر است کمتر از شش حرف نباشد، نام و یا نام خانوادگی، شماره شناسنامه و یا کد ملی نیز نباشد. اگر اطلاعات بسیار حساس در کامپیوترتان وجود دارد توصیه می کنیم با این کامپیوتر به اینترنت وصل نشوید. متاسفانه از آنجا که بسیاری از نرم افزارهای به ظاهر موجه که بر روی کامپیوترها نصب شده اند، قفل شکسته هستند،

دارای لایسنس نمی باشند و هیچ گونه پشتیبانی نیز در کشور ندارند اطمینانی به این گونه نرم افزارها نمی توان داشت. از طرفی این نرم افزارها به صورت کد بسته می باشند (از کدهای برنامه نویسی آن اطلاعی در دست نیست)، بنابراین اگر در بخشی از آن نرم افزار کد جاسوسی تعبیه شده باشد می تواند به راحتی اطلاعات کامپیوترتان را جمع آوری کرده، به یک سایت در خارج از کشور وصل شده و اقدام به ارسال آنها نماید. اگر به خاطر داشته باشید چند سال گذشته دولت آلمان ادعا کرد نرم افزار ویندوز مدیا پلیر که برای پخش فیلم و موسیقی استفاده می شود اقدام به جاسوسی از کامپیوترهای این کشور می کرده است. احتمالا داستان نرم افزار دیکشنری بابیلون را هم شنیده اید.

حتما بر روی کامپیوترتان آنتی ویروس نصب کنید و آن را به روز نگه دارید. سعی کنید نرم افزاری که تهیه می کنید شامل آنتی تروجان و آنتی اسپای نیز باشد. آنتی ویروس های لایسنس دار در ایران نیز یافت می شود. برای آنکه تبلیغ آنها نشود اسامی آنها را ذکر نمی کنیم. علاوه بر آن آنتی ویروسهای مجانی نیز در اینترنت وجود دارد که قابل اطمینان هستند. می توانید آن را دانلود، نصب و آپدیت کنید. آنتی ویروسهای Avira، Avast، Comodo،AVG از سری آنتی ویروسهای معروف و مجانی هستند.