خبرنامه امنیت رایانه ای
کمیته امداد امام خمینی (ره)

سال اول، شماره دوم نیمه اول اردیبهشت ۱۳۸۶

دفتر آمار و فناوری اطلاعات

اخبار امنیت

در هفته های اخیر یکی از بزرگترین مشکلات امنیتی، مربوط به ایراداتی بود که عمدتاً به دلیل نقص در برخی قسمتهای گرافیکی شامل هفت نقص مختلف مثل ایراد در نمایش دهنده مکان نماهای انیمیشنی یا ایرادات در موتور گرافیکی، ویندوز متافایل و مانند آنها، نفوذگرها می توانستند کد دلخواهی را بر روی سیستم قربانی نصب کنند، کنترل کامل سیستم را به دست بگیرند و به دلخواه فایلهای او را ببینند، کپی کنند یا حذف کنند.

این اشکال در انواع ویندوزهای ۲۰۰۰، XP، سرور ۲۰۰۳ و ویستا یافت شده است و عملاً تمام نسخه ها حتی نسخه های ۶۴ بیتی را در معرض خطر قرار داده است. اهمیت این موضوع در حدی است که مایکروسافت اوایل آوریل بولتن ویژه امنیتی را خارج از روال عادی تناوب ارائه بولتنهایش برای این مورد ارسال کرده است.

توصیه می شود در صورتی که به روزرسانی خودکار ویندوز شما به هر دلیل فعال نمی باشد یا رایانه شما به اینترنت متصل نمی باشد در اولین فرصت برای دریافت فایل به روزرسانی از طریق یک رایانه متصل به اینترنت که این مشکل را برطرف می کند به آدرس زیر بروید و برحسب نوع ویندوز خود از لیست فایل مورد نظر را دریافت کنید:

http://www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

پیشنهاد می شود این به روزرسانی را حتماً زیر نظر یک کارشناس اجرا نمایید.

اگر به اینترنت پر سرعت یا دائم دسترسی دارید...

در این شماره هم ضد ویروس رایگان آنلاین دیگری را به شما معرفی می کنیم.

سرویس ActiveScan شرکت پاندا، که از آدرس اینترنتی زیر قابل استفاده است به صورت آنلاین به بررسی و حذف ویروسهای شما می پردازد:

http://pandasoftware.com/activescan

در استفاده از این ضدویروس به خاطر داشته باشید که این نرم افزار انوع تهدیدها را در سطح کاملی مورد بررسی قرار می دهد و به عنوان نمونه علاوه بر ویروسها، سامانه های نمایش دهنده تبلیغ و ابزارهای آنها را هم به عنوان خطر امنیتی شناسایی می کند و خطرهایی که تحت عنوان Cookie نشان می دهد ممکن است اصولاً خطر مهمی نباشند به همین دلیل ات که این برنامه برخی از مشکلاتی که اعلام می کند را به طور خودکار از سیستم شما حذف نمی کند و فقط اخطار می دهد که اغلب این موارد بی خطر هستند.

پیشنهاد می شود این برنامه آنلاین را نیز حتماً زیر نظر یک کارشناس اجرا نمایید.

در مدت اجرای این برنامه، لازم است متصل به اینترنت باقی بمانید.

مهندسی اجتماعی

Social Engineering

مهندسی اجتماعی
Social Engineering

در مباحث امنیت رایانه اصطلاح Social Engineering یا مهندسی اجتماعی، به نفوذهایی اشاره دارد که به جای استفاده از ضعفهای تکنیکی بر استفاده از ارتباطات انسانی و اغلب فریب دادن افراد متکی است. با وجود آنکه در بسیاری از شرکتها و سازمانها اصولی به کارمندان توصیه می شود که تا حدودی جلوی این حملات را بگیرد، آمار ها نشان می دهد افراد این نکات را جدی نمی گیرند و بسیاری از کارمندان و حتی مدیران از اهمیت اطلاعات به ظاهر کوچکی که به راحتی در اختیار نفوذگران قرار می دهند آگاه نیستند.

Social Engineeringچنانکه گفته شد مفهوم گسترده ای است که از دیدن رمز عبور از روی کیبورد هنگامی که فردی آنرا تایپ می کند تا سناریوهای پیچیده ای که روزها بر روی آنها وقت صرف می شود یا حتی جستجو درون زباله های شرکتها و سازمانها را شامل می شود. در نظر سنجی سال ۲۰۰۳ Info security نکته جالب و در عین حال دردناکی مشخص گردید و آن این بود که ۹۰% کارمندان در خارج از ساختمان کار خود، حاضر بودند رمز عبور خود را در پاسخ یکی از سؤالات آمارگیر ارائه کنند تا در انتها یک خودکار به دلیل شرکت در این آمارگیری دریافت کنند!

در سالهای اخیر و با توجهی که معمولاً به امنیت تکنیکی سامانه های رایانه ای از بعد نرم افزار و سخت افزار صورت می گیرد اغلب ساده تر است که فرد را فریب دهند تا به گونه ای اطلاعات لازم برای ورود به سیستم را ناخواسته در اختیارشان قرار دهد تا اینکه تلاش کنند راه نفوذی برای هک از روشهای سنتی پیدا کنند. افرادی که رمز عبور خود را از دست داده اند به نوعی Social Engineering را تجربه کردند و به خوبی می دانیم که تعداد این افراد کم نیست.

روشهای نفوذ با Social Engineering از تنوع گسترده ای برخوردارند ولی این بدان معنی نیست که قابل جلوگیری نیستند. در هنگام تهیه سند امنیت اطلاعات و امنیت رایانه ای هر شرکت یا سازمانی با در نظر قرار دادن این مطلب ضمن ارائه آموزشهای لازم، ساختار ارتباط با افراد مطلع نیز باید به گونه مناسبی چیده شده باشد زیرا بسیاری از حملات مهندسی اجتماعی از طریق تلفن انجام می پذیرند. به عنوان نمونه افراد با تماس تلفنی با مسئول پشتیبانی نرم افزار یا شبکه سعی می کنند با استفاده از احساسات وی اطلاعات مورد نیاز خود را بدست آورند مثلاً با انتقاد ساختگی از سطح امنیت سیستم او را عصبانی می کنند تا روشهای امنیتی که به کار گرفته را با آب و تاب توضیح دهد و یا با تماس گرفتن از طرف کارمندی که مثلاً رمز عبور را گم کرده و رئیسش عصبانی است و عجله دارد.

اگرچه بحث گسترده درباره Social Engineering در این بولتن نمی گنجد، با مروری سریع بر برخی سناریوهای معمول امیدواریم بتوانیم نقشی در افزایش آگاهی عمومی و لذا کاهش آمار هک شدن از این طریق داشته باشیم.

یکی از سناریوهای معمول Social Engineering استفاده از ایمیل است. متأسفانه شما به سادگی می توانید هر ایمیلی را ازطرف هر کسی به هر کس دیگری ارسال کنید. یعنی هر کسی می تواند بدون داشتن رمز عبور ایمیل شما و یا بدون اینکه دسترسی به شما یا اکانت شما داشته باشد یک نامه الکترونیکی از هر جهت به نظر می رسد از طرف شما ارسال شده است را برای فرد دیگری ارسال نماید و از دید کاربران عادی (و حتی کاربران متخصص وقتی عجله دارند یا انگیزه ای برای شک کردن به آن ندارند) به هیچ عنوان بدلی بودن ایمیل قابل تشخیص نخواهد بود. حال ممکن است

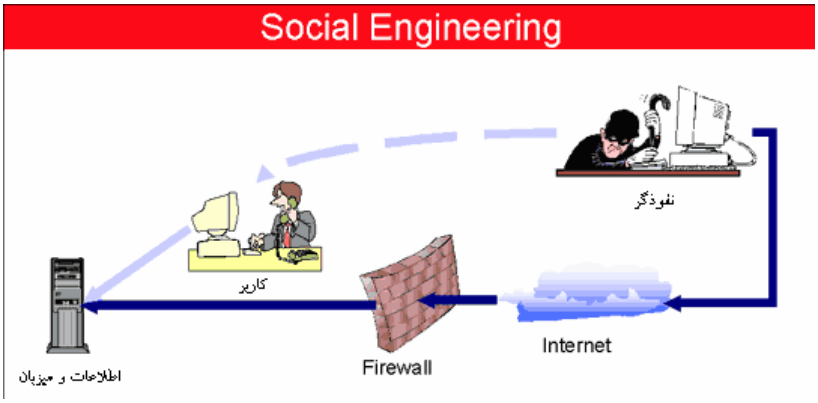
Social Engineering

با استفاده از نکته فوق و یا حتی بدون استفاده از آن به چندین طریق برای بدست آوردن اطلاعات شخصی یا رمزهای عبور از طریق ایمیل اقدام کنند. یک راه لینکی است که به شکلی شمار را به کلیک روی آن ترغیب کرده اند مثلاً خبر یا تصویری جالب را قرار است آنجا ملاحظه نمایید. اگر شما روی لینک کلیک کنید ممکن است صفحه ای باز شود که با استفاده از نواقص ویندوز که شما هنوز به روز رسانی مربوط به آنرا نصب نکرده اید بر روی سیستم شما برنامه ای جهت ربودن رمزهای عبور یا اعطای دسترسی از راه دور نصب کند و یا به سادگی صفحه ای باشد که از شما اطلاعات Login بخواهد مثلاً صفحه ای با ظاهر شبیه صفحه ورود به ایمیل شما باز شود و شما هم بدون دقت اطلاعات خود را در آن صفحه که متعلق به فرد نفوذگر است وارد کنید و به این صورت رمز خود را دو دستی تقدیم وی نمایید که از بهترین راههای جلوگیری از بروز این مشکل عدم ورود رمز در صفحه ای که پس از کلیک بر لینک باز می شود (مثلاً اگر صفحه ای شبیه به ورود به ایمیل شما آمد، آنرا ببندید و از ابتدا اکسپلورر دیگری باز کنید و آدرس صفحه ورود به وبلاگتان را در آن وارد کنید) و یا تکنیک کمکی برخی سایتها مانند یاهو است که احتمالاً دیده اید مدتی است که می توانید عکس یا نوشته ای را به یاهو بدهید تا روی کامپیوتر شما کنار صفحه Login آنرا نمایش دهد. تا زمانی که فرد نفوذگر ندانند شما چه تصویر یا نوشته ای را مورد استفاده قرار داده اید، اگر صفحه شبیه به صفحه ورود به یاهو بسازد، نبودن نوشته یا تصویر شما سبب می شود شما متوجه شوید در سایت یاهو نیستید و رمز خود را وارد نخواهید کرد. در مورد جالبی اخیراً یک فرد نفوذگر پس از آنکه تلفنی با فردی در قسمت مناسبی از سازمانی ارتباط گرفته بود، ضمن رفع اشکال فنی خود به وی گفت که ماشین خود را به قیمت بسیار خوبی برا ی فروش گذاشته است و بدین شکل آدرس ایمیل او را گرفت تا عکس ماشین را برایش ارسال کند که البته همراه با آن اسب تروایی هم ارسال کرده بود تا از آن طریق با تحت کنترل گرفتن رایانه وی به راحتی اعمال نفوذگرانه خود را انجام دهد. در مورد اسب تروا که آنرا را هم می توان یکی از روشهای Social Engineering به حساب آورد در شماره های آینده خواهیم نوشت.

در بسیاری از موارد Social Engineering شامل جمع آوری ذره ذره اطلاعات و استفاده از اطلاعات قبلی برای بدست آوردن اطلاعات جدید است. به عنوان نمونه ممکن است فرد نفوذگر ابتدا با مراجعه به وبسایت مجموعه ای که قصد نفوذ به آنرا دارد اسامی برخی از مدیران و یا کارمندان را به دست آورد و سپس با تماسهای تلفنی اتفاقی با آنها از منشی یا کارمندان اطلاعاتی مانند اینکه چه روز و ساعتی آنجا هستند یا نیستند و وقتی نیستند چه کسی مسئولیتشان را بر عهده دارد و.... را به دست آورد و از آن اطلاعات در ارتباطات ایمیلی، تلفنی و یا حتی حضوری استفاده کند.

هنگامی که فردی با لباسهای بسیار شیک و ظاهری آراسته و اعتماد به نفس و روابط عمومی بالا وارد مجموعه ای می شود معمولاً برایش بسیار ساده است که با استفاده از اطلاعات کمی که از قبل دارد اطلاعات بیشتری به دست آورد و یا حتی به نزدیک رایانه ها هدایت شود به ویژه در بسیاری از سازمانها و شرکتهای بسیار بزرگ، آمدن فردی از پایتخت در شعبات شهرستانها با مشخصات فوق که ادعا می کند از شعبه مرکزی برای بازرسی یا رفع مشکلی در نرم افزار اصلی و مانند آنها آمده است اغلب باعث می شود به راحتی به وی اجازه دسترسی به شبکه و رایانه ها را بدهند یا خصوصیات و تکنیکهای امنیتی به کار گرفته شده را برایش شرح دهند و یا اگر مشکلی در کار با نرم افزار ها یا شبکه شان داشته باشند از او بخواهند در حل آن کمکشان کند و از این طریق به او دسترسی بدهند.

از روشهای ساده ای که شاید شما هم چند نمونه از آن را دیده باشید ارسال ایمیلهایی بود که مثلاً ادعا می کردند قرار است سرویسی که شما از آن استفاده می کنید قطع شود یا اگر رایگان بوده است پولی شود و یا شما را می ترساندند که کسی از اکانت شما استفاده نابجایی کرده است و شما برای حل آن مشکل باید روی لینکی کلیک کنید



یا به آدرسی ایمیل بزنید و در آن رمز خود را بنویسید که بدیهی است در اینجا هم هدف سوق دادن شما به سمت ارسال داوطلبانه رمزتان برای او بوده است. مورد مشابهی که حدوداً شش سال پیش به عنوان ایده ای قدیمی مورد بررسی قرار دادیم و به نظر می رسد که هنوز هم قدیمی نشده است استفاده از آدرسهایی مثل Auto_pass_sender@yahoo.com یا مشابه آنهاست که در این تکنیک هم عملاً از فرد درخواست می شود که خود رمز عبور خود را هدیه کند یعنی مثلاً ادعا می شود با ارسال ایمیلی با ساختار خاص به آدرس یاد شده می توان رمز آدسهای دیگر را به دست آورد و در ساختار ایمیل ارسالی در قسمتی باید رمز خود را بنویسد.

نلسون در مقاله ای در بررسی روش "Social Engineering معکوس" که یکی دیگر از روشهای نفوذ به این طریقه است آنرا شامل سه مرحله تخریب، تبلیغ و کمک می داند به عنوان نمنه فرد نفوذگر ایرادی در داخل شبکه شما ایجاد می کند و سپس به طریقی شما را به ایم باور می رساند که برای رفع مشکلی که در شبکه شما پیش آمده است به او مراجعه کنید سپس به شما در رفع این مشکل کمک می کند و در این میان اطلاعاتی را که نیاز دارد می رباید. شما ممکن است که هرگز متوجه نشوید و را فردی بدانید که رفع مشکلات به شما کمک کرده است. تکنیک مشابه دیگری که ممکن است به کار گرفته شود شامل تماس گرفتن اتفاقی با شماره های بخشهای مختلف سازمان یا شرکت و اداعای اینکه «از بخش فنی تماس گرفته اند تا مطمئن شوند مشکلی وجود ندارد» می باشد. معمولاً در یکی از بخش مشکلی وجود دارد و از تماس فرد بسیار استقبال می کند. چون فرد با رایانه آشنایی کاملی ندارد، نفوذگر ضمن راهنمایی هایی که برای رفع مشکل به او می دهد کارها یا اطلاعاتی را از او می خواهد که منجر به ایجاد دسترسی وی به اطلاعات شود.

در انتها جمله ای از کوین میتنیک را نقل به مضمون می کنم که نوشته است: «ممکن است شما میلیون ها تومان خرج تکنولوژیها و سرویسهای امنیت شبکه کرده باشید اما ساختار شما هنوز در برابر روشهای قدیمی آسیب پذیر باشد» امیدوارم با آنچه در این بولتن خواندید و با نگاهی جدید به مقوله امنیت بطور همه جانبه آنرا مورد بررسی قرار دهید. به یاری خدا به زودی سمینارها و جلسات آموزشی مناسبی به طور جداگانه برای مدیران، کارشناسان IT و سایر کاربران جهت فرهنگ سازی و آموزشهای ساده و کاربردی برگزار خواهد شد.

تهیه شده در دفتر آمار و فناوری اطلاعات
با همکاری شرکت گسترش فناوری اطلاعات و ارتباطات خاورمیانه
نگارش و مشاوره علمی: احسان ریاضی اصفهانی