بسم الله الرحمن الرحیم

برنامه افزایش آگاهی در برابر تهدیدات سایبری (مخصوص کاربران نهایی)

Cyber Awareness Program

Mohammad Ezzatzadeh
https://www.github.com/pakoti

درباره نویسنده

یک برنامه نویس علاقه مند به امنیت و همچنین نویسندگی !

درباره این برنامه

این برنامه را در جهت افزایش آگاهی کاربران شبکه های سازمانی نوشته شده است تا از خطرات و تهدیدات و همچنین راه های مقابله با آن آشنا باشند تا بردار تهدیداتی که از سمت کاربران خود شبکه های سازمانی میاد به حداقل ترین اندازه ممکن برسد.شاید بتوان ادعا کرد که بزرگترین تهدید ایمن ترین شبکه های سازمانی در جهان همین تهدیدی است که از سمت خود کاربران شبکه می اید.

چکیده

امروزه بزرگترین بردار تهدید شبکه های ایمن شده کاربران نهایی هستند که آموزش های لازم را دریافت نکرده اند یا این که آموزش دیده اند ولی دقیقا نمی دانند که چرا این اقدامات (حتی به ظاهر سخت گیرانه) توسط مدیران شبکه گوشزد می شود.در این سند چرایی این اقدامات به صورت خیلی ساده برای کاربران نهایی اموزش خواهد داده شد.

اهداف

1. افزایش آگاهی کاربران نهایی در برابر تهدیدات و کاهش بردار تهدیدات سازمانی
2. مدیریت بهتر حوادث امنیتی

مهم ترین بردار تهدیدات امنیت سازمان

بردار تهدیدات شبکه های سازمانی بسیار زیاد و پیچیده هستند اما آنهایی که از سمت کاربر نهایی داخل سازمان می آیند محدود به این ها می شود:

- مهندسی اجتماعی و ایمیل های فیشینگ
- احراز هویت دو مرحله ایی و مدیریت رمز
- بدافزار ها
- تهدیدات درون سازمانی
- شاخص های نفوذ به شبکه
- امنیت دستگاه های همراه

برای هر کدام از این تهدیدات باید کاربران نهایی آموزشات لازم رو ببینند و به طور کل اکثر تهدیدات از نوع خارج نیستند.

مهندسی اجتماعی و ایمیل های فیشینگ

این عبارت رو حتما زیاد شنیدید,اگر بخواهم خیلی ساده این رو توضیح بدهم می شود: "که یعنی چه طوری میشه یه نفر گول زد تا کاری می خوام رو انجام بده برام!".مثلا اگر شنیده باشید چه طور عده ایی با شما تماس می گیرند و وانمود می کنند که از طرف رادیو و یا حتی صدا سیما هستید و شما برنده فلان قدر جایزه شده اید و برای دریافت جایزه باید مبلغ ناچیزی رو برای یه حساب شخصی کسی واریز بکنید.قسمت عجیب این ماجرا این هستش که چرا باید رادیو یا صدا سیما از ما بخواهند که برای یک حساب شخصی پول واریز تا جایزه برای ما ارسال کنند؟

این قسمت جالب مهندسی اجتماعی که کلا بر بنای تظاهر به اعتبار ساخته شده است.حالا این چه طور می تواند برای شما به عنوان کاربر نهایی خطرساز باشد؟

بیایم با هم یه سناریویی را بررسی کنیم:

شما در واحد فنی و تعمیرات مشغول هستید.ایمیل سازمانی برای شما در نظر گرفته شده است.ایمیلی رو شما دریافت می کنید در حساب ایمیل خارج از شرکت (مثلا جیمیل) دریافت می کنید که بخش IT سازمان از شما درخواست می کند که هر چه زودتر وارد این لینک بشوید و حساب و رمز ایمیلتون وارد کنید تا ایمیل مهمی را که از سمت سازمان اومده را بخوانید.شما وارد لینک می شوید و تمامممم .....

الان فرد مهاجم با تظاهر به این که از سمت شرکتی که شما در ان کار می کنید ,حساب و رمز شما را دارد و حتما وارد ایمیل سازمانی شما می شود.

این جور حملات برای هر کسی ممکنه اتفاق بیفتد,در صورتی که این جور ایمیلی رو دریافت کردید به واحد IT سازمانتون اطلاع بدید.همچنین رعایت این موارد هم ضروری است:

1.منبع ایمیل های دریافتی به دقت بررسی شود

2.از فرستادن رمز و اطلاعات حساب بانکی برای دیگران در بستر ایمیل و حتی تلفن همراه خودداری شود

3.از باز کردن لینک ها و ضمیمه های ایمیل های ناشناس خودداری شود.

4.در صورت فرستادن ایمیل به شخص دیگر حتما آدرس ایمیل به دقت بررسی شود.

مدیریت رمز و احراز هویت دو مرحله ایی

امروزه رمزها جای کلید و قفل رو تا حدی در زندگی روزمره ما گرفتند.از رمز دوم بانکی تا رمز ایمیل و حساب کاربری سایت ها و ... .

در چند کار ساده می شود خلاصه کرد:

1.رمز را در کاغذ در کنار مانیتور و ... در معرض دید بگذاریم

2.رمزهای حساب های مهم را دوره ایی عوض کنیم

3.احراز هویت دو مرحله ایی را برای ایمیل فعال کنیم

4.هیچ وقت رمزهای حساب هایمان را با دیگر همکاران در میان نگذاریم

بدافزارها

اگر بخواهیم از بدافزار ها صحبت کنیم میشود کتاب ها نوشت و ... .ولی خیلی خلاصه عرض کنم خدمت شما.بدافزارها تو این چند طبقه تقسیم می شوند و گاها همه انها را شامل می شوند:

1.کرم (Worm)

2.ویروس (Virus)

3.باج افزار(Ransomware)

4.تبلیغ افزار(Adware)

5.جاسوس افزار(Spyware)

6.تروجان (Trojan)

7. ...

این لیست ادامه دارد ولی برای سادگی مطالب به همین مقدار کافی است.به صورت خیلی مختصر برای شما شرح داده خواهد شد که هر کدام به چه شکل کار انجام می دهد.

1. کرم‌ها: برنامه‌های خودتکثیری که نسخه‌هایی از خود را از رایانه‌ای به رایانه دیگر بدون نیاز به عمل انسانی پخش می‌کنند. آنها پهنای باند و منابع سیستم را در حین انتشار مصرف می کنند و به طور بالقوه باعث ازدحام و کندی شبکه می شوند.

2. ویروس ها: مانند کرم ها، ویروس ها نیز خود را تکثیر می کنند و فایل ها یا برنامه های کاربردی را در کامپیوتر میزبان آلوده می کنند. با این حال، برخلاف کرم‌ها، ویروس‌ها معمولاً برای فعال شدن و انتشار به تعامل انسانی نیاز دارند - مانند باز کردن پیوست ایمیل یا دانلود یک فایل آلوده.

3. باج افزار: بدافزاری که فایل ها را رمزگذاری می کند یا رایانه را قفل می کند تا زمانی که قربانی برای باز کردن قفل آن باج بپردازد. اغلب از آسیب‌پذیری‌ها در نرم‌افزارهای قدیمی سوء استفاده می‌کند یا از طریق تکنیک‌های مهندسی اجتماعی مانند ایمیل‌های فیشینگ، وارد می‌شود.

4. Adware: نرم افزار طراحی شده برای نمایش تبلیغات ناخواسته، معمولا در یک برنامه یا پنجره مرورگر. برخی از ابزارهای تبلیغاتی مزاحم مشروع هستند، اما برخی دیگر از تاکتیک های فریبنده

برای نصب مخفیانه خود استفاده می کنند، کاربران را با پنجره های بازشو(پاپ اپ) مزاحم بمباران می کنند یا حتی صفحات اصلی مرورگر را تغییر می دهند.

5. نرم افزارهای جاسوسی: نرم افزار نظارتی که فعالیت آنلاین، فشردن دکمه های کیبورد، رمز عبور یا اطلاعات شخصی کاربر را کنترل می کند. مانند بسیاری دیگر از بدافزارها، نرم افزارهای جاسوسی اغلب حضور خود را پنهان می کنند و تشخیص را دشوار می کنند.

6. تروجان‌ها: برنامه‌های مخربی که به عنوان نرم‌افزارهای خوش‌خیم پنهان می‌شوند و به عنوان چیزی مفید یا جالب برای فریب قربانیان برای نصب آنها ظاهر می‌شوند. پس از نصب، تروجان‌ها می‌توانند داده‌های حساس را بدزدند، فایل‌ها را خراب کنند یا به هکرها دسترسی از راه دور را برای به خطر انداختن سیستم‌های بیشتر در همان شبکه ارائه دهند.

این دسته‌ها متقابلاً انحصاری نیستند و بدافزار مدرن اغلب ویژگی‌ها یا رفتارهای متعددی را از یک یا چند کلاس ترکیب می‌کند. راه حل های آنتی ویروس از امضاها، تجزیه و تحلیل رفتار و مدل های یادگیری ماشین برای شناسایی و خنثی کردن تهدیدات استفاده می کنند. به روز نگه داشتن نرم افزار امنیتی شما برای محافظت در برابر حملات سایبری در حال تکامل بسیار مهم است.

تهدیدات درون سازمانی

این شکل تهدیدات شکل انسانی تر دارند و عملا توسط خود کارمندان انجام می شود. مثلا آلوده کردن عمدی دستگاه ها و یا از بین بردن عمدی داده های شرکت و یا حتی افشای اطلاعات سازمانی.این شکل از تهدیدات هم قابلیت این را دارند که از سدهای مهم دفاعی بگذرند و می تواند عملا تمام زحمات مدیران شبکه های سازمانی یک شبه از بین ببرند.

بررسی چگونگی پاسخ دادن به این شکل از تهدیدات بسیار طولانی می باشد.فقط می شود به همین نکته بسنده کرد که این شکل از تهدیدات هم قابل شناسایی اند و هم قابل پاسخ هستند.

برای مقابله با نوع تهدید شما به عنوان کاربر نهایی این چند مورد را رعایت بکنید:

1.رمز سیستم تان در اختیار کسی قرار ندهید.

2.بدون اجازه کسی وارد سیستم شخصی آنها نشوید.

3.از کسی درخواست رمز نکنید و به کسی رمز خودتان را ندهید.

4.در صورت دیدن هرگونه فعالیت مشکوک اطلاع بدید.

شاخص های نفوذ به شبکه

وقتی اولین بار که وارد حساب کاربری خود در شبکه سازمانی می شود و چیزی که می بینید جز یک تصویر پیش زمینه سیاه یا قرمز هستید یا این که کامپیوتر شما بیش از حد کنده یا خیلی ناگهانی برنامه ها در سیستم شما باز و بسته می شوند ...

این نشانه ها ممکن نشان دهنده نفوذ به سامانه شما باشه!

در این صورت کافیه فقط به واحد IT سازمان تان اطلاع بدهید!

امنیت دستگاه های همراه

امروزه دستگاه های تلفن همراه و تبلت و ... جز جدا نشدنی سازمانها شده اند.تقریبا تمامی موارد امنیتی که برای سیستم های رومیزی و لب تاب هست برای این جور دستگاه ها هم صدق می کنند.چندین نکته است که علاوه بر این نکات باید رعایت شود.مثلا :

1.رمز وای فای شبکه سازمانی رو در طریق کسی قرار ندهید.

2.برنامه ها رو از منابع نامشخص و نا معتبر دانلود نکنید.

3.سیستم تون به روز نگه دارید.

خلاصه مطالب

تمامی موارد را می شود در این جملات خلاصه کرد:

- منبع ایمیل های دریافتی به دقت بررسی شود.
- از فرستادن رمز و اطلاعات حساب بانکی برای دیگران در بستر ایمیل و حتی تلفن همراه خودداری شود
- از باز کردن لینک ها و ضمیمه های ایمیل های ناشناس خودداری شود.
- رمزهای حساب های مهم را دوره ایی عوض کنیم.
- رمز را در کاغذ در کنار مانیتور و ... در معرض دید بگذاریم.
- احراز هویت دو مرحله ایی را برای ایمیل فعال کنیم.
- هیچ وقت رمزهای حساب هایمان را با دیگر همکاران در میان نگذاریم.
- در صورت فرستادن ایمیل به شخص دیگر حتما آدرس ایمیل به دقت بررسی شود.
- از کسی درخواست رمز نکنید و به کسی رمز خودتان را ندهید.
- بدون اجازه کسی وارد سیستم شخصی آنها نشوید.
- رمز سیستم تان در اختیار کسی قرار ندهید.
- از کسی درخواست رمز نکنید و به کسی رمز خودتان را ندهید
- سیستم تون به روز نگه دارید.
- سیستم تون به روز نگه دارید.(تلفن همراه,لب تاب, ...).
- برنامه ها رو از منابع نامشخص و نا معتبر دانلود نکنید.
- رمز وای فای شبکه سازمانی رو در طریق کسی قرار ندهید.
- در صورت دیدن هرگونه فعالیت مشکوک اطلاع بدید.

کلام آخر

در این دوره سعی شده بود که در کم ترین زمان ممکن و در خلاصه ترین روش انواع تهدیدات شرح داده شود و همچنین بتوان راه های مقابله با آن آموزش داده شود.

شما در آخرین دوره آموزشی تقریبا از بزرگترین تهدیدات که شما به عنوان کاربر نهایی با ان روبرو می شوید در این دوره اشنا شدید.تنها چیزی که الان باید نگران آن بود این که بتوانید این کارها رو وارد فرهنگ کاری خودتون بکنید.