وزارت ترانسپورت

ریاست عمومی اداره تنظیم منابع

ریاست تکنالوژی معلوماتی

آمریت شبکه

چپتر آموزشی امنیت سایبری

مقدمه

تهدیدهای سایبری پدیده ای جدید است که در دهه های اخیر، همزمان با تحول فن آوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیدا کرده است، به گونه ای که امروزه چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظرمی رسد ولی ما باید در مقابل آن باید امنیت سایبری خوب داشته باشیم.

محتوا:

فصل اول

مفهوم امنیت سایبری(Cyber Security):

امنیت سایبری عملی است که از سیستم ها،شبکه ها وبرنامه ها در برابر حملاتی الکترونیکی محافظت می کند.این حملاتی سایبری معمولا به هدف دستیابی ،تغیر یا از بین بردن اطلاعات حساس انجام میشود.

شکل 1-1 (Cyber security)

امنیت کمپیوتر(Computer security):

یکی از موضوعات مهم در جامعه امروزی مصئون نگهداشتن معلومات درسیستم کمپیوتر است .زیرا معلومات که در سیستم کمپیوتر ذخیره میشود به مثابه سرمایه است بنابر این لازم است تا معلومات محرم خود را از دسترسی اشخاص غیرمجاز محفوظ نگهداریم تا سبب تغیر, تخریب , افشا و از بین بردن معلومات نگردند.امنیت کمپیوتر معمولا به دو دسته کلی امنیت فزیکی و نرم افزاری تقسیم بندی می گردند.

امنیت فزیکی(physical Security)

خطرات فزیکی شامل مواردی ذیل میشود.

- سرقت کمپیوتر
- شرایط نامساعدجوی که سبب از بین بردن اطلاعات میشود.
- حوادث غیرمترقبه مثل آتش سوزی.

نکاتی که برای امنیت فزیکی باید در نظر گرفته شود.

- از قفل های مطمئن داخلی برای درهای ورودی اصلی استفاده کنید.
- در اتاق کامپیوتر همیشه قفل باشد.
- یک سیستم نظارت و مراقبت دائمی داشته باشید.
- تمامی ابزارهای در معرض خطر، در محل امنی قرار داشته باشند.

شکل 1-2 (Physical security)

امنیت نرم افزاری(Logical Security)

نه تنها معلومات که در کمپیوتر شخصی ذخیره میشود بلکه تمام معلومات ما که درسایت های اجتماعی وانترنتی حفظ میشود باید مصئون و محفوظ باشد. پس لازم است که در مورد خطرات که معلومات را تهدید میکند آگاهی حاصل نماییم. که این خطرات بنام Malicious Softwareیا پروگرام های تخریبی یاد میشود.

سافت ویر های تخریبی (Malicious Software):

مجموعه بعضی سافت ویر های که به سیستم کمپیوتر ضرر میرساند.

مانند:

1. Trojan Horse
2. Phishing
3. Virus
4. Spam

شکل 1-3 (Malicious Software)

تورجن هورس(Trojan Horse):

این نوع وایرس خود را با پروگرام دیگر ضمیمه میسازد و ظاهراً پروگرام فعال ومفید به نظر میرسد اما در عقب به هر هدف که دارد آنرا انجام میدهد اطلاعات و بعضا کنترول سیستم را در اختیار فرد سوم(هکر)قرار میدهد. به سادگی از طریق یک وب سایت یا یک دانلود آلوده میتوانند وارد سیستم شود.

شکل 1-4 (Trojan Horse)

فیشینگ(Phishing)

کلمه فیشینگ از عبارت Password Harvesting Fishing که به معنی بدست آوردن پاسورد است گرفته شده است. این حملات به اساس Social engineering صورت میگیرد که با فریب دادن یک استفاده کننده و یا گروهی از استفاده کننده گان به هدف به دست آوردن معلومات استفاده کننده مانند پاسورد حساب بانکی ، معلومات شخصی و اجتماعی وغیره میباشد.

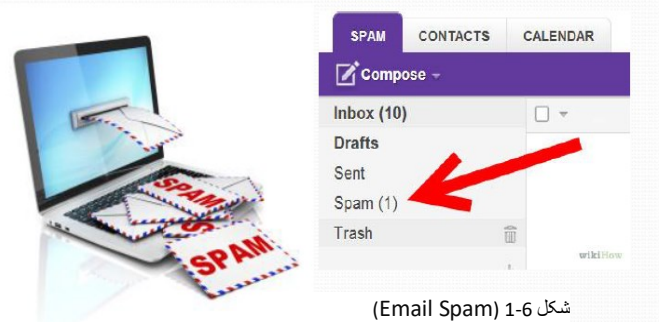
هکر با استفاده از یکی از این چهار طرق حمله فیشینگ را انجام میدهد.

1. Harvesting:
یعنی هکر به استفاده کننده یک لنیک را میفرستد ، با کلیک بالای آن استفاده کننده را به صفحه جعلی راجع میکند و از استفاده کننده نام و پاسورد خواسته میشود.
2. Malicious Link:لنیک های مشکوک
3. Malicious Attachment یعنی فایل های مشکوک
4. Email phishing:
در این نوع حمله ، حمله کننده یک ایمیل را با محتوای تقلبی مثلاً کاپی یک ایمیل رسمی را به استفاده کننده ارسال میکند.

شکل 1-5 (Phishing)

Email spam:

Email Spam که بنام ایمیل ناخواسته نیزنامیده میشود، عمل ارسال پیامهای ایمیلی بدون درخواست و بطور مکرر با محتوای تجارتی میباشد. این نوع وایرس با صفحات انترنتی خود را ضمیمه میکند و بدون آگاهی ما خود را وارد کمپیوتر میسازد.این نوع وایرس اکثراً اعلانات تجارتی یا بعضی اعلانات دیگر را که هیچ مهم نیست میفرستد که سبب ضایع ساختن وقت استفاده کننده میشود. این نوع وایرس حملات DOS (Denial of Services) را در کمپیوتر ها انجام میدهد یعنی خدمات کمپیوتر را متوقف میسازد.



شکل 1-6 (Email Spam)

طریقه انتقال وایروس:

به سه طریق انتشار می یابد.

1. Removable Media (flash Mobiles, External HD, etc.....)
   از طریق USB های دیسک های بیرونی مثل فلش ،هاردیسک وغیره.
2. From downloads off the Internet
   از طریق انترنت هنگام که دانلود صورت می گیرد.
3. From e-mail attachments
   لنیک های که از طریق email می آید.

شکل 1-7 (Media)

علایم آلوده یک کمپیوتر به وایروس:

- کامپیوتر آهسته و کند تر از حد معمول کار میکند .
- هنگام اجرای سافت ویر ها ، آنها هیچ عکس العملی نشان نمی دهند ویا مرتباً سیستم توقف می کند.
- کامپیوتر شما خودبخود Restart می شود و عملکرد معمولی ندارد.
- سافت ویرهایی که نصب کردید بخوبی کار نمی کنند.
- هیچ آنتی وایروسی را نمی توانید بر روی سیستم خود نصب کنید و یا نمی توانید آنرا اجرا کنید.
- Icons بر روی دسکتاپ شما ظاهر شده که شما آنرا بر روی دسکتاپ کامپیوتر خودتان قرار نداده بودید و یا Icons در کامپیورتان ایجاد شده که با هیچ نرم افزاری قادر به اجرا کردن آنها نمی باشید.

شکل 1-8 (Virus)

طریقه جلوگیری حملات وایروس :

اقدامات بسیار زیادی وجود دارد که با انجام رعایت اصول آنها، می توان از هر آسیب و حمله اطلاعاتی (نرم افزاری) به کمپیوتر ها جلوگیری کرد. از مهمترین این اقدامات می توان به موارد ذیل اشاره نمود:

- نصب انتی وایروس سافت ویر (Antivirus Software's)
- آپدیت کردن انتی وایروس سافت ویر (Antivirus should be updated)
- آپدیت کردن فایروال (Using Firewall)
- آپدیت کردن سیستم عامل (Update Operating System)
- تهیه نسخه بکاپ از اصلاعات وفایل های ضروری(Backup)
- نصب سافت ویر های مطمئن (Software installation reliable resource)
- جلوگیری از رفتن به سایت های غیر مجاز(unreliable websites)

استفاده از رمز عبور قوی (strong password)

استفاده از رمزهای عبور با امنیت بالا و ترکیبی از حروف بزرگ ، کوچک وعلایم استفاده از رمز عبور های طولانی (More 8 character)

شکل 8-1 (strong password)

امنیت تلیفون همراه:

امروزه ارتباطات و تبادیله اطلاعات از طریق تیلیفون ها ی هوشمند صورت می گیرید. پس اگر تیلیفون هوشمند هک شود دردسرهای خود را دارد براین اساس باید همواره نکات امنیتی را رعایت کرده و نحوه نگهداری اطلاعات تیلیفون هوشمند نوین را بیاموزیم چرا که این آموزش برای همه لازم و ضروری است.

تمام امکانات امنیتی که برای کمپیوتر ها ذکر می‌شود، تقریباً برای تیلیفون های همراه هم کاربرد دارد. بیشتر تیلیفون های همراه از سیستم‌های‌عامل مخصوص استفاده می‌کنند و تقریبا فارمت بیشتر فایل‌های کمپیوتری را تشخیص می‌دهند. بنابراین برخی ویروس‌ها و بدافزارها نیز در تیلیفون‌های همراه نفوذ می‌کنند. دقت در انتقال فایل‌های کمپیوتری و استفاده از آنتی ویروس‌های مخصوص موبایل برای در امان ماندن از آسیب‌ها و تهدیدها را باید جدی گرفت که به نکاتی چند در این مورد اشاره می شود.

1) گوشی‌های تیلیفون‌همراه مجهز به امکانات ارتباطی متنوعی مثل Wi-Fi ، Bluetooth، hotspot، Mobile data هستند. در هنگامی که از این امکانات ارتباطی استفاده نمی‌کنید، آنها را غیرفعال کنید. مجرمان قادر هستند تا با هک و نفوذ به تیلیفون شما، اختیار آن را در دست گرفته، ضمن برقراری تماس‌های تیلیفونی به حساب شما، اطلاعات و محتواهای درون گوشی شما را به سرقت ببرند.

2) طلاعات محرمانه، عکس، ویدئو شخصی و خانوادگی خود را برروی تیلیفون خود نگهداری نکنید. در هنگام خرابی تیلیفون‌همراه خود، حتی الامکان پس از تخلیه کامل اطلاعات و محتواهای موجود در آن برای تعمیر به تعمیر کاران مجرب و قابل اعتماد مراجعه کنید.

3) احتمال گم شدن یا به سرقت رفتن تیلیفون‌های‌همراه، بیشتر از سایر ابزارهای کمپیوتری است. از این رو، اطلاعات و محتواهای ذخیره شده در آن، در معرض خطر و آسیب های جدی ناشی از دسترسی سارق به آن ها قرار دارد.

4) تیلیفون‌های‌همراه دارای قابلیت‌هایی هستند که می‌توانند به عنوان ابزارهای جاسوسی مورد استفاده قرار بگیرند. بنابراین در اماکن مهم و حساس، به توصیه‌های امنیتی مبنی بر عدم استفاده از تیلیفون‌های همراه توجه کنید.

5) به پیغام‌های دریافتی از طریق پیام و ایمیل که به شیوه‌های مختلف مثل اعلام برنده شدن شما در مسابقات و قرعه کشی‌ها، امور خیریه و مواردی از این دست، اطلاعات کارت بانکی شما را درخواست می‌کنند، اعتماد نکرده و به آنها پاسخ ندهید.

6) موقعیت یاب جهانی Gps را فقط در مکان‌هایی که به آن نیاز دارید روشن کنید. مراقب اپلیکیشن هایی که نصب می‌کنید، باشید.

7) همیشه از کود امنیتی استفاده کنید.

8) از اطلاعات خود نسخه بکاپ تهیه کنید. اطلاعاتی را که یک اپلیکیشن می‌تواند به آن‌ها دسترسی داشته باشد، کنترل کنید، سیستم‌عامل گوشی خود را آپدیت کنید و وایرلس و بلوتوث را خاموش کنید.

شکل 9-1 (secure password phone)

فصل دوم

Virtual Private Network

وی پی ان یا Virtual Private Network به معنای شبکه مجازی اختصاصی نیز شناخته می شود و همواره یکی از مهم ترین ابزارهای برقراری ارتباط در یک شبکه می باشد. در واقع شما با استفاده از یک VPN می توانید یک محیط شبکه را به صورت کامل خصوصی سازی کنید و کنترل دقیق تری را بر روی عملکرد داشته باشید. با تعریف VPN در یک شبکه می توانید دسترسی ها را به صورت اصولی تر محدود کنید و همچنین برخی از محدودیت هایی را اعمال کنید که صرفا متعلق به این ابزار می باشد (مانند کاهش یا افزایش سرعت برای برخی از استفاده کننده ها).

انواع VPN

- Legal VPN
- Free VPN

Legal VPN:

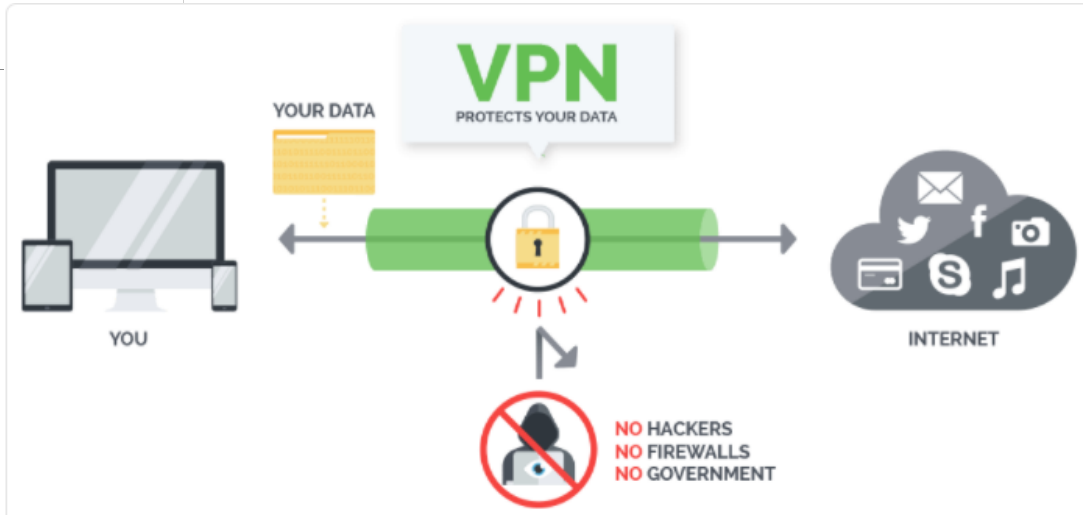
VPNقانونی مجموعه ای از اتصالات مجازی است که از طریق اینترنت مسیر یابی می شوند و داده های شما را به صورت رمزنگاری در میان اینترنت جا به جا می کند. بسیاری از پروتکل های اینترنتی مانند HTTPS، NNTPS، SSH و LDAPS از رمزنگاری داخلی استفاده می کنند. بنابراین اگر از این پورت ها به اینترنت دسترسی پیدا کنید یعنی داده های شما حداقل دو بار رمزنگاری می شود.که امنیت اطلاعات را بالا می بردیکی از مهم ترین مزیت هایی که برای وی پی ان های قانونی بیان می شود محیط امن این وی پی ان هاست. بر اساس این گفته ها با استفاده از وی پی ان قانونی مطمئن هستید که اطلاعات شخصی، رمزهای حساب های بانکی و اطلاعات هویتی تان افشا نخواهد شد.

که به دو نوع است.

1) Remote Access
2) Site to Site

Remote Access:

Remote Access VPN بستری را ایجاد می کند که دستگاه های خارج از شبکه یک اتصال ایمن و پایدار را به داخل شبکه های خود داشته باشند. این دستگاه ها به عنوان Endpoint شناخته می شوند و ممکن است کامپیوتر، لپ تاپ، تبلت و یا تلفن های هوشمند باشند. پیشرفت تکنولوژی VPN باعث شده است که بررسی های امنیتی برای Endpoint ها انجام شود تا اطمینان حاصل شود که آن ها قبل از اتصال شرایط لازم برای برقراری ارتباط را دارند.

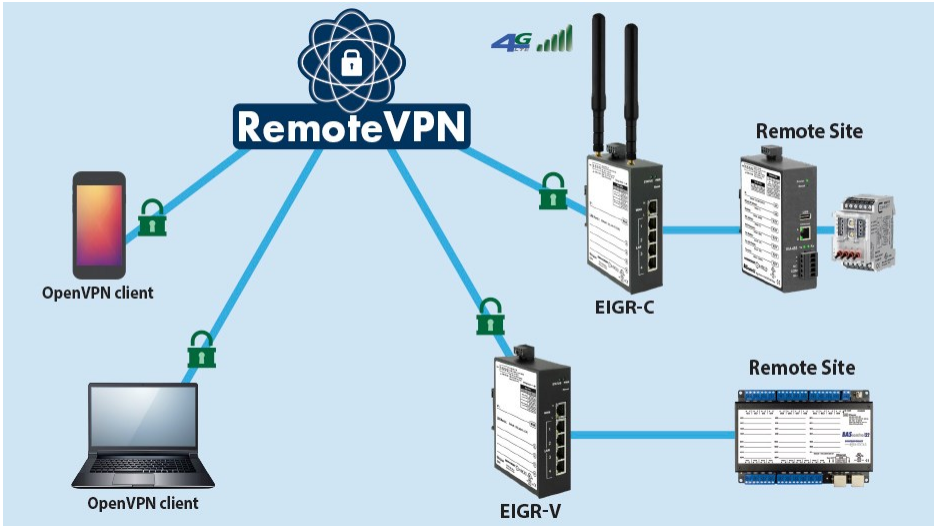


شکل 1-10 (Remote VPN)

Site to Site:

Site-to-Site VPN معمولا برای اتصال دستگاه ها در شعبه های یک شرکت به شعبه اصلی از طریق انترنت استفاده می گردد.

در این تکنالوژی دستگاه های خروجی بین دو شرکت یک اتصال ایمن را فراهم می کنند که کاربران می توانند اطلاعات خود را در این بستر به صورت بسیار امن ارسال نمایند این تکنولوژی با داشتن مکانیزم هایی مانع از دست رسی توسط افراد غیر مجاز می شود.



شکل 1-11 (Site to site VPN)

فلتر شکن(Free VPN)

از این نوع VPN برای دسترسی به وبسایت های مسدود شده استفاده می کنند. این سرویس ها به برنامه های مخرب وهکر ها اجازه می دهند تا به اطلاعات شخصی شما دسترسی داشته . اما اغلب افراد متاسفانه اهمیتی به امنیت اطلاعاتشان نمی دهند و فکر می‌کنند که این فیلترشکن‌ها و وی‌پی‌ان ها خطری برایشان به حساب نمی‌آید. اگر سرور وی‌پی‌ان توسط یک هکر کنترل شود، بدون مشکلی به ارتباط بین شما و وب سایت مد نظر دسترسی خواهد داشت. یعنی اگر درخواست ورود به حساب کاربری را بدهید، چون رمز و نام کاربری همراه با درخواست ارسال می‌شوند، به راحتی می‌تواند آن‌ها را مشاهده کند! توجه به این نکته ضروری است که اگر نگوییم همه سرورهای فیلتر شکن، بسیاری از آن‌ها از این طریق اطلاعات شناسایی ،هویتی و دیگر اطلاعات حساس مثل رمزهای عبور، کوکی مرورگرتان،

اطلاعات بانکی و ... استفاده کننده را می دزدند.

شکل 1-11 (Free VPN)