مبانی امنیت — استاد حسین زاده

علت اهمیت امنیت در سالهای اخیر:

۱- سازمانها امروزه وابستگی زیادی به ساختار IT خود دارند , به طوریکه اگر زیرساخت روابط IT آنها مختل شود , فعالیتهای سازمانی نیز به تبع آن مختل می شود .

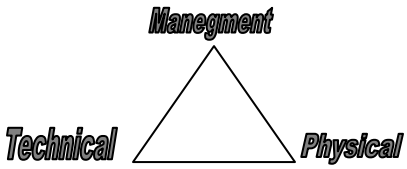
۲- اطلاعات نسبت به گذشته بیشتر به شکل دیجیتال درآمده است , بنابراین نگرانی های امنیتی بیشتر شده است .

۳- حضور کسب و کار الکترونیکی در گذشته وجود نداشته است

۴- حضور نرم افزارهای نا ایمن که Secure نیستند .

امنیت اطلاعات (*Information Secureti*):

امنیت اطلاعات از مثلث زیر تشکیل شده است .



مثال هایی برای حوزه Technical :

۱) امنیت نرم افزار (Application)

۲) امنیت شبکه (Network) ۳) امنیت در حوزه Data Base ۴) امنیت در حوزه Cloud Computing

تعریف ریسک (Risk):

هرآن چیزی است که به فرآیند تداوم کسب و کار سازمان , لطمه وارد کرده و سازمان را از اهداف سازمانی خود دور کند .

مثال : لو رفتن اطلاعات محرمانه مشتریان

تعریف تهدید (Threat):

هرگونه اتفاق عمدی یا غیر عمدی که ریسک را بوجود آورد تهدید به حساب می آید .

مثال : عدم به روز رسانی ویندوز , آنتی ویروس , عدم نصب آنتی ویروس= (Vulnerability)

نفوذ و به دست گرفتن کنترل سیستم (Explpit):

استفاده از Vulnerability (Vul) یک نرم افزار یا سیستم عامل در جهت نفوذ و به کنترل گرفتن یک سیستم را Exploit کردن می گویند .

حمله روز صفر (Zero Day Attack):

به حمله ایی که هنوز به صورت عمومی اطلاعاتی از آن در دسترس نیست و هنوز می توان از آن استفاده کرد گفته می شود.

انگیزه های یک هکر:

۱) مادی : مثل سرقت و فروش اطلاعات , جابه جایی اطلاعات

۲) معنوی : مثل شهرت , تبلیغات ۳) جنگ نرم : مثل مختل کردن یک سیستم

طبقه بندی هکر ها :

۱) کلاه سفید ها(White Hat) : این دسته با دانش نفوذ خود در جهت ایمن سازی یک سازمان , راهکارهای امنیتی ارائه می دهند . به آنها Ethical Hack نیز گفته می شود .

۲) کلاه سیاه ها (Black Hat): نفوذگرها هستند . انگیزه آنها خرابکاری و کارهای منفی می باشد .

۳) کلاه خاکستری (Gray Hat): هر کجا که پول باشد , آنها هم هستند .
۴) هکرهای انتحاری (Suicide Hackers): داشتن اهداف آسمانی
۵) Hacktivism : به مطرح کردن یک ایده سیاسی , مذهبی , نژادپرستارانه و غیره بوسیله هک کردن گفته می شود .

فاز ها یا مراحل هک :

۱) Footprinting(Reconnaissance): به دست آوردن اطلاعات اولیه از قربانی (Viktim) و جمع آوری آن به شکلی نظام مند
۲) Scanning : به فرآیند پویش و مانیتورینگ شبکه قربانی و تشخیص نقاط ضعف آن گفته می شود .
۳) Gaining Accesse : به بدست آوردن دسترسی به منابع نرم افزاری و سخت افزاری قربانی گفته می شود .
۴) Main taining Accesse : به توانایی نگه داشتن دسترسی به منابع نرم افزاری و سخت افزاری قربانی گفته می شود .
۵) Clearing & Coverting Track : به پاک کردن ردپای خود از روی سیستم قربانی و شبکه گفته می شود .

راه های کار با روش Foot printing :

۱) جستجو در موتورهای جستجو ۲) جستجو در شبکه های اجتماعی ۳) Who is گرفتن
۴) تماس با خود شخص یا اطرافیان وی جهت دسترسی به اطلاعات شخص مورد نظر

تست نفوذ (Peneteration Testing) :

ارزیابی میزان ایمنی امنیت اطلاعات یک سازمان به شبیه سازی کردن ۱ حمله را تست نفوذ یا Pen test گویند .
Pen Test میتواند از درون سازمان (اینترنال) و یا خارج از سازمان (اکسترنال) باشد .

انواع Pen test :

۱) White Box : در حد ادمین به شخص هکر اطلاعات می دهیم . برای چک کردن تنظیمات امنیتی
۲) Gray Box : اطلاعاتی در حد کارمند معمولی سازمان (کاربر محدود شده) (User) را به هکر می دهیم .
۳) Black Box : هیچ اطلاعاتی به هکر نمی دهیم . در واقع می خواهیم ببینیم ۱ هکر خارج از سازمان چه کار می تواند انجام دهد

انواع پورت ها (Ports) :

۱) Well Known Ports : محدوده پورت از شماره ۱ تا ۱۰۲۳ می باشد .
۲) Registered / private ports : محدوده پورت از شماره ۱۰۲۴ تا ۴۹۱۵۱ می باشد .
۳) Dynamic Ports : محدوده پورت از شماره ۴۹۱۵۱ تا ۶۵۵۳۵ می باشد .

انواع نرم افزارهای تحت شبکه :

۱) نرم افزارهای کلاینت (Client): از پورت های Dynamic استفاده می کنند .
مثال : وب بروزرها (Web browser) , پیغام رسان ها (Instant masengers) , نرم افزار Out Lock
۲) نرم افزارهای شبکه(Server): از پورتهای Well Known یا Registered استفاده می کنند .
مثال : DNS , I I S , Apache , DFCP , DHCP , SQL Server

تروجان ها , بک دورها (Trojans , Back Door) :

به هرگونه نرم افزاری که در کار عادی شبکه ایجاد اختلال کند , بد افزار یا Mal Ware گفته می شود .

انواع Mal Ware :

۱) ویروس ها و کرم ها : (Viruse & Worms) :

شباهت ویروس و کرم : هر ۲ می توانند هم Local منتشر شوند و هم تحت شبکه
تفاوت ویروس و کرم : ویروس به فایل اجرایی یا exe می چسبد ولی کرم نیاز به فایل اجرایی ندارد .

۲) جاسوس افزار (Spy ware) : کار آنها جستجوی اطلاعات و ارسال آنها برای شخص حمله کننده (Attaker) می باشد .

۳) Back Doors : استفاده از منابع سیستم از راه دور مثلاً اتصال بهد سیستم از راه دور یا اجرای نرم افزار

۴) Key Logger : هرآنچه که تایپ می کنید توسط Key Logger ثبت شده و برای Attaker ارسال می کند که این ارسال میتواند از طریق Email باشد .

۵) Bot : کامپیوتر به زامبی تبدیل می شود و برای شخص Attaker کارهای خاصی انجام می دهد .

۶) شوخی (Hoax): صدمه نمی زند , بیشتر منابع سیستم را به خود اختصاص می دهد .

۷) Ad Ware : به تول بارهایی که بالای صفحات مرورگرها نصب می شوند می گویند .

۸) Root Kit : نوعی بدافزار می باشد که شناسایی آنها بسیار مشکل می باشد و عموماً بر روی kernel سیستم عامل می نشیند .

۹) Trojan Horses : در واقع یک بخش ظاهری دارد که در باطن آن فعالیت خاصی برای Attaker انجام می دهد .

DOS Attack : در این روش پکت هایی بسیار زیاد بهصورت پشت سر هم و در بازه زمانی کوتاه به سمت قربانی (Viktim) ارسال می شود. این پکت ها از حالت استاندارد خارج شده و موجب از کار افتادن سرور می شوند .

DDOS Attack : در این حالت Attacker تعدادی کامپیوتر را به حالت Bot تبدیل کرده و هر یک را به سمت Web Server می فرستد تا هر کدام با ارسال پکت های فراوان Web Server را Down کنند .

مهندسی اجتماعی (Social Engineering) :

به هنر و روشهای فریب دادن افراد با هدف کسب اطلاعات از آنها مهندسی اجتماعی گفته می شود .
SE بر این حقیقت استوار است که افراد از میزان ارزش اطلاعاتی که در اختیار دارند , آگاه نیستند بنابراین در حفظ و نگهداری آن اطلاعات , دقت لازم را به عمل نمی آورند . تنها راه جلوگیری از حملات مهندسی اجتماعی , دادن آگاهی و آموزش به افراد است .

انواع مهندسی اجتماعی :

الف) Eaves droping : به فرآیند شنود مکالمات افراد (تلفنی , شبکه ای , حضوری) گفته می شود .
ب) Shoulder Surfing : کسی چیزی را تایپ کرده و Attacker آن را مشاهده می کند .
ج) Dumpster Diving : جستجو در سطل آشغال
د) Tail Gating : کسی که پشت سر کسی وارد محدودهء امنیتی شود .
ه) Piggy Backing : کسی که می گوید کارتش را جا گذاشته و از کسی می خواهد درب را برایش باز کند .

Information Risk Manegment :

به پروسه شناسایی و ارزیابی ریسک , کاهش آن به یک سطح قابل قبول و اجرای مکانیزم های صحیح برای نگهداری آن سطح گفته می شود .

The Risk Manegment Team :

هیچکس در سازمان نمی داند که سازمان چگونه کار می کند , به همین علت به کمیته Risk Manegment نیاز داریم .

اعضاء تیم Risk Manegment :

الف) مدیر کل ب) مدیران هر دپارتمان ج)کارشناسان دپارتمان امنیت می باشد .

مهمترین وظیفه این گروه , اطمینان از حفاظت امنیتی یک سازمان با استفاده از راه حل های مقرون به صرفه (**Cost effective**)

سایر وظایف این گروه به شرح زیر است :

۱) مشخص کردن سطح پذیرش ریسک از طرف مدیران رده بالا ۲) مستند سازی فرآیند و رویه های ارزیابی ریسک

۳) مشخص کردن رویه های شناسایی و کاهش ریسک ۴) اختصاص بودجه کافی از طریق مدیران رده بالا

۵) تدوین آموزش آگاهی های امنیتی

۶) بازنگری دوره ای ریسک که به سیکل زیر مربوط می شود .

الف) **Identifynig Risk** = شناخت ریسک

ب) **Identifynig Threat** = شناخت تهدید

ج) **Identifynig Vul** = شناسایی آسیب پذیری

د) **Eliminating Vul** = نابود کردن آسیب پذیری

مراحل بالا به صورت سیکل ادامه دارد .

Risk Analysis :

روشی است برای شناسایی , تخمین و ارزیابی ریسک ها در یک سازمان که ۴ هدف اصلی دارد :

الف)شناسایی **Asset** ها و ارزش آنها ب) شناسایی **Vul** و **Threat** ها

ج) اندازه گیری احتمال وقوع و تأثیر **Threat** ها بر روی کسب و کار

د) ایجاد یک توازن اقتصادی بین تأثیر **Threat** ها و هزینه ها

Handeling Risk : روشهای زیر را اجام می دهیم :

۱) هیچ کاری نمی کنیم , چون می گوئیم احتمال وقوع آن کم است .

۲) **Reduce Risk** : کاهش ریسک ها از طریق **Safeguard**

۳) **Transfer** کردن : به پیمانکار واگذار می کنیم . مثال بانک **X** بدهد به شرکت **Y**

۴) **Avoid the risk** : دوری کردن از ریسک مثلاً حذف فرآیند تجاری به خاطر خطرهایش

طبقه بندی اطلاعات در یک شرکت بازرگانی :

۱) **Confidential** : مثل فرمول یا اسرار کاری شرکت

۲) **Private** : مثل **user , password** کاربرهای شرکت یا اینکه هر یک از کارمندان درگیر چه پرژه ای هستند .

۳) **Sensitive** : مثل رزومه کارمندان

۴) **Public** : مثل آدرس و تلفن شرکت

آگاهی امنیتی کارکنان در هنگام استخدام :

۱) **Privius Employment Verification** : اعتبار سنجی و تحقیق از محل کار قبلی شخص

۲) **Education Verification** : اعتبار سنجی و تحقیق در مورد سوابق تحصیلی

۳) **Personal Refrance Checks** : مراجعه و تحقیق از معرف های شخص

آگاهی امنیتی کارکنان در هنگام قطع همکاری :

۱) هر امکاناتی که به شخص داده اند را باید پس بگیرند . (Facility)

۲) هنگام استخدام باید آن شخص توافق نامه عدم افشا اطلاعات (NDA) را پر کند .

۳) در هنگام قطع همکاری باید NDAبه شخص یادآوری شود .

۴) باید رویه ای باشد که واحد IT کلیه دسترسی های وی را ببندد .

Password Maneagment :

مدیریت Password کارکنان در یک سازمان می باشد . مثلاً یکی از حالتهای آن تعریف تاریخ انقضاء پسورد می باشد جهت جلوگیری از حمله حدس زدن پسورد (Password Guesing)

Job Description :

برای هر شخص , شرح وظایف آن را مشخص می کند .

چرخش شغلی (Job Rotation) :

به جابه جایی یا تغییر موقعیت کاری کارکنان در یک سازمان در بازه های زمانی مشخص را چرخش شغلی می گویند .

مرخصی اجباری (Mandatory Vacation) :

زمانی که شخصی معلق می شود برای بررسی مدارک وی تا زمانی که تحقیقات کامل شود مرخصی اجباری می گویند .

سطح دسترسی (Access Control):

یکی از مفاهیم امنیت است که کنترل می کند , چطور کاربران و سیستم ها با سایر سیستم ها و منابع ارتباط برقرار کنند . در حقیقت AC از دسترسی غیر مجاز به منابع حفاظت می کند .

برای مشخص کردن سطح دسترسی کاربران می بایست قبل از AC فرآیند Authentication (احراز هویت)با موفقیت انجام شود و همچنین قبل از احراز هویت نیز باید پروسه Identification (تشخیص هویت) باید انجام شود .

همچنین به تعیین سطح دسترسی برای هر کاربر Permition گفته می شود .

مدل های Access Control :

۱) Discretionary Access Control (DAC) :

در DAC مشخص می شود که کاربران به چه پوشه هایی دسترسی داشته باشند که عموماً توسط مالک Owner تعیین می شود .

۲) Mandatory Access Control (MAC) :

در MAC تنها یک مرجع داریم و آن مرجع برای همه تصمیم گیری می کند و آن مرجع عموماً مدیر شبکه یا Admin است . همانطور که مشخص است این مرجع حالت نظارتی دارد .

۳) Role Based Access Control (RBAC) :

یک سری گروه داریم R & D و منابع انسانی و IT و پشتیبانی و مالی حسابداری , هر گروه به Object های خودش دسترسی دارد و در واقع این حالت ارتباط ۱ به ۱ داریم یعنی یک نفر مشخص می کند که هر کس عضو چه گروهی است .

قانون حداقل دسترسی ممکن : (Rule Of Least Privilege) :

این قانون باید در تمام شبکه ها اعمال شود , بر طبق این قانون باید همه کمترین سطح دسترسی را داشته باشند. در واقع هر کاربر تنها به اطلاعاتی که نیاز دارد باید دسترسی پیدا کند , این قانون براساس Need to Know Policy (نیاز به دانستن) می باشد .

Access Matrix Model :

مشخص می کند که چه کاربری بر روی چه **Object** دسترسی دارد . که شامل ۲ مدل زیر می شود .

۱) **Conten Based Access** : تعریف این نوع دسترسی بر اساس محتویات است , که اگر کاربری می خواهد به یک محتوای خاص دسترسی داشته باشد , اجازه بدهیم یا نه . مثل فیلترینگ اینترنت یا هر گونه فیلترینگ دیگر

۲) **Context Based Access** : این نوع دسترسی بر اساس شرایط و زمینه کاری است . مثلاً اگر فرد **X** در یک شرکت مسئول مذاکرات است و در سازمان ۲ پروژه داریم , دسترسی فرد **X** را برای پروژه **A** یا **B** مشخص می کنیم نه هر ۲ پروژه

امنیت فیزیکی (Physical Security) :

عموماً در سازمانهای ایرانی این قسمت از امنیت برعهده لخش حراست سازمان می باشد . در واقع می توان مهمترین امنیت فیزیکی را مقابله با تهدیدات فیزیکی دانست .

انواع تهدیدات فیزیکی (Physical Threats) :

۱) تهدیدات طبیعی (**Natural Threat**) : تهدیدات محیطی طبیعی مثل سیل یا زلزله

۲) تهدیدات منابع (**Supply System Threats**): مثل قطع برق و قطع ارتباطات

۳) تهدیدات عمدی یا دستی (**Manmade Threat**): مثل دسترسی غیرمجاز یا تهدیدات افراد ناراضی در سازمان ها تخریب اموال عمومی (**Vandalism**)نیز در این دسته قرار می گیرد .

CPTED (Crime Prevention Through Environment Design):

این مفهوم اشاره دارد به یک طراحی فیزیکی صحیح و اصولی که باعث می شود , افراد مواظب رفتار خود باشند و در نتیجه جرائم فیزیکی کاهش یابد .

انواع CPTED :

۱) **Natural Access Control** : مثل کشیدن فنس , سیم خاردار , دیوار و گذاشتن علائم و خط کشی . کلاً با علائم فیزیکی افراد را هدایت می کنیم و هرکس تخطی کرد یعنی می خواهد جرمی را انجام دهد .

۲) **Natural Surveillnce** : نظارت طبیعی در سازمان باشد . مثل گذاشتن دوربین یا گارد امنیتی یا سگ نگهبان

۳) **Territorial Reinfarcment** : مثلاً ایجاد پارتیشن بندی در سازمان ها تا هرکسی یک محدوده مختص به خود داشته باشد .

مفهوم امنیت در شبکه :

در هر شبکه به ارتباطی می توان یک ارتباط ایمن گفت که ۴ آیتم زیر در آن رعایت شده باشد :

۱) محرمانگی **Confidentialit** رمز نگاری **Encryption**

۲) **integrity** جامعیت و صحت **Hashing**

۳) **Non Repudiation** عدم انکار و تکذیب **Digital Signature** امضای دیجیتال

۴) **Authentication** احراز هویت

پنهان نگاری (Stegano graphy) :

به تفکیک پنهان کردن اطلاعات در داخل یک فایلگفته می شود . در واقع **Steganography** به پنهان سازی یک پیغام در یک متن , در یک عکس , ویدئو یا فایل صوتی گفته می شود .