مبانی امنیت اطلاعات

همزمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه های کامپیوتری و به دنبال آن اینترنت)بزرگترین شبکه جهانی (، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده است .استفاده کنندگان کامپیوتر به منظور استفاده از دستاوردها و مزایای فن آوری اطلاعات و ارتباطات ، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه های تاثیر گذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می باشند .**امنیت اطلاعات** و ایمن سازی شبکه های کامپیوتری از جمله این مولفه ها بوده که نمی توان آن را مختص یک فرد و یا سازمان در نظر گرفت .پرداختن به مقوله **امنیت اطلاعات** و ایمن سازی شبکه های کامپیوتری در هر کشور ، مستلزم توجه تمامی کاربران صرفنظر از موقعیت شغلی و سنی به جایگاه **امنیت اطلاعات** و ایمن سازی شبکه های کامپیوتری بوده و می بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد .وجود ضعف امنیتی در شبکه های کامپیوتری و اطلاعاتی ، عدم آموزش و توجیه صحیح تمامی کاربران صرفنظر از مسئولیت شغلی آنان نسبت به جایگاه و **اهمیت امنیت اطلاعات** ، عدم وجود دستورالعمل های لازم برای پیشگیری از نقایص امنیتی ، عدم وجود سیاست های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی ، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملا" زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می دهد .در این مقاله قصد داریم به بررسی مبانی و اصول اولیه **امنیت اطلاعات** و ایمن سازی شبکه های کامپیوتری پرداخته و از این رهگذر با مراحل مورد نیاز به منظور حفاظت کامپیوترها در مقابل حملات ، بیشتر آشنا شویم .

اهمیت امنیت اطلاعات و ایمن سازی کامپیوترها

تمامی کامپیوترها از کامپیوترهای موجود در منازل تا کامپیوترهای موجود در سازمان ها و موسسات بزرگ ، در معرض آسیب و تهدیدات امنیتی می باشند .با انجام تدابیر لازم و استفاده از برخی روش های ساده می توان پیشگیری لازم و اولیه ای را خصوص ایمن سازی محیط کامپیوتری خود انجام داد.علیرغم تمامی مزایا و دستاوردهای اینترنت ، این شبکه عظیم به همراه فن آوری های مربوطه ، دریچه ای را در مقابل تعداد زیادی از تهدیدات امنیتی برای تمامی استفاده کنندگان)افراد ، خانواده ها ، سازمان ها ، موسسات و (. ... گشوده است .با توجه به ماهیت حملات ، می بایست در انتظار نتایج نامطلوب متفاوتی بود)از مشکلات و مزاحمت های اندک تا از کار انداختن سرویس ها و خدمات . (در معرض آسیب قرار گرفتن **داده** ها و اطلاعات حساس ، تجاوز به حریم خصوصی کاربران ، استفاده از کامپیوتر کاربران برای تهاجم بر علیه سایر کامپیوترها ، از جمله اهداف مهاجمانی است که با بهره گیری از آخرین فن آوری های موجود ، حملات خود را سازماندهی و بالفعل می نمایند .بنابراین ، می بایست به موضوع **امنیت اطلاعات** ، ایمن سازی کامپیوترها و شبکه های کامپیوتری، توجه جدی شده و از فرآیندهای متفاوتی در جهت مقاوم سازی آنان ، استفاده گردد .

داده ها و اطلاعات حساس در معرض تهدید

تقریبا" هر نوع تهاجم ، تهدیدی است در مقابل حریم خصوصی ، پیوستگی ، اعتبار و صحت **داده** ها .یک سارق اتومبیل می تواند در هر لحظه صرفا" یک اتومبیل را سرقت نماید ، در صورتی که یک مهاجم با بکارگیری صرفا" یک دستگاه کامپیوتر ، می تواند آسیب های فراوانی را متوجه تعداد زیادی از شبکه های کامپیوتری نموده و باعث بروز اشکالاتی متعدد در زیرساخت اطلاعاتی یک کشورگردد .آگاهی لازم در رابطه با تهدیدات امنیـتی و نحوه حفاظت خود در مقابل آنان ، امکان حفاظت اطلاعات و **داده** های حساس را در یک شبکه کامپیوتری فراهم می نماید .

ویروس ها

ویروس های کامپیوتری ، متداولترین نوع تهدیدات امنیتی در سالیان اخیر بوده که تاکنون مشکلات گسترده ای را ایجاد و همواره از خبرسازترین موضوعات در زمینه کامپیوتر و شبکه های کامپیوتری ، بوده اند .**ویروس ها** ، برنامه هائی کامپیوتری می باشند که توسط برنامه نویسان گمراه و در عین حال ماهر نوشته شده و بگونه ای طراحی می گردند که قادر به تکثیر خود و آلودگی کامپیوترها بر اثر وقوع یک رویداد خاص ، باشند .مثلا "**ویروس ها** ئی که از آنان با نام "ماکرو ویروس " یاد می شود ، خود را به فایل هائی شامل دستورالعمل های ماکرو ملحق نموده و در ادامه ، همزمان با فعال شدن ماکرو ، شرایط لازم به منظور اجرای آنان نیز فراهم می گردد.برخی از **ویروس ها** بی آزار بوده و صرفا" باعث بروز اختلالات موقت در روند انجام عملیات در کامپیوتر می شوند)نظیر نمایش یک پیام مضحک بر روی صفحه نمایشگر همزمان با فشردن یک کلید خاص توسط کاربر . (برخی دیگر از **ویروس ها** دارای عملکردی مخرب تر بوده و می توانند مسائل و مشکلات بیشتری نظیر حذف فایل ها و یا کاهش سرعت سیستم را به دنبال داشته باشند .یک کامپیوتر صرفا" زمانی آلوده به یک ویروس می گردد که شرایط و امکان ورود ویروس از یک منبع خارجی)اغلب از طریق فایل ضمیمه یک نامه الکترونیکی و یا دریافت و نصب یک فایل و یا برنامه آلوده از اینترنت (، برای آن فراهم گردد .زمانی که یک کامپیوتر در شبکه ای آلوده گردید ، سایر کامپیوترها ی موجود در شبکه و یا سایر کامپیوترهای موجود در اینترنت، دارای استعدادی مناسب به منظور مشارکت و همکاری با ویروس،خواهند بود.

برنامه های اسب تروا)دشمنانی در لباس دوست (

برنامه های اسب تروا و یا Trojans ، به منزله ابزارهائی برای توزیع کد های مخرب می باشند .تروجان ها ، می توانند بی آزار بوده و یا حتی نرم افزاری مفیدی نظیر بازی های کامپیوتری باشند که با تغییر قیافه و با لباسی مبدل و ظاهری مفید خود را عرضه می نمایند .تروجان ها ، قادر به انجام عملیات متفاوتی نظیر حذف فایل ها ، ارسال یک نسخه از خود به لیست آدرس های پست الکترونیکی ، می باشند .این نوع از برنامه ها صرفا" می توانند از طریق تکثیر **برنامه های اسب تروا** به یک کامپیوتر،دریافت فایل از طریق اینترنت و یا باز نمودن یک فایل ضمیمه همراه یک نامه الکترونیکی ، اقدام به آلودگی یک سیستم نمایند.

ویرانگران

در وب سایت های متعددی از نرم افزارهائی نظیر اکتیوایکس ها و یا اپلت های جاوا استفاده می گردد .این نوع برنامه ها به منطور ایجاد انیمیشن و سایر افکت های خاص مورد استفاده قرار گرفته و جذابیت و میزان تعامل با کاربر را افزایش می دهند .با توجه به دریافت و نصب آسان این نوع از برنامه ها توسط کاربران ، برنامه های فوق به ابزاری مطئمن و آسان به منظور آسیب رسانی به سایر سیستم ها تبدیل شده اند .این نوع برنامه ها که به "ویرانگران" شهرت یافته اند ، به شکل یک برنامه نرم افزاری و یا اپلت ارائه و در دسترس استفاده کنندگان قرار می گیرند .برنامه های فوق ، قادر به ایجاد مشکلات متعددی برای کاربران می باشند)از بروز اشکال دریک فایل تا ایجاد اشکال در بخش اصلی یک سیستم کامپیوتری . (

حملات

تاکنون حملات متعددی متوجه شبکه های کامپیوتری بوده که می توان تمامی آنان را به سه گروه عمده تقسیم نمود : حملات شناسائی : در این نوع حملات ، مهاجمان اقدام به جمع آوری و شناسائی اطلاعات با هدف تخریب و آسیب رساندن به آنان می نمایند .مهاجمان در این رابطه از نرم افزارهای خاصی نظیر Sniffer و یا Scanner به منظور شناسائی نقاط ضعف و آسیب

پذیر کامپیوترها ، سرویس دهندگان وب و برنامه ها ، استفاده می نمایند .در این رابطه برخی تولیدکنندگان ، نرم افزارهائی را با اهداف خیرخواهانه طراحی و پیاده سازی نموده اند که متاسفانه از آنان در جهت اهداف مخرب نیز استفاده می شود.مثلا" به منظور تشخیص و شناسائی رمز های عبور، نرم افزارهای متعددی تاکنون طراحی و پیاده سازی شده است .نرم افرارهای فوق با هدف کمک به مدیران شبکه ، افراد و کاربرانی که رمز عبور خود را فراموش کرده و یا آگاهی از رمز عبور افرادی که سازمان خود را بدون اعلام رمز عبور به مدیر شبکه ، ترک نموده اند،استفاده می گردند .به هر حال وجود این نوع نرم افزارها واقعیتی انکارناپذیر بوده که می تواند به منزله یک سلاح مخرب در اختیار مهاجمان قرار گیرد .حملات دستیابی : دراین نوع حملات، هدف اصلی مهاجمان ، نفوذ در شبکه و دستیابی به آدرس های پست الکترونیکی ، اطلاعات ذخیره شده در بانک های اطلاعاتی و سایر اطلاعات حساس، می باشد .حملات از کار انداختن سرویس ها : در این نوع حملات ، مهاجمان سعی در ایجاد مزاحمت به منظور دستیابی به تمام و یا بخشی از امکانات موجود در شبکه برای کاربران مجازمی نمایند .حملات فوق به اشکال متفاوت و با بهره گیری از فن آوری های متعددی صورت می پذیرد .ارسال حجم بالائی از **داده** ها ی غیرواقعی برای یک ماشین متصل به اینترنت و ایجاد ترافیک کاذب در شبکه ، نمونه هائی از این نوع حملات می باشند.

ره گیری داده)استراق سمع(

بر روی هر شبکه کامپیوتری روزانه اطلاعات متفاوتی جابجا می گردد و همین امر می تواند موضوعی مورد علاقه برای مهاجمان باشد .در این نوع حملات ، مهاجمان اقدام به استراق سمع و یا حتی تغییر بسته های اطلاعاتی در شبکه می نمایند .مهاجمان به منظور نیل به اهداف مخرب خود از روش های متعددی به منظور شنود اطلاعات ، استفاده می نمایند .کلاهبرداری)ابتدا جلب اعتماد و سپس تهاجم (کلاهبرداران از روش های متعددی به منظور اعمال شیادی خود استفاده می نمایند .با گشترش اینترنت این نوع افراد فضای مناسبی برای اعمال مخرب خود یافته اند)چراکه می توان به هزاران نفر در زمانی کوتاه و از طریق اینترنت دستیابی داشت . (در برخی موارد شیادان با ارسال **نامه های الکترونیکی** وسوسه انگیز از خوانندگان می خواهند که اطلاعاتی خاص را برای آنان ارسال نموده و یا از یک سایت به عنوان طعمه در این رابطه استفاده می نمایند .به منظور پیشگیری از اینگونه اعمال ، می بایست کاربران دقت لازم در خصوص درج نام ، رمز عبور و سایر اطلاعات شخصی در سایت هائی که نسبت به هویت آنان شک و تردید وجود دارد را داشته باشند .با توجه به سهولت جعل آدرس های پست الکترونیکی ؛ می بایست به این نکته توجه گردد که قبل از ارسال اطلاعات شخصی برای هر فرد ، هویت وی شناسائی گردد.هرگز بر روی لینک ها و یا ضمائمی که از طریق یک نامه الکترونیکی برای شما ارسال شده است ، کلیک نکرده و همواره می بایست به شرکت ها و موسساتی که به طور شفاف آدرس فیزیکی و شماره تلفن های خود را ذکر نمی نمایند ، شک و تردید داشت .

نامه های الکترونیکی ناخواسته

از واژه Spam در ارتباط با **نامه های الکترونیکی** ناخواسته و یا پیام های تبلیغاتی ناخواسته ، استفاده می گردد .این نوع از **نامه های الکترونیکی** ، عموما" بی ضرر بوده و صرفا" ممکن است مزاحمت و یا دردسر ما را بیشتر نمایند .دامنه این نوع مزاحمت ها می تواند از به هدر رفتن زمان کاربر تا هرز رفتن فضای ذخیره سازی بر روی کامپیوترهای کاربران را شامل می شود .

ابزارهای امنیتی

پس از آشنائی با تهدیدات، می توان تمهیدات امنیتی لازم در خصوص پیشگیری و مقابله با آنان را انجام داد .بدین منظور می توان از فن آوری های متعددی نظیر **آنتی ویروس** ها و یا فایروال ها ، استفاده بعمل آورد .

نرم افزارهای آنتی ویروس

نرم افزارهای **آنتی ویروس** ، قادر به شناسائی و برخورد مناسب با اکثر تهدیدات مربوط به **ویروس ها** می باشند) .مشروط به اینکه این نوع نرم افزارها به صورت منظم بهنگام شده و بدرستی پشتیبانی گردند . (نرم افزارهای **آنتی ویروس** درتعامل اطلاعاتی با شبکه ای گسترده از کاربران بوده و در صورت ضرورت پیام ها و هشدارهای لازم در خصوص ویروس های جدید را اعلام می نمایند .بدین ترتیب ، پس از شناسائی یک ویروس جدید ، ابزار مقابله با آن سریعا" پیاده سازی و در اختیار عموم کاربران قرار می گیرد .با توجه به طراحی و پیاده سازی ویروس های متعدد در سراسر جهان و گسترش سریع آنان از طریق اینترنت ، می بایست بانک اطلاعاتی **ویروس ها** بر اساس فرآیندی مشخص و مستمر ، بهنگام گردد .

سیاست های امنیتی

سازمان های بزرگ و کوچک نیازمند ایجاد **سیاست های امنیتی** لازم در خصوص استفاده از کامپیوتر و ایمن سازی اطلاعات و شبکه های کامپیوتری می باشند .**سیاست های امنیتی** ، مجموعه قوانین لازم به منظور استفاده از کامپیوتر و شبکه های کامپیوتری بوده که در آن وظایف تمامی کاربران دقیقا" مشخص و در صورت ضرورت ، هشدارهای لازم به کاربران در خصوص استفاده از منابع موجود در شبکه **داده** می شود .دانش تمامی کاربرانی که به تمام و یا بخشی از شبکه دستیابی دارند ، می بایست به صورت منظم و با توجه به سیاست های تدوین یافته ، بهنگام گردد)آموزش مستمر و هدفمند با توجه به سیاست های تدوین شده . (

رمزهای عبور

هر سیستم کامپیوتری می بایست دارای ایمنی مناسبی در خصوص رمز های عبور باشد .استحکام **رمزهای عبور** ، ساده ترین و در عین حال متداولترین روش به منظور اطمینان از این موضوع است که صرفا" افراد تائید شده و مجاز قادر به استفاده از کامپیوتر و یا بخش های خاصی از شبکه می باشند .فراموش نکنیم که زیرساخت های امنیتی ایجاد شده ، در صورتی که کاربران دقت لازم در خصوص مراقبت از **رمزهای عبور** خود را نداشته باشند ، موثر نخواهد بود)خط بطلانی بر تمامی تلاش های انجام شده . (اکثر کاربران در زمان انتخاب رمز عبور، از اعداد و یا کلماتی استفاده نمایند که بخاطر آوردن آنان ساده باشد)نظیر تاریخ تولد ، شماره تلفن .(برخی دیگر از کاربران علاقه ای به تغییر منظم **رمزهای عبور** خود در مقاطع زمانی خاصی نداشته و همین امر می تواند زمنیه تشخیص **رمزهای عبور** توسط مهاجمان را فراهم نماید .در زمان تعریف رمز عبور می بایست تمهیدات لازم در خصوص استحکام و نگهداری مطلوب آنان اندیشیده گردد:

- حتی المقدور سعی گردد از رمز های عبور فاقد معنی خاصی استفاده گردد .
- به صورت منظم و در مقاطع زمانی مشخص شده ، اقدام به تغییر **رمزهای عبور** گردد .
- عدم افشای **رمزهای عبور** برای سایرین
- فایروال ها

فایروال ، راه حلی سخت افزاری و یا نرم افزاری به منظور تاکید)اصرار (بر **سیاست های امنیتی** می باشد .یک فایروال نظیر قفل موجود بر روی یک درب منزل و یا بر روی درب یک اطاق درون منزل می باشد .بدین ترتیب صرفا" کاربران تائید شده)آنانی که دارای کلید دستیابی می باشند (، امکان ورود به سیستم را خواهند داشت .فایروال ها دارای فیلترهای از قبل تعبیه شده ای بوده که امکان دستیابی افراد غیر مجاز به منابع سیستم را سلب می نمایند .

رمزنگاری

فن آوری **رمزنگاری** ، امکان مشاهده ، مطالعه و تفسیر پیام های ارسالی توسط افراد غیر مجاز را سلب می نماید .از **رمزنگاری** به منظور حفاظت **داده** ها در شبکه های عمومی نظیر اینترنت استفاده می گردد .در این رابطه از الگوریتم های پیشرفته ریاضی به منظور رمزنمودن پیام ها و ضمائم مربوطه ، استفاده می شود .چند نکته اولیه در خصوص ایمن سازی اطلاعات و شبکه های کامپیوتری:

- **پذیرش مسئولیت به عنوان یک شهروند سایبر**

در صورتی که از اینترنت استفاده می نمائید ، شما به عنوان عضوی از جامعه جهانی و یا شهروند سایبر، محسوب شده و همانند یک شهروند معمولی ، دارای مسئولیت های خاصی بوده که می بایست پذیرای آنان باشیم .

- **استفاده از نرم افزارهای آنتی ویروس**

یک ویروس کامپیوتری ، برنامه ای است که می تواند به کامپیوتر شما نفوذ کرده و صدمات فراوانی را باعث گردد .نرم افزارهای **آنتی ویروس** به منظور حفاظت اطلاعات و کامپیوترها در مقابل ویروس های شناخته شده ، طراحی شده اند .با توجه به این که روزانه شاهد عرضه ویروس های جدید می باشیم ، می بایست برنامه های **آنتی ویروس** به صورت منظم و مرتب بهنگام گردند .

- **عدم فعال نمودن نامه های الکترونیکی ارسال شده توسط منابع نامشخص و گمنام**

نامه های الکترونیکی ارسالی توسط منابع ناشناس را می بایست همواره حذف نمود .به فایل هائی که به عنوان ضمیمه همراه یک نامه الکترونیکی ارسال می گردند، توجه گردد .حتی در صورتی که این نوع از **نامه های الکترونیکی** را از طریق دوستان و آشنایان خود دریافت می نمائید)خصوصا" اگر دارای انشعاب . exe باشند . (.برخی فایل ها مسئولیت توزیع **ویروس ها** را برعهده داشته و می توانند باعث بروز اشکالات فراوانی نظیر حذف دائم فایل ها و یا بروز اشکال در یک وب سایت گردند .هرگز نمی بایست اقدام به فوروارد نمودن **نامه های الکترونیکی** برای سایر کاربران قبل از حصول اطمینان از ایمن بودن آنان نمود .از رمزهای عبوری که تشخیص آنان مشکل می باشد ، استفاده نموده و آنان را محرمانه نزد خود نگه دارید هرگز **رمزهای عبور** خود را بر روی کاغذ ننوشته و آنان را به کامپیوتر نچسبانید . !تعداد زیادی از کاربران کامپیوتر دقت لازم در خصوص نگهداری رمز عبور خود را نمی نمایند و همین امر می تواند مشکلات متعددی را متوجه آنان ، نماید .رمزهای عبوری که تشخیص و یا حدس آنان آسان است ، گزینه های مناسبی در این رابطه نمی باشند .مثلا" در صورتی که نام شما Ali می باشد ، هرگز رمز عبور خود را با همین نام در نظر نگیرید .در فواصل زمانی

مشخص و به صورت مستمر ، اقدام به تغییر رمز عبور خود نمائید .هرگز رمز عبور خود را در اختیار اشخاص دیگری قرار ندهید.برای انتخاب یک رمز عبور از ترکیب اعداد ، حروف و علائم استفاده گردد تا حدس و ردیابی آنان توسط افراد غیرمجاز ، مشکل شود .

- **استفاده از فایروال ها به منظور حفاظت کامپیوترها**

نصب و پیکربندی یک فایروال کار مشکلی نخواهد بود .یک فایروال ، امکان دستیابی و کنترل سیستم توسط مهاجمان را سلب نموده و پیشگیری لازم در خصوص سرقت اطلاعات موجود بر روی کامپیوتر را انجام می دهد .

- **Back-upگرفتن منظم از اطلاعات ارزشمند موجود بر روی کامپیوتر**

در فواصل زمانی مشخص و بر اساس یک برنامه خاص از اطلاعات ارزشمند موجود بر روی کامپیوتر backup گرفته شده و آنان را بر روی رسانه های ذخیره سازی نظیر لوح های فشرده ذخیره نمود .

- **دریافت و نصب منظم Patch های بهنگام شده مربوط به نقایص امنیتی**

نقایص امنیتی به صورت مرتب در سیستم های عامل و برنامه های کاربردی کشف می گردند .شرکت های تولید کننده نرم افزار ، به سرعت اقدام به ارائه نسخه های بهنگام شده ای با نام Patch نموده که کاربران می بایست آنان را دریافت و بر روی سیستم خود نصب نمایند.در این رابطه لازم است به صورت منظم از سایت های مربوط به تولید کنندگان نرم افزار بازدید بعمل آمده تا در صورت ارائه Patch ، آن را دریافت و بر روی سیستم نصب نمود .

- **بررسی و ارزیابی امنیتی کامپیوتر**

وضعیت امنیتی کامپیوتر خود را در مقاطع زمانی مشخصی ، بررسی نموده و در صورتی که خود نمی توانید این کار را انجام دهید از کارشناسان ذیربط استفاده نمائید .

- **غیر فعال نمودن ارتباط با اینترنت در زمان عدم استفاده**

اینترنت نظیر یک جاده دو طرفه است .شما اطلاعاتی را دریافت و یا ارسال می نمائید .غیرفعال نمودن ارتباط با اینترنت در مواردی که به آن نیاز نمی باشد، امکان دستیابی سایرین به کامپیوتر شما را سلب می نماید.

- **عدم اشتراک منابع موجود بر روی کامپیوتر با کاربرانی که هویت آنان نامشخص است**

سیستم عامل نصب شده بر روی یک کامپیوتر، ممکن است امکان به اشتراک گذاشتن برخی منابع موجود نظیر فایل ها را با سایر کاربران شبکه ، فراهم نماید .ویژگی فوق ، می تواند زمینه بروز تهدیدات امنیتی خاصی را فراهم نماید .بنابراین می بایست نسبت به غیرفعال نمودن ویژگی فوق ، اقدام لازم صورت پذیرد.