موضوع:

امنیت اطلاعات در اینترنت

گردآورنده:

اداره کل ارتباطات و فناوری اطلاعات استان کرمانشاه

https://Kermanshah.ict.gov.ir

فهرست:

22. **آشنائی با محتویات فعال و کوکی**

23. **محتویات فعال چیست ؟**

24. **کوکی چیست ؟**

25. **جایگاه نرم‌افزارهای ضد ویروس**

مقدمه:

در سال‌های اخیر امنیت اطلاعات یکی از شاخه‌های مهم کامپیوتر می‌باشد.

جایگاه امنیت در اینترنت:

قطعا" تاکنون اخبار متعددی را در خصوص سرقت اطلاعات حساس نظیر شماره کارت اعتباری و یا شیوع یک ویروس کامپیوتری شنیده‌اید و شاید شما نیز از جمله قربانیان این نوع حملات بوده‌اید. آگاهی از تهدیدات موجود و عملیات لازم به منظور حفاظت در مقابل آنان، یکی از روش‌های مناسب دفاعی است.

اهمیت امنیت در اینترنت:

بدون شک کامپیوتر و اینترنت در مدت زمان کوتاهی توانسته‌اند حضور مشهود خود را در تمامی عرصه های حیات بشری به اثبات برسانند . وجود تحولات عظیم در ارتباطات (نظیر Email و تلفن‌های سلولی)، تحولات گسترده در زمینه تجهیزات الکترونیکی و سرگرمی (کابل دیجیتال، mp3)، تحولات گسترده در صنعت حمل و نقل (سیستم هدایت اتوماتیک اتومبیل، ناوبری هوائی) ، تغییرات اساسی در روش خرید و فروش کالا (فروشگاههای online، کارت‌های اعتباری)، پیشرفت های برجسته در عرصه پزشکی، صرفا" نمونه‌هائی اندک در این زمینه می‌باشد .

اجازه دهید به منظور آشنائی با جایگاه کامپیوتر در زندگی انسان عصر حاضر و اهمیت امنیت اطلاعات، این پرسش‌ها را مطرح نمائیم که در طی یک روز چه میزان با کامپیوتر درگیر هستید؟ چه حجمی از اطلاعات شخصی شما بر روی کامپیوتر خود و یا سایر کامپیوترهای دیگر، ذخیره شده است ؟ پاسخ به سوالات فوق،جایگاه کامپیوتر و اهمیت ایمن سازی اطلاعات در عصر اطلاعات را بخوبی مشخص خواهد کرد .

امنیت در اینترنت ، حفاظت از اطلاعات با استناد به سه اصل اساسی زیر است:

- نحوه پیشگیری از بروز یک تهاجم
- نحوه تشخیص یک تهاجم
- نحوه برخورد با حملات

1. انواع تهدیدات:

اینترنت، علیرغم تمامی جنبه‌های مثبت دارای مجموعه‌ای گسترده از خطرات و تهدیدات امنیتی است که برخی از آنان بسیار جدی و مهم بوده و برخی دیگر از اهمیت کمتری برخوردار می‌باشند :

- عملکرد ویروس‌های کامپیوتری که می‌تواند منجر به حذف اطلاعات موجود بر روی یک کامپیوتر شود .
- نفوذ افراد غیر مجاز به کامپیوتر شما و تغییر فایل‌ها
- استفاده از کامپیوتر شما برای تهاجم علیه دیگران
- سرقت اطلاعات حساس نظیر شماره کارت اعتباری و خرید غیر مجاز با استفاده از آن

با رعایت برخی نکات می توان احتمال بروز و یا موفقیت این نوع از حملات را به حداقل مقدار خود رساند.

2. نحوه حفاظت

اولین مرحله به منظور حفاظت و ایمن سازی اطلاعات، شناخت تهدیدات و آگاهی لازم در خصوص برخی مفاهیم اولیه در خصوص ایمن سازی اطلاعات است .

- **Hacker, attacker و یا Intruder** . اسامی فوق به افرادی که همواره در صدد استفاده از نقاط ضعف و آسیب پذیر موجود در نرم افزارها می‌باشند، اطلاق می‌گردد . با این که در برخی حالات ممکن است افراد فوق اهداف غیر مخربی را نداشته و انگیزه آنان صرفا" کنجکاوی باشد، ماحصل عملیات آنان می تواند اثرات جانبی منفی را به دنبال داشته باشد .
- **کد مخرب** : این نوع کدها شامل ویروس‌ها ، کرم‌ها و برنامه‌های تروجان (Trojan) بوده که هر یک از آنان دارای ویژگی های منحصر بفردی می باشند :

□ **ویروس‌ها** : نوع خاصی از کدهای مخرب می باشند که شما را ملزم می نمایند به منظور آلودگی سیستم، عملیات خاصی را انجام دهید. این نوع از برنامه‌ها به منظور نیل به اهداف مخرب خود نیازمند یاری کاربران می باشند. باز نمودن یک فایل ضمیمه همراه Email و یا مشاهده یک صفحه وب خاص، نمونه‌هائی از همکاری کاربران در جهت گسترش این نوع از کدهای مخرب است.

□ **کرم‌ها** : این نوع از کدهای مخرب بدون نیاز به دخالت کاربر، توزیع و گسترش می یابند . کرم‌ها، عموما" با سوء استفاده از یک نقطه آسیب‌پذیر در نرم‌افزار فعالیت خود را آغاز نموده و سعی می‌نمایند که کامپیوتر هدف را آلوده نمایند. پس از آلودگی یک کامپیوتر، تلاش برای یافتن و آلودگی سایر کامپیوتر انجام خواهد شد . همانند ویروس‌های کامپیوتری، کرم‌ها نیز می‌توانند از طریق Email، وب‌سایت‌ها و یا نرم‌افزارهای مبتنی بر شبکه، توزیع و گسترش یابند . توزیع اتوماتیک کرم‌ها نسبت به ویروس‌ها یکی از تفاوت‌های محسوس بین این دو نوع کد مخرب، محسوب می‌گردد .

□ **برنامه‌های تروجان** : این نوع از کدهای مخرب، نرم‌افزارهائی می باشند که ادعای ارائه خدماتی را داشته ولی در عمل، اهداف خاص خود را دنبال می‌نمایند . (تفاوت در

حرف و عمل) . مثلا" برنامه‌ای که ادعای افزایش سرعت کامپیوتر شما را می‌نماید، ممکن است در عمل اطلاعات حساس موجود برروی کامپیوتر شما را برای یک مهاجم و یا سارق از راه دور، ارسال نماید .

برای آشنائی با جایگاه امنیت در اینترنت و انجام عملیات لازم به منظور افزایش ضریب حفاظتی سیستم، مطالعه مقالات زیر توصیه می‌گردد :

- آشنائی با حملات DoS
- مزایای استفاده از BCC
- حفاظت کامپیوتر قبل از اتصال به اینترنت
- پیشگیری از حملات مهندسی اجتماعی و کلاهبرداری
- توصیه‌هائی برای کاهش Spam
- آشنائی با محتویات فعال و کوکی
- جایگاه نرم افزارهای ضدویروس
- چند عادت خوب امنیتی
- فایروال چیست ؟
- Patch چیست ؟
- مراقب ضمائم نامه‌های الکترونیکی باشید !
- نحوه انتخاب و حفاظت رمزهای عبور
- استفاده ایمن از برنامه های IM و Chat
- مبانی امنیت اطلاعات
- انواع حملات در شبکه های کامپیوتری (بخش دوم)
- انواع حملات در شبکه های کامپیوتری (بخش اول)

۳. آشنائی با حملات DoS

شاید تاکنون شنیده باشید که یک وب سایت مورد تهاجمی از نوع DoS قرار گرفته است. این نوع از حملات صرفا" متوجه وب سایت ها نبوده و ممکن است شما قربانی بعدی باشید. تشخیص حملات DoS از طریق عملیات متداول شبکه امری مشکل است ولی با مشاهده برخی علائم در یک شبکه و یا کامپیوتر می توان از میزان پیشرفت این نوع از حملات آگاهی یافت .

۴. حملات از نوع DoS (denial-of-service)

در یک تهاجم از نوع DoS، یک مهاجم باعث ممانعت دستیابی کاربران تائید شده به اطلاعات و یا سرویس‌های خاصی می‌نماید . یک مهاجم با هدف قرار دادن کامپیوتر شما و اتصال شبکه‌ای آن و یا کامپیوترها و شبکه ای از سایت‌هائی که شما قصد استفاده از آنان را دارید، باعث سلب دستیابی شما به سایت‌های Email، وب‌سایت‌ها، account های online و سایر سرویس های ارائه شده بر روی کامپیوترهای سرویس دهنده می گردد .

متداولترین و مشهودترین نوع حملات DoS، زمانی محقق می گردد که یک مهاجم اقدام به ایجاد یک سیلاب اطلاعاتی در یک شبکه نماید. زمانی که شما آدرس URL یک وب‌سایت خاص را از طریق مرورگر خود تایپ می‌نمائید، درخواست شما برای سرویس دهنده ارسال می‌گردد. سرویس‌دهنده در هر لحظه قادر به پاسخگوئی به حجم محدودی از درخواست‌ها می‌باشد، بنابراین اگر یک مهاجم با ارسال درخواست‌های متعدد و سیلاب گونه باعث افزایش حجم عملیات سرویس دهند گردد، قطعا" امکان پردازش درخواست شما برای سرویس‌دهنده وجود نخواهد داشت. حملات فوق از نوع DoS می باشند، چرا که امکان دستیابی شما به سایـت مورد نظر سلب شده است.

یک مهاجم می‌تواند با ارسال پیام‌های الکترونیکی ناخواسته که از آنان با نام Spam یاد می‌شود، حملات مشابهی را متوجه سرویس دهنده پست الکترونیکی نماید. هر account پست الکترونیکی (صرفنظر از منبعی که آن را در اختیار شما قرار می دهد، نظیر سازمان مربوطه و یا سرویس های رایگانی نظیر یاهو و hotmail) دارای ظرفیت محدودی می‌باشند. پس از تکمیل ظرفیت فوق، عملا" امکان ارسال Email دیگری به account فوق وجود نخواهد داشت. مهاجمان با ارسال نامه‌های الکترونیکی ناخواسته سعی می‌نمایند که ظرفیت account مورد نظر را تکمیل و عملا" امکان دریافت email های معتبر را از account فوق سلب نمایند .

۵. حملات از نوع DDoS (distributed denial-of-service)

در یک تهاجم از نوع DDoS، یک مهاجم ممکن است از کامپیوتر شما برای تهاجم بر علیه کامپیوتر دیگری استفاده نماید . مهاجمان با استفاده از نقاط آسیب پذیر و یا ضعف امنتیی موجود بر روی سیستم شما می توانند کنترل کامپیوتر شما را بدست گرفته و در ادامه از آن به منظور انجام عملیات مخرب خود استفاده نمایند. ارسال حجم بسیار بالائی داده از طریق کامپیوتر شما برای یک وب‌سایت و یا ارسال نامه‌های الکترونیکی ناخواسته برای آدرس های Email خاصی، نمونه‌هائی از همکاری کامپیوتر شما در بروز یک تهاجم DDOS می‌باشد . حملات فوق، "توزیع شده " می‌باشند، چراکه مهاجم از چندین کامپیوتر به منظور اجرای یک تهاجم DoS استفاده می نماید.

۶. نحوه پیشگیری از حملات

متاسفانه روش موثری به منظور پیشگیری در مقابل یک تهاجم DoS و یا DDoS وجود ندارد . علیرغم موضوع فوق، می‌توان با رعایت برخی نکات و انجام عملیات پیشگیری،

احتمال بروز چنین حملاتی (استفاده از کامپیوتر شما برای تهاجم بر علیه سایر کامپیوترها) را کاهش داد .

- نصب و نگهداری نرم افزار آنتی ویروس (جایگاه نرم افزارهای ضدویروس) .
- نصب و پیکربندی یک فایروال (فایروال چیست ؟)
- تبعیت از مجموعه سیاست‌های خاصی در خصوص توزیع و ارائه آدرس Email (توصیه هائی برای کاهش Spam) .

۷. چگونه از وقوع حملات DoS و یا DDoS آگاه شویم ؟

خرابی و یا بروز اشکال در یک سرویس شبکه، همواره بدلیل بروز یک تهاجم DoS نمی‌باشد . در این رابطه ممکن است دلایل متعددی فنی وجود داشته و یا مدیر شبکه به منظور انجام عملیات نگهداری موقتا" برخی سرویس ها را غیر فعال کرده باشد . وجود و یا مشاهده علائم زیر می تواند نشان‌دهنده بروز یک تهاجم از نوع DoS و یا DDoS باشد :

- کاهش سرعت و یا کارایی شبکه به طرز غیرمعمول (در زمان باز نمودن فایل ها و یا دستیابی به وب‌سایت ها) .
- عدم در دسترس بودن یک سایـت خاص (بدون وجود دلایل فنی)
- عدم امکان دستیابی به هر سایتی (بدون وجود دلایل فنی)
- افزایش محسوس حجم نامه‌های الکترونیکی ناخواسته دریافتی

8. در صورت بروز یک تهاجم، چه عملیاتی را می‌بایست انجام داد ؟

حتی در صورتی که شما قادر به شناسائی حملات از نوع DoS و یا DDoS باشید، امکان شناسائی مقصد و یا منبع واقعی تهاجم، وجود نخواهد داشت . در این رابطه لازم است با

کارشناسان فنی ماهر، تماس گرفته تا آنان موضوع را بررسی و برای آن راهکار مناسب را ارائه نمایند .

- در صورتی که برای شما مسلم شده است که نمی‌توانید به برخی از فایل‌های خود و یا هر وب سایتی خارج از شبکه خود دستیابی داشته باشید، بلافاصله با مدیران شبکه تماس گرفته و موضوع را به اطلاع آنان برسانید . وضعیت فوق می تواند نشان‌دهنده بروز یک تهاجم بر علیه کامپیوتر و یا سازمان شما باشد .

در صورتی که وضعیت مشابه آنچه اشاره گردید را در خصوص کامپیوترهای موجود در منازل مشاهده می‌نمائید با مرکز ارائه دهنده خدمات اینترنت (ISP) تماس گرفته و موضوع را به اطلاع آنان برسانید . ISP مورد نظر می تواند توصیه های لازم به منظور انجام عملیات مناسب را در اختیار شما قرار دهد .

۹. مزایای استفاده از BCC

به منظور ارسال نامه‌های الکترونیکی از برنامه‌های متعددی نظیر Outlook استفاده می‌گردد. برای مشخص نمودن آدرس دریافت‌کنندگان یک Email می توان از فیلدهای To و یا CC استفاده نمود . در برخی موارد استفاده از فیلد BCC گزینه‌ای مناسب و در عین حال ایمن‌تر به منظور ارسال نامه های الکترونیکی است.

10. BCC چیست ؟

BCC از کلمات blind carbon copy، اقتباس شده است. با استفاده از BCC، امکان مخفی نگه داشتن آدرس دریافت‌کنندگان یک Email، فراهم می‌گردد. بر خلاف آدرس‌هائی که در فیلد To و یا CC درج و امکان مشاهده آنان توسط سایر دریافت کنندگان وجود دارد، امکان مشاهده آدرس‌های درج شده در فیلد BCC توسط سایر

دریافت‌کنندگان وجود نخواهد داشت (ارسال نسخه ای از نامه به شخص ثالث بدون این که به دریافت کننده اولیه نامه اطلاعی داده شده باشد).

11. چرا می‌بایست از BCC استفاده نمود ؟

در این رابطه می توان به دلایل زیر اشاره نمود :

- **محرمانگی** : در برخی موارد لازم است که به دریافت‌کنندگان یک Email این امکان داده شود تا بدانند چه افراد دیگری نیز آن را دریافت داشته‌اند . در برخی حالات دیگر ممکن است شما قصد ارسال یک Email برای چندین دریافت‌کننده را دارید و نمی‌خواهید آنان نسبت به این موضوع آگاه گردند که نامه ارسالی توسط چه افراد دیگری نیز دریافت شده است . مثلا" زمانی که شما یک Email را به نمایندگی از سازمان و یا یک موسسه تجاری برای مشتریان خود ارسال می‌نمائید، صیانت از لیست مشتریان، بسیار حائز اهمیت می‌باشد. در صورتی که از فیلدهای To و یا CC به منظور ارسال یک Email برای دریافت‌کنندگان متعددی استفاده می‌گردد، دریافت کنندگان Email هرگونه پاسخی که به پیام ارسالی داده خواهد شد را نیز دریافت خواهند کرد (مگر این که فرستنده آنان را از لیست حذف نماید).
- **پیگیری** : در صورتی که قصد پیگیری، دستیابی و یا آرشیو نامه‌های الکترونیکی ارسالی بر روی یک account دیگر را داشته باشید، می توان از BCC استفاده نمود . در چنین مواردی یک نسخه از نامه‌های الکترونیکی ارسالی به صورت اتوماتیک به یک account دیگر و بدون اطلاع دریافت کنندگان Email ارسال می‌گردد .
- **رعایت حقوق دریافت کنندگان** : نامه‌های الکترونیکی فوروارد شده ، اغلب شامل لیست‌های طولانی از آدرس‌هائی است که توسط فرستنده قبلی و با استفاده از فیلد CC، ارسال شده است . اینگونه آدرس‌ها عموما" فعال و معتبر بوده و خوراک مناسبی برای

توزیع‌کنندگان نامه‌های الکترونیکی ناخواسته، خواهند بود. علاوه بر این، تعداد زیادی از نامه‌های الکترونیکی حاوی ویروس از آدرس‌های Email موجود در پیام‌هائی که شما دریافت می‌نمائید، استفاده نموده و اقدام به جمع‌آوری آدرس‌های فوق می‌نمایند. بنابراین، وجود اینگونه لیست‌های طولانی در پیام‌های فورورد شده، تمامی آدرس‌های موجود در لیست را در معرض تهدید قرار خواهد داد (در صورت آلودگی پیام‌های دریافتی).

تعداد زیادی از استفاده‌کنندگان نامه‌های الکترونیکی، پیام‌های دریافتی را با استفاده از فیلد CC برای تمامی اعضاء موجود در دفترچه آدرس خود، فورورد می‌نمایند. پیشنهاد می‌گردد، دوستان خود را تشویق نمائید در مواردی که قصد فورورد پیام‌هائی را برای شما دارند از فیلد BCC، استفاده نمایند. در چنین مواردی، امکان مشاهده آدرس Email شما توسط سایر افراد کمتر می گردد. به منظور پیشگیری در مقابل اینگونه مسائل، پیشنهاد می‌گردد علاوه بر استفاده از BCC در صورت فورورد نمودن پیام‌ها، تمامی آدرس‌های Email موجود در پیام، نیز حذف گردد.

۱۲. چگونه می توان از BCC استفاده نمود ؟

اکثر برنامه‌های ارسال Email دارای گزینه‌ای به منظور استفاده از فیلد BCC (پائین‌تر از فیلد To)، می باشند. در برخی موارد، ممکن است گزینه فوق به صورت پیش فرض فعال نشده باشد و لازم است از یک گزینه دیگر به منظور فعال نمودن آن استفاده گردد. مثلا" در برنامه Outlook به منظور فعال نمودن فیلد BCC، می‌توان از طریق منوی View گزینه All headers را در زمان ایجاد یک نامه الکترونیکی جدید، انتخاب نمود .

در صورتی که قصد دارید تمامی دریافت کنندگان یک Email را در فیلد BCC مشخص نمائید و برنامه ارسال کننده، اجازه ارسال یک نامه الکترونیکی بدون درج یک آدرس در فیلد To را نمی‌دهد، می توانید آدرس Email خود را در فیلد To درج نمائید. بدین ترتیب، علاوه بر مخفی نگه داشتن هویت سایر دریافت‌کنندگان می توان از ارسال موفقیت آمیز یک پیام نیز اطمینان حاصل نمود .

13.حفاظت کامپیوتر قبل از اتصال به اینترنت

تعداد بسیار زیادی از کاربران اینترنت را افرادی تشکیل می‌دهند که فاقد مهارت‌های خاصی در زمینه فن آوری اطلاعات بوده و از امکانات حمایتی مناسبی نیز برخوردار نمی‌باشند. سیستم‌های اینگونه کاربران دارای استعداد لازم به منظور انواع تهاجمات بوده و بطور غیر مستقیم شرایط مناسبی را برای مهاجمان به منظور نیل به اهداف مخرب آنان، فراهم می‌نمایند. بر اساس گزارشات متعددی که در چندین ماه اخیر منتشر شده است، تعداد حملات و آسیب پذیری اینگونه سیستم‌ها، بطرز کاملا" محسوسی افزایش یافته است. علت این امر را می توان در موارد زیر جستجو نمود :

- تعداد بسیاری از تنظیمات پیش‌فرض کامپیوترها، غیر ایمن می‌باشد .
- کشف نقاط آسیب پذیر جدید در فاصله بین زمانی که کامپیوتر تولید و پیکربندی می‌گردد و تنظیماتی که اولین مرتبه توسط کاربر انجام می شود.
- در مواردی که ارتقاء یک نرم‌افزار از طریق رسانه‌های ذخیره‌سازی نظیر CD و یا DVD انجام می شود، همواره این احتمال وجود خواهد داشت که ممکن است نقاط آسیب پذیر جدیدی نسبت به زمانی که نرم افزار بر روی رسانه مورد نظر مستقر شده است، کشف شده باشد .
- مهاجمان دارای آگاهی لازم در خصوص دامنه‌های آدرس های IP از نوع Dial-up و یا Broadband بوده و آنان را بطور مرتب پایش می نمایند .

•کرم های بسیار زیادی بطور مرتب و پیوسته بر روی اینترنت در حال فعالیت بوده تا کامپیوترهای آسیب پذیر را شناسائی نمایند .

با توجه به موارد فوق، متوسط زمان لازم به منظور یافتن کامپیوترهای آسیب پذیر در برخی شبکه‌های کامپیوتر به مرز دقیقه رسیده است .

توصیه‌های استاندارد به کاربران خانگی، Download و نصب Patch های نرم افزاری در اسرع وقت و پس از اتصال یک کامپیوتر جدید بر روی اینترنت است. فرآیند فوق، با توجه به این که مهاجمان به صورت دائم اقدام به پایش و یافتن قربانیان خود می نمایند، ممکن است در موارد متعددی توام با موفقیت کامل نگردد .

به منظور حفاظت کامپیوترها قبل از اتصال به اینترنت و نصب هر یک از Patch های مورد نیاز، موارد زیر پیشنهاد می‌گردد :

- **در صورت امکان، کامپیوتر جدید را از طریق یک فایروال شبکه‌ای (مبتنی بر سخت افزار) و یا روتر فایروال به شبکه متصل نمائید.**

یک فایروال شبکه‌ای و یا روتر فایروال، سخت‌افزاری است که کاربران می‌توانند آن را بین کامپیوترهای موجود در یک شبکه و دستگاههای Broadband نظیر مودم کابلی و یا DSL نصب نمایند. با بلاک نمودن امکان دستیابی به کامپیوترهای موجود بر روی یک شبکه محلی از طریق اینترنت، یک فایروال سخت‌افزاری قادر به ارائه یک سطح حفاظتی مناسب برای کاربران در خصوص دریافت و نصب patch های نرم افزاری ضروری خواهد بود.

در صورتی که قصد اتصال کامپیوتر خود به اینترنت را از طریق یک فایروال و یا روتری با پتانسیل NAT: Network Address Translation، داشته باشید و یکی از موارد زیر درست باشد: الف) ماشین جدید تنها کامپیوتر متصل شده به شبکه محلی از طریق

فایروال است. ب) سایر ماشین های متصل شده به شبکه محلی پشت فایروال نسبت به نصبpatch های مورد نیاز بهنگام بوده و بر روی آنان کرم‌ها و یا ویروس هائی وجود نداشته باشد، ممکن است به وجود یک فایروال نرم‌افزاری نیاز نباشد.

- **در صورت امکان، از فایروال نرم‌افزاری همراه کامپیوتر نیز استفاده نمائید.**

در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال نرم افزاری از قبل تعبیه شده می‌باشد، پیشنهاد می‌گردد آن را فعال نموده تا امکان اتصال سایرین به شما وجود نداشته باشد. همانگونه که اشاره گردید، در صورتی که کامپیوتر شما از طریق یک فایروال به شبکه متصل است و تمامی کامپیوترهای موجود در شبکه محلی نسبت به نصب هر یک از Patch های مورد نیاز بهنگام شده می‌باشند، این مرحله می تواند اختیاری باشد. علیرغم موضوع فوق، در بخشی از استراتژی "دفاع در عمق" به این موضوع اشاره شده است که بهتر است فایروال نرم افزاری ارائه شده همراه سیستم عامل، همواره فعال گردد. در صورتی که سیستم عامل موجود برروی کامپیوتر شما دارای یک فایروال نرم افزاری از قبل تعبیه شده نمی‌باشد ، می توان یک نرم افزار فایروال مناسب را تهیه نمود. پیشنهاد می گردد که اینگونه نرم افزارها از طریق رسانه های ذخیره سازی نظیر CD و یا DVD نصب گردند (در مقابل اتصال به یک شبکه و دریافت نرم افزار مورد نیاز از یک کامپیوتر حفاظت نشده). در غیر اینصورت همواره این احتمال وجود خواهد داشت که کامپیوتر شما قبل از اینکه قادر به دریافت و نصب اینچنین نرم‌افزارهائی گردد، مورد تهاجم واقع شود.

- **غیرفعال نمودن سرویس‌های غیرضروری نظیر "اشتراک فایل و چاپگر"**

اکثر سیستم‌های عامل به صورت پیش‌فرض پتانسیل "اشتراک فایل و چاپ " را فعال نمی‌نمایند. در صورتی که شما سیستم خود را به یک سیستم‌عامل جدید ارتقاء داده‌اید

و کامپیوتر دارای گزینه فعال "اشتراک فایل و چاپ " می باشد، بدیهی است که سیستم عامل جدید نیز این گزینه را فعال نماید. سیستم‌عامل جدید ممکن است دارای نقاط آسیب‌پذیری باشد که شما آنان را در نسخه قبلی سیستم عامل مربوطه از طریق نصب تمامی patchهای مورد نیاز، برطرف کرده باشید و در سیستم عامل جدید این وضعیت وجود ندارد. برای حل مشکل فوق پیشنهاد می‌گردد قبل از ارتقاء سیستم عامل، پتانسیل "اشتراک فایل و چاپ " را غیرفعال نموده و در ادامه فرآیند ارتقاء را انجام دهید. پس از ارتقاء سیستم و نصب Patch های مورد نیاز ، می توان در صورت ضرورت اقدام به فعال نمودن پتانسیل "اشتراک فایل و چاپ " نمود.

- **دریافت و نصب patch های مورد نیاز**

پس از ایمن‌سازی کامپیوتر در مقابل حملات با استفاده از فایروال های سخت افزاری و یا نرم افزاری و غیرفعال نمودن پتانسیل "اشتراک فایل و چاپ "، می توان با اطمینان بیشتری سیستم خود را به منظور دریافت و نصب patch های مورد نیاز به شبکه متصل نمود. به منظور دریافت patch های نرم‌افزاری، توصیه می‌گردد که حتما" از سایت‌های ایمن و مطمئن (وب‌سایت تولیدکنندگان) استفاده گردد. بدین ترتیب احتمال این که یک مهاجم قادر به دستیابی سیستم شما از طریق برنامه هائی موسوم به Trojan گردد، کاهش می‌یابد.

14. پیشگیری از حملات مهندسی اجتماعی و کلاهبرداری

آیا شما از جمله افرادی می باشید که به ظاهر افراد و نحوه برخورد آنان بسیار اهمیت داده و با طرح صرفا" یک سوال از جانب آنان، هر آنچه را که در ارتباط با یک موضوع خاص می دانید در اختیار آنان قرار می‌دهید؟ رفتار فوق گرچه می تواند در موارد زیادی دستاوردهای مثبتی را برای شما بدنبال داشته باشد، ولی در برخی حالات نیز ممکن است

چالش ها و یا مسائل خاصی را برای شما و یا سازمان شما، ایجاد نماید. آیا وجود اینگونه افراد در یک سازمان مدرن اطلاعاتی (خصوصا" سازمانی که با داده های حساس و مهم سروکار دارد) نمی‌تواند تهدیدی در مقابل امنیت آن سازمان محسوب گردد ؟ به منظور ارائه اطلاعات حساس خود و یا سازمان خود از چه سیاست‌ها و رویه‌هائی استفاده می‌نمائید؟ آیا در چنین مواردی تابع مجموعه مقررات و سیاست‌های خاصی می‌باشید؟ صرفنظر از پاسخی که شما به هر یک از سوالات فوق خواهید داد، یک اصل مهم در این راستا وجود دارد که می بایست همواره به آن اعتقاد داشت : " هرگز اطلاعات حساس خود و یا سازمان خود را در اختیار دیگران قرار نداده مگر این که مطمئن شوید که آن فرد همان شخصی است که ادعا می‌نماید و می بایست به آن اطلاعات نیز دستیابی داشته باشد ."

15. یک حمله مهندسی اجتماعی چیست ؟

به منظور تدارک و یا برنامه‌ریزی یک تهاجم از نوع حملات مهندسی اجتماعی، یک مهاجم با برقراری ارتباط با کاربران و استفاده از مهارت‌های اجتماعی خاص (روابط عمومی مناسب، ظاهری آراسته و ...) ، سعی می نماید به اطلاعات حساس یک سازمان و یا کامپیوتر شما دستیابی و یا به آنان آسیب رساند. یک مهاجم ممکن است خود را به عنوان فردی متواضع و قابل احترام نشان دهد. مثلا" وانمود نماید که یک کارمند جدید است، یک تعمیرکار است و یا یک محقق و حتی اطلاعات حساس و شخصی خود را به منظور تائید هویت خود به شما ارائه نماید. یک مهاجم، با طرح سوالات متعدد و برقراری یک ارتباط منطقی بین آنان، می‌تواند به بخش‌هائی از اطلاعات مورد نیاز خود به منظور نفوذ در شبکه سازمان شما دستیابی پیدا نماید. در صورتی که یک مهاجم قادر به اخذ اطلاعات مورد نیاز خود از یک منبع نگردد، وی ممکن است با شخص دیگری از همان

سازمان ارتباط برقرار نموده تا با کسب اطلاعات تکمیلی و تلفیق آنان با اطلاعات اخذ شده از منبع اول، توانمندی خود را افزایش دهد. (یک قربانی دیگر !).

۱۶. یک حمله Phishing چیست ؟

این نوع از حملات شکل خاصی از حملات مهندسی اجتماعی بوده که با هدف کلاهبرداری و شیادی سازماندهی می‌شوند. در حملات فوق از آدرس‌های Email و یا وب‌سایت‌های مخرب به منظور جلب نظر کاربران و دریافت اطلاعات شخصی آنان نظیر اطلاعات مالی استفاده می گردد. مهاجمان ممکن است با ارسال یک Email با ظاهری قابل قبول و از یک شرکت معتبر کارت اعتباری و یا موسسات مالی ، از شما درخواست اطلاعات مالی را نموده و اغلب عنوان نمایند که یک مشکل خاص ایجاد شده است و ما درصدد رفع آن می‌باشیم. پس از پاسخ کاربران به اطلاعات درخواستی، مهاجمان از اطلاعات اخذ شده به منظور دستیابی به سایر اطلاعات مالی و بانکی استفاده می‌نمایند.

17. نحوه پیشگیری از حملات مهندسی اجتماعی و کلاهبرداری

- به تلفن‌ها، نامه‌های الکترونیکی و ملاقات‌هائی که عموما" ناخواسته بوده و در آنان از شما درخواست اطلاعاتی خاص در مورد کارکنان و یا سایر اطلاعات شخصی می‌گردد، مشکوک بوده و با دیده سوء ظن به آنان نگاه کنید. در صورتی که یک فرد ناشناس ادعا می‌نماید که از یک سازمان معتبر است، سعی نمائید با سازمان مورد ادعای وی تماس گرفته و نسبت به هویت وی کسب تکلیف کنید .
- هرگز اطلاعات شخصی و یا اطلاعات مربوط به سازمان خود را (مثلا" ساختار و یا شبکه ها) در اختیار دیگران قرار ندهید، مگر این که اطمینان حاصل گردد که فرد متقاضی مجور لازم به منظور دستیابی به اطلاعات درخواستی را دارا می‌باشد .

• هرگز اطلاعات شخصی و یا مالی خود را در یک email افشاء نکرده و به نامه‌های الکترونیکی ناخواسته‌ای که درخواست این نوع اطلاعات را از شما می‌نمایند، پاسخ ندهید(به لینک های موجود در اینگونه نامه‌های الکترونیکی ناخواسته نیز توجهی نداشته باشید) .

• هرگز اطلاعات حساس و مهم شخصی خود و یا سازمان خود را بر روی اینترنت ارسال ننمائید. قبل از ارسال اینگونه اطلاعات حساس، می بایست Privacy وب‌سایت مورد نظر به دقت مطالعه شده تا مشخص گردد که اهداف آنان از جمع‌آوری اطلاعات شخصی شما چیست و نحوه برخورد آنان با اطلاعات به چه صورت است ؟

• دقت لازم در خصوص آدرس URL یک وب‌سایت را داشته باشید. وب‌سایت‌های مخرب ممکن است خود را مشابه یک وب‌سایت معتبر ارائه نموده که آدرس URL آنان دارای تفاوت اندکی با وب‌سایت‌های شناخته شده باشد. وجود تفاوت اندک در حروف استفاده شده برای نام سایت و یا تفاوت در domain، نمونه‌هائی در این زمینه می‌باشند (مثلا" com . در مقابل net .) .

• در صورت عدم اطمینان از معتبر بودن یک Email دریافتی، سعی نمائید با برقراری تماس مستقیم با شرکت مربوطه نسبت به هویت آن اطمینان حاصل نمائید. از اطلاعات موجود بر روی یک سایت مخرب به منظور تماس با آنان استفاده نمائید چرا که این اطلاعات می تواند شما را به مسیری دیگر هدایت نماید که صرفا" اهداف مهاجمان را تامین نماید. به منظور آگاهی از این نوع حملات که تاکنون به‌وقوع پیوسته است، می‌توانید به آدرس http://www.antiphishing.org/phishing_archive.html، مراجعه نمائید .

• با نصب و نگهداری نرم‌افزارهای آنتی‌ویروس، فایروال‌ها و فیلترینگ نامه‌های الکترونیکی ناخواسته (spam)، سعی نمائید یک سطح حفاظتی مناسب به منظور کاهش این نوع حملات را ایجاد نمائید .

18. اقدامات لازم در صورت بروز تهاجم

- در صورتی که فکر می‌کنید به هر دلیلی اطلاعات حساس سازمان خود را در اختیار دیگران (افراد غیرمجاز) قرار داده‌اید، بلافاصله موضوع را به اطلاع افراد ذیربط شاغل در سازمان خود (مثلا" مدیران شبکه) برسانید. آنان می‌توانند در خصوص هرگونه فعالیت‌های غیرمعمول ویا مشکوک، هشدارهای لازم را در اسرع وقت در اختیار دیگران قرار دهند .
- در صورتی که فکر می‌کنید اطلاعات مالی شما ممکن است در معرض تهدید قرار گرفته شده باشد، بلافاصله با موسسه مالی خود تماس حاصل نموده و تمامی حساب‌های مالی در معرض تهدید را مسدود نمائید. در این رابطه لازم است دقت، حساسیت و کنترل لازم در خصوص هر گونه برداشت از حساب‌های بانکی خود را داشته باشید .
- گزارشی در خصوص نوع تهاجم را تهیه نموده و آن را در اختیار سازمان‌های ذیربط قانونی قرار دهید.

19. توصیه‌هائی برای کاهش Spam

Spam یکی از متداولترین و در عین حال منفی‌ترین جنبه های دارا بودن یک آدرس Email است. با این که در حال حاضر و با توجه به تکنولوژی‌های موجود امکان حذف کامل این نوع از نامه‌های الکترونیکی ناخواسته وجود ندارد، ولی می‌توان با استفاده از برخی روش‌های موجود تعداد آنان را کاهش داد.

۲۰. Spam چیست ؟

Spam، نسخه الکترونیکی از " نامه های بدرد نخور " است . واژه Spam به پیام‌های الکترونیکی ناخواسته، اطلاق می‌گردد . این نوع از نامه‌های الکترونیکی ارتباط مستقیمی با ویروس نداشته و حتی ممکن است پیام‌هائی که از منابع معتبر ارسال شده‌اند نیز در زمره این گروه قرار گیرند .

21.چگونه می‌توان میزان Spam را کاهش داد ؟

با رعایت برخی نکات، می‌توان میزان Spam دریافتی را بطرز محسوسی کاهش داد :

- **آدرس Email خود را بدون دلیل در اختیار دیگران قرار ندهید** . آدرس‌های پست الکترونیکی به اندازه‌ای متداول شده‌اند که شما می‌توانید بر روی هر فرمی که به منظور کسب اطلاعات شما در نظر گرفته می‌شود، وجود فیلد خاصی به منظور دریافت آدرس Email را مشاهد نمائید. تعدادی زیادی از مردم بدون درنظر گرفتن مسائل جانبی، آدرس Email خود را در هر محلی و یا هر فرمی درج می‌نمایند. مثلا" شرکت‌ها، اغلب آدرس‌ها را در یک بانک اطلاعاتی ثبت تا بتوانند وضعیت مشتیریان خود را در آینده دنبال نمایند. برخی اوقات، اطلاعات فوق به سایر شرکت‌ها فروخته شده و یا امکان استفاده مشترک برای آنان، فراهم می‌گردد. بدیهی است در چنین مواردی ممکن است برای شما یک Email و از طرف شرکتی ارسال شود که نه توقع آن را داشته‌اید و نه از آنان درخواستی مبنی بر ارائه اطلاعات خاصی را داشته‌اید.
- **بررسی سیاست‌های محرمانگی**: قبل از ارسال آدرس Email خود به صورت online، بدنبال Privacy سایت مورد نظر بگردید. تعداد بسیار زیادی از سایت های شناخته شده و خوشنام دارای یک لینک خاص بر روی سایت خود به منظور آشنائی کاربران با سیاست‌های آن سایت در خصوص نحوه برخورد با اطلاعات ارسالی شما می‌باشند. (همواره این پرسش را برای خود مطرح نمائید که آیا ما آدرسEmail خود را در سایت‌هائی درج می‌نماییم که نسبت به آنان شناخت کافی داریم ؟) . شما

می‌بایست قبل از ارسال آدرس Email خود و یا سایر اطلاعات شخصی، سیاست‌های اعلام شده توسط سایت مورد نظر را مطالعه نموده و از این موضوع آگاه شوید که مالکین و یا مسئولین سایت قصد انجام چه کاری را با اطلاعات ارسالی شما دارند .

- **دقت لازم در خصوص گزینه‌هائی که به صورت پیش‌فرض فعال شده‌اند** .

زمانی که شما برای دریافت خدمات و یا Account جدید عملیات sign in را انجام می‌دهید، ممکن است بخشی وجود داشته باشد که به شما مجموعه‌ای از گزینه ها را در خصوص دریافت email در خصوص محصولات و یا سرویس های جدید، ارائه نماید. در برخی مواقع، گزینه‌ها به صورت پیش‌فرض انتخاب شده‌اند، بنابراین در صورتی که شما آنان را به همان وضعیت باقی بگذارید، در آینده نه چندان دور برای شما حجم زیادی از نامه‌های الکترونیکی که شاید انتظار آنان را نداشته باشد، ارسال گردد .

- **استفاده از فیلترها** : تعدادی زیادی از برنامه‌های پست الکترونیکی امکان فیلترینگ را ارائه می‌نمایند. پتانسیل فوق به شما این اجازه را خواهد داد که آدرس‌های خاصی را بلاک نموده و یا امکان دریافت نامه را صرفا" از طریق لیست تماس موجود بر روی کامپیوتر خود، داشته باشید. برخی مراکز ارائه دهنده خدمات اینترنت (ISP) نیز سرویس فیلترینگ و علامت‌گذاری مربوط به مقابله با Spam را ارائه می‌نمایند. در چنین مواردی ممکن است پیام‌های معتبری که بدرستی طبقه بندی نشده باشند به عنوان spam درنظر گرفته شده و هرگز به صندوق پستی شما ارسال نگردند .
- **هرگز برروی لینک‌های موجود در یک Spam ،کلیک ننمائید** . برخی از منابع ارسال‌کننده Spam با ارسال آدرس های Email متغیر در یک Domain خاص، سعی در تشخیص معتبر بودن یک آدرس Email می‌نمایند. (مثلا" تشخیص آدرس‌های Email معتبر موجود بر روی hotmail و یا yahoo). در صورتی که شما بر روی یک لینک ارسالی توسط یک Spam کلیک نمائید، صرفا" معتبر بودن

آدرس Email خود را به اطلاع آنان رسانده‌اید. پیام‌های ناخواسته‌ای که یک گزینه "عدم عضویت " وسوسه انگیز را در اختیار شما قرار می‌دهند، اغلب به عنوان روشی به منظور جمع‌آوری آدرس‌های Email معتبر مورد استفاده قرار گرفته که در آینده از آنان به منظور ارسال Spam استفاده گردد.

- **غیرفعال نمودن گزینه دریافت اتوماتیک گرافیک در نامه‌های الکترونیکی با فرمت HTML** . تعداد زیادی از شرکت‌ها، نامه‌های الکترونیکی را با فرمت HTML و همراه با یک فایل گرافیکی لینک شده ارسال نموده که در ادامه از آن به منظور ردیابی فردی که پیام الکترونیکی را باز نموده است، استفاده می‌نمایند. زمانی که برنامه سرویس گیرنده پست الکترونیکی شما، اقدام به download گرافیک از سرویس‌دهنده آنان می‌نماید، آنان می‌دانند که شما پیام الکترونیکی را باز نموده‌اید. با غیرفعال نمودن HTML mail و مشاهده پیام‌ها با فرمت صرفا" متن، می‌توان پیشگیری لازم در خصوص این مسئله را انجام داد .

- **ایجاد و یا بازنمودن Account های جدید اضافی** : تعداد زیادی از سایت‌ها، اقدام به عرضه آدرس پست الکترونیکی به صورت رایگان می‌نمایند. در صورتی که شما بطور مداوم اقدام به ارسال آدرسEmail خود می‌نمائید (برای خرید online، دریافت سرویس و ...) ، ممکن است مجبور به ایجاد یک account دیگر به منظور حفاظت آدرسaccount اولیه خود در مقابل spam شوید. شما همچنین می‌بایست از یک account دیگر در زمانی که اطلاعاتی را بر روی بولتن‌های خبری online، اطاق‌های چت، لیست‌های عمومی Mailing و یا USENET ارسال می‌نمائید، استفاده نمائید . بدین ترتیب می توان یک سطح حفاظتی مناسب در خصوص دریافت spam به آدرس Email اولیه خود را ایجاد کرد.

برای سایرین Spam ارسال ننمائید . یک کاربر متعهد و دلسوز باشید. در خصوص پیام‌هائی که قصد فوروارد نمودن آنان را دارید، سختگیرانه عمل کنید. هرگز هرگونه پیامی را برای هر شخص موجود در لیست دفترچه آدرس خود فوروارد نکرده و اگر فردی از شما بخواهد که پیامی را برای وی فوروارد ننمائید، به درخواست وی احترام بگذارید .

22.آشنائی با محتویات فعال و کوکی

هر یک از ما در مدت زمان اتصال به اینترنت از وب‌سایت‌ها و یا وبلاگ‌های متعددی دیدن می‌نمائیم. طراحان و پیاده‌کنندگان وب‌سایت‌ها و وبلاگ‌ها به منظور ارائه خدمات مورد نظر خود از امکانات و یا بهتر بگوئیم تکنولوژی های متفاوتی استفاه می‌نمایند. اغلب ملاقات‌کنندگان، احساس خاصی نسبت به این تکنولوژی‌ها نداشته و صرفا" برای آنان نوع سرویس‌ها و خدمات ارائه شده دارای اهمیت است. برخی از تکنولوژی‌های استفاده شده علیرغم داشتن جنبه‌های مثبت و مهم به ابزارهائی برای برنامه‌ریزی برخی حملات تبدیل شده و حریم خصوصی کاربران را به‌مخاطره می اندازد. محتویات فعال (Active contents) و کوکی‌ها (Cookies) از جمله موارد فوق، می‌باشند.

23. کوکی چیست ؟

در زمان استفاده از اینترنت، امکان جمع‌آوری و ذخیره اطلاعات شما وجود خواهد داشت. اطلاعات فوق ممکن است اطلاعاتی عمومی در خصوص کامپیوتر شما نظیر آدرس IP، نام Domain استفاده شده به منظور ارتباط با اینترنت، نوع مرورگر و سیستم عامل باشد. اطلاعات جمع‌آوری شده می‌تواند شامل موارد خاصی نظیر آخرین مرتبه‌ای که یک وب‌سایت را ملاقات نموده‌اید و یا اطلاعات شخصی شما در زمان استفاده از یک وب‌سایت خاص نظیر آدرس پست الکترونیکی باشد .

- **Session cookie** . این نوع کوکی‌ها صرفا" و تا زمانی که از مرورگر استفاده می‌گردد، اطلاعاتی را ذخیره نموده و پس از بستن مرورگر اطلاعات از بین می‌رود. هدف از بکارگیری این نوع کوکی‌ها، ارائه تسهیلات لازم در خصوص حرکت بین صفحات متعدد است. مثلا" تشخیص مشاهده یک صفحه خاص و یا نگهداری اطلاعاتی در خصوص داده‌های مرتبط با یک صفحه .
- **cookie Persistent** : این نوع کوکی‌ها اطلاعاتی را بر روی کامپیوتر شما ذخیره می‌نمایند. بدین ترتیب امکان نگهداری اطلاعات شخصی مرتبط با شما فراهم می‌گردد . در اکثر مرورگرها برای این نوع از کوکی‌ها می توان یک مدت زمان خاص را مشخص نمود(عمر مفید) . در صورتی که یک مهاجم امکان دستیابی به کامپیوتر شما را پیدا نماید، می‌تواند با مشاهده محتویات فایل های فوق به اطلاعات شخصی شما دسترسی نماید.

به منظور افزایش سطح ایمنی خود، می بایست تنظیمات امنیتی لازم در خصوص اعمال محدودیت و یا بلاک نمودن کوکی‌ها را در جهت حفظ حریم خصوصی، انجام داد. در صورتی که از یک کامپیوتر عمومی استفاده می‌نمائید، می‌بایست کوکی‌ها را غیرفعال نموده تا پیشگیری لازم در خصوص دستیابی سایرین به اطلاعات شخصی شما، صورت پذیرد.

24. جایگاه نرم افزارهای ضدویروس

با استفاده از نرم افزارهای ضدویروس، امکان شناسائی و بلاک نمودن ویروسها قبل از آسیب رساندن به سیستم شما، فراهم می‌گردد. با نصب این نوع نرم‌افزارها بر روی سیستم خود یک سطح حفاظتی مناسب در خصوص ایمن‌سازی کامپیوتر و اطلاعات موجود بر روی آن ایجاد خواهد شد. به منظور استمرار سطح حفاظتی ایجاد شده، می‌بایست نرم

افزارهای ضدویروس بطور دائم بهنگام شده تا امکان شناسائی ویروس‌های جدید، وجود داشته باشد.

25. نرم‌افزارهای ضد ویروس، چه کار می‌کنند ؟

جزئیات عملکرد هر یک از برنامه‌های ضد ویروس با توجه به نوع هر یک از نرم‌افزارهای موجود، متفاوت است. اینگونه نرم‌افزارها فایل‌های موجود بر روی کامپیوتر و یا حافظه کامپیوتر شما را به منظور وجود الگوهایی خاص که می‌تواند باعث ایجاد آلودگی گردند را پویش می‌نمایند. برنامه‌های ضد ویروس بدنبال الگوهائی مبتنی بر علائم خاص، تعاریفی خاص و یا ویروس‌های شناخته شده، می‌گردند. نویسندگان ویروس‌های کامپیوتری همواره اقدام به نوشتن ویروس‌های جدید نموده و ویروس‌های نوشته شده قبلی خود را بهنگام می‌نمایند. بنابراین لازم است که همواره بانک اطلاعاتی شامل تعاریف و الگوهای ویروس‌های کامپیوتری مربوط به نرم افزار، بهنگام گردد. پس از نصب یک نرم‌افزار آنتی‌ویروس بر روی کامپیوتر خود، می‌توان عملیات پویش و بررسی سیستم به منظور آگاهی از وجود ویروس را در مقاطع زمانی مشخص و بصورت ادواری انجام داد. در این رابطه می توان از دو گزینه متفاوت استفاده نمود :

- **پویش اتوماتیک** : برخی از برنامه‌های ضدویروس دارای پتانسیلی به منظور پویش اتوماتیک فایل‌ها و یا فولدرهایی خاص و در یک محدوده زمانی مشخص شده، می‌باشند.
- **پویش دستی** : پیشنهاد می‌گردد، پس از دریافت هرگونه فایلی از منابع خارجی و قبل از فعال نمودن و استفاده از آن، عملیات بررسی و پویش آن به منظور شناسائی ویروس صورت پذیرد. بدین منظور عملیات زیر توصیه می‌گردد:

- ذخیره و پویش ضمائم نامه‌های الکترونیکی و یا نرم‌افزارهائی که از طریق اینترنت Download می نمایید (هرگز ضمائم نامه‌های الکترونیکی را مستقیما" و بدون بررسی آن توسط یک برنامه ضدویروس، فعال ننمائید) .

- بررسی فلاپی دیسک‌ها ، CD و یا DVD به منظور یافتن ویروس بر روی آنان قبل از باز نمودن هر گونه فایلی

26. از کدام نرم‌افزار می‌بایست استفاده نمود ؟

تولیدکنندگان متعددی اقدام به طراحی و پیاده‌سازی نرم‌افزارهای آنتی‌ویروس می‌نمایند. عملکرد این نوع نرم‌افزارها مشابه یکدیگر می‌باشد. به منظور انتخاب یک نرم‌افزار ضدویروس می‌توان پارامترهای متعددی نظیر ویژگی‌های ارائه شده توسط نرم افزار، قیمت و میزان انطباق آنان با خواسته‌های موجود را بررسی نمود. نصب هر نوع نرم افزار ضدویروس (صرفنظر از نرم افزاری انتخاب شده)، باعث افزایش حفاظت شما در مقابل ویروس‌ها می‌گردد. برخی از پیام‌های ارسالی که ادعا می‌نمایند شامل نرم‌افزارهای ضدویروس بوده و یا اینگونه نرم‌افزارها را به شما معرفی می‌نمایند، خود به منزله یک ویروس بوده و می‌بایست دقت لازم در خصوص بازنمودن آنان و ضمائم مربوطه را داشته باشیم .

۲۷. چگونه می‌توان از آخرین اخبار و اطلاعات مربوط به ویروس‌ها، آگاهی یافت ؟

فرآیند بهنگام سازی در هر نرم‌افزار ضدویروس متفاوت بوده و می‌بایست در زمان انتخاب اینگونه نرم‌افزارها، پتانسیل آنان در خصوص بهنگام سازی بانک اطلاعاتی تعاریف الگوها، بررسی گردد. تعداد زیادی از نرم‌افزاری ضدویروس دارای گزینه‌ای به منظور بهنگام سازی اتوماتیک، می‌باشند. استفاده از پتانسیل فوق با توجه ایجاد ویروس‌های جدید، امری لازم و اجتناب ناپذیر است .

نصب یک نرم افزار ضدویروس، یکی از ساده‌ترین و در عین حال موثرترین روش‌های حفاظت از کامپیوتر است. آیا صرفا" با یک نصب همه چیز تمام شده و ما همواره دارای ایمنی لازم و حفاظت مطلوب خواهیم بود؟ پاسخ به سوال فوق قطعا" منفی بوده و این نوع نرم‌افزارها دارای محدودیت‌های خاص خود نیز می باشند. نرم افزارهای ضد ویروس به منظور شناسائی و برخورد با ویروس ها از الگوهای شناخته شده، استفاده می نمایند . بنابراین طبیعی است که اینگونه نرم افزارها صرفا" قادر به شناسائی و برخورد با ویروس‌هائی می‌باشند که قبلا" الگوی آنان برای نرم افزار معرفی شده باشد. به منظور حفظ اقتدار نرم‌افزارهای ضد ویروس و کمک به آنان در جهت شناسائی و برخورد با ویروس‌های جدید، می‌بایست فرآیند بهنگام‌سازی آنان بطور مداوم و در محدوده‌های زمانی مشخص، تکرار گردد.

۲۸. چگونه می‌توان امکان دستیابی سایر افراد به اطلاعات موجود برروی یک کامپیوتر را به حداقل مقدار ممکن رساند؟

دستیابی به یک کامپیوتر به دو صورت فیزیکی و از راه دور ، امکان‌پذیر می‌باشد. شما می‌توانید بسادگی افرادی را که قادر به دستیابی فیزیکی به سیستم و کامپیوتر شما می‌باشند را شناسائی نمائید. (مثلا" افراد خانواده و یا همکاران) . آیا شناسائی افرادیکه می توانند از راه دور به سیستم شما متصل گردند، نیز امری ساده است ؟ پاسخ سوال فوق، منفی است و شناسائی افرادی که از راه دور به سیستم شما متصل می‌شوند، بمراتب مشکل‌تر خواهد بود. اگر شما دارای یک کامپیوتر هستید و آن را به یک شبکه (مثلا" اینترنت) متصل نموده‌اید، قطعا" در معرض تهدید و آسیب خواهید بود. استفاده‌کنندگان کامپیوتر و کاربران شبکه‌های کامپیوتری (خصوصا" اینترنت)، می‌توانند با رعایت برخی نکات که می‌بایست به عادت تبدیل شوند، ضریب مقاومت و ایمنی سیستم خود را افزایش دهند. در ادامه به برخی از این موارد اشاره می‌گردد :

• قفل نمودن کامپیوتر زمانی که از آن دور هستیم: حتی اگر صرفا" برای چند دقیقه کامپیوتر خود را ترک می‌کنید، زمان کافی برای افراد دیگر به منظور آسیب رساندن به اطلاعات شما وجود خواهد داشت. شما با قفل نمودن کامپیوتر خود، عرصه را برای افرادیکه با نشستن پشت کامپیوتر شما قصد دستیابی بدون محدودیت به تمامی اطلاعات شما را دارند، تنگ خواهید کرد.

•قطع ارتباط با اینترنت زمانی که از آن استفاده نمی‌گردد. پیاده‌سازی فن‌آوری‌هائی نظیر DSL و مودم های کابلی این امکان را برای کاربران فراهم نموده است که همواره به اینترنت متصل و اصطلاحا" online باشند. این مزیت دارای چالش‌های امنیتی خاص خود نیز می‌باشد. باتوجه به این که شما بطور دائم به شبکه متصل می‌باشید، مهاجمان و ویروس‌های کامپیوترهای فرصت بیشتری برای یافتن قربانیان خود خواهند داشت. در صورتی که کامپیوتر شما همواره به اینترنت متصل است. می بایست در زمانی که قصد استفاده از اینترنت را ندارید، اتصال خود را غیرفعال نمائید. فرآیند غیرفعال نمودن اتصال به اینترنت به نوع ارتباط ایجاد شده، بستگی دارد. مثلا" قطع خط تلفن ارتباطی، خاموش نمودن کامپیوتر و یا مودم.

•بررسی تنظیمات امنیتی : اکثر نرم‌افزارها نظیر برنامه‌های مرورگر و یا پست الکترونیکی، امکانات متنوعی را به منظور پیکربندی سفارشی متناسب با شرایط و خواسته استفاده کنندگان، ارائه می‌نمایند. در برخی موارد همزمان با فعال نمودن برخی از گزینه ها از یکطرف امکان استفاده از سیستم راحت‌تر شده و از طرف دیگر ممکن است احتمال آسیب‌پذیری شما در مقابل حملات، افزایش یابد. در این رابطه لازم است تنظیمات امنیتی موجود در نرم‌افزار را بررسی نموده و گزینه‌هایی را انتخاب نمائید که علاوه بر تامین نیاز شما، آسیب‌پذیری سیستم شما در مقابل حملات را افزایش ندهد. در صورتی که یک Patch و یا نسخه جدیدی از یک نرم‌افزار را بر روی سیستم خود نصب می‌نمائید که ممکن است تغییراتی را در تنظیمات انجام شده، اعمال نماید، می‌بایست

بررسی مجدد در خصوص تنظیمات امنیتی را انجام تا این اطمینان حاصل گردد که سیستم دارای شرایط مناسب و مقاوم در مقابل تهدیدات است.

به منظور افزایش مقاومت سیستم در مقابل خرابی و از دست دادن اطلاعات، می‌بایست به ابعاد دیگری نیز توجه داشت. برخی مواقع تهدید اطلاعات و در معرض آسیب قرار گرفتن آنان از جانب افراد نبوده و این موضوع به عوامل طبیعی و فنی دیگری بستگی دارد. با اینکه روشی برای کنترل و یا پیشگیری قطعی این نوع از حوادث وجود ندارد ولی می توان با رعایت برخی نکات میزان خرابی را کاهش داد :

- حفاظت کامپیوتر در مقابل نوسانات جریان برق : در صورت وجود نوسانات شدید برق، می‌بایست کامپیوتر را خاموش و کابل‌های آن را از پریز مربوطه جدا نمود. با اینکه برخی از منابع تغذیه، امکان حفاظت سیستم در مقابل نوسانات برق را افزایش می‌دهند، ولی آنان به تنهائی به منظور حفاظت سیستم در مقابل نوسانات جریان برق کافی نبوده و می‌توان در این رابطه از محصولاتی دیگر نظیر ups در زمان ایجاد نوسانات برق و یا قطع برق، استفاده نمود.
- backup گرفتن از داده‌ها : صرفنظر از این که شما خود را در مقابل مسائل ایمنی محافظت نموده باشید، همواره احتمال بروز حوادثی وجود خواهد داشت که باعث از دست دادن اطلاعات می‌گردد. شما ممکن است حداقل دارای یک مورد تجربه باشید که در آن یک و یا چندین فایل خود را در اثر بروز حادثه‌ای از دست داده باشید (مثلا" توسط عملکرد یک کرم و یا ویروس، یک حادثه طبیعی و یا یک مشکل خاص که در سخت افزار سیستم ایجاد شده باشد). تهیه منظم فایل backup بر روی یک CD و یا شبکه، نگرانی‌های احتمالی را کاهش خواهد داد. تشخیص این که در چه مقاطع زمانی و به چه صورت از اطلاعات backup گرفته شود یک تصمیم شخصی است. در صورتی که شما بطور دائم در حال افزودن و یا تغییر داده‌های موجود بر روی کامپیوتر می‌باشید،

می‌توان عملیات backup را با فرکانس بیشتر و در محدوده زمانی کوتاهتری، تکرار نمود .

29. چند عادت خوب امنیتی

به نظر شما به منظور افزایش ایمن‌سازی و حفاظت مطلوب اطلاعات موجود بر روی یک کامپیوتر، صرفا" می‌بایست در انتظار معجزه‌ای بود که از آستین نرم‌افزار و یا سخت‌افزار بیرون خواهد آمد؟ ما به عنوان عوامل انسانی و افرادیکه مشهور به کاربران کامپیوتر شده‌ایم، چه نوع تغییری را در رفتار خود می‌بایست انجام داده تا ما هم سهمی در پیشگیری از فجایع اطلاعاتی را داشته باشیم؟ آیا می‌بایست برخی عادات را ترک و برخی دیگر را ملکه ذهن خود نماییم؟ انسان عصر اطلاعات می‌بایست در کنار استفاده از فن‌آوری‌های متعدد، سعی نماید که برخی عادات و حرکات پسندیده را برای خود اصل قرار داده و با تکرار مدوام آنان، امکان و یا بهتر بگوئیم شانس خرابی اطلاعات و یا کامپیوتر را کاهش دهد.

30. فایروال چیست ؟

در صورت دستیابی سایرین به سیستم شما، کامپیوتر شما دارای استعداد بمراتب بیشتری در مقابل انواع تهاجمات می‌باشد. شما می‌توانید با استفاده و نصب یک فایروال، محدودیت لازم در خصوص دستیابی به کامپیوتر و اطلاعات را فراهم نمایید .

۳۱. فایروال چه کار می‌کند ؟

فایروال‌ها حفاظت لازم در مقابل مهاجمان خارجی را ایجاد و یک لایه و یا پوسته حفاظتی پیرامون کامپیوتر و یا شبکه را در مقابل کدهای مخرب و یا ترافیک غیرضروری اینترنت، ارائه می‌نمایند. با بکارگیری فایروال‌ها، امکان بلاک نمودن داده از مکانی خاص

فراهم می‌گردد. امکانات ارائه شده توسط یک فایروال برای کاربرانی که همواره به اینترنت متصل و از امکاناتی نظیر DSL و یا مودم‌های کابلی استفاده می‌نمایند، بسیار حیاتی و مهم می‌باشد.

۳۲. نوع فایروال‌هایی وجود دارد ؟

فایروال‌ها به دو شکل سخت‌افزاری (خارجی) و نرم‌افزاری (داخلی) ، ارائه می شوند. با اینکه هر یک از مدل های فوق دارای مزایا و معایب خاص خود می باشند، تصمیم در خصوص استفاده از یک فایروال بمراتب مهمتر از تصمیم در خصوص نوع فایروال است .

- فایروال‌های سخت افزاری: این نوع از فایروال‌ها که به آنان فایروال‌های شبکه نیز گفته می‌شود، بین کامپیوتر شما (و یا شبکه) و کابل و یا خط DSL قرار خواهند گرفت. تعداد زیادی از تولیدکنندگان و برخی از مراکز ISP دستگاههائی با نام "روتر" را ارائه می‌دهند که دارای یک فایروال نیز می‌باشند. فایروال‌های سخت‌افزاری در مواردی نظیر حفاظت چندین کامپیوتر مفید بوده و یک سطح مناسب حفاظتی را ارائه می‌نمایند (امکان استفاده از آنان به منظور حفاظت یک دستگاه کامپیوتر نیز وجود خواهد داشت) . در صورتی که شما صرفا" دارای یک کامپیوتر پشت فایروال می‌باشید و یا این اطمینان را دارید که سایر کامپیوترهای موجود بر روی شبکه نسبت به نصب تمامی patchها، بهنگام بوده و عاری از ویروس‌ها و یا کرم‌ها می باشند، ضرورتی به استفاده از یک سطح اضافه حفاظتی (یک نرم‌افزار فایروال) نخواهید داشت. فایروال‌های سخت‌افزاری، دستگاه‌های سخت‌افزاری مجزایی می باشند که دارای سیستم عامل اختصاصی خود می‌باشد. بنابراین بکارگیری آنان باعث ایجاد یک لایه دفاعی اضافه در مقابل تهاجمات می‌گردد.
- فایروال‌های نرم‌افزاری: برخی از سیستم‌های عامل دارای یک فایروال تعبیه شده درون خود می‌باشند. در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای

ویژگی فوق می‌باشد، پیشنهاد می‌گردد که آن را فعال نموده تا یک سطح حفاظتی اضافی در خصوص ایمن‌سازی کامپیوتر و اطلاعات، ایجاد گردد .(حتی اگر از یک فایروال خارجی یا سخت‌افزاری استفاده می‌نمایید). در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما دارای یک فایروال تعبیه شده نمی‌باشد، می توان اقدام به تهیه یک فایروال نرم‌افزاری کرد. با توجه به عدم اطمینان لازم در خصوص دریافت نرم‌افزار از اینترنت با استفاده از یک کامپیوتر محافظت نشده، پیشنهاد می‌گردد برای نصب فایروال از CD و یا DVD مربوطه استفاده گردد.

۳۳. نحوه پیکربندی بهینه یک فایروال به چه صورت است ؟

اکثر محصولات فایروال تجاری(هم سخت‌افزاری و هم نرم‌افزاری)دارای امکانات متعددی به منظور پیکربندی بهینه می‌باشند. با توجه به تنوع بسیار زیاد فایروال‌ها، می‌بایست به منظور پیکربندی بهینه آنان به مستندات ارائه شده، مراجعه تا مشخص گردد که آیا تنظیمات پیش‌فرض فایروال نیاز شما را تامین می‌نماید یا خیر؟ پس از پیکربندی یک فایروال یک سطح امنیتی و حفاظتی مناسب در خصوص ایمن سازی اطلاعات انجام شده است. لازم است به این موضوع مهم اشاره گردد که پس از پیکربندی یک فایروال نمی‌بایست بر این باور باشیم که سیستم ما همواره ایمن خواهد بود. فایروال‌ها یک سطح مطلوب حفاظتی را ارائه می‌نمایند ولی هرگز عدم تهاجم به سیستم شما را تضمین نخواهند کرد. استفاده از فایروال به همراه سایر امکانات حفاظتی نظیر نرم‌افزارهای آنتی ویروس و رعایت توصیه‌های ایمنی می‌تواند یک سطح مطلوب حفاظتی را برای شما و شبکه شما بدنبال داشته باشد.

۳۴. Patch چیست ؟

تولیدکنندگان نرم‌افزار پس از آگاهی از وجود نقاط آسیب پذیر در محصولات خود، با ارائه Patchهای لازم اقدام به برطرف نمودن مسئله و حل مشکل ایجاد شده، می‌نمایند. تمامی کاربران کامپیوتر می‌بایست از نصب آخرین Patchهای ارائه شده مرتبط با محصولات نرم‌افزاری که بر روی سیستم خود استفاده می‌نمایند، مطمئن گردند. اعتقاد عملی به سیاست فوق، ضریب حفاظتی و امنیتی سیستم شما را افزایش خواهد داد. همانند وصله‌های یک لباس که باعث بهبود روزنه‌های موجود می‌گردد ، وصله‌های نرم افزاری باعث بهبود حفره‌های موجود در برنامه‌های نرم‌افزاری می‌گردند. Patchها، یک مشکل خاص و یا نقطه آسیب‌پذیر در یک نرم افزار را برطرف می‌نمایند. در برخی موارد تولیدکنندگان نرم‌افزار در مقابل ارائه یک patch، اقدام به ارائه یک نسخه جدید از نرم افزارهای خود می‌نمایند (ارتقاء نرم‌افزار). تولیدکنندگان نرم‌افزار ممکن است به نسخه جدید ارتقاء یافته به عنوان یک patch مراجعه نمایند .

۳۵. انتخاب و حفاظت رمزهای عبور

رمزهای عبور، روشی به منظور تائید کاربران بوده و تنها حفاظ موجود بین کاربر و اطلاعات موجود بر روی یک کامپیوتر می‌باشند. مهاجمان با بکارگیری برنامه‌های متعدد نرم افزاری، قادر به حدس رمزهای عبور و یا اصطلاحا" "کراک" نمودن آنان می‌باشند. با انتخاب مناسب رمزهای عبور و نگهداری ایمن آنان، امکان حدس آنان مشکل و بالطبع افراد غیرمجاز قادر به دستیابی اطلاعات شخصی شما نخواهند بود.

۳۶. چرا به یک رمز عبور نیاز است ؟

انسان عصر اطلاعات در طی مدت زمان حیات خود و متناسب با فعالیت‌های روزانه خود نیازمند استفاده از رمزهای عبور متفاوتی می‌باشد. بخاطر سپردن شماره کد دستگاه

موبایل خود، شماره کد دستگاه‌های متفاوتی نظیر دستگاه‌های ATMبرای دریافت پول، شماره کد لازم به منظور ورود به یک سیستم کامپیوتری، شماره کد مربوط به برنامه‌های کامپیوتری نظیر برنامه‌های پست الکترونیکی،امضای دیجیتالی درون یک بانک Online و یا فروشگاه‌های مجازی و موارد بسیار دیگر، نمونه‌هائی در این زمینه می‌باشند. نگهداری این همه عدد، حرف و شاید هم ترکیب آنان، کاربران را مستاصل و گاها" نگران می‌نماید. مهاجمان با آگاهی از رمز عبور شما قادر به برنامه‌ریزی یک تهاجم بزرگ و دستیابی به اطلاعات شما می‌باشند.

یکی از بهترین روش‌های حفاظت از اطلاعات، حصول اطمینان از این موضوع است که صرفا" افراد مجاز قادر به دستیابی به اطلاعات می‌باشد. فرآیند تائید هویت و اعتبار کاربران در دنیای سایبر شرایط و ویژگی‌های خاص خود را داشته و شاید بتوان این ادعا را داشت که این موضوع بمراتب پیچیده تر از دنیای غیرسایبر است. رمزهای عبور یکی از متداولترین روش‌های موجود در خصوص تائید افراد می‌باشد. در صورتی که شما رمزهای عبور را بدرستی انتخاب نکرده و یا از آنان بدرستی مراقبت ننمائید، قطعا" پتانسیل فوق جایگاه و کارایی واقعی خود را از دست خواهد داد. تعداد زیادی از سیستم‌ها و سرویس‌ها صرفا" بدلیل عدم ایمن بودن رمزهای عبور با مشکل مواجه شده و برخی از ویروس‌ها و کرم‌ها با حدس و تشخیص رمزهای عبور ضعیف، توانسته‌اند به اهداف مخرب خود دست یابند.

37. چگونه می‌توان یک رمزعبور خوب را تعریف کرد ؟

اکثر افراد از رمزهای عبوری استفاده می‌نمایند که مبتنی بر اطلاعات شخصی آنان می‌باشد، چراکه بخاطر سپردن این نوع رمزهای عبور برای آنان ساده‌تر می‌باشد. بدیهی است به همان نسبت، مهاجمان نیز با سادگی بیشتری قادر به تشخیص و کراک نمودن رمزهای عبور خواهند بود. به عنوان نمونه، یک رمز عبور چهار حرفی را در نظر بگیرید،

ممکن است این عدد ارتباطی با تاریخ تولد شما داشته و یا چهار شماره آخر شماره دانشجوئی و یا کارمندی و شماره تلفن باشد. این نوع رمزهای عبور دارای استعداد لازم برای حملات از نوع "دیکشنری "، می‌باشند. مهاجمان در این نوع از حملات با توجه به کلمات موجود در دیکشنری، سعی در حدس و تشخیص رمزهای عبور می‌نمایند.

با این که تایپ نادرست برخی کلمات نظیر daytt در مقابل استفاده از date ممکن است مقاومت بیشتری در مقابل حملات از نوع دیکشنری را داشته باشد، یک روش مناسب دیگر می‌تواند شامل استفاده از مجموعه‌ای کلمات و بکارگیری روش هائی خاص به منظور افزایش قدرت بخاطر سپردن اطلاعات در حافظه باشد. مثلا" در مقابل رمز عبور "hoops"، از "IITpbb"، استفاده نمائید. (برگرفته شده از کلمات عبارت : I Like To Play Basketball). استفاده از حروف بزرگ و کوچک و ترکیب آنان با یکدیگر نیز می‌تواند ضریب مقاومت رمزهای عبور را در مقابل حملات از نوع "دیکشنری" تا اندازه‌ای افزایش دهد. به منظور افزایش ضریب مقاومت رمزهای عبور، می‌بایست از رمزهای عبور پیچیده‌ای استفاده نمود که از ترکیب اعداد، حروف الفبائی و حروف ویژه، ایجاد شده باشند .

پس از تعریف یک رمز عبور مناسب، برخی از کاربران از آن به منظور دستیابی به هر سیستم و یا برنامه‌های نرم‌افزاری استفاده می‌نمایند.(کلید جادوئی !) این نوع از کاربران می‌بایست به این نکته توجه نمایند که در صورتی که یک مهاجم رمز عبور شما را حدس و تشخیص دهد، وی به تمامی سیستم‌هائی که با این رمز عبور کار می‌کنند، دستیابی پیدا می‌نماید. به منظور تعریف رمزعبور، موارد زیر پیشنهاد می‌گردد:

- عدم استفاده از رمزهای عبوری که مبتنی بر اطلاعات شخصی می‌باشند. این نوع رمزهای عبور به سادگی حدس و تشخیص داده می‌شوند .
- عدم استفاده از کلماتی که می توان آنان را در هر دیکشنری و یا زبانی پیدا نمود .

- پیاده‌سازی یک سیستم و روش خاص به منظور بخاطرسپردن رمزهای عبور پیچیده
- استفاده از حروف بزرگ و کوچک در زمان تعریف رمزعبور
- استفاده از ترکیب حروف، اعداد و حروف ویژه
- استفاده از رمزهای عبور متفاوت برای سیستم‌های متفاوت

38.نحوه حفاظت رمزهای عبور

پس از انتخاب یک رمز عبور که امکان حدس و تشخیص آن مشکل است، می‌بایست تمهیدات لازم در خصوص نگهداری آنان پیش‌بینی گردد. در این رابطه موارد زیر پیشنهاد می‌گردد :

- از دادن رمز عبور خود به سایر افراد جدا" اجتناب گردد.
- از نوشتن رمز عبور بر روی کاغذ و گذاشتن آن بر روی میز محل کار، نزدیک کامپیوتر و یا چسباندن آن بر روی کامپیوتر، جدا" اجتناب گردد. افرادیکه امکان دستیابی فیزیکی به محل کار شما را داشته باشند، براحتی قادر به تشخیص رمز عبور شما خواهند بود.
- هرگز به خواسته افرادیکه (مهاجمان) از طریق تلفن و یا نامه از شما درخواست رمز عبور را می‌نمایند، توجه ننمائید .

در صورتی که مرکز ارائه‌دهنده خدمات اینترنت شما، انتخاب سیستم تائید را برعهده شما گذاشته است، سعی نمایید یکی از گزینه‌های Kerberos challenge/response و یا public key encryption را در مقابل رمزهای عبور ساده، انتخاب نمایید .

تعداد زیادی از برنامه‌ها امکان بخاطر سپردن رمزهای عبور را ارائه می‌نمایند، برخی از این برنامه‌ها دارای سطوح مناسب امنیتی به منظور حفاظت از اطلاعات نمی‌باشند. برخی برنامه‌ها نظیر برنامه‌های سرویس گیرنده پست الکترونیکی، اطلاعات را به صورت متن (غیررمزشده) در یک فایل بر روی کامپیوتر ذخیره می‌نمایند. این بدان معنی است

که افرادیکه به کامپیوتر شما دستیابی دارند، قادر به کشف تمامی رمزهای عبور و دستیابی به اطلاعات شما خواهند بود. بدین دلیل، همواره بخاطر داشته باشید زمانی که از یک کامپیوتر عمومی (در کتابخانه، کافی نت و یا یک کامپیوتر مشترک در اداره)، استفاده می‌نمائید، عملیات logout را انجام دهید. برخی از برنامه‌ها از یک مدل رمزنگاری مناسب به منظور حفاظت اطلاعات استفاده می‌نمایند. این نوع برنامه‌ها ممکن است دارای امکانات ارزشمندی به منظور مدیریت رمزهای عبور باشند.

۳۹. استفاده ایمن از برنامه های IM و Chat

با این که برنامه های IM و Chat، روشی مناسب به منظور ارتباط با سایر افراد می‌باشند، ابزارهای استفاده شده برای این نوع از مبادلات اطلاعاتی online می‌تواند خطرناک بوده و نتایج مخربی را به دنبال داشته باشد.

۴۰. تفاوت ابزارهای استفاده شده برای مبادلات online

به منظور مبادله اطلاعاتی online بر روی اینترنت، از ابزارهای متعددی استفاده می‌گردد. بررسی ویژگی هر یک از این ابزارهای موجود بهمراه تهدیدات مربوطه، امکان استفاده ایمن و مطمئن از این نوع ابزارها را فراهم می‌نماید.

برنامه‌های IM (Instant messaging) : از این نوع برنامه‌ها به منظور تفریح، سرگرمی، ارسال پیام، ارتباط صوتی و یا تصویری با سایر افراد استفاده می‌گردد. از برنامه‌های فوق در سازمان‌ها به منظور ارتباط بین کارکنان نیز استفاده می‌گردد. صرفنظر از نوع برنامه انتخابی IM، این نوع برنامه‌ها بستر مناسبی به منظور ارتباط یک به یک را ایجاد می‌نماید.

اطاق‌های چت: اطاق‌های چت صرفنظر از عمومی بودن و یا خصوصی بودن، تالارهایی برای گروه‌های خاص از مردم و به منظور ارتباط با یکدیگر می‌باشند. اکثر اطاق‌های چت مبتنی بر خصایص مشترکی می‌باشند : مثلا" اطلاق‌هائی مختص افرادی با سن خاص و یا علایق مشترک. با اینکه اکثر برنامه‌های سرویس گیرنده IM از چت، حمایت می‌کنند، برنامه‌های IM همچنان و بر اساس روش سنتی خود ابزاری برای ارتباطات یک به یک می‌باشند. در حالی که چت به صورت سنتی ابزاری برای ارتباط چند نفر به چند نفر می‌باشد.

به‌منظور طراحی و پیاده‌سازی برنامه‌های فوق از فن‌آوری‌های متعددی نظیر: IM، IRC و یا Jabber استفاده می‌گردد. برخی از نرم‌افزارهای ارائه شده با ترکیب چندین قابلیت توانسته‌اند پاسخگوی خواسته‌های متنوع کاربران باشند.

41. تهدیدات این نوع برنامه‌ها چیست ؟

وجود ابهام در خصوص هویت مخاطب. در برخی موارد نه تنها شناسائی مخاطب و شخصی که در حال ارتباط با وی هستید مشکل می‌باشد بلکه ماهیت انسانی و رفتاری وی نیز قابل پیش‌بینی نخواهد بود. مردم ممکن است در رابطه با هویت خودشان، گزاف گفته، account ها ممکن است در معرض سوءظن باشند و یا ممکن است کاربران عملیات logout را فراموش نمایند. در برخی موارد ممکن است یک account توسط چندین نفر و به صورت مشترک استفاده می‌گردد. تمامی موارد فوق، دلیلی است بر این ادعا که نمی‌توان بطور واقعی و حقیقی در رابطه با ماهیت شخصی که در حال گفتگو با وی هستید، قضاوت کرده و به یک سطح مطلوب از اطمینان دست پیدا کرد.

کاربران، مستعد انواع حملات می‌باشند. سعی کنید به شخصی بقبولانید که برنامه‌ای را اجرا و یا بر روی یک لینک، کلیک نماید. اجرای یک برنامه به توصیه دیگران و یا کلیک

بر روی یک لینک پیشنهادی توسط سایرین، یکی از روش‌های متداول به منظور انجام برخی تهاجمات می‌باشد. این موضوع در اطاق‌های چت و یا برنامه‌های IM امری متداول و مرسوم است. در محیطی که یک کاربر در این اندیشه است که در یک جو مطمئن و اعتمادپذیر در حال گفتگو با اشخاص است، یک کد مخرب و یا یک مهاجم می‌تواند شانس بیشتری برای رسیدن به اهداف خود و به دام انداختن سایر افراد را داشته باشد.

عدم وجود آگاهی لازم در خصوص سایر افراد درگیر و یا ناظر گفتگو :

مبادلات online بسادگی ذخیره می‌گردند و در صورتی که شما از یک سرویس اقتصادی رایگان استفاده می‌نمائید، ماحصل گفتگوی انجام شده می تواند بر روی یک سرویس دهنده ذخیره شده (logs) و شما هیچگونه کنترلی در خصوص این logs نخواهید داشت. شما نمی‌دانید که آیا اشخاص و افراد دیگر نظاره گر این گفتگو می باشند یا خیر ؟ یک مهاجم می‌تواند بسادگی اقدام به شنود اطلاعات و رهگیری آنان از طریق مبادلات اطلاعاتی انجام شده در اطاق‌های چت نماید .

نرم افزاری که شما بدین منظور استفاده می‌نمائید ممکن است دارای نقاط آسیب‌پذیر خاص خود باشد. همانند سایر نرم‌افزارها، نرم‌افزارهای چت، ممکن است دارای نقاط آسیب‌پذیری باشند که مهاجمان با استفاده از آنان می‌توانند به اهداف خود نائل گردند.

تنظیمات امنیتی پیش‌فرض انجام شده، ممکن است به درستی مقداردهی نشده باشند. تنظیمات امنیتی در نرم‌افزارهای چت، با نگرشی خیرخواهانه و ساده در نظر گرفته شده تا بدینوسیله و به رغم خود پتانسیل‌های بیشتری را در اختیار متقاضیان قرار دهند. رویکرد فوق، کاربران و استفاده‌کنندگان از این نوع برنامه‌ها را مستعد انواع حملات توسط مهاجمان می‌نماید.

42.چگونه می‌توان از این ابزارها به صورت ایمن استفاده نمود ؟

بررسی و ارزیابی تنظیمات امنیتی : در این رابطه لازم است تنظیمات پیش فرض در نرم‌افزار به منظور بهینه‌سازی امینتی آنان بررسی گردد. مطمئن شوید که ویژگی دریافت اتوماتیک فایل (Download)، غیرفعال شده باشد. برخی از نرم‌افزارهای چت، امکان ارتباط محدود با افراد را ارائه می‌نماید. در صورتی که از این نوع برنامه‌ها استفاده می‌نمائید، پیشنهاد می‌گردد ویژگی فوق فعال گردد.

هشیاری و دقت لازم در خصوص افشای اطلاعات. تا زمانی که نسبت به هویت طرف درگیر در ارتباط اطمینان لازم را کسب نکرده اید، از افشای اطلاعات شخص و مهم خود جدا" اجتناب کنید. مبادله اطلاعات در اطاق‌های چت می‌بایست با دقت و حساسیت بالا، انجام شود. هرگز اطلاعات تجاری و حساس مربوط به سازمان خود را در اطاق‌های چت و یا برنامه‌های عمومی IM افشا و برملا ننمایید.

شناسائی هویت افرادیکه در حال گفتگو با آنان هستید(حتی المقدور). در برخی موارد تشخیص هویت فردی که در حال گفتگو با وی می‌باشید، چندان حائز اهمیت نمی‌باشد. در صورتی که شما نیازمند سطح خاصی از اطمینان در خصوص شخص مورد نظر می‌باشید و یا قصد اشتراک اطلاعاتی خاص با وی را دارید، شناسائی هویت مخاطب بسیار حائز اهمیت است (مطمئن شوید شخصی که در حال گفتگو با وی هستید، همان شخص مورد نظر شما است).

عدم اعتماد و باور هر چیز: اطلاعات و یا توصیه‌هائی که شما از طریق یک اطاق چت و یا برنامه‌های IM دریافت می‌نماید، ممکن است نادرست، غلط و حتی مخرب باشند. در اینگونه موارد می‌بایست در ابتدا بررسی لازم در خصوص صحت اطلاعات و یا دستورالعمل‌های ارائه شده، انجام و در ادامه از آنان استفاده گردد.

بهنگام نگهداشتن نرم‌افزارها: فرآیند بهنگام سازی نرم‌افزارها شامل نرم افزار چت، مرورگر وب، سیستم عامل، برنامه سرویس گیرنده پست الکترونیکی و برنامه آنتی ویروس است. عدم بهنگام بودن هر یک از برنامه‌های فوق می‌تواند زمینه بروز تهاجمات توسط مهاجمان را فراهم نماید .

۴۳. مبانی امنیت اطلاعات

امروزه شاهد گسترش حضور کامپیوتر در تمامی ابعاد زندگی خود می‌باشیم. کافی است به اطراف خود نگاهی داشته باشیم تا به صحت گفته فوق بیشتر واقف شویم. همزمان با گسترش استفاده از کامپیوترهای شخصی و مطرح شدن شبکه‌های 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 فن‌آوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مولفه‌های تاثیرگذار در تداوم ارائه خدمات در یک سیستم کامپیوتری می‌باشند. امنیت اطلاعات و ایمن سازی شبکه‌های کامپیوتری از جمله این مولفه‌ها بوده که نمی‌توان آن را مختص یک فرد و یا سازمان در نظر گرفت. پرداختن به مقوله امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری در هر کشور، مستلزم توجه تمامی کاربران صرفنظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری بوده و می‌بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد. وجود ضعف امنیتی در شبکه‌های 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 سیاست‌های 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 می‌دهد .

در این مقاله قصد داریم به بررسی مبانی و اصول اولیه امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری پرداخته و از این رهگذر با مراحل مورد نیاز به منظور حفاظت کامپیوترها در مقابل حملات، بیشتر آشنا شویم.

44. اهمیت امنیت اطلاعات و ایمن‌سازی کامپیوترها

تمامی کامپیوترها از کامپیوترهای موجود در منازل تا کامپیوترهای موجود در سازمان‌ها و موسسات بزرگ، در معرض آسیب و تهدیدات امنیتی می‌باشند. با انجام تدابیر لازم و استفاده از برخی روش‌های ساده می‌توان پیشگیری لازم و اولیه‌ای را خصوص ایمن‌سازی محیط کامپیوتری خود انجام داد. علیرغم تمامی مزایا و دستاوردهای اینترنت، این شبکه عظیم به همراه فن‌آوری‌های مربوطه، دریچه‌ای را در مقابل تعداد زیادی از تهدیدات امنیتی برای تمامی استفاده کنندگان (افراد، خانواده‌ها، سازمان‌ها، موسسات و ...)، گشوده است. با توجه به ماهیت حملات، می‌بایست در انتظار نتایج نامطلوب متفاوتی بود (از مشکلات و مزاحمت‌های اندک تا از کار انداختن سرویس‌ها و خدمات). در معرض آسیب قرار گرفتن داده‌ها 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 بهره‌گیری از آخرین فن‌آوری‌های موجود، حملات خود را سازماندهی و بالفعل می‌نمایند. بنابراین، می‌بایست به موضوع امنیت اطلاعات، ایمن‌سازی کامپیوترها و شبکه‌های کامپیوتری، توجه جدی شده و از فرآیندهای متفاوتی در جهت مقاوم‌سازی آنان، استفاده گردد.

۴۵. داده‌ها 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 می‌تواند در هر لحظه صرفا" یک اتومبیل را سرقت نماید، در صورتی که یک مهاجم با بکارگیری صرفا" یک دستگاه کامپیوتر، می‌تواند آسیب‌های فراوانی را متوجه تعداد زیادی از شبکه‌های 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 داده‌های حساس را در یک شبکه کامپیوتری فراهم می‌نماید.

۴۶. ویروس‌ها

ویروس‌های کامپیوتری، متداولترین نوع تهدیدات امنیتی در سالیان اخیر بوده که تاکنون مشکلات گسترده‌ای را ایجاد و همواره از خبرسازترین موضوعات در زمینه کامپیوتر و شبکه‌های کامپیوتری، بوده اند. ویروس ها، برنامه‌هایی کامپیوتری می‌باشند که توسط برنامه‌نویسان گمراه و در عین حال ماهر نوشته شده و به گونه‌ای طراحی می‌گردند که قادر به تکثیر خود و آلودگی کامپیوترها بر اثر وقوع یک رویداد خاص، باشند. مثلا" ویروس‌هایی که از آنان با نام "ماکرو ویروس " یاد می‌شود، خود را به فایل‌هایی شامل دستورالعمل‌های ماکرو ملحق نموده و در ادامه، همزمان با فعال شدن ماکرو، شرایط لازم به منظور اجرای آنان نیز فراهم می‌گردد. برخی از ویروس‌ها 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 ویروس‌ها دارای عملکردی مخرب‌تر بوده و می‌توانند مسائل و مشکلات بیشتری نظیر حذف فایل‌ها و یا کاهش سرعت سیستم را به دنبال داشته باشند. یک کامپیوتر صرفا" زمانی آلوده به یک ویروس می‌گردد 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 شبکه‌ای آلوده گردید، سایر کامپیوترهای موجود در شبکه و یا سایر کامپیوترهای موجود در اینترنت، دارای استعدادی مناسب به منظور مشارکت و همکاری با ویروس، خواهند بود.

۴۷. برنامه‌های اسب تروا (دشمنانی در لباس دوست)

برنامه‌های اسب تروا و یا Trojans، به منزله ابزارهائی برای توزیع کدهای مخرب می‌باشند. تروجان‌ها، می‌توانند بی‌آزار بوده و یا حتی نرم‌افزاری مفیدی نظیر بازی‌های کامپیوتری باشند که با تغییر قیافه و با لباسی مبدل و ظاهری مفید خود را عرضه می‌نمایند. تروجان‌ها، قادر به انجام عملیات متفاوتی نظیر حذف فایل‌ها، ارسال یک نسخه از خود به لیست آدرس‌های پست الکترونیکی، می‌باشند. این نوع از برنامه‌ها صرفا" می‌توانند از طریق تکثیر برنامه‌های 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.

48. ویرانگران

در وب‌سایت‌های متعددی از نرم‌افزارهایی نظیر اکتیوایکس‌ها و یا اپلت‌های جاوا استفاده می‌گردد. این نوع برنامه‌ها به منظور ایجاد انیمیشن و سایر افکت‌های خاص مورد استفاده قرار گرفته و جذابیت و میزان تعامل با کاربر را افزایش می‌دهند. با توجه به دریافت و نصب آسان این نوع از برنامه‌ها توسط کاربران، برنامه‌های فوق به ابزاری مطئمن و آسان به منظور آسیب‌رسانی به سایر سیستم‌ها تبدیل شده‌اند. این نوع برنامه‌ها که به "ویرانگران" شهرت یافته اند، به شکل یک برنامه نرم‌افزاری و یا اپلت ارائه و در دسترس استفاده کنندگان قرار می‌گیرند. برنامه‌های فوق، قادر به ایجاد مشکلات متعددی برای

کاربران می‌باشند(از بروز اشکال دریک فایل تا ایجاد اشکال در بخش اصلی یک سیستم کامپیوتری) .

۴۹. حملات

اکنون حملات متعددی متوجه شبکه‌های کامپیوتری بوده که می‌توان 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 می‌نمایند. مهاجمان در این رابطه از نرم‌افزارهای خاصی نظیر Sniffer و یا Scanner به منظور شناسائی نقاط ضعف و آسیب‌پذیر کامپیوترها، سرویس دهندگان وب و برنامه‌ها، استفاده می‌نمایند. در این رابطه برخی تولیدکنندگان، نرم‌افزارهائی را با اهداف خیرخواهانه طراحی و پیاده سازی نموده‌اند که متاسفانه از آنان در جهت اهداف مخرب نیز استفاده می‌شود. مثلا" به منظور تشخیص و شناسائی رمزهای عبور، نرم‌افزارهای متعددی تاکنون طراحی و پیاده‌سازی شده است. نرم‌افزارهای 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 نموده‌اند، استفاده می‌گردند. به هر حال وجود این نوع نرم‌افزارها 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 آدرس‌های پست الکترونیکی، اطلاعات ذخیره شده در بانک‌های اطلاعاتی و سایر اطلاعات حساس، می‌باشد.

حملات از کار انداختن سرویس‌ها : در این نوع حملات، مهاجمان سعی در ایجاد مزاحمت به منظور دستیابی به تمام و یا بخشی از امکانات موجود در شبکه برای کاربران مجازمی‌نمایند. حملات فوق به اشکال متفاوت و با بهره‌گیری از فن‌آوری‌های متعددی صورت می‌پذیرد. ارسال حجم بالایی از داده‌های غیرواقعی برای یک ماشین متصل به اینترنت و ایجاد ترافیک کاذب در شبکه، نمونه‌هایی از این نوع حملات می‌باشند.

50. رهگیری داده (استراق سمع)

بر روی هر شبکه کامپیوتری روزانه اطلاعات متفاوتی جابجا می‌گردد و همین امر می‌تواند موضوعی مورد علاقه برای مهاجمان باشد. در این نوع حملات، مهاجمان اقدام به استراق سمع و یا حتی تغییر بسته‌های اطلاعاتی در شبکه می‌نمایند. مهاجمان به منظور نیل به اهداف مخرب خود از روش‌های متعددی به منظور شنود اطلاعات، استفاده می‌نمایند.

51. کلاهبرداری (ابتدا جلب اعتماد و سپس تهاجم)

کلاهبرداران از روش‌های متعددی به منظور اعمال شیادی خود استفاده می‌نمایند. با گسترش اینترنت این نوع افراد فضای مناسبی برای اعمال مخرب خود یافته‌اند (چرا که می‌توان به هزاران نفر در زمانی کوتاه و از طریق اینترنت دستیابی داشت). در برخی موارد شیادان با ارسال نامه‌های الکترونیکی وسوسه انگیز از خوانندگان می‌خواهند که اطلاعاتی خاص را برای آنان ارسال نموده و یا از یک سایت به عنوان طعمه در این رابطه استفاده می‌نمایند. به منظور پیشگیری از اینگونه اعمال، می‌بایست کاربران دقت لازم در خصوص درج نام، رمز عبور و سایر اطلاعات شخصی در سایت‌هائی که نسبت به هویت آنان شک و تردید وجود دارد را داشته باشند. با توجه به سهولت جعل آدرس‌های پست الکترونیکی؛ می‌بایست به این نکته توجه گردد که قبل از ارسال اطلاعات شخصی برای

هر فرد، هویت وی شناسائی گردد. هرگز بر روی لینک‌ها و یا ضمایمی که از طریق یک نامه الکترونیکی برای شما ارسال شده است، کلیک نکرده و همواره می‌بایست به شرکت‌ها و موسساتی که به طور شفاف آدرس فیزیکی و شماره تلفن‌های خود را ذکر نمی‌نمایند، شک و تردید داشت.

52. نامه‌های الکترونیکی ناخواسته

از واژه Spam در ارتباط با نامه‌های الکترونیکی ناخواسته و یا پیام‌های تبلیغاتی ناخواسته، استفاده می‌گردد. این نوع از نامه‌های الکترونیکی، عموما" بی‌ضرر بوده و صرفا" ممکن است مزاحمت و یا دردسر ما را بیشتر نمایند. دامنه این نوع مزاحمت‌ها می‌تواند از به هدر رفتن زمان کاربر تا هرز رفتن فضای ذخیره‌سازی بر روی کامپیوترهای کاربران را شامل می‌شود.

۵۳. ابزارهای امنیتی

پس از آشنائی با تهدیدات، می‌توان تمهیدات امنیتی لازم در خصوص پیشگیری و مقابله با آنان را انجام داد. بدین منظور می‌توان از فن‌آوری‌های متعددی نظیر آنتی‌ویروس‌ها و یا فایروال‌ها، استفاده بعمل آورد.

۵۴. نرم‌افزارهای آنتی ویروس

نرم‌افزارهای آنتی ویروس، قادر به شناسائی و برخورد مناسب با اکثر تهدیدات مربوط به ویروس‌ها می‌باشند. (مشروط به اینکه این نوع نرم‌افزارها به صورت منظم بهنگام شده و بدرستی پشتیبانی گردند). نرم‌افزارهای آنتی‌ویروس درتعامل اطلاعاتی با شبکه‌ای گسترده از کاربران بوده و در صورت ضرورت پیام‌ها و هشدارهای لازم در خصوص ویروس‌های جدید را اعلام می‌نمایند. بدین ترتیب، پس از شناسائی یک ویروس جدید،

ابزار مقابله با آن سریعا" پیاده سازی و در اختیار عموم کاربران قرار می‌گیرد. با توجه به طراحی و پیاده‌سازی ویروس‌های متعدد در سراسر جهان و گسترش سریع آنان از طریق اینترنت، می‌بایست بانک اطلاعاتی ویروس‌ها بر اساس فرآیندی مشخص و مستمر، بهنگام گردد.

۵۵. سیاست‌های امنیتی

سازمان‌های بزرگ و کوچک نیازمند ایجاد سیاست‌های امنیتی لازم در خصوص استفاده از کامپیوتر و ایمن‌سازی اطلاعات و شبکه‌های کامپیوتری می‌باشند. سیاست‌های امنیتی، مجموعه قوانین لازم به منظور استفاده از کامپیوتر و شبکه‌های 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 می‌شود. دانش تمامی کاربرانی که به تمام و یا بخشی از شبکه دستیابی دارند، می‌بایست به صورت منظم و با توجه به سیاست های تدوین یافته، بهنگام گردد(آموزش مستمر و هدفمند با توجه به سیاست‌های تدوین شده).

56. رمزهای عبور

هر سیستم کامپیوتری می‌بایست دارای ایمنی مناسبی در خصوص رمزهای عبور باشد. استحکام رمزهای عبور، ساده‌ترین 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 بخش‌های خاصی از شبکه می‌باشند. فراموش نکنیم که زیرساخت‌های 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 تلاش‌های 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 علاقه‌ای به تغییر منظم

رمزهای عبور خود در مقاطع زمانی خاصی نداشته و همین امر می‌تواند زمینه تشخیص رمزهای عبور توسط مهاجمان را فراهم نماید.

در زمان تعریف رمزعبور می‌بایست تمهیدات لازم در خصوص استحکام و نگهداری مطلوب آنان اندیشیده گردد:

- حتی المقدور سعی گردد از رمزهای 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.

57. فایروال‌ها

فایروال، راه‌حلی سخت‌افزاری و یا نرم‌افزاری به منظور تاکید (اصرار) بر سیاست‌های امنیتی می‌باشد. یک فایروال نظیر قفل موجود بر روی یک درب منزل و یا بر روی درب یک اطاق درون منزل می‌باشد. بدین ترتیب صرفا" کاربران تائید شده (آنانی که دارای کلید دستیابی می‌باشند)، امکان ورود به سیستم را خواهند داشت. فایروال‌ها دارای فیلترهای از قبل تعبیه شده‌ای بوده که امکان دستیابی افراد غیر مجاز به منابع سیستم را سلب می‌نمایند.

58. رمزنگاری

فن‌آوری رمزنگاری، امکان مشاهده، مطالعه و تفسیر پیام‌های ارسالی توسط افراد غیرمجاز را سلب می‌نماید. از رمزنگاری به منظور حفاظت داده‌ها در شبکه‌های عمومی نظیر اینترنت استفاده می‌گردد. در این رابطه از الگوریتم‌های پیشرفته ریاضی به منظور رمزنمودن پیام ها و ضمایم مربوطه، استفاده می‌شود.

66.چند نکته اولیه در خصوص ایمن سازی اطلاعات و شبکه های کامپیوتری

1.پذیرش مسئولیت به عنوان یک شهروند سایبر

در صورتی که از اینترنت استفاده می‌نمایید، شما به عنوان عضوی از جامعه جهانی و یا شهروند سایبر، محسوب شده و همانند یک شهروند معمولی، دارای مسئولیت‌های خاصی بوده که می‌بایست پذیرای آنان باشیم.

2.استفاده از نرم افزارهای آنتی ویروس

یک ویروس کامپیوتری، برنامه‌ای است که می‌تواند به کامپیوتر شما نفوذ کرده و صدمات فراوانی را باعث گردد. نرم‌افزارهای آنتی‌ویروس به منظور حفاظت اطلاعات و کامپیوترها در مقابل ویروس‌های شناخته شده، طراحی شده‌اند. با توجه به این که روزانه شاهد عرضه ویروس‌های جدید می‌باشیم، می‌بایست برنامه‌های آنتی‌ویروس به صورت منظم و مرتب بهنگام گردند.

3.عدم فعال نمودن نامه‌های الکترونیکی ارسال شده توسط منابع نامشخص و گمنام

نامه‌های الکترونیکی ارسالی توسط منابع ناشناس را می‌بایست همواره حذف نمود. به فایل‌هایی که به عنوان ضمیمه همراه یک نامه الکترونیکی ارسال می‌گردند، توجه گردد. حتی در صورتی که این نوع از نامه‌های الکترونیکی را از طریق دوستان و آشنایان خود دریافت می‌نمائید (خصوصا"اگر دارای انشعاب exe. باشند). برخی فایل‌ها مسئولیت توزیع ویروس‌ها را برعهده داشته و می‌توانند باعث بروز اشکالات فراوانی نظیر حذف دائم فایل‌ها و یا بروز اشکال در یک وب‌سایت گردند. هرگز نمی‌بایست اقدام به فوروارد نمودن نامه‌های الکترونیکی برای سایر کاربران قبل از حصول اطمینان از ایمن بودن آنان نمود.

نتیجه‌گیری :

نتیجه می‌گیریم که امنیت اطلاعات یکی از شاخه‌های مهم کامپیوتر است که برای طراحی برنامه کاربردی از آن استفاده می‌کنند و همچنین از آن در طراحی وب استفاده می‌شود این امنیت اطلاعات در کامپیوتر شخصی خود هم موجود می‌باشد و از آن به عنوان دیوار آتش یاد می‌کنند در نتیجه که امنیت اطلاعات یکی از محور اصلی کامپیوتر می‌باشد.