بسمه تعالی

بولتن علمی و آموزشی پیام

«(حراست دانشگاه)» آموزش

شماره دوم – آذر ماه ۱۳۸۷

« ویژهٔ امنیت شبکه های رایانه ای »

دانشگاه علوم پزشکی و خدمات بهداشتی درمانی گلستان

مقدمه :

در عصر دانش مهمترین وظیفه بشر جمع آوری داده , ایجاد اطلاعات, پردازش اطلاعات و رسیدن به دانش در زمینه های مختلف و در نهایت به اشتراک گذاشتن و تبادل دانش است. ولی استفاده از شبکه‌های کامپیوتری و همچنین اینترنت به عنوان ابزارهای اصلی برای این فرایند، با مخاطرات بسیاری همراه شده و امنیت داده ها را با چالش‌های جدی مواجه نموده و به همین سبب حفظ امنیت و مدیریت داده‌های سازمانی در راس اهداف و احد های فناوری اطلاعات سازمان ها قرار گرفته است

تعریف امنیت شبکه :

پردازه ایست که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می شود.

اهداف امنیت شبکه Security Center & Network Security

۱. ثابت کردن محرمانگی داده ها
۲. نگهداری جامعیت داده ها
۳. نگهداری در دسترس بودن داده ها

انواع تهدیدات به زبان ساده :

۱-کپی برداری غیرمجاز
۲- ارسال اطلاعات
۳- منتشر کردن اطلاعات
۴- تغییر در ساختار ظاهری پایگاه
۵- تخریب پایگاههای اطلاعاتی
۶ ایجاد تغییر و دستکاری در اطلاعات

نکته: چیزی به اسم حفاظت صددرصد وجود ندارد .

به همان تعداد که برنامه ها و قابلیت هایی برای ایمن سازی فایل ها و پوشه ها وجود دارد، به همان تعداد نیز دستورالعمل هایی برای کشف کلمات رمز وجود دارد. اما روش هایی که در این ویژه نامه به آن اشاره می شود، اطلاعات شما را از گزند بیشتر تلاش ها برای دستبرد حفظ می کند. اگر اطلاعات مورد نظر واقعا اهمیت حیاتی دارد، استفاده از نرم افزارهای شناخته شده و معتبر پیشنهاد می شود.

مهمانان ناخوانده !! ممکن است هم اکنون در کامپیوتر شما حضور داشته باشند.

که قادرند امنیت ارتباط برقرارشده شما رامورد تهدید قراردهندعبارتنداز:

۱) هکرها (Hakers)
۲) ویروس ها (viruse)
۳)کرمهای شبکه (worms)

چگونه مراقب رایانه و اطلاعات درون آنها و یا دسترسی غیر مجاز به منابع سیستم باشیم؟

الف : حفاظت فیزیکی

- اولین گام ((حفاظت فیزیکی)) از رایانه است. ایمنی در برابر سرقت و آتش سوزی و سیستم کنترل حریق باید به شکلی باشد که به نیروی انسانی و سیستم های الکترونیکی آسیب وارد نکند و همچنین موارد ناشی از نگهداری غیر استاندارد ((وضعیت فیزیکی محل و پایه های سیستمها و ...))
- باید کنترل کنیم که UPSها (برق اضطراری) قدرت لازم را برای تامین نیروی الکتریکی جهت کارکرد صحیح سخت افزار ها در زمان اضطراری داشته باشند.
- سیستم رایانه شما از رطوبت و سرمایش استاندارد برخوردار باشد.
- تهیه یک نسخه پشتیبان از فعالیتهای روزانه و حفاظت از منابع ایجاد شده در خارج از سیستم جاری

ب : حفاظت نرم افزاری

- قراردادن password مناسب در رایانه و فایلهای ذخیره شده
- نصب یک نرم افزارویروس یاب و به روز رسانی آن به طور مرتب
- به روز رسانی مرتب سیستم عامل
- نصب یک نرم افزار firewall در صورت استفاده از اینترنت و شبکه
- رعایت نکات ایمنی در هنگام استفاده از اینترنت و پست الکترونیک

آیا می دانید!

کامپیوتر شما معمولاً از راههای زیر ویروسی می شود؟!

۱- از طریق ایمیل (شایع ترین راه)
۲- دریافت فایل از اینترنت یا از دوستان در Chat
۳ - استفاده از CD یا فلاپی حاوی ویروس
۴- مشاهده صفحات وب در اینترنت
۵- اجرای فایلهای Downloud شده از منابع بی اعتبار
۶- دیدن لینک مشکوک در صفحات وب

توصیه حراستی: از طریق رایانه ای که دارای اطلاعات محرمانه می باشد به اینترنت و شبکه LAN وصل نشوید .

بولتن علمی آموزشی پیام هر ماهه توسط حراست دانشگاه علوم پزشکی گلستان تهیه می شود.

مؤمن چون اندرز داده شود، باز ایستد. چون ترسان شود، کناره گیرد و چون پند داده شود، پند پذیرد و چون تذکر داده شود، متذکر گردد . امام علي ع

آیا میدانید !

راهکارهـــای پیشـــگیری از ویروسی شـدن کـامپیوتر شـما معمولاً روشهای زیر می باشد؟

۱. نصب ویروس یاب مطمئن و به روز نگه داشتن آن

۲. باز نکردن ایمیل هایی که فرستنده آن را نمی‌شناسید.

۳. ایمیل خود را از جایی تهیه کنید کـه سـرویس دهنـده ایمیـل دارای ویروس یاب باشند. (مثل Yahoo – Hot mail)

۴. اکثر ایمیل های ویروسی به قسمت Bulk ایمیل فرستاده مـی شـود. لذا در باز کردن ایمیل های فرستاده شده به Bulk دقت شود.

در صورت ابتلای کامپیوتر شما به ویروس چه باید کرد؟

۱- اسکن کردن (بازبینی) کل هارد توسط ویروس کش ها.

۲- تهیه یک نسخه پشتیبان از اطلاعات و نگهداری آن در CD

۳- در صورت حاد بودن مشکل اگر امکان دارد ویندوز خـود را عـوض کنید و درایو ویندوز قبلی را فرمت نمایید.

نکات امنیتی در حفاظت رایانه

با فراهم شدن شـبکه هـای رایانـه ای و ورود ایـن شـبکه هـا بـه زنـدگی شخصـی و اجتمـاعی و سیسـتم هـای دولتـی و شـرکتهای خصوصـی و همچنین با ورود به دنیای ارتباطـات مـی تـوان شـاهد و نظـاره گـر انـواع تهدیدات امنیتی در شبکه های رایانه ای باشیم.

- اگر نامه شما دارای پیوستی با موضوع و عنوان مشکوک و یا غیر منتظره می باشد، از باز کردن آن پرهیز نمایید. اگر می خواهید پیوست را باز کنید ابتدا آن را بر رایانه خود ثبت کنید وسپس توسط یک ضدویروس معتبر آنرا اسکن نمایید .
- نامه های زنجیره ای و نا خواسته را پاک کنید. این دسته از نامه ها را هرزنامه می نامند زیرا بدون درخواست و در تعداد زیاد ارسال می گردند. هرزنامه ها را برای کسی نفرستید .
- سرویس ها و نرم افزارهایی که به صورت روزانه به آنها نیاز ندارید مانند ((remote desktop و File sharing services)) را بر روی رایانه خود نصب نکنید. اینگونه سرویسها نقاطی هستند که میتواند درگاه های ورودی و نفوذ به رایانه شما باشد .
- نرم افزارها و سیستم خود را در کمترین زمان بروز رسانی نمایید.
- از اطلاعات و فایلهای مهم به صورت دوره ای ، کپی پشتیبان تهیه نموده و این کپی ها را بر روی CD و یا DVD و یا هر نوع منابع خارجی ذخیره کرده و در جای امن نگه دارید.
- از برنامه های غیر قانونی که معمولا به صورت رایگان در اینترنت ارائه می شود استفاده نکنید؛ همین طور از برنامه های ارائه دهنده موسیقی و فیلم مجانی. صرف نظر از غیر قانونی بودن آنها، این برنامه‌ها معمولا سرشار از انواع نرم افزار های مخرب از جمله spyware ها هستند.
- فرمت درایو ها را به NTFS برای امنیت بیشتر تبدیل نمائید .

NTFS چیست ؟

روش قدیمی قالب بندی دیسک (سخت و نرم) بصورت FAT 32 بوده است. در این روش ، فقط می توان از دسترسی ناخواسته کاربران شبکه به اطلاعات کامپیوتر و آنهم از طریق Share Permissions جلوگیری کرد و هیچ راهی برای محدود کردن دسترسی کاربران دیگر وجود ندارد. بنابراین سیستم فایل FAT32 تا زمانی امن است که فردی ناخواسته پشت کامپیوتر ننشیند. NTFS نوع خاصی از قالب بندی است کـه در WIN-XP اجـرا مـی شـود. NTFS از یـک سیسـتم امنیـت اطلاعات بصورت توکار (داخلی) بهره مند است. NTFS امکان اِعمال محدودیت های دسترسی به فایل ها و پوشه ها مطابق بـا معمـاری امنیـت اشیاء در ویندوز را فراهم می کند. می توان به فایل ها و پوشه ها، اجازه دسترسی (permissions – برای کاربران خاص یا گروه ها) اعطا کرد. در این صورت، ویندوز از این اطلاعات در برابر دسترسی افراد غیرمجاز جلوگیری می کند. این محدودیت ها، هم برای کاربرانی که از شبکه به اطلاعات دسترسی پیدا می کنند و هم برای آن هایی که پشت کامپیوتر از اکانت (account – حساب کاربری) خودشان استفاده مـی کننـد اعمال می شود.

SSL چیست؟

نکته امنیتی ویژه نامه بعدی خواهد بود. لطفا جهت همکاری با نشریه پیام، در این خصوص به آدرس دفتر حراست دانشگاه مکاتبه فرمائید.

توصیه حراستی: کامپیوتر امانتی است که در اختیار شما قرار گرفته، لطفاً در حفظ و امنیت اطلاعات آن کوشا باشید.

تلفن تماس با دفتر حراست دانشگاه : مدیریت ۴۴۳۰۳۲۶ کارشناسان ۴۴۷۰۰۹۱ فکس ۰۱۷۱-۴۴۲۱۸۰۰