YAHoo ID: sinatak_bir WwW.sinacmd.co.sr

نام مقاله : ۱۰ نکته برای حفظ امنیت
نام نویسنده : ساسان سیفی (Invisible)
سطح مقاله : مقدماتی به حرفه ای

با تشکر فراوان از دوستان :

Of Invisible Team = (Alikhoub – Hacker – Subzero – Agape – Mehrun)
Of IHS Team = (Majid NT – C0d3r – L0rd)
Of IBBH Team = (yt3m_$h4r3 – l2odon – MaX666)
Of IHC Team = (ErRoR_Sir)
Of Y! Team = (Y4ho0 – Sisil – Satanic_Soulfol)
Of Emper0r Team = (Im4n – Farhad)
Eblis_Empire & All Other Friends That Help Me To Write Journals …….

امیدواریم جنبه یاد گیری این مقاله را داشته با شید.

10نکته برای حفظ امنیت

هر روزه اخبار جدیدی در مورد حملات و تهدیدات کامپیوتری در رسانه های مختلف انتشار می یابد. این تهدیدات شامل ویروس های جدید و یا انواع هک و نفوذ در سیستم های کامپیوتری است. انتشار این گونه اخبار باعث شیوع اضطراب و نگرانی در بین کاربرانی می شود که به صورت مستمر از کامپیوتر بهره می گیرند و یا اطلاعاتی ارزشمند بر روی کامپیوترهای خود دارند.

در این مقاله سعی شده چند نکته که در رابطه با امنیت کامپیوتر اهمیت اساسی دارند به صورت مختصر شرح داده شوند. یک کاربر در صورت رعایت این نکات می تواند تا حدود زیادی از حفظ امنیت سیستم کامپیوتری خود مطمئن باشد. در رابطه با بعضی از نکات که توضیحات بیشتری لازم بوده، مقالات جامع تری معرفی گردیده اند.

۱. استفاده از نرم افزارهای محافظتی) مانند ضدویروس ها) و به روز نگه داشتن آنها

از وجود ضدویروس بر روی دستگاه خود اطمینان حاصل کنید. این نرم افزارها برای محافظت از کامپیوتر در برابر ویروس های شناخته شده به کارمی روند و در صورت استفاده از آنها کاربر نیاز به نگرانی در مورد ویروس ها نخواهد داشت. در شرایطی که روزانه ویروس های جدید تولید شده و توزیع می شوند، نرم افزارهای ضدویروس برای تشخیص و از بین بردن آنها باید به صورت منظم به روز شوند. برای این کار می توان به سایت شرکت تولید کننده ضدویروس مراجعه کرد و اطلاعات لازم در مورد نحوه به روز رسانی و نیز فایل های جدید را دریافت نمود. عموما نرم

افزارهای ضدویروس ابزار های به روز رسانی و زمان بندی این فرایند را در خود دارند. برای مطالعه بیشتر در مورد ویروس ها و آشنایی با طرز کار و قابلیت های ضدویروس ها به سایت گروه امداد امنیت کامپیوتری ایران مراجعه نمایید.

۲. باز نکردن نامه های دریافتی از منابع ناشناس

این قانون ساده را پیروی کنید، «اگر فرستنده نامه را نمی شناسید، نسبت به نامه و پیوست های آن بسیار با دقت عمل نمایید». هرگاه یک نامه مشکوک دریافت کردید، بهترین عمل حذف کل نامه همراه با پیوست های آن است.

برای امنیت بیشتر حتی اگر فرستنده نامه آشنا باشد هم باید با احتیاط بود. اگر عنوان نامه نا آشنا و عجیب باشد، و بالاخص در صورتی که نامه حاوی لینک های غیرمعمول باشد باید با دقت عمل کرد. ممکن است دوست شما به صورت تصادفی ویروسی را برای شما فرستاده باشد. ویروس "I Love You" دقیقا به همین صورت میلیون ها کامپیوتر را در سراسر دنیا آلوده نمود. تردید نکنید، نامه های مشکوک را پاک نمایید.

مقالات محافظت در برابر خطرات ایمیل ۱ و ۲ به صورت مفصل در رابطه با این موضوع نگاشته شده است.

۳. استفاده از گذرواژه های مناسب

گذرواژه تنها در صورتی دسترسی غریبه ها به منابع موجود را محدود می کند که حدس زدن آن به سادگی امکان پذیر نباشد. گذرواژه های خود را در اختیار دیگران قرار ندهید و از یک گذرواژه در بیشتر از یک جا استفاده نکنید. در این صورت اگر یکی از گذرواژه های شما لو برود، همه منابع در اختیار شما در معرض خطر قرار نخواهند گرفت. قانون طلایی برای انتخاب گذرواژه شامل موارد زیر است:

- گذرواژه باید حداقل شامل ۸ حرف بوده، حتی الامکان کلمه ای بی معنا باشد. در انتخاب این کلمه اگر از حروف کوچک، بزرگ و

اعداد استفاده شود (مانند xk27D8Fy) ضریب امنیت بالا تر خواهد رفت .
- به صورت منظم گذرواژه های قبلی را عوض نمایید .
- گذرواژه خود را در اختیار دیگران قرار ندهید .

در مقاله انتخاب و محافظت از کلمات عبور نکات دقیق تری در این رابطه بیان شده است.

۴. محافظت از کامپیوتر در برابر نفوذ با استفاده از حفاظ (Firewall)

حفاظ دیواری مجازی بین سیستم کامپیوتری و دنیای بیرون ایجاد می کند. این محصول به دو صورت نرم افزاری و سخت افزاری تولید می شود و برای حفاظت کامپیوترهای شخصی و نیز شبکه ها به کار می رود. حفاظ داده های غیر مجاز و یا داده هایی که به صورت بالقوه خطرناک می باشند را فیلتر کرده و سایر اطلاعات را عبور می دهد. علاوه بر این حفاظ در شرایطی که کامپیوتر به اینترنت وصل است، مانع دسترسی افراد غیرمجاز به کامپیوتر می شود.

مقاله مقدمه ای بر فایروال به معرفی نحوه عملکرد حفاظ ها می پردازد و یکی از رایج ترین حفاظ های شخصی در مقاله حفاظ شخصی ZoneAlarm معرفی شده است.

۵. خودداری از به اشتراک گذاشتن منابع کامپیوتر با افراد غریبه

سیستم های عامل این امکان را برای کاربران خود فراهم می آورند که با هدف به اشتراک گذاری فایل، دسترسی دیگران را از طریق شبکه و یا اینترنت به دیسک سخت محلی فراهم آورند. این قابلیت امکان انتقال ویروس از طریق شبکه را فراهم می آورد. از سوی دیگر در صورتی که کاربر دقت کافی را در به اشتراک گذاشتن فایل ها به عمل نیاورد، امکان مشاهده فایل های خود را به دیگرانی که مجاز نیستند ایجاد می کند. بنابراین درصورتی که نیاز واقعی به این قابلیت ندارید، به اشتراک گذاری فایل را متوقف نمایید.

۶. قطع اتصال به اینترنت در مواقع عدم استفاده

به خاطر داشته باشید که بزرگ راه دیجیتال یک مسیر دوطرفه است و اطلاعات ارسال و دریافت می شوند. قطع اتصال کامپیوتر به اینترنت در شرایطی که نیازی به آن نیست احتمال اینکه کسی به دستگاه شما دسترسی داشته باشد را از بین می برد.

۷. تهیه پشتیبان از داده های موجود بر روی کامپیوتر

همواره برای از بین رفتن اطلاعات ذخیره شده بر روی حافظه دستگاه خود آمادگی داشته باشید. امروزه تجهیزات سخت افزاری و نرم افزاری متنوعی برای تهیه نسخه های پشتیبان توسعه یافته اند که با توجه به نوع داده و اهمیت آن می توان از آنها بهره گرفت. بسته به اهمیت داده باید سیاست گذاری های لازم انجام شود. در این فرایند تجهیزات مورد نیاز و زمان های مناسب برای تهیه پشتیبان مشخص می شوند. علاوه بر این باید همواره دیسک های Start up در دسترس داشته باشید تا در صورت وقوع اتفاقات نامطلوب بتوانید در اسرع وقت سیستم را بازیابی نمایید.

۸. گرفتن منظم وصله های امنیتی (Patches)

بیشتر شرکت های تولید کننده نرم افزار هر از چند گاهی نرم افزارهای به روز رسان و وصله های امنیتی جدیدی را برای محصولات خود ارائه می نمایند. با گذر زمان اشکالات جدید در نرم افزارهای مختلف شناسایی می شوند که امکان سوءاستفاده را برای هکرها بوجود می آورند. پس از شناسایی هر اشکالی شرکت تولید کننده محصول اقدام به نوشتن وصله های مناسب برای افزایش امنیت و از بین بردن راه های نفوذ به سیستم می کنند. این وصله ها بر روی سایت های وب شرکت ها عرضه می شود و کاربران باید برای تامین امنیت سیستم خود همواره آخرین نسخه های وصله ها را گرفته و بر روی سیستم خود نصب کنند. برای راحتی کاربران ابزارهایی توسعه داده شده اند که به صورت

اتوماتیک به سایت های شرکت های تولید کننده محصولات وصل شده، لیست آخرین وصله ها را دریافت می نمایند. سپس با بررسی سیستم موجود نقاط ضعف آن شناسایی و به کاربر اعلام می شود. به این ترتیب کاربر از وجود آخرین نسخه های به روز رسان آگاه می شود.

۹. **بررسی منظم امنیت کامپیوتر**

در بازه های زمانی مشخص وضعیت امنیتی سیستم کامپیوتری خود را مورد ارزیابی قرار دهید. انجام این کار در هر سال حداقل دو بار توصیه می شود. بررسی پیکربندی امنیتی نرم افزارهای مختلف شامل مرورگرها و حصول اطمینان از مناسب بودن تنظیمات سطوح امنیتی در این فرایند انجام می شوند.

۱۰. **حصول اطمینان از آگاهی اعضای خانواده و یا کارمندان از نحوه برخورد با کامپیوترهای آلوده**

هر کسی که از کامپیوتر استفاده می کند باید اطلاعات کافی در مورد امنیت داشته باشد. چگونگی استفاده از ضدویروس ها و به روز رسانی آنها، روش گرفتن وصله های امنیتی و نصب آنها و چگونگی انتخاب گذرواژه مناسب از جمله موارد ضروری می باشد.

Invisible Man
Invisible Digital Security Team
Www.InvisibleTeam.NeT

We Are :
Invisible – Alikhoub – Hacker_Boy – Subzero
Mehrun – Agape

Yahoo ID : Invisible.Sasan
E-mail : Sasan.Seyfi@gmail.com
Upload Center : Www.Invisible.Persiangig.coM

!~! My Dreams Always Is A Girl Standing In The Sun !~!

Special Thanks To All Invisible Team Moderators & Users