خبرنامه امنیت رایانه ای
کمیته امداد امام خمینی (ره)

سال اول، شماره اول نیمه دوم فروردین ۱۳۸۶

دفتر آمار و فناوری اطلاعات

آغاز بولتنهای امنیت رایانه ای همزمان با آغاز سال جدید خورشیدی و تقارن ربیع الاول با بهار را به فال نیک می گیریم و امیدواریم این بولتنها سهم خود را در کمک به افزایش امنیت رایانه ای و کاهش مشکلا ناشی از ویروسها و برنامه های ناخواسته به خوبی ایفا نمایند.

ویروسهای رایانه های خود را حذف کنید

اگرچه در شماره های آینده بولتن به طور دقیقتر نکات پیشگیرانه برای جلوگیری از آلوده شدن به ویروس و روشهای دستی حذف ویروسها و برنامه های ناخواسته را بیان خواهیم کرد، با توجه به نیازی که برای ارائه راه حلهای فوری و قابل اطمینان در کاهش مشکلات ناشی از ویروسها احساس می شد، در این بخش با ضدویروس قدرتمند رایگانی آشنا می شویم که حتی رابط کاربر فارسی هم دارد و کار کردن با آن بسیار ساده است.

با وجود سادگی آموزشهای این بولتن، لطفاً آنها را فقط تحت نظارت یکی از کارشناسان دفتر آمار و فناوری اطلاعات انجام دهید.

اینترنت اکسپلورر خود را باز کنید، این آدرس را در آدرس بار بنویسید و Enter کنید: www.freedrweb.com/cureit

گزینه دانلود کردن CureIt را که احتمالاً ظاهری شبیه تصویر زیر دارد پیدا کنید و روی آن کلیک کنید:

پس از گذشت چند دقیقه (بر حسب سرعت اینترنت شما) نرم افزار CureIt دانلود شده و قابل استفاده خواهد بود.

روزانه صدها ویروس جدید کشف می شوند و CureIt هم هر چند دقیقه یکبار به روز می شود! بنابراین توصه می شود همیشه جدیدترین نسخه آن را دانلود بفرمایید.

از آنجایی که این برنامه نیاز به نصب ندارد، می توانید نسخه ای از آنرا با حافظه USB یا حتی روی یک CD کوچک به سادگی به رایانه های دیگر انتقال دهید. همراه داشتن این فایل کمک می کند تا در شرایط مشاهده ویروس به سادگی با اجرای آن از روی CD همراهتان مشکل را برطرف نمایید.

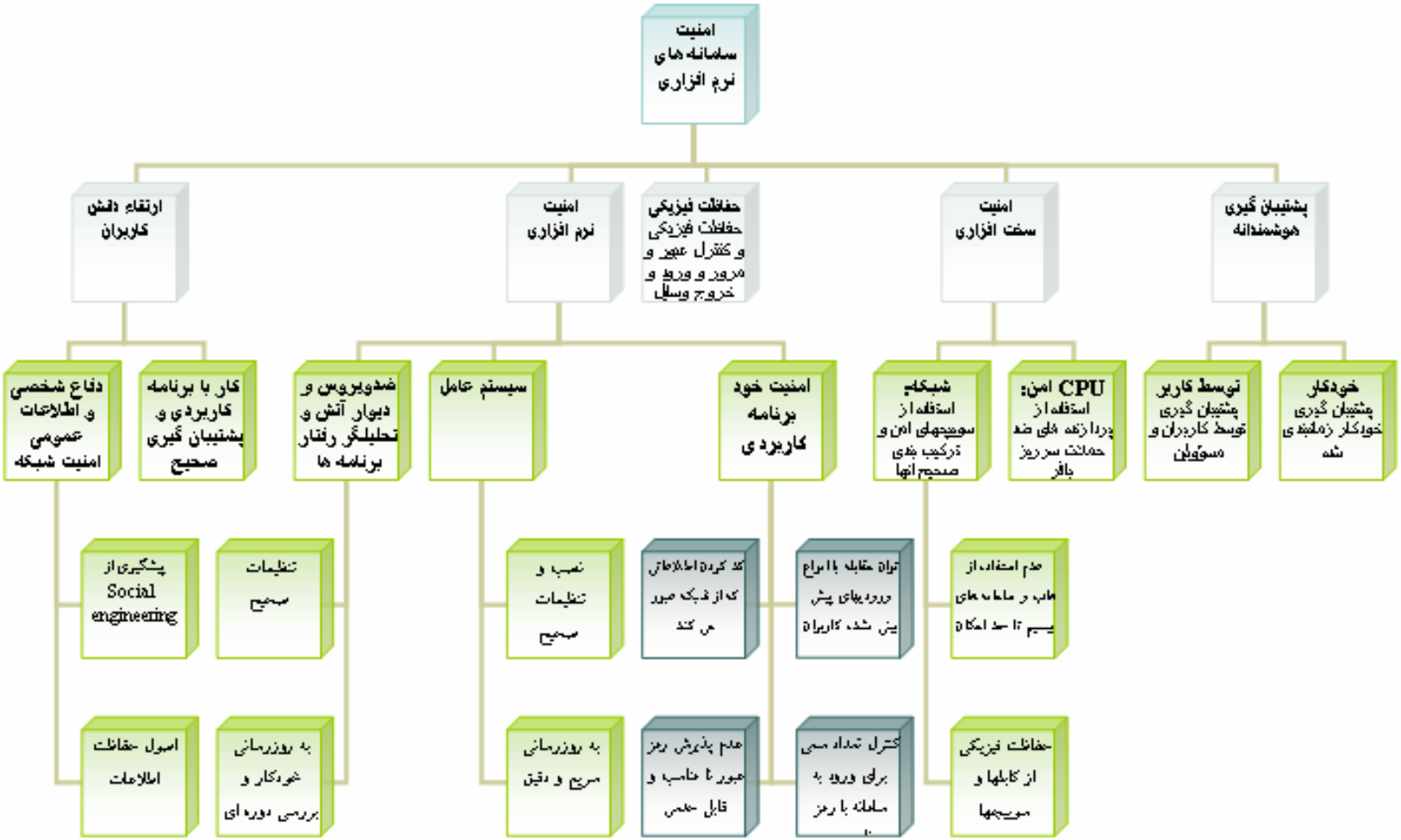
اگر به اینترنت پر سرعت یا دائم دسترسی دارید...

وبگاه Live.com که درگاه جدید مایکروسافت می باشد یک نرم افزار رایگان آنلاین برای بررسی مشکلات رایانه ارائه کرده است که نه تنها مشکلات ناشی از اغلب ویروسها را بر طرف می کند بلکه با بررسی رجیستری ویندوز و نیاز سیستم به اجرای Defragmenter، عملاً سرعت و کارایی را هم افزایش می دهد.

برای استفاده از این برنامه کافیست به آدرس http://safety.live.com بروید، زبانی که با آن راحت هستید (مثلاً انگلیسی) را انتخاب کنید و از صفحه جدیدی که باز می شود روی گزینه مورد نظر مثلاً Full Service Scan کلیک نمایید.

در مدت اجرای این برنامه، لازم است متصل به اینترنت باقی بمانید.

چشم‌های امنیت رایانه‌ای



پایه های امنیت رایانه ای

امروزه امنیت رایانه ها در برابر ویروسها، تلاش برای خرابکاری یا نفوذ و مشکلات مشابه یکی از دغدغه های اصلی هر مجموعه می باشد که با توجه و انجام اقدامات صحیح تا حد امکان می توان از بروز هرگونه مشکلی پیشگیری نمود. در ادامه به بررسی کلیاتی از امنیت رایانه ها و مشکلات پیش رو می پردازیم تا این بولتن زمینه ای باشد برای جلسات و سمینارهای توجیهی آتی که در آنها به تفضیل به بررسی موارد لازم و راههای پیشگیری خواهیم پرداخت. به طور کلی امنیت سامانه های رایانه ای باید در همه ابعاد زیر و به طور همزمان تامین شود:

الف – امنیت از دید سخت افزاری

ب – امنیت از دید نرم افزاری

پ – حفاظت فیزیکی

ت – ارتقاء دانش کاربران

ث – پشتیبان گیری هوشمندانه

اگرچه اهمیت هیچکدام از موارد فوق را نباید دست کم گرفت، موارد "ب" و "ت" به طور معمول بزرگترین نقایص یک سیستم به ظاهر امن هستند. بخصوص در مورد "ارتقاء دانش کاربران" باید توجه داشت که تا زمانی که ما یک ضد ویروس و FireWall روی ذهن کاربران نداشته باشیم، داشتن بهترین سخت افزارها و نرم افزارها کمک چندانی نخواهد کرد.

الف – امنیت از دید سخت افزاری

از دید سخت افزاری به طور کلی باید به تمام نکات از انتخاب قطعات سخت افزاری سیستمها (بخصوص CPU و مادربورد) تا طراحی شبکه از دید توپولوژی و انتخاب سوئیچهای مناسب برای شبکه دقت کامل مبذول گردد. حضور فردی مسلط به تنظیم سوییچ و شبکه به عنوان مدیر شبکه که دائماً در محل حاضر باشد نیز الزامی به نظر می رسد. همچنین بر حسب نیاز استفاده از دیوار آتش سخت افزاری و سوئیچهای هوشمند توصیه می شود.

همچنین حذف سخت افزارهای غیر لازم (مانند حذف مودم از روی سیستمی که از آن استفاده ندارد) و حتی تا حد امکان مسدود کردن پورتهای غیر لازم USB و حذف CD writer و Floppy های غیر ضروری نیز قابل توصیه می باشد.

بسیار مهم است که هرگونه خرید سخت افزاری با مشورت تیم IT مسلط به مبانی امنیت رایانه ای انجام پذیرد و سپس تنظیمات لازم برای امن کردن آنها بر روی سیستم عاملشان انجام پذیرد.

ب – امنیت از دید نرم افزاری

در اینجا نرم افزار به طور کلی شامل سیستم عامل، نرم افزارهای اداری و سایر نرم افزارهای نصب شده بر روی سیستم و در نهایت نرم افزارهای کاربردی مانند یک نرم افزار اتوماسیون مربوطه می باشد. هرگونه ایراد در طراحی هر کدام از موارد یاد شده می تواند منجر به کاهش ضریب امنیت شود. مهمترین موارد در این زمینه انتخاب بهترین گزینه ها، به روز رسانی مداوم، عدم نصب برنامه های غیر لازم و بررسی دقیق نرم افزارهای کاربردی طراحی شده توسط مشاوران با تجربه می باشد. در این قسمت همچنین دیواره های آتش، ضد ویروسها و نرم افزارهای هوشمند نظارت بر شبکه قرار می گیرند که هر کدام باید به دقت انتخاب و پیکربندی شود. استفاده از نرم افزارهایی که عملکرد برنامه های در حال اجرا بر روی سیستم را زیر نظر می گیرند و جلوی مشکلات را از اول می گیرند هم بر روی بسیاری از سیستمها الزامی است.

نرم افزارهای کاربردی، به عنوان نمونه نرم افزار اتوماسیون اداری، لازم است علاوه بر رعایت اصول معمول ایمنی، کاملاً آماده پذیرش انوع ورودیهای ناصحیح (مثلاً حروف در جایی که عدد انتظار می رود یا دستورات برنامه نویسی در جایی که ورود یک کلمه انتظار می رود) باشد و همچنین بتواند انواع تغییرات (تغییرات در سورس HTML صفحات، تغییرات در آدرس و...) یک کاربر کنجکاو را به بهترین شکل مدیریت و در صورت نیاز در یک Log file ذخیره نماید. لازم است تاریخ و ساعت آخرین دسترسی کاربران، IP آنها و کارهای مهم آنها در سیستم Log شود به طوری که قابل تغییر یا حذف از راه دور نباشد. همچنین این نرم افزار باید از انتخاب رمزهای نامناسب از طرف کاربران ممانعت کند و نیز با روشهای مختلف جلوی Brute force (به زبان ساده امتحان کردن کلمات مختلف به جای رمز تا رسیدن به رمز

درست) را بگیرد.

پ - حفاظت فیزیکی

به طور کلی هرجا که دسترسی فیزیکی به یک رایانه وجود داشته باشد، به تمام اطلاعات آن دسترسی وجود خواهد داشت (حتی اگر همه چیز با رمز محافظت شده باشد هم به هیچ عنوان نباید به آن اعتماد کرد) لذا مهمترین موضوع محدود کردن دسترسی فیزیکی افراد به سیستمها است و بخصوص کنترل ورود و خروج به اتاق سرور توسط ماموران آموزش دیده است (در دنیا استفاده از ساختمانهای ضد گلوله ای که ۲۴ ساعته محافظ دارند برای سرورهای ساده سایتهای اینترنتی امری طبیعی است).

این موضوع شامل جلوگیری از اقدامات نادرستی مثل رها کردن سیستمهای روشن برای خروج موقت از اتاق یا رها کردن پرونده های مهم بر روی پرینتر نیز می باشد. همچنین حفاظت کابلهای شبکه از طریق حفاظت فیزیکی و همزمان تعریف آدرسهای MAC بر روی سوئیچ جهت جلوگیری از اتصال یک رایانه همراه به شبکه نباید فراموش شود.

حفاظت فیزیکی شامل حذف سخت افزارهای غیر لازم مانند مودم بر روی سیستمی که از مودم استفاده ندارد و حتی تا حد امکان مسدود کردن پورتهای غیر لازم USB و حذف CD writer و Floppy غیر ضروری نیز می باشد.

حتی الامکان باید دسترسی رایانه ها به اینترنت نیز هم محدودیت زمانی و هم مکانی داشته باشد. یعنی علاوه بر اینکه فقط به رایانه های خاصی اتصال اینترنت داده می شود، لازم است محدوده زمانی استفاده آنها نیز مشخص شود و بخصوص در روزهای تعطیل و خارج از ساعات کار حتماً اتصال آن رایانه به اینترنت (و حتی در صورت امکان برق آن) قطع شود.

ت - ارتقای دانش کاربران

اگر شما قویترین ضد ویروسها و دیواره های آتشین را داشته باشید اما تا زمانی که یک ضد ویروس و FireWall روی ذهن کاربران نداشته باشید، داشتن بهترین سخت افزارها و نرم افزارها کمک چندانی نخواهد کرد. امروزه اکثریت نفوذها بر مبنای اشتباهات کاربران و بخصوص عدم انتخاب رمز عبورهای غیر قابل حدس و فریب خوردن از روشهای مهندسی اجتماعی یا اسب تروا می باشند و هرچه بیشتر روی این قسمت سرمایه گذاری شود مناسبتر است.

آشنایی افراد در هر سطحی بر حسب نیازهای آنها در شغل و سمتشان با اصول امنیت رایانه و اینترنت اصل مهمی است که امیدواریم با توجه بیشتر به این مقوله مهم شاهد روزی باشیم که حداقل آموزشهای امنیت رایانه همراه با آموزشهای آشنایی با رایانه و اینترنت به همه ارائه شود و این بولتن نیز گامی در همین راستاست که امید است این تلاش زمینه ساز جلسات و سمینارهای حضوری به زبانی ساده شود تا مسائل به خوبی بیان و درک شود.

ث - پشتیبان گیری هوشمندانه

با وجود تمام موارد فوق، ارزش پشتیبان گیری هرگز قابل انکار نیست. هوشمندانه بودن پشتیبان گیری به این مفهوم است که ما همیشه یک پشتیبان سالم جدید داشته باشیم. جمله فوق بدین معناست که در شرایط حمله یا تخریب سیستم باید به نوعی پشتیبان گیری را متوقف کند یا اصولاً فاصله زمانی مناسب بین پشتیبانگیریها باشد تا عجله بیش از حد در پشتیبانگیری دائم باعث جایگزینی نسخ پشتیبان با اطلاعات نادرست نشود.

تهیه شده در دفتر آمار و فناوری اطلاعات
با همکاری شرکت گسترش فناوری اطلاعات و ارتباطات خاورمیانه
نگارش و مشاوره علمی: احسان ریاضی اصفهانی