تنظیمات سخت افزاری و نرم افزاری

☐ به صورت زمان بندی شده منظم از داده ها و پرونده ها پشتیبان گیری نمایید.

☐ سرور های خود را (شامل سرورهای ایمیل و فایروال) با نرم افزار ضد ویروس محافظت نمایید.

☐ در تمام کامپیوترهای ایستگاه کاری ضد ویروس نصب کنید.

☐ گزینه محافظت از ویروس را در تنظیمات CMOS (در صورت وجود) فعال کنید.

☐ فایروال شبکه ای را نصب و به طور مناسب تنظیم نمایید.

☐ یک فایروال نرم افزاری را مانند ZoneAlarm یا فایروال ویندوز (در ویندوز ایکس پی) در کلیه کامپیوترهای ایستگاه کاری نصب کنید.

☐ فقط پورت های مورد نیاز را در تنظیمات فایروال باز بگذارید. توجه ویژه به پورت های مورد استفاده نرم افزارهای FTP یا اشتراک فایل مانند iMesh ، Kazaa ، Gnutella ، Morpheus و Grokster داشته باشید.

☐ به طور منظم شبکه خود را برای بررسی پورت های باز اسکن کنید.

☐ کامپیوترهای ایستگاه کاری را طوری محدود کنید که کاربران عادی نتوانند نرم افزارهای غیر مجاز مانند برنامه های تأیید نشده دریافت ایمیل، چت، FTP و برنامه های اشتراک فایل نصب نمایند.

☐ در صورت امکان فایل های حساس سیستم عامل (مانند win.ini، system.ini، autoexec.bat ، config.sys ، boot.ini) را با مشخصه فقط خواندنی تنظیم کنید تا تغییری در آنها داده نشود.

☐ مجوز های دسترسی به رجیستری ویندوز و سایر فایل های سیستم عامل را به گونه ای تنظیم کنید که از تغییرات غیر مجاز آنها جلوگیری شود.

☐ ضد ویروس را طوری تنظیم کنید که در صورت قدیمی شدن بانک اطلاعات شناسایی ویروس، به شما اخطار بدهد.

☐ سرور ها را طوری تنظیم کنید که تمامی فایل های ورودی و خروجی را برای شناسایی ویروس اسکن کنند.

☐ تمامی انواع فایل ها را موقع اسکن ویروس انتخاب نمایید؛ مانند فایل های zip ، exe و dll.

☐ از نرم افزارهایی استفاده کنید که فایل های را قرنطینه می کنند. این کار باعث می شود که کاربران نتوانند به فایل های آلوده دسترسی پیدا کنند و ویروس را منتشر نمایند.

☐ در صورتی که اشکالی پیش نمی آید در کامپیوترهای ایستگاه کاری حساس، دسترسی به درایو فلاپی را از طریق CMOS با کلمه رمز محدود کنید. اگر این امکان وجود ندارد حداقل گزینه بوت از طریق فلاپی را غیر فعال نمایید.

☐ اخطار صوتی را برای زمان تشخیص ویروس فعال نمایید.

☐ پاسخ کاربران به ضد ویروس را به هنگام برخورد و کشف ویروس روی حداقل گزینه قابل قبول مانند پاکسازی یا قرنطینه تنظیم کنید و اجازه انصراف از ترمیم را به کاربران ندهید.

☐ محافظت از ویروس های ماکرو را در نرم افزارهایی مانند ورد و اکسل فعال نمایید.

☐ فهرست استثناء فایل ها (file exclusion) را در ضد ویروس طوری تنظیم کنید که فایل های exe و dll حتما ویروس یابی شوند؛ چون اغلب ویروس ها به این نوع فایل ها حمله می کنند.

☐ دیسکت های راه انداز اضطراری را ایجاد و نگهداری کرده، دکمه حفاظت از نوشتن را فعال نمایید.

☐ از هارد دیسک هایی که در ایستگاه های کاری معمولی استفاده می شوند، کپی استاندارد (image) تهیه کنید. زمانی که برای نصب مجدد سیتسم عامل و نرم افزار ها نیساز به فورمت مجدد هارد دیسک باشد، داشتن این کپی روی هارد باعث سریع تر شدن زمان راه اندازی و آماده سازی سیستم خواهد شد.

☐ تمامی مودم های داخلی را از کامپیوتر های ایستگاه کاری خارج کنید، تا اتصال آن ها به اینترنت فقط از طریق فایروال سازمان باشد.

☐ کلمات رمز ساده یا پیش فرض را برای سرور ها، تجهیزات شبکه، کاربران مدیر شبکه و امثالهم استفاده نکنید.

☐ شبکه ی سازمان را به طور مرتب بررسی کنید تا کاربران غیر مسؤول انفورماتیک، سیستم عامل سرور بر روی آن ها نصب نکنند.

سیستم عامل و دیتابیس ویروس

☐ به طور مرتب آخرین به روز رسانی های امنیتی و ترمیمی را در سیستم عامل های سرور و کلاینت خود نصب کنید. در صورت امکان سیستم ☐ ها را طوری تنظیم کنید که به روز رسانی ها مذکور را به طور خودکار دریافت کنند. (automatic updates)

☐ به طور منظم و زمان بندی شده فایل های دیتابیس ویروس ها را به روز رسانی نمایید و در صورت امکان نرم افزار ضد ویروس خود را طوری ☐ تنظیم کنید که به صورت خودکار از طریق سایت کمپانی سازنده ی ضد ویروس یا یک سرور داخل سازمان به روز شود.

☐ به روز رسانی ها را بین کامپیوترهای کلاینت توزیع کنید. در صورتی که سیستم عامل شبکه ای (NOS = Network Operating System) به شما امکان نمی دهد که به روز رسانی ها را از راه دور نصب (push) کنید آنها را به صورت ضمیمه ی ایمیل (یا هر ابزار استاندارد ارتباطی که استفاده می کنید) به کاربران تان ارسال کنید..

☐ یک سرور اختصاصی برای دریافت به روز رسانی ها تنظیم کنید که کاربران از طریق اتصال به آن به روز رسانی های مورد نیاز خود را دریافت نمایند. با این کار حداقل در مصرف پهنای باند اینترنت صرفه جویی خواهید کرد.

☐ به روز رسانی ها را در صورت امکان از طریق دستورهای اسکرپت ورود به سیستم (login script) برای کاربران ارسال نمایید.

☐ در صورتی که امکانی برای توزیع به روز رسانی ها در شبکه ندارید، یک نرم افزار برای مدیریت کلاینت های شبکه مانند Novell Zenworks Configuration Management یا Sysmantec Altiris Client Management Suite خریداری کنید. این نرم افزار ها به شما امکان نصب از راه دور به روز رسانی ها در کامپیوتر های اسیتگاه کاری را می دهند.

☐ هر زمان که فایل های سیستم عامل به روز رسانی می شوند دیسک های راه انداز محافظ شده (write protected) خود را به روز رسانی کنید.

☐ صرفا به یک منبع برای دانسته های امنیتی خود بسنده نکنید. همیشه چند وب سایت امنیتی را بررسی کرده، برای دریافت اخطارها و خبرنامه های امنیتی در آن ها ثبت نام کنید.

مدیریت حافظه های قابل انتقال مانند فلاپی ها، سی دی، دی وی دی، حافظه ی فلاش و ...

☐ حافظه هایی را که از جای نامعلوم دریافت می کنید استفاده نکنید.

☐ مقرراتی وضع کنید تا کاربران ملزم شوند هر حافظه ای را که از خارج از سازمان تهیه کرده باشند، حتما ویروس یابی کنند.

☐ تعدادی دیسکت (یا هر حافظه ی جانبی مشابه) بدون ویروس در سازمان تهیه کنید که کاربران در مواقع نیاز که با کامپیوتر خانه شان کار بکنند از آن ها استفاده نمایند. پس از بازگرداندن دیسک به داخل سازمان مجددا آن ها را ویروس یابی کنید تا آلودگی احتمالی از کامپیوتر خانه شان به داخل سازمان منتقل نشود.

☐ تمامی دیسکت (یا حافظه جانبی مشابه) های حاوی داده یا برنامه را در برابر نوشتن محافظت کنید.

ویروس یابی (scanning)

☐ کامپیوتر اختصاصی در نظر بگیرید که به طور مداوم پوشه های حاو ی داده ها را در شبکه ویروس یابی کند.

☐ به طور زمان بندی شده ویروس یابی کامل (Full Scan) را برای کامپیوترهای ایستگاه کاری در نظر بگیرید به طوری که کمترین تداخل و درگیری با کاربر پیش بیاید. مانند زمان ناهار یا ساعت غیر کاری.

☐ از حالت ویروس یابی پس زمینه (background scanning/stealth mode) استفاده کنید که کمترین تداخل با کاربر سیستم پیش بیاید.

☐ این امکان را که کاربران بتوانند در کار ضد ویروس مداخله کنند، غیر فعال نمایید.

☐ حالت نظارت پس زمینه و ویروس یابی بلادرنگ (real time scanning) را برای تمامی کامپیوتر های ایستگاه کاری فعال کنید.

☐ در صورت امکان از ابزار (add on/plug in) ویروس یابی برای مرورگر استفاده کنید که قبل از دانلود، فایل را ویروس یابی کند. اگر چنین ابزاری در دسترس نیست مطمئن شوید که همه ی فایل های دانلود شده قبل از استفاده یا نصب ویروس یابی می شوند.

☐ در شرکت های کوچک می توانید تاریخ آخرین ویروس یابی کامل را برای هر کامپیوتر ایستگاه کاری مستند کرده، به مسؤول انفورماتیک تحویل دهید.

☐ کامپیوترهای جدید را خریده اید اگر می خواهید از سیتم عاملی که فروشنده نصب کرده استفده بکنید، حتما قبل از استفاده ویروس یابی کنید.

ایمیل

☐ سرور ایمیل را طوری تنظیم کنید تا ایمیل های هرزنامه را – که ممکن است حاوی ویروس یا کد مخرب باشند – حذف کند.

☐ سرور را به گونه ای تنظیم کنید که بلافاصله برای مدیر شبکه و کاربر مذکور اخطار امنیتی بفرستد که پیغام آلوده به ویروس را باز نکند.

☐ تمامی ایمیل های وارده و صادره و فایل های ضمیمه ی آن ها را ویروس یابی کنید.

☐ دانلود فایل های ضمیمه ی غیر کاری را در محیط کار ممنوع کنید.

☐ به کابران اجازه ندهید که جوک یا ایمیل های زنجیره ای را ارسال کنند.

☐ از یک سرویس ویروس یابی ایمیل (خارج از شبکه) ثبت نام و استفاده نمایید که حتی الامکان ایمیل های آلوده وارد شبکه تان نشوند.

☐ با فرستنده ی ایمیل آلوده به ویروس تماس بگیرید یا ایمیل بزنید. چون اغلب ارسال کنندگان از ارسال ایمیل آلوده آگاه نیستند.

☐ یک روش ارتباطی دیگر برای زمانی که سرویس ایمیل از کار بیفتد پیش بینی کنید.

کاربران

☐ روشی برای آموزش همه ی کاربران در باره ی سیاست های امنیتی (مانند قانون ممنوعیت دانلود) پیاده کنید.

☐ هر گونه نصب نرم افزار باید با تأیید بخش انفورماتیک صورت گیرد.

☐ هر گونه دانلود برنامه های تأیید نشده و نصب آن ها (مانند بازی یا اسکرین سیور) توسط کاربران را ممنوع کنید.

☐ کاربران را ملزم کنید که تحت هیچ شرایطی دیسک (یا هر حافظه ی جانبی) را - که در خانه استفاده کرده اند – در سازمان استفاده نکنند، ☐ مگر این که پشی از استفاده توسط مسؤول انفورماتیک ویروس یابی و تأیید بشود.

☐ دسترسی به سایت ها را توسط مرورگر یا پروکسی محدود کرده، فقط به سایت های مورد تأیید اجازه دهید.

☐ مجموع ای از نرم افزار ها را که کاربران برای انجام کارهای خود استفاده می کنند، تعیین نمایید و اجازه ندهید نرم افزار دیگری را نصب کنند.

☐ به کاربرانی که از راه دور به شبکه وصل می شوند اجازه ی کپی فایل را ندهید مگر این که کامپیوتری که برای دسترسی از راه دور به کار می رود توسط بخش انفورماتیک قابل بررسی و کنترل باشد.

آموزش کاربران

☐ لینک های مربوط به دائره المعارف های ویروس ها را برای آشنایی و استفاده ی کاربران منتشر کنید:

- Computer Associates http://www3.ca.com/securityadvisor/virusinfo/browse.aspx
- F-Secure http://www.f-secure.com/v-descs/
- Kaspersky http://www.viruslist.com/en/viruses/encyclopedia
- McAfee http://www.mcafeesecurity.com/us/security/vil.htm
- Symantec http://www.symantec.com/avcenter/
- TechRepublic's Virus Threat Center http://www.virusthreatcenter.com/library.aspx
- Trend Micro http://www.trendmicro.com/vinfo/

☐ از کاربران بخواهید که در وقت آزاد شان، یا زمانی که متوجه ی آلودگی به ویروس می شوند یا جهت بیشتر شدن اطلاعات شان در مورد ویروس ها، این سایت ها را ببینند.

☐ کاربران را تشویق کنید که در کامپیوتر خانه شان ضد ویروس نصب کنند. همنی برای کامپیوترهایی که از راه دور به شبکه تان وصل می شوند ضد ویروس را الزامی کنید.

☐ کاربران را تشویق کنید که ایمیل ها و فایل های مهم شان را در یک سرور که شما به طور منظم پشتیبان می گیرید، ذخیره نمایند.

☐ کابران را تشویق کنید که به محض مشاهده ی ویروس روی کامپیوتر شان به شما اطلاع دهند تا بتوانید تعقیب کنید که کدام ویروس ها در شبکه تان ظاهر می شوند.

☐ یک سایت اینترانتی یا وب سایت اختصاصی برای ارائه ی اطلاعات در مورد ویروس ها و لینک های مربوط به شرکت های سازنده ی ضد ویروس ایجاد نمایید. در صورتی که این مورد را نمی توانید انجام دهید یک خبرنامه ی الکترونیکی تهیه کنید که همان اطلاعات را به کاربران ارایه دهید.

☐ کاربران را از خطرات و ویروس های جدید مطلع کنید تا نسبت به این موضوع هشیار تر باشند.

☐ به کاربران تان روش صحیح محافظت از ویروس های ماکرو را آموزش دهید. از آنان بخواهید تا زمانی که از سالم و مورد تأیید بودن یک فایل مطمئن نشده اند، همه ی ماکرو ها را غیر فعال نمایند.

☐ کاربران خطا کار را جریمه کنید. بدین ترتیب که اگر کاربری مقررات وضع شده ی امنیتی را زیر پا گذاشت یا ویروسی را وارد محیط کار کرد، باید برای ویروس یابی دستگاه های آلوده شده به بخش انفورماتیک کمک کند.