



وزارت ارتباطات و فناوری اطلاعات



سازمان فناوری اطلاعات ایران

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری اطلاعات

توصیه نامه شماره ۵: کنترل بد افزارها

توصیه نامه	نوع سند
عمومی	سطح دستیابی سند
عادی	سطح امنیتی سند
فیلی فوری	اولویت سند
فرداد ۹۰	تاریخ ارائه سند
۱	نگارش سند
۵	تعداد صفحات
سازمان فناوری اطلاعات	مؤلف/مؤلفین سند
R900310-5	کد سند

هدف:

هدف از تدوین این توصیه نامه جلوگیری از اختلال در عملکرد شبکه یا تجهیزات متصل به آن، به دلیل نفوذ بد افزارها^۱ و محافظت از دارایی های اطلاعاتی در مقابل تهدیدهای ناشی از عملکرد کدهای مخرب^۲ می باشد.

ضرورت:

بد افزارها یا کدهای مخرب (که در اذهان عمومی علیرغم ماهیت و عملکردهای مختلف به نام ویروس رایانه ای شناخته می شوند) جزء تهدیدهای عمدی برنامه ریزی شده دسته بندی می شوند و پیامدهای ناشی از فعال شدن آنها بسیار خطرناک ارزیابی می شود. عملکرد بد افزار یا کد مخرب در درجه اول، جامعیت و صحت داده ها را تهدید کرده و ضربه به محرمانگی اطلاعات، عملکرد نادرست سخت افزارها و نرم افزارها و یا اشکال در دسترسی نیز می تواند از پیامدهای آن باشد.

برنامه کامپیوتری عبارت است از مجموعه ای از علائم و عبارات متوالی قابل درک و اجرا توسط کامپیوتر برای دست یافتن به یک عملکرد مطلوب. بد افزار یا کد مخرب عبارت است از هر برنامه نرم افزاری اعم از برنامه نوشته شده با هدف تخریب یا اهداف و تاثیر سوء و یا برنامه عادی یا پر قدرت به کار گرفته شده با هدف غیرقانونی، که به منظور تخریب و تغییر عملکرد یک سیستم رایانه ای (معمولاً بدون آگاهی

¹- Malware

² - Malicious Codes

کاربران) به رایانه های میزبان وارد شده و همان رایانه و یا رایانه های دیگر را تحت تهدید یا تاثیر قرار می دهد.

الزامات:

- مسئولیت حفاظت از هر دارایی نرم افزاری و یا سخت افزاری در مقابل کدهای مخرب (از طریق اطمینان از نصب و به هنگام بودن نرم افزارهای محافظتی) بر عهده متصدی و یا تحویل گیرنده دارایی اطلاعاتی است.

- تامین نرم افزارهای حفاظت در مقابل کدهای مخرب (و یا سخت افزارهای لازم برای اجرای این نرم افزارها) بر عهده بالاترین مقام اجرایی سازمان یا دستگاه می باشد.

- غیرفعال کردن نرم افزار ضد بدافزار توسط کاربران ممنوع است.

- باید اطمینان حاصل شود که تمام ایستگاههای کاری خارج از ابنیه و یا نصب شده در سایت های دور و ایستگاه های کاری یا سرورهای متعلق به کارکنان، پیمانکاران و اشخاص ثالث که به شبکه های سازمانی دسترسی دارند به وسیله ضد بدافزار محافظت می شوند.

- ضد بدافزار باید در تمام شبکه (بی سیم و باسیم)، ایستگاههای کاری یا سرویس دهنده ها نصب و پیکربندی شود. پیکربندی آن باید حداقل موارد زیر را شامل شود:

- نرم افزار باید به طور خودکار و مرتب به هنگام سازی¹ شود.

¹ - Update

- هر داده ای که از یک منبع خارجی مثل اینترنت و یا رسانه های ذخیره سازی داده، مانند فلاپی دیسک، CD-Rom، USB/flash (حافظه های ذخیره سازی) و مانند آن، یا هر وسیله ارتباطی به رایانه ها انتقال^۱ می یابد قبلاً از لحاظ عاری بودن از کدهای مخرب بررسی شده و در صورت مشکوک بودن، پاکسازی شده یا از انتقال آن جلوگیری شود.

- هر فایل دریافت شده از سرویس دهنده های شبکه در ایستگاه های کاری و یا انتقال یافته از ایستگاه های کاری به سرویس دهنده ها باید جهت اطمینان از عدم آلودگی به کدهای مخرب به صورت خودکار پوشش^۲ شود و در صورت آلوده بودن، پاکسازی و در غیر این صورت از انتقال آن جلوگیری به عمل آید.

- ضد بدافزار باید بر روی تمامی ایستگاه های کاری که به طور مستقل کار می کنند و تمام وسایل قابل حمل (اعم از متصل یا غیرمتصل به شبکه) نصب شود.

- لازم است تمامی Email های دریافتی و ضمیمات^۳ آنها برای جلوگیری از ورود بدافزارها یا کدهای مخرب به سیستم پوشش شوند.

- لازم است بدافزارها و کدهای مخرب به محض کشف، ریشه کن شوند (کد مربوط بطور کامل پاک شده و آثار آن نیز از کلیه مکان های محتمل مثل Boot Sector، FAT، NFS، فایل های رجیستری حذف شود).

1 - Download
2 - Scan
3 - Attachments

- اکثر سرویس‌های پیام رسان فوری^۱، IRC^۲ و اشتراک فایل نقطه به نقطه^۳ دارای پتانسیل دسترسی غیر مجاز از دور هستند. استفاده از این سرویس‌ها ممنوع است و باید از روی کلیه ایستگاه‌های کاری حذف شوند مگر آنکه وجود آنها کاملاً ضروری تشخیص داده شود و ریسک حاصل از استفاده از آنها ارزیابی شود. (اکثر این سرویس‌ها کم حجم بوده و یا سرویس‌های امنیتی بر روی آنها نصب نمی‌باشد و از پروتکل‌های اختصاصی استفاده می‌کنند).

- نصب سرویس‌های پیام رسان فوری، IRC، اشتراک فایل نقطه به نقطه، تبادل پست الکترونیک و یا هر سرویس غیر ضروری دیگر بر روی سرورها ممنوع است.

- در صورت نیاز به استفاده از سرویس‌های پیام رسان فوری، IRC و تبادل ضمیمه‌های پست الکترونیک یا فایل، لازم است داده‌های مربوطه از دیواره آتش و یا دروازه‌های امنیتی عبور داده شده و با هدف‌عاری بودن از کدهای مخرب بررسی شوند.

- مدیر ارشد شبکه باید کلیه مشتریان، کاربران و سایر افراد درگیر کار با دارایی‌های اطلاعاتی نرم‌افزاری و سخت‌افزاری را از وظیفه خود مبنی بر قرنطینه کردن و پاکسازی نرم‌افزارهای آلوده در ایستگاه‌های کاری، ایستگاه‌های غیرمتصل به شبکه و دستگاه‌های قابل حمل آگاه سازد.

فرآیند:

مراحل پیاده‌سازی این توصیه‌نامه به شرح زیر می‌باشد:

- ¹ - Instant Messaging
- ² - Internet Relay Chat
- ³ - Peer to Peer File Sharing

- ابتدا کلیه الزامات امنیتی در خصوص کنترل کدهای مخرب تدوین می شود. در صورتی که سازمان دارای الزامات اختصاصی باشد الزامات مورد نظر به الزامات بیان شده در این سند افزوده خواهد شد.

- سپس مکانیزم ها و ابزار لازم اعم از تجهیزات سخت افزاری و نرم افزاری تامین خواهند شد. نمونه ای از این ابزار عبارتند از:

- نرم افزار ضد بدافزار

- ابزار پیکارچه مدیریت تهدیدات¹ UTM

- ابزار تشخیص و یا پیشگیری نفوذ

- پس از تامین مکانیزم ها و ابزار لازم، موارد مذکور مانند ضد بدافزار و دیواره آتش نصب و پیاده سازی می شود.

- پس از نصب ابزار و پیاده سازی مکانیزم ها بایستی پیکربندی های مناسب بر روی هر یک از آنها تنظیم و اجرا گردد.

- عملکرد اجزای نصب شده از طریق کنترل مستمر گزارش های ثبت فعالیت² مورد پایش قرار می گیرد.

- در مواقع نیاز، پیکربندی ابزارها بر اساس نیازهای سازمانی یا پیشنهاد تولیدکنندگان مربوط یا مراجع امنیتی به هنگام می شود.

¹ - Unified Threat Management

² - Log