وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز مدیریت، توسعه و اعتباربخشی
نظام ملی مدیریت امنیت اطلاعات

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری اطلاعات

توصیه نامه شماره ۵ :کنترل بد افزارها

نوع سند	توصیه نامه
سطح دستیابی سند	عمومی
سطح امنیتی سند	عادی
اولویت سند	خیلی فوری
تاریخ ارائه سند	خرداد ۹۰
نگارش سند	۱
تعداد صفحات	۵
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات ایران
کد سند	R9003105

هدف:

هدف از تدوین این توصیه نامه جلوگیری از اختلال در عملکرد شبکه یا تجهیزات متصل به آن، به دلیل نفوذ بدافزارها[1] و محافظت از دارایی های اطلاعاتی در مقابل تهدیدهای ناشی از عملکرد کدهای مخرب[2] می باشد.

ضرورت:

بدافزارها یا کدهای مخرب (که در اذهان عمومی علیرغم ماهیت و عملکردهای مختلف به نام ویروس رایانه‌ای شناخته می شوند) جزء تهدیدهای عمدی برنامه‌ریزی شده دسته‌بندی می‌شوند 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. بدافزار یا کد مخرب عبارت است از هر برنامه نرم‌افزاری اعم از برنامه نوشته شده با هدف تخریب یا اهداف وتاثیر سوء و یا برنامه عادی یا پرقدرت به کارگرفته 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 می‌دهد.

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 نرم‌افزار 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 (بی‌سیم و باسیم)، ایستگاه‌های کاری یا سرویس دهنده ها نصب و پیکربندی شود. پیکربندی آن باید حدقل موارد زیر را شامل شود:

- نرم‌افزار باید به طور خودکار و مرتب به هنگام سازی[1] 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 (حافظه‌های ذخیره‌سازی) و مانند آن، یا هر وسیله ارتباطی به رایانه ها انتقال[1] می‌یابد 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 ایستگاه‌های 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 پویش[2] 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 ایستگاه‌های کاری که به طور مستقل کار می‌کنند و تمام وسایل قابل حمل (اعم از متصل یا غیرمتصل به شبکه) نصب شود.

– لازم است تمامی Email های دریافتی و ضمائم[3] آنها برای جلوگیری از ورود بدافزارها یا کدهای مخرب به سیستم پویش شوند.

– لازم است بدافزارها و کدهای مخرب به محض کشف، ریشه‌کن 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[1]، IRC[2] و اشتراک فایل نقطه به نقطه[3] دارای پتانسیل دسترسی غیر مجاز از دور هستند. استفاده از این سرویس ها ممنوع است و باید از روی کلیه ایستگاه های 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 نمی باشد و از پروتکل‌های اختصاصی استفاده می‌کنند.)

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

- در صورت نیاز به استفاده از سرویس‌های پیام رسان فوری، IRC و تبادل ضمیمه های پست الکترونیک یا فایل، لازم است داده های مربوطه از دیواره آتش و یا دروازه های امنیتی عبور داده شده و با هدف عاری بودن از کدهای مخرب بررسی شوند.

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

فرآیند:

مراحل پیاده سازی این توصیه نامه به شرح زیر می باشد:

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

- ابتدا کلیه الزامات امنیتی در خصوص کنترل کد های 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 یکپارچه مدیریت تهدیدات[1] 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 فعالیت[2] 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