وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز مدیریت، توسعه و اعتاربخشی
نظام ملی مدیریت امنیت اطلاعات

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری اطلاعات

توصیه نامه شماره ۴:کنترل درگاه های ورودی و خروجی

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	۷
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات ایران
کد سند	R90030904

هدف

هدف از تدوین این توصیه نامه بیان اهمیت کنترل درگاههای ورودی و خروجی جهت جلوگیری از اختلال در عملکرد شبکه، پیشگیری از دسترسی غیرمجاز به سرویس‌های شبکه یا شبکه‌های تحت اختیار یا مالکیت (از طریق تسلط نفوذگر بر درگاه[1] های نرم افزاری حفاظت نشده) و محافظت از کلیه دارایی های اطلاعاتی نرم افزاری و سخت افزاری می باشد.

ضرورت:

معمولا در شبکه ها ارتباط سیستم‌های کامپیوتری با یکدیگر از طریق درگاه‌ها برقرار می‌شود. در صورت عدم پیکربندی مناسب نرم افزارها یا پروسه هایی که درگاه ها را مدیریت می کنند، راه نفوذ برای دسترسی غیرمجاز ایجاد می‌شود. در واقع درگاه‌های باز آسانترین راه نفوذ به سیستم‌های کامپیوتری متصل به شبکه هستند. به عنوان مثال اسب‌های تروا می‌توانند با استفاده از درگاه‌های باز وارد سیستم شده و اطلاعات سیستم میزبان خود را برای حمله کنندگان ارسال نمایند. هکر از طریق درگاهی خاص به اسب ترویی که بر روی سیستم قرار دارد، وصل شده و برای انجام وظایف مورد نظر خود (همانند گرفتن یک عکس از صفحه کاربر یا ارسال اطلاعات خاص) درخواست صادر می کند. اسب تروا وظیفه مورد نظر را انجام داده و تصویر یا اطلاعات را از طریق همان درگاه یا درگاه دیگری برای هکر ارسال می کند.

[1]- Port

الزامات:

- به دلیل آنکه اجرای هر سرویس در شبکه موجب باز شدن درگاه های مربوط می شود، ضروری است با تحلیل نیازهای شبکه ارتباطی موجود، سرویس‌ها و پروتکل‌های غیرضروری شبکه شناسایی شده و از نصب آنان جلوگیری به عمل آید.

- لازم است قبل از نصب و پیکربندی سرویس‌ها و پروتکل‌های ضروری، نکات و مسائل امنیتی مربوط به هر سرویس و نحوه بهره‌برداری از آن در قالب مراحل تحلیل ریسک (که در مراکز حساس و حیاتی باید به صورت رسمی اجراء شود) مورد رسیدگی قرار گیرد.

- ضروری است قبل از اجرای هر سرویس، پیکربندی خاص مربوط به آن تعیین و تدوین گردد و پس از اجرا و به صورت دوره‌ای، پیکربندی‌های مربوط بازنگری و کنترل شود.

- ضروری است در مراکزی که از منظر پدافند غیرعامل به عنوان مراکز حساس و حیاتی دسته‌بندی می‌شوند، کلیه سرویس‌ها و پروتکل‌های مورد نیاز از لحاظ امنیتی در برابر آسیب‌پذیری‌های احتمالی آزمایش شوند و مورد تأیید افراد متخصص قرار گیرند.

- اطلاعات پیکربندی سرویس‌های شبکه باید به عنوان اطلاعات محرمانه (و در مراکز حساس و حیاتی و یا مراکز حیاتی سازمان های مهم به عنوان اطلاعات خیلی محرمانه) طبقه بندی شوند. بدیهی است در هیچ حالتی نباید رده طبقه بندی حفاظتی اطلاعات پیکربندی سرویس های شبکه یا تجهیزات ارائه دهنده آنها پایین تر از رده طبقه بندی حفاظتی سرویس یا تجهیزات مربوط باشد.

- باید برای تمامی تجهیزات مدیریت و کنترل شبکه از رمزهای عبور مستحکم و قوانین دسترسی محدود شده استفاده شود.

- وقایع ثبت شده درمورد تلاش برای دسترسی‌های غیرمجاز به سرویس های شبکه ای و یا دایرکتوری‌ها و فایل‌های مربوط به آنها بایستی به طور منظم و در بازه های از پیش تعیین شده بررسی شوند.

- لازم است دسترسی راه دور از طریق شناسه Admin (یا هر شناسه دیگری که دارای حق دسترسی ممتاز[1] به ماشین‌ها یا نرم افزارهایی است که سرویس‌های اصلی شبکه را ارائه می‌نمایند)، مسدود شده باشد.

- لازم است با استفاده از بخش بندی[2] مناسب شبکه ترتیبی اتخاذ شود تا سرویس‌های ضروری در هر بخش، فقط در اختیار افراد مستقر در آن قرار گیرد و سایر افراد به چنین سرویس‌هایی دسترسی نداشته باشند.

- آرایش هندسی شبکه و دیوار آتش[3] (که برای کنترل درگاه ها به کار گرفته می شود) باید به گونه‌ای تنظیم شود که دسترسی مستقیم به سرویس های درون شبکه ای (به خصوص سرویس‌دهنده پایگاه داده)، برای افراد خارج از سازمان غیرممکن باشد.

- ضروری است تجهیزات سرویس‌های شبکه در مکان‌هایی استقرار یابند که از دسترسی‌های فیزیکی غیرمجاز محفوظ بمانند.

[1] - Privilege Access
[2] - Segmentation
[3] - Firewall

- هرگونه اتصال غیرامن به سرویس‌های شبکه که می‌تواند موجب اثرات سوء بر عملکرد کلی شبکه باشد، باید حذف گردد.

- باید از عدم وجود کامپایلرها [1]، پوسته‌های نرم افزاری [2]، موتورهای اجرای قطعه برنامه‌ها [3] و سایر ابزارهای نرم افزاری در رایانه های کاربران عادی یا سایر تجهیزات پردازشی اطمینان حاصل شود.

- ضروری است کلیه درگاه‌هایی که برای دسترسی‌های خارجی استفاده می‌شود با محافظت از طریق کلمه عبور کنترل شوند.

- باید فایل های راه انداز به صورت زمانبندی شده بازدید شوند و از عدم وجود نرم‌افزارهای مخرب در فایل های مذکور اطمینان حاصل شود.

فرآیند:

در ابتدا لازم است دسته بندی سازمان از دیدگاه پدافند غیرعامل و همچنین طبقه بندی حفاظتی بخش های مختلف شبکه سازمان مورد بررسی قرار گیرد. تحلیل نیازهای شبکه بمنظور شناسایی کلیه سرویس‌های مورد نیاز و همچنین غیرضروری در شبکه سازمان در این مرحله انجام می شود. با توجه به لیست سرویس های مورد نیاز یا غیر ضرور، فهرست درگاه هایی که باید در مورد آنها تصمیم گیری شود مشخص می گردد.

پس از تحلیل و شناسایی و در مرحله بعد، فهرستی از سرویس های مجاز قابل ارائه در شبکه سازمان از قبیل پروتکل های مجاز ارتباطی، خدمات مجاز اشتراک فایل و منابع، سرویس های مجاز تشخیص

[1] - Compilers
[2] - shells
[3] - CGI components

هویت یا احراز صلاحیت و سرویس های مجاز کنترل دسترسی تهیه می شود. همچنین در کنار فهرست مذکور، لیستی از سرویس ها و پروتکل های غیرضروری شبکه تهیه می شود.

پیش از هر گونه اقدامی، لازم است ارزیابی ریسک درباره نصب هر یک از سرویس های شبکه و بهره برداری از آنها انجام شده و مخاطرات آن برآورد شود. در صورتی که ریسک ارزیابی شده قابل پذیرش نباشد ادامه این فرآیند متوقف شده و خاتمه می‌یابد. در این حالت باید از بسته بودن درگاه های مربوط به سرویس های دارای ریسک غیر قابل پذیرش اطمینان حاصل شود.

در صورت قابل پذیرش بودن ریسک ارزیابی شده،ه الزامات امنیتی در خصوص چگونگی نصب و نحوه بهره برداری از هر سرویس تدوین می شود. همچنین در این مرحله پیکربندی مناسب هر سرویس متناسب با الزامات امنیتی تدوین می شود. در این مرحله درگاه هایی که باید باز باشند فهرست شده و مکانیزم ها و منابع مورد نیاز جهت امن سازی هریک تامین می شود.

پس از تامین موارد فوق، به پیاده سازی مکانیزم ها، اجرای کلیه الزامات و نصب و پیکر بندی سرویس های مورد نیاز شبکه مطابق با پیکربندی تدوین شده اقدام می شود. در صورت بر آورده شدن کلیه الزامات، مجوز بهره برداری از سرویس توسط نهاد متصدی امنیت اطلاعات سازمان صادر شده و سرویس مزبور مورد بهره برداری و استفاده قرار می گیرد.

تعاریف:

درگاه: در پروتکل TCP/IP هر بسته‌ای که بر روی شبکه قرار می‌گیرد علاوه بر آدرس IP کامپیوتر گیرنده اطلاعات، شماره درگاه مربوطه را نیز در خود دارد. از آنجا که در کامپیوتر دریافت کننده (میزبان)، پروسه ای باید وجود داشته باشد تا اطلاعات را دریافت کرده و پردازش نماید، شماره درگاه

به این پروسه اشاره می نماید. به عبارت دیگر باز بودن درگاه به این معنی است که پروسه ای وجود دارد که اطلاعات ارسال شده را دریافت و پردازش می نماید. نفوذگران می توانند از قابلیت ها یا ضعف های این پروسه ها استفاده نموده و کنترل رایانه هدف را در دست گرفته، عملکرد آن را مختل نموده و یا آن را مجبور به اجرای فرمان مورد نظر خود نمایند.

IDS: سامانه تشخیص نفوذ (Intrusion Detecting System) ابزاری است که از طریق پایش بسته های عبوری و مقایسه آن با الگوهای داده ای از پیش شناخته شده، نفوذ های احتمالی را کشف و ثبت نموده و نسبت به ارائه اخطار و گزارشات مربوطه و انجام سایر عکس‌العملهای از پیش تعریف شده متناسب با آن اقدام می کند. HIDS به سامانه تشخیص نفوذ به یک میزبان و NIDS به سامانه تشخیص نفوذ به یک شبکه گفته می شود.

IPS: سامانه پیشگیری از نفوذ (Intrusion Preventing System) ابزاری است که از طریق پایش عملکرد رایانه و مقایسه آن با الگوهای عملکردی از پیش شناخته شده، نفوذ های احتمالی را کشف و ثبت نموده و نسبت به متوقف سازی عملیات نفوذ و انجام سایر عکس‌العمهای از پیش تعریف شده متناسب با آن اقدام می کند. HIPS به سامانه پیشگیری از نفوذ به یک میزبان و NIPS به سامانه پیشگیری از نفوذ به یک شبکه گفته می شود.

- بخش‌بندی: بخش بندی با هدف جداسازی فیزیکی یا منطقی قسمتهای مختلف شبکه از یکدیگر بنا بر ماموریت سازمانی و یا مکان جغرافیایی انجام می شود.

- دیوار آتش: دیوارآتش (Firewall) ابزاری است که از طریق پایش و غربال بسته های اطلاعاتی سعی می‌کند از ورود یا خروج بسته های ناخواسته جلوگیری نماید.