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 ۱۳ : امنیت شبکه

نوع سند	توصیه نامه
سطح دستیابی سند	عمومی
سطح امنیتی سند	عادی
اولویت سند	خیلی فوری
تاریخ ارائه سند	تیر ۹۰
نگارش سند	۱
تعداد صفحات	۱۲
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات ایران
کد سند	R90040413

هدف:

هدف از تدوین این توصیه نامه بیان لزوم رعایت امنیت در طراحی و بهره برداری از شبکه های ارتباطی از طریق لحاظ نمودن معیارهای امنیتی در طرح معماری و هنگام بهره برداری از شبکه می باشد.

ضرورت:

سیستم های متصل به شبکه نسبت به سیستم های مجزا در معرض تهدیدهای بیشتری می باشند. شبکه های متصل به شبکه های عمومی یا شبکه های متعلق به سازمان های دیگر نیز طبیعتا آسیب پذیری بیشتری نسبت به شبکه های مستقل دارند. سیستم های متصل به شبکه علاوه بر آنکه خود در مقابل حملات آسیب پذیر هستند می توانند به پلی برای حمله به سیستم ها یا شبکه های دیگر تبدیل شوند. علاوه بر موارد گفته شده، باید توجه داشت که بسیاری از کاربران رایانه‌های متصل به شبکه‌ها، فاقد تخصص در بهره‌برداری از رایانه بوده و اصولا درک صحیحی از آسیب پذیری تجهیزات در اختیار خود و تهدیدهای موجود در شبکه ندارند. حتی با وجود داشتن تخصص، بسیاری از افراد ممکن است به دلیل اعتماد به تخصص طراحان یا راهبران شبکه، خود را ملزم به رعایت الزامات امنیتی ندانند یا در اجرای آنها سهل انگاری کنند.

وابستگی کامل بسیاری از سازمان ها به عملکرد صحیح شبکه های ارتباطی نیز عامل دیگری است که امن سازی شبکه های رایانه ای را در راس عملیات امن سازی قرار می دهد.

الزامات:

- طراحی معماری شبکه باید با توجه به سطح طبقه‌بندی حفاظتی اطلاعات جاری در آن و دسته‌بندی سازمان بهره‌بردار از دیدگاه پدافند غیرعامل و نیازمندی های امنیتی در جهت جلوگیری از اختلال در شبکه به دلایل تخریب فیزیکی یا حمله های رایانه‌ای انجام شود. این طرح باید با نگرش به ضرورت‌های زیر تدوین گردد:
  - افراز[1] بخش های مختلف شبکه از یکدیگر بر اساس ماموریت سازمانی بخش ها و کارکرد اجزای شبکه.
  - تعبیه خطوط اتصال بخش های مختلف شبکه بر اساس سیاست گذاری اتصال.
  - تعبیه نقطه امن در نقاط اتصال. (نقطه امن محلی است که در آن ابزار اعمال کلیه الزامات امنیتی که باید در تبادل بسته ها با خارج از شبکه رعایت شوند تامین شده باشد)
  - محدودسازی دسترسی آزاد از یک ایستگاه کاری به ایستگاه کاری دیگر و اعطای حقوق دسترسی بر اساس نیازهای کاری و تهیه فهرست های کنترل دسترسی[2].
  - جداسازی فیزیکی ایستگاه های کاری یا شبکه هایی که اتصال آنها به شبکه اصلی سازمان الزام ندارد و یا به دلایل حفاظتی باید جدا نگهداشته شوند.
- در هنگام طراحی پلان معماری شبکه باید (حداقل) بخش های زیر در نظر گرفته شده و در مورد حفاظت و تامین آنها تصمیم گیری شود:

[1] - Segmentation
[2] - ACLs: Access Control Lists

- ناحیه کاملاً امن (برای استقرار تجهیزات حاوی اطلاعات بسیار مهم مانند کلیدهای رمزنگاری، اطلاعات کارت های اعتباری، بایگانی اطلاعات پیکربندی تجهیزات مهم و اسرار سازمانی).
- ناحیه امن عملیاتی (برای استقرار تجهیزات، نرم افزارها و اطلاعات مهم سازمانی مانند سرورهای برنامه های کاربردی و بانک های اطلاعاتی مهم).
- ناحیه امن ارتباطی (برای استقرار تجهیزات مسیریابی و کنترل شبکه).
- نواحی کاری افراز شده (محل استقرار ایستگاه های کاری بر اساس ماموریت سازمانی).
- ناحیه کاربران راه دور قابل اعتماد (برای اتصال کاربرانی که از طریق شبکه های راه دور غیراینترنت و از طریق خطوط پهن باند به شبکه سازمان متصل می شوند).
- ناحیه کاربران راه دور تلفنی (برای اتصال کاربرانی که از طریق خطوط تلفنی عادی [1] به شبکه سازمان متصل می شوند).
- ناحیه DMZ [2] (برای استقرار تجهیزات برقراری ارتباط کاربران داخلی با شبکه های اطلاع رسانی عمومی مثل اینترنت و یا ارائه سرویس غیرمستقیم سازمان به این نوع شبکه ها)

- اتصال فیزیکی بین ناحیه کاملاً امن و سایر نواحی بجز ناحیه امن عملیاتی ممنوع است.
- اتصال فیزیکی بین هریک از بخش های فوق با شبکه باید از طریق مکانیزم نقطه امن محافظت شود.
- دسترسی به تجهیزات مدیریت یا مسیریابی شبکه باید با توجه به سطح طبقه بندی حفاظتی و با استفاده از قفل‌های مکانیکی و مکانیزم های کنترل دسترسی منطقی محدود شود.

[1] - PSTN: Public Switched Telephone Network
[2] - Demilitarized Zone

- اطلاعات دسترسی به تجهیزات مدیریت یا مسیریابی شبکه شامل زمان دسترسی، مکان و شناسه کاربری مورد استفاده باید به نحو مناسب ثبت و نگهداری گردد. در صورتی که هدف از جمع آوری این اطلاعات، استفاده از آنها در مراجع قانونی باشد مستندات مذکور می‌بایست به صورت محکمه پسند گردآوری و نگهداری شود.

- لازم است در مراکز حساس و حیاتی جهت مقابله با شنود خطوط انتقال، حتی‌الامکان از کابل‌های فیبر نوری استفاده شود و شبکه های این گونه مراکز به صورت تصادفی و در فواصل زمانی معین مورد بررسی قرار گیرند.

- باید در فواصل زمانی منظم و یا زمانی که پیکربندی تجهیزات تغییر می‌یابد، از پرونده‌های پیکربندی تجهیزات، نسخه پشتیبان تهیه شود.

- کلیه دارایی‌های اطلاعاتی مورد استفاده در فرآیند احراز هویت [1] بایستی در مقابل دسترسی‌های غیرمجاز محافظت شوند.

- لازم است به روز رسانی ضد بدافزارها در همه ایستگاه های کاری و سرورها طبق برنامه زمانی منظم اجرا گردد.

- نصب آخرین وصله‌های امنیتی و به روز رسانی امنیتی سیستم عامل و سرویس‌های موجود در شبکه باید به صورت مداوم صورت گیرد. در این مرحله علاوه بر اقدامات ذکر شده لازم است کلیه سرورها، سوئیچ‌ها، مسیریاب‌ها و سایر تجهیزاتی که دارای سیستم عامل هستند با ابزارهای شناسایی حفره‌های امنیتی

[1]- Authentication

بررسی شوند تا علاوه بر شناسایی و رفع حفره‌های امنیتی، سرویس‌های غیرضروری هم شناسایی و غیرفعال شوند.

- لازم است تمهیدات لازم در خصوص امن‌سازی فیزیکی اجزای شبکه طبق دستورالعمل‌های تأمین امنیت محیطی و فیزیکی انجام گیرد.

- ضروری است برای جلوگیری از بروز وقفه در فعالیت مراکزی که از دیدگاه پدافند غیرعامل جزء مراکز حیاتی دسته بندی شده‌اند، شبکه دیگری مشابه شبکه در حال کار (از بعد تجهیزات و کارکرد)، در محلی که از نظر جغرافیایی با شبکه اول دارای فاصله مطمئن است، ایجاد و عملیاتی گردد.

- برای تأمین امنیت شبکه و مقابله با حملاتی نظیر پیکربندی غیرمجاز سیستم و حملات DoS، لازم است امنیت سرویس‌های شبکه و کنترل تجهیزات شبکه (همچون مسیریاب‌ها، سوئیچ‌ها، دیواره‌های آتش و سایر ابزارهای مسیریابی و امنیتی) بررسی و کنترل گردد.

- ضروری است فعالیت‌های کاربران در جهت مقابله با تخلفاتی نظیر نصب هرگونه نرم‌افزار پویش پورت، پویش شبکه، عبور از فیلترهای اینترنتی و نفوذگری در سیستم‌های فردی- شبکه‌ای کنترل و بررسی شود.

- از ضرورت‌های ایجاد امنیت پایدار برای شبکه متصل به اینترنت، اجرای نرم‌افزارهای ضد جاسوسی [1] و ضد تبلیغ افزارها[2] به صورت منظم می‌باشد.

[1]- Anti Spyware
[2]- Anti Adware

- نرم‌افزارهای جدید باید با هماهنگی مدیر ارشد شبکه نخست به صورت آزمایشی بر روی یک دستگاه یا در صورت حساس و یا حیاتی بودن سازمان بهره‌بردار روی یک شبکه آزمایشی جداگانه نصب شود و سپس در صورت تأیید نهاد متصدی امنیت اطلاعات، بر روی ایستگاه های کاری مورد نظر نصب گردد.

- بازدید از صفحات وب در اینترنت فقط مختص وظایف سازمانی و علایق کاری متخصص مربوط و فقط در قلمرو عملیات سازمان مجاز است. ضروری است عملکرد کاربران در این زمینه کنترل شود. همچنین لازم است این موضوع قبلاً به اطلاع کلیه کاربران رسیده باشد.

- لازم است نسخ پشتیبان از پیکربندی تجهیزاتی که بروز اختلال در کارایی آنها می‌تواند منجر به ایجاد اختلال در کل شبکه شود، تهیه گردد تا درصورت بروز اختلال، در کوتاه‌ترین زمان ممکن با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه به آخرین حالت بی‌نقص پیش از اختلال بازگردانده شود. مراحل بازگشت به آخرین وضعیت پایدار قبلی بر اساس طرح احیای سیستم(DRP)[1] و حداکثر زمان مجاز خارج از سرویس بودن شبکه یا برخی از اجزای آن بر اساس الزامات طرح پیوستگی عملیات (BCP)[2] معین خواهد گردید.

- سرویس‌های قابل ارائه توسط هر رایانه بایستی کنترل و بررسی گردد و سرویس‌های غیرضروری نظیر اشتراک فایل و چاپگر، غیرفعال شود.

[1]- Disaster recovery plan
[2]- Business continuity plan

- لازم است مدیر شبکه جهت امور روزانه از یک شناسه کاربری با سطح دسترسی عادی استفاده کرده و تنها در جهت انجام فعالیت‌هایی که نیاز به سطح دسترسی بالاتری می باشد، از شناسه کاربری خاص مدیریتی (حق دسترسی ممتاز) استفاده نماید.

- ردیابی و مشاهده فعالیت‌ها و ارتباطات کاربران باید برای دیگر کاربران غیرممکن باشد و همچنین برای جلوگیری از شنود پیام‌هایی که در شبکه ارسال و یا دریافت می‌شود باید این پیامها به صورت مناسب رمزگذاری شود.

- هنگام ارسال پیام می‌بایست کاربران از هویت و اصالت طرف مقابل اطمینان حاصل نمایند و مطمئن شوند که کاربری که با آن تماس گرفته‌اند واقعاً همان فردی است که انتظارش را داشته‌اند. همچنین ارسال کننده یک پیام نباید بتواند پیامی را که فرستاده انکار نماید. در صورتی که تبادل پیام منجر به ایجاد تعهد قانونی برای طرفین تبادل شود لازم است اصالت طرفین، صحت پیام و عدم انکار از طریق استفاده از امضای الکترونیکی قابل پذیرش توسط مراجع قانونی تضمین گردد.

- لازم است کلیدهای رمزنگاری اطلاعات در فواصل زمانی از پیش تعیین شده تغییر پیدا کند تا از افشاء و دسترسی غیرمجاز به اطلاعات جلوگیری گردد. همچنین لازم است از کلیدهای رمزنگاری فاقد اعتبار همانند کلیدهای رمزنگاری معتبر حفاظت و نگهداری شود زیرا ممکن است برای دسترسی مجدد به داده‌های رمزنگاری شده قدیمی، مجدداً به آنها نیاز باشد.

- ممکن است سیاست‌های امنیتی، ابلاغ دستورالعمل و بخشنامه‌ها توسط کارکنان فرصت‌طلب یا سهل‌انگار با بی‌توجهی مواجه شود. لذا می‌بایست تجهیزات و سرویس دهنده‌های آسیب‌پذیر با بکارگیری ابزارهای

احتمالی که نفوذگر برای نفوذ به شبکه استفاده می‌کند، کشف گردند. ضروری است فرآیند فوق طی زمانبندی معین و با رعایت جنبه های قانونی، حقوقی و مدیریتی تکرار پذیرد.

- در مراکز حساس و حیاتی لازم است تمام رایانه‌ها و تجهیزات شبکه پلمپ شده و شماره‌گذاری شوند. افراد غیرمجاز حق باز کردن بدنه رایانه‌ها و تجهیزات شبکه را به هر منظوری ندارند.
- لازم است نقاط اتصال شبکه بصورت مداوم و در بازه های زمانی از پیش تعیین شده از لحاظ عدم وجود اتصال های فیزیکی غیر مجاز (اعم از کابلی یا بی سیم) بازبینی شود.
- لازم است مستندات نحوه اتصال فیزیکی و مسیرهای عبوری در نقاط اتصال شبکه بصورت کاملاً شفاف و به روز تهیه و نگهداری شده تا در صورت بروز مشکل بتوان از آنها استفاده کرد.
- لازم است ترافیک عبوری از نقاط ارتباطی شبکه در بخش های مختلف به صورت منظم و خودکار مانیتور و Log برداری گردد (برای این کار باید از نرم افزارهای مانیتورینگ تائید شده استفاده شود. زیرا برخی از نرم افزارهای مانیتورینگ به صورت عامل شنود و جاسوسی عمل می کنند).
- لازم است در مواقع لزوم از مکانیزم های امنیتی مناسب مثل Access List ها (ACLs) و یا محدود کننده های ترافیک و یا مکانیزم های اولویت بندی و دسته بندی ترافیک (QoS[1] و CoS[2]) بر اساس مشخصات مبداء و مقصد از جمله آدرس IP و آدرس فیزیکی مبداء و مقصد استفاده شود.
- لازم است در نقاط اتصال با شبکه های دیگر و یا در ایستگاه های کاری حساس از مکانیزم های فایروال، IDS و IPS برای تشخیص و جلوگیری از نفوذ استفاده شود.

[1] Quality of Service
[2] Class of Service

- تخطی از سیاستگذاری کنترل دسترسی، کنترل اتصال های شبکه یا کشف ترافیک ناشناس یا غیر مجاز باید به عنوان رخداد امنیتی ثبت و مورد رسیدگی قرار گیرد.

- لازم است عملکرد پروتکل ها و تجهیزات مسیریابی شبکه از طریق شناسایی آدرس های مبداء و مقصد بسته های اطلاعاتی و بررسی مجاز بودن ارسال آنها تحت کنترل قرار گیرد.

- حتی الامکان بایستی از مکانیزم تبدیل آدرس های شبکه (NAT) در نقاط اتصال شبکه های داخلی و خارج از سازمان و یا برای جداسازی و حفاظت از بخش های خاص شبکه استفاده شود.

- حتی الامکان باید از پروتکل های مسیریابی ایستا (Static) جهت مسیریابی شبکه به خصوص در لایه های مرزی استفاده شود.

- در صورت استفاده از الگوریتم های مسیریابی دینامیک داخلی یا خارجی (Dynamic Routing) باید از مکانیزم های تشخیص هویت جهت امن سازی تبادل اطلاعات مسیریابی استفاده شود.

- لازم است امکانات اتصال مستقیم به مسیریاب یا سوئیچ های شبکه ای مثل پورت Console یا Aux تحت کنترل کامل قرار داشته باشد تا از سوء استفاده از این امکانات برای دخالت در مسیریابی جلوگیری شود.

- پیکربندی، راه اندازی و یا نصب مجدد مسیریاب باید توسط افراد معتمد انجام شود.

- در صورت استفاده از الگوریتم های مسیریابی دینامیک لازم است از مکانیزم های مناسب برای جلوگیری از انتشار اطلاعات مسیریابی داخلی به شبکه های خارجی استفاده شود.

- لازم است مکانیزم های غیر ضروری مسیریاب ها غیر فعال گردند.

- جداسازی شبکه ها باید در دو سطح منطقی (با استفاده از تعریف منطقی شبکه های مجزا از یکدیگر و بکارگیری مکانیزم های کنترل دسترسی برای برقراری ارتباط بین آنها) و یا سطح فیزیکی (با استفاده از قطع اتصال های کابلی و بی سیم بین شبکه تحت حفاظت، از سایر شبکه ها) انجام شود.

- بطور کلی لازم است شبکه ها به دو دسته شبکه داخلی (شامل LANها و DMZ) و خارجی (شامل کلیه شبکه های خارج از کنترل سازمان) دسته بندی شوند.

- اتصال بین شبکه های داخلی و شبکه خارجی عمومی باید از طریق DMZ انجام شود.

- اگر از شبکه های خارجی عمومی برای اتصال بین دو شبکه داخلی سازمان استفاده می شود لازم است همراه با DMZ، از مکانیزم نقطه امن نیز برای جداسازی شبکه ها از یکدیگر استفاده شود.

- بطور کلی لازم است جهت جداسازی شبکه های داخلی متفاوت از لحاظ طبقه بندی حفاظتی نیز از مکانیزم نقطه امن استفاده شود.

- شبکه هایی که اطلاعات جاری در آنها دارای طبقه بندی حفاظتی بالاتر از خیلی محرمانه است باید بصورت فیزیکی از سایر شبکه ها جداسازی شوند.

- لازم است حداکثر زمان نشست ارتباطی بین دو برنامه (که از طریق شبکه با یکدیگر تبادل اطلاعات می نمایند) به نحوی تعیین شود تا با محدودسازی فرصت حمله، از امکان سوءاستفاده از سیستم و نقض امنیت آن، حتی در صورت سرقت نشست یا جعل IP، جلوگیری شود.

- لازم است تدابیر لازم برای جلوگیری از ایجاد کانال های پنهان[1] (مثلاً با استفاده از پروتکل ICMP برای عبور از فایروال) جهت برقراری نشست های غیرمجاز، بکار گرفته شود و پس از پایان مدت زمان منظور شده برای یک نشست، بصورت خودکار به نشست پایان داده شود.

- پس از پایان یک نشست بصورت خودکار، لازم است از دسترسی به ترمینال ارتباطی جلوگیری شود.

- در صورت تجاوز زمان یک نشست از زمان تعیین شده برای آن، لازم است علاوه بر قطع خودکار نشست، وضعیت بوجود آمده به عنوان یک رخداد امنیتی ثبت و پیگیری گردد.

- لازم است مکانیزم های مناسب برای پایان دادن خودکار به نشست جاری در صورت قطع ارتباط هر یک از طرفین نشست پیاده سازی شود.

- پس از تکمیل عملیات روی کامپیوترهای Main frame علاوه بر خاموش کردن PC یا ترمینال طرف ارتباط، لازم است به نشست جاری نیز پایان داده شود.

-هنگامی که از یک سیستم حساس در محیط اشتراکی استفاده می شود، لازم است سیستم های دیگری که به صورت اشتراکی با این سیستم مورد استفاده قرار می گیرند، شناسایی شده و توافق متصدی سیستم حساس در کار همزمان با بقیه سیستم ها کسب شود.

-بهره برداری از تجهیزات بی سیم در شبکه های حاوی اطلاعات محرمانه یا سری‌تر از آن ممنوع است مگر آنکه قبلاً تحلیل ریسک رسمی در خصوص آن انجان شده و موافقت کتبی مدیر ارشد سازمان کسب شده باشد.

[1]- Covert Channel

فرآیند:

امنیت به عنوان یکی از مولفه های اصلی در مراحل طراحی شبکه مورد توجه قرار می گیرد. به عبارت دیگر هنگامی یک طرح به عنوان طرحی مناسب قابل پذیرش خواهد بود که در آن نیازهای امنیتی نیز لحاظ شده و روش های مناسب برای پاسخ به آن نیازها طراحی شده باشد. در این مرحله باید هدف از ایجاد شبکه، محیط استقرار شبکه، ماهیت و حجم داده های جاری در آن و خصوصیات کاربران در کنار محدودیت های بودجه ای و تهدیدات احتمالی مورد توجه قرار گیرد. طراحی مکانیزم های حفظ امنیت در این مرحله باید انجام شود.

لحاظ کردن امنیت در مرحله پیاده سازی به معنی اجرای دقیق عملیات نصب تجهیزات و نرم افزارها بر اساس طرح معماری است. در این مرحله ممکن است به دلیل واقعیت های موجود که در مرحله طراحی قابل احصاء نبوده است نیاز به تغییر در روش یا تجهیزات باشد. هر گونه تغییر در مرحله پیاده سازی باید با لحاظ کردن پیامدهای احتمالی آن و با اطلاع گروه طراح یا ناظر بر پیاده سازی انجام شود.

رعایت امنیت در مرحله بهره برداری مهمترین موضوع در امنیت شبکه است. حتی اگر شبکه ای به صورت امن طراحی یا پیاده سازی نشده باشد می توان با رعایت نکات امنیتی به بهره برداری امن از آن پرداخت. بدیهی است نکات متعددی در این زمینه باید رعایت شوند که به فراخور هر شبکه یا سازمان تعیین خواهند شد.