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 ۸:ارزیابی امنیتی و حسابرسی

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	۱۱
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات ایران
کد سند	R90040108

هدف:

هدف از تدوین این توصیه نامه بیان لزوم شناخت حوزه های ارائه خدمات رایانه ای در سازمان، شناخت آسیب پذیری ها در مقابل تهدیدهای سایبری، ارزیابی ریسک های عملیاتی، انتخاب مکانیزم های کنترل و مدیریت ریسک، و ممیزی اجرای مکانیزم های کنترلی می باشد.

ضرورت:

بهره برداری از روش‌های ارائه خدمات رایانه‌ای، بخصوص خدمات غیرحضوری(از طریق شبکه های داخلی، گسترده، اینترنت ویا سایر روشهای دسترسی از راه دور) هر روز ابعاد گسترده‌تری می یابد. تنوع و قدرت ابزار(سخت‌افزاری و نرم‌افزاری) مورد نیاز برای ارائه این نوع خدمات نیز به سرعت رو به افزایش هستند. این وضعیت باعث آسیب پذیری بیشتر بهره برداران از این ابزار در مقابل تهدیدات ناشی از عملکرد نادرست ابزار یا سوء استفاده از آنها می شود.

برای جلوگیری از این آسیب پذیری ها باید مکانیزم های حفاظتی یا کنترلی لازم تعریف شده و به اجراء گذاشته شوند. به علاوه باید از کفایت و اجرای صحیح این مکانیزم ها اطمینان حاصل شود. بنابراین لازم است روشهای ارائه خدمات سازمان و ریسک های ناشی از تهدیدات سایبری پیش روی آن شناسایی شده و روش های مناسبی برای بهره برداری امن از این گونه خدمات به کارگرفته شود و در بازه های زمانی مناسب مورد ممیزی و بازنگری قرار گیرد.

الزامات:

- لازم است گزارش شناخت که برای ارزیابی امنیت فناوری اطلاعات سازمان تهیه می شود حداقل دارای بخش های زیر باشد:
  - خلاصه تاریخچه بهره برداری از سامانه های رایانه ای
  - ساختار و چارت سازمانی
  - وضعیت فعلی سازمان، نحوه بهره برداری از سامانه های رایانه ای و خدمات قابل ارائه توسط آنها
  - آخرین تحول مهم در وضعیت سامانه های پردازشی و ارائه خدمات رایانه ای
  - هدف گذاری و برنامه های آینده تحول در نحوه ارائه خدمات (تبدیل خدمات معمولی به خدمات رایانه ای و یا بهبود روش های فعلی ارائه خدمات رایانه ای)
  - نقشه مکان های استقرار املاک سازمان (که بر اساس سند تعیین قلمرو پیاده سازی نظام مدیریت امنیت اطلاعات تعیین شده اند)
  - نقشه مکان های استقرار تجهیزات و دارایی های اطلاعاتی و جانمایی آنها
  - مکان های ارائه خدمات رایانه ای از قبیل سایت سازمانی، کیوسک های اطلاعاتی، تجهیزات دریافت و پرداخت، محیط Web و غیره
  - نقشه معماری و توپولوژی شبکه های ارتباطی سازمان (LAN، CAN، MAN، WAN)

- فهرست کانال های ارتباطی با سایر شبکه های خارج از کنترل سازمان شامل نوع، ظرفیت، نام مرجع کنترل کننده شبکه، اعم از شبکه های باسیم، بی سیم، ماهواره ای یا فیبر نوری که برای انتقال داده، صوت و یا تصویر بکار گرفته می شوند.
- فهرست موجودی دارایی های اطلاعاتی همراه ذکر نام مالک، متصدی و یا تحویل گیرنده هر یک از اجزای آن
- مکانیزم های کنترلی و امنیتی فعلی برای حفاظت از دارایی های اطلاعاتی

- مسئولیت ارزیابی ریسک مرتبط با هر فرآیند یا هر جزء از دارایی های اطلاعاتی با مالک، متصدی و یا تحویل گیرنده فرآیند یا دارایی اطلاعاتی می باشد. به عنوان مثال مسئول اتاق سرور، مسئول ارزیابی و مستندسازی ریسک کلیه فرآیندهای مرتبط با فعالیت تجهیزات مستقر در اتاق سرور و استخراج شاخص ریسک مربوط می باشد.
- مسئولیت ارزیابی ریسک کلی و مقایسه ریسک واحدهای مختلف با یکدیگر و تعیین اولویت های امن سازی بخش ها، فرآیندها و یا دارایی های اطلاعاتی بر عهده نهاد متصدی امنیت اطلاعات (به عنوان مثال مرکز حراست فناوری اطلاعات یا ارتباطات و یا نهادهای معادل آن) می باشد. در صورت عدم وجود این نهاد، این مسئولیت به عهده کمیته امنیت اطلاعات (که با حکم مدیر ارشد سازمان تشکیل می شود) خواهد بود.
- لازم است ارزیابی ریسک برای کلیه بخش ها، فرآیندها و دارایی های اطلاعاتی موجود در سند قلمرو پیاده سازی سامانه مدیریت امنیت اطلاعات به انجام رسد. این ارزیابی باید برای کلیه دارایی

های اطلاعاتی لازم در اجرای هر فرآیند و کلیه فرآیندهای قابل اجرا در هر بخش از سازمان به عمل آید، به نحوی که بتوان:

- اولاً دارایی های اطلاعاتی را از لحاظ مقدار ریسک مرتبط با استفاده از آنها نسبت به یکدیگر رده بندی کرد. (مثال: ریسک سرقت اطلاعات از کامپیوترهای متصل به شبکه بیشتر از ریسک سرقت اطلاعات از کامپیوترهای مجزا می باشد. همچنین استفاده از شبکه های بی سیم ریسک را افزایش می دهد.)
- ثانیاً فرآیندهای اجرایی مختلف را از لحاظ مقدار ریسک مرتبط با اجرای آنها نسبت به یکدیگر رده بندی کرد. (مثال: ریسک امنیتی فروش تلفنی بیشتر از فروش معمولی و ریسک امنیتی فروش الکترونیکی بیش از فروش معمولی یا تلفنی می باشد.)
- ثالثاً بخش های مختلف سازمان را از لحاظ پتانسیل آسیب پذیری در مقابل تهدیدهای مختلف موجود در زمینه امنیت اطلاعات دسته بندی نمود. (مثال: ریسک امنیتی مکان هایی که به ارایه خدمات حضوری به ارباب رجوع می پردازند بیشتر از مکان های دیگر سازمان است و به همین ترتیب ریسک امنیتی مرکزداده ای که در مجاورت یک پمپ بنزین قرار گرفته بیشتر از مراکز داده دیگر است.)

– لازم است فعالیت های امن سازی بر اساس تحلیل نتایج حاصل از ارزیابی ریسک اولویت بندی شوند به نحوی که:

- دارایی های اطلاعاتی دارای بیشترین آسیب پذیری (با ریسک بالا) در اولویت قرار گرفته و رویه های مدیریت و کنترل ریسک در مورد آنها به اجرا گذاشته شود.
- پس از امن سازی دارایی های اطلاعاتی فوق، فرآیندهای دارای بیشترین آسیب پذیری (با ریسک بالا) در اولویت قرار گرفته و رویه های مدیریت و کنترل ریسک در مورد آنها به اجراء گذاشته شود.
- پس از طی دو مرحله فوق به عنوان مراحل اضطراری ، اولویت بندی سایر دارایی ها و فرآیندهای اجرایی تعیین و رویه های مدیریت و کنترل ریسک در مورد آنها به اجراء گذاشته شود.
- در آخرین مرحله، وضعیت ریسک باقیمانده [1] بخش های مختلف سازمان نسبت به یکدیگر مجدداً ارزیابی شده و برنامه مدیریت و کنترل آنها تدوین شود.

- لازم است ارزیابی ریسک برای کلیه دارایی های اطلاعاتی مندرج در فهرست موجودی دارایی های اطلاعاتی به انجام رسد.
- ارزیابی آسیب پذیری های فنی که در قالب آزمون نفوذ (تست نفوذپذیری) انجام می شود باید با رعایت الزامات حقوقی و پس از ارزیابی ریسک آزمون انجام شود.
- لازم است کلیه دارایی های اطلاعاتی قبلاً ارزش گذاری شوند. ارزش هر دارایی اطلاعاتی به وسیله مالک، متصدی و یا تحویل گیرنده آن دارایی تعیین خواهد شد. هنگام ارزش گذاری باید

[1] - ریسک باقیمانده عبارت است از آن مقدار از ریسک که پس از اجرای امن سازی بطور طبیعی باقی خواهد ماند و یا با نظر مدیریت قابل پذیرش محسوب می شود.

کلیه آثار ناشی از فقدان یا عدم عملکرد صحیح هر یک از دارایی های اطلاعاتی و زیان حاصل از آن برای سازمان و یا مشتریان و ارباب رجوع در نظر گرفته شود. ارزش گذاری می تواند بصورت کیفی یا کمی باشد.

- لازم است آسیب پذیری های احتمالی هر دارایی فهرست شوند. نقاط آسیب پذیر نشان دهنده نقاط ضعف هر دارایی و عوامل تولید ریسک می باشد.
- لازم است تهدیدهای موجود برای هر دارایی فهرست شوند. تهدیدها عبارتند از شرایطی که ممکن است باعث سوء استفاده از نقاط آسیب پذیر هر دارایی اطلاعاتی یا فرآیند شده و یا موجب ضربه پذیری از آن نقطه شوند.
- لازم است برای هر یک از تهدیدهای فهرست شده فوق، مکانیزم های کنترلی مناسب بر اساس مدل استاندارد مرجع شناسایی شده و طبق دستورالعمل مدیریت و مقابله با ریسک به اجراء گذاشته شود.
- لازم است گزارش جمع بندی ارزیابی ریسک امنیتی به کمیته امنیت اطلاعات ارسال شود. در این گزارش باید به نام دارایی هایی که حفاظت از آنها دارای اهمیت زیاد می باشد اشاره شود.
- لازم است کمیته امنیت اطلاعات امن سازی دارایی های اطلاعاتی دارای اهمیت زیاد را مستقیماً تحت نظر بگیرد.
- لازم است سایر دارایی ها بر اساس رهنمودهای مندرج در سند راهنمای سیاست گذاری امنیت اطلاعات تحت محافظت قرار گیرند.

- ممکن است برخی دارایی های اطلاعاتی در مرحله اول ارزیابی از نظر پوشیده باقی بمانند. بنابراین لازم است شناسایی دارایی های اطلاعاتی بصورت مستمر (و در دوره های زمانی قابل توجیه) و بخصوص هنگام تغییر در فرآیندهای اجرایی، تغییر در روش انجام کار، تغییر مکان دارایی های اطلاعاتی و یا بهره برداری از فرآیندها یا دارایی های اطلاعاتی جدید انجام پذیرد.
- برقراری ارتباط با سایی شبکه ها، تبادل اطلاعات یادداه و تعامل الکترونیکی فقط پس از اثبات الزام قانونی، مقرراتی یا تجاری مجاز است و لازم است قبل از آن ارزیابی ریسک انجام شود.

- لازم است کلیه ریسک های شناسایی شده در مرحله ارزیابی ریسک مورد بررسی قرار گرفته و یکی از تصمیمات زیر در خصوص آنها اتخاذ شود:

الف- اجتناب از ریسک، از طریق تغییر فرآیند یا خودداری از استفاده از دارایی اطلاعاتی مربوط و یا تغییر در روش استفاده از آن به نحوی که عامل ایجاد ریسک از بین رفته و ریسک مربوط حذف گردد.

ب- کاهش ریسک به حد قابل قبول، از طریق تغییر در فرآیند یا روش استفاده از دارایی اطلاعاتی به نحوی که مقدار ریسک مربوطه به حد قابل قبولی کاهش یابد. به عنوان مثال می توان به جداسازی رایانه های حاوی اطلاعات دارای طبقه بندی خیلی محرمانه از شبکه LAN سازمان برای کاهش خطر سرقت از طریق شبکه یا دستکاری آنها اشاره کرد.

ج- انتقال ریسک از طریق عقد قرارداد با سایر طرف های تجاری برای پذیرفتن یا جبران خسارات ناشی از حوادث رایانه ای توسط ایشان. برای مثال می توان به قرارداد بانک ها با شرکت های بیمه در خصوص پرداخت خسارت های احتمالی سرقت های رایانه ای از حساب مشتریان توسط شرکت های بیمه اشاره کرد.

د- پذیرش و پایش ریسک، از طریق پذیرش ریسک استفاده از دارایی اطلاعاتی یا فرآیند ریسک دار و تحت نظر داشتن ریسک‌های پذیرفته شده برای جلوگیری از افزایش مقدار ریسک از حد قابل قبول و تعیین شده توسط مدیریت ارشد سازمان. مانند تحت نظر داشتن گزارش وقایع امنیتی و بررسی آنها برای آگاهی از روند تلاش برای دسترسی غیر مجاز به دارایی های اطلاعاتی سازمان از طریق اینترنت (در سازمان هایی که به دلیل ضرورت کاری مجبور به پذیرش ریسک موجود در اتصال به اینترنت می باشند) از جمله این موارد به شمار می آید.

-پس از تصمیم در خصوص نحوه تعامل با ریسک (شامل اجتناب، کاهش، انتقال و یا پذیرش ریسک) لازم است نحوه تعامل با ریسک به تفکیک هر نوع از ریسک های شناسایی شده مستند شده و بصورت گزارشی مکتوب برای اطلاع کمیته امنیت اطلاعات ارسال شود.

-در خصوص ریسک های پذیرش شده (اعم از ریسک های کاهش یافته به حد قابل قبول و یا پذیرفته شده) لازم است رویه های چگونگی کنترل آنها مستند شود. در رویه های کنترلی بایستی به موارد زیر اشاره شود:

- چه چیزی تحت حفاظت قرار گیرد.
- در مقابل چه چیزی حفاظت انجام شود.
- حفاظت چگونه انجام شود.
- برای حفاظت به چه ابزار و روشی نیاز است.

-لازم است رویه های کنترلی به تفکیک رویه های حفاظت از فرآیندها و رویه های حفاظت از دارایی های اطلاعاتی در دو نوع تهیه و تدوین شوند.

- اولویت تدوین رویه های کنترلی بر اساس شاخص اهمیت فرآیند و یا شاخص ریسک جغرافیایی تعیین می شود. به این معنی که فرآیندها یا مکان های استقراری که دارای اهمیت یا ریسک زیادتری برای سازمان هستند بایستی در اولویت حفاظت قرار گیرند.
- لازم است به منظور اطمینان از کفایت و رعایت دستورالعمل ها و مکانیزم های امنیت اطلاعات، ممیزی های مستقل به صورت دوره ای و بر اساس توصیه های ممیزی نظام استاندارد مرجع انجام شود. این گونه ممیزی ها باید توسط نهادها یا مراکزی انجام شود که صلاحیت آنها از سوی مراجع ذیصلاح صحه گذاری شده باشد.
- حتی الامکان لازم است ممیزی سامانه مدیریت امنیت اطلاعات بر اساس متدهای تعریف شده در استانداردهای پذیرفته شده امنیت اطلاعات (مانند استاندارد ISO-27001) انجام پذیرد.
- لازم است فعالیت های ممیزی به نحوی انجام شود که خود تبدیل به منبع تولید ریسک نگردد.

- حفاظت از گزارش های تولید شده در حین ممیزی ضروری است و سطح طبقه بندی این گزارش ها، یک رده بالاتر از سطح طبقه بندی دارایی اطلاعاتی ممیزی شده خواهند بود.
- در کلیه سازمانها، ادارات و نهادهای دولتی، و همچنین در مراکزی که توسط سازمان پدافند غیر عامل به عنوان سازمانهای حیاتی، حساس یا مهم دسته بندی شده اند، سپردن ممیزی به اتباع یا شرکتهای خارجی ممنوع است.
- در کلیه فعالیت های ممیزی اولاً لازم است استقلال ممیزی کننده به رسمیت شناخته شده و رعایت گردد و ثانیاً حقوق ممیزی شونده رعایت گردد.

فرآیند:

مسئولیت تهیه گزارش شناخت سازمان را می توان بر عهده کارگروهی متشکل از افراد آگاه به ماموریت سازمان، روش های ارائه خدمات رایانه ای سازمان و همچنین آگاه به امنیت اطلاعات گذاشت. این گزارش که باید به رؤیت بالاترین مقام اجرایی سازمان برسد، به عنوان نقطه شروع عملیات ارزیابی ریسک مورد استفاده قرار می گیرد.

معمولاً ارزیابی ریسک نیز بر عهده کارگروه فوق گذاشته می شود. در این حالت کارایی فعالیت ها افزایش خواهد یافت. البته در هر حالت باید روشی قاعده مند برای ارزیابی ریسک انتخاب یا طراحی و اجراء شود، به طوری که اجرای آن توسط افراد مختلف منجر به خروجی یکسان شود.

از نتایج ارزیابی ریسک برای انتخاب مکانیزم های امن سازی استفاده می شود. مکانیزم های امنیتی دارایی های اطلاعاتی مهم یا فرآیندهای مهم باید مکتوب بوده و به صورت رسمی به اطلاع کاربران برسد و تعهد کتبی ایشان به رعایت آنها اخذ شود.

برای اطمینان از رعایت مکانیزم ها می توان از روش های بازرسی یا ممیزی استفاده کرد. از آنجا که گرایش کلی در سامانه های مدیریت اطلاعات حرکت به سمت تعالی سازمان و بهبود مستمر وضعیت است روش ممیزی ترجیح داده می شود. در این حالت باید الزامات ممیزی از قبیل فعالیت های پیشنیاز ، اجرای نظام‌مند و بازنگری های مدیریتی مورد توجه قرار گیرد.