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 ۱۱ : امنیت نرم افزارها

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	R90040411

هدف:

هدف از تدوین این توصیه نامه بیان لزوم رعایت الزامات امنیتی در نصب، نگهداری و استفاده از سیستم عامل، بانک های اطلاعاتی و برنامه های کاربردی دفتری و عملیاتی می باشد.

ضرورت:

سیستم عامل برقراری ارتباط بین سخت افزارها و برنامه های کاربردی از یک طرف و کاربر با سامانه پردازشی از طرف دیگر را به عهده دارد. به همین دلیل از یک سو دارای امکانات پرقدرت تعامل با بخش های مختلف سخت افزاری از طریق امکان بهره برداری از زبان ماشین بوده و از طرف دیگر دسترسی کاربر به سیستم را (از طریق کنترل دسترسی) ایجاد و مدیریت می نماید.

بانک های اطلاعاتی حاوی اطلاعات ارزشمند سازمانی است که باید همیشه حاوی اطلاعات صحیح و قابل اعتماد باشد. ارزش این اطلاعات ممکن است از اهمیت ذاتی یا مدت زمان گردآوری آن سرچشمه گرفته باشد.

برنامه های کاربردی دفتری یا عملیاتی، بهره برداری از اطلاعات را در قالبهای مورد نیاز یا مورد علاقه امکان پذیر می سازند.

به دلیل وابستگی روزافزون ارائه خدمات سازمان به عملکرداین ابزار، ایجاد و حفظ شرایط عملکرد صحیح آنها ضروری است. در برخی از سازمان ها وابستگی به حدی است که توقف عملکرد هر یک از اجزای فوق منجر به توقف عملیات سازمان می شود.

الزامات:

- سیاست های کنترل دسترسی به سیستم های عامل مورد استفاده در سرورهای شبکه و کلیه ایستگاه های کاری متصل به آن و سیستم عامل های خاص تجهیزات مسیریابی باید به صورت مکتوب تدوین گردد.

- سیاست های کنترل دسترسی به سیستم های عامل مورد استفاده درسرورهای دارای کاربرد امنیتی و کلیه ایستگاه های کاری مربوط به مانیتورینگ و سیستم عامل های خاص تجهیزات امنیتی از قبیل فایروال و سامانه های تشخیص نفوذ(IDS) باید به صورت جداگانه تدوین و تصویب شود.

- مسئولیت نظارت بر اجرای سیاست های کنترل دسترسی در حوزه سیستم عامل به عهده مدیر نهاد متصدی امنیت اطلاعات میباشد.

- لازم است با استفاده از امکانات امنیتی در سطح سیستم عامل، از دسترسی غیر مجاز به دارایی های اطلاعاتی به وسیله تجهیزات کامپیوتری جلوگیری کرد. این امکانات باید توانایی انجام فعالیت های زیر را ایجاد نمایند :

الف) شناسایی و بررسی هویت و درصورت ضرورت پایانه یا مکان هر یک از کاربران مجاز

ب) ثبت اقدامات موفق یا غیر موفق ورود به سیستم

ج) فراهم آوری امکانات مناسب برای تصدیق هویت

ت) محدود ساختن زمان های ارتباط کاربران

- لازم است دسترسی به خدمات اطلاعاتی از طریق یک فرآیند امن شروع به کار، امکان پذیر باشد. رویه شروع به کار و ورود به هر سیستم رایانه ای یا دسترسی به هر دارایی اطلاعاتی باید به نحوی طراحی شود که هرگونه فرصت دسترسی غیرمجاز را به حداقل برساند.

- لازم است رویه ورود به سیستم، حاوی حداقل اطلاعات مربوط به سیستم باشد تا از ارائه اطلاعات ی که ممکن است منجر به شناسایی سیستم توسط افرادی شود که قصد ورود غیرمجاز به آن را دارند جلوگیری به عمل آید. هر رویه ورود مناسب باید :

الف) قبل از تکمیل موفقیت آمیز رویهٔ ورود، هیچ شناسه ای از سیستم یا برنامه های کاربردی آن را نمایش ندهد.

ب) هنگام ورود یک اخطار عام در مورد اینکه فقط افراد مجاز اجازه استفاده از سیستم دارند را نمایش دهد.

ج) هیچ گونه پیام کمکی را که اطلاعات مندرج در آن بتواند در شناسایی سیستم، مورد استفاده کاربران غیرمجاز قرارگیرد نمایش ندهد.

د) فقط پس از ورود کامل اطلاعات احراز هویت، مراحل ارزیابی را انجام دهد و درصورت بروز اشکال، نباید محل و دلیل وقوع آن را نمایش داده و یا صحیح بودن یا نبودن هر قسمت از اطلاعات را گزارش کند.

ه) تعداد دفعات ورود ناموفق را به حداکثر سه بار محدود نماید و :

– تلاش های ناموفق را ثبت کند.

– درصورت وقوع یک تلاش ناموفق، (برای جلوگیری از اجرای حمله های فرهنگ لغت یا حدس کلمه عبور) تاخیر زمانی مناسب برای تلاش بعدی ایجاد شود و یا نیاز به تصدیق هویت خاصی الزامی باشد.

– در صورت مشکوک بودن درخواست دسترسی، خط ارتباطی مربوط قطع شود.

– حداقل و حداکثر زمان صرف شده برای اجرای رویهٔ ورود را محدود نماید و درصورت تجاوز از این محدوده، خط ارتباطی قطع شود.

و) پس از موفقیت آمیز بودن اجرای رویهٔ ورود، اطلاعات زیر نمایش داده شود:

– تاریخ و زمان آخرین ورود موفقیت آمیز قبلی

– جزئیات کلیه تلاش های ناموفق ورود از زمان آخرین ورود موفق

– برای هر یک از سه سطح کاربران عادی، کاربران دارای حق دسترسی ممتاز و مدیران شبکه بایستی سیستم‌های عامل مناسب به صورت مستدل و با توجه به نیازمندیهای امنیتی آنها انتخاب شود و پیکربندی امنیتی آنها با عنایت به دستورالعمل‌های منتشر شده از سوی مدیر ارشد شبکه یا مدیر امنیت اطلاعات انجام شود.

– ارتقاء نسخه سیستم‌های عامل مورد استفاده در سازمان بایستی با پیشنهاد مدیر ارشد شبکه و تائید مدیر نهاد متصدی امنیت اطلاعات صورت گیرد.

– نصب آخرین وصله‌های امنیتی (Security Patches) الزامی می باشد. در این زمینه باید قبلاً تحلیل ریسک و مقررات نحوه استفاده قابل قبول از تجهیزات رایانه ای رعایت شده باشد.

– رویدادهای امنیتی رخ داده در هنگام آغاز به کار سیستم‌های عامل بایستی به عنوان حادثه امنیتی ثبت و گزارش شود.

– مجوز استفاده از ابزار دفتری تولید محتوای الکترونیکی [1] و تعیین نوع آنها مثل اجزای نرم افزار Microsoft Office از قبیل واژه پرداز [2]، صفحه گسترده [3]، بانک اطلاعاتی، تولید نمودار یا فایل های گرافیگی، ارسال و دریافت پیام الکترونیک متنی یا چند رسانه ای و جلسه مجازی، کارتابل الکترونیک، منشی الکترونیک و مشابه آنها که به صورت نرم افزارهای آماده خریداری می شوند، فقط باید پس از اثبات نیاز سازمان صادر شود.

– مسئولیت بهره برداری امن از این گونه نرم افزارها و حفظ امنیت داده ها، اطلاعات و محتوای تولید شده یا دریافت شده توسط آنها بر عهده متقاضی استفاده می باشد.

– در صورتی که ابزار فوق برای پردازش یا تبادل اطلاعات دارای طبقه بندی حفاظتی استفاده شوند لازم است ابزار نرم افزاری یا سخت افزاری لازم برای حفاظت یا رمزنگاری داده ها و اطلاعات تولید یا تبادل شده توسط آنها تامین شود.

– لازم است نسخه‌های الکترونیکی اطلاعات تولید شده در نرم‌افزارهای نشر رومیزی، قبل از توزیع، به نسخه‌های غیرقابل تغییر تبدیل شوند.

---

[1] - Electronic Content
[2] - Word Processor
[3] - Spreadsheet

- لازم است کلیه افرادی که محتوای تولید شده توسط نرم‌افزارهای دفتری (مثل مجموعه Microsoft Office یا سایر نرم‌افزارهای رومیزی تولید محتوا) را در اختیار دارند، طبق روش تهیه نسخه پشتیبان، از اطلاعات در اختیار خود نسخه پشتیبان تهیه کرده و با توجه به طبقه‌بندی حفاظتی داده‌ها از آنها نگهداری نمایند.

- لازم است در نرم‌افزارهای تولید محتوای چند رسانه‌ای، وب و گرافیکی، فرمت اطلاعات الکترونیکی به نحوی ایجاد شوند تا در صورت لزوم پس از دریافت توسط گیرنده، قابل تغییر نباشد.

- در مراکز حساس و حیاتی ضرورت دارد در راستای اصل انکار ناپذیری، هنگام تبادل رسمی اطلاعات از سامانه امضاء دیجیتال استفاده شود.

- ضرورت دارد نرم‌افزارهای تولید محتوای خریداری شده، قبل از نصب بر روی سیستم‌ها در محیط آزمایش کنترل شده، تست شود.

- لازم است سیستم های اطلاعاتی اختصاصی سازمان شامل فایل های داده، بانک های اطلاعاتی، پایگاه های دانش، نرم افزار های کاربردی مدیریت و بهره برداری از بانک های اطلاعاتی و پایگاه های دانش اختصاصی سازمان و فایل های پیکربندی، شناسایی شده و به عنوان بخش مستقلی از فهرست دارایی های اطلاعاتی فهرست بندی شوند.

- از آنجا که سیستم های اطلاعاتی سازمان (بخصوص فایل های داده، بانک های اطلاعاتی و پایگاه های دانش) دارای ماهیتی یکتا بوده و در صورت لطمه دیدن، تنش زیادی را متوجه سازمان خواهد نمود، لازم

است فرآیندهای انتخاب محیط‌های مدیریت بانک های اطلاعاتی، تهیه نسخه پشتیبان[1] و احیای سیستم[2] و طرح های تداوم و عملیات[3] با توجه به نیازهای عملیاتی آنها تدوین شود.

- افرادی که به کار با سیستم های اطلاعاتی اختصاصی سازمان (فایل های داده، بانک های اطلاعاتی، پایگاه های دانش، نرم افزارهای کاربردی مدیریت و بهره برداری از آنها و فایل های پیکربندی مربوط) می پردازند باید در دو سطح کار با سیستم اطلاعاتی و حفظ امنیت آن آموزش داده شوند.

- در صورتی که فایل های داده، بانک های اطلاعاتی و پایگاه های دانش اختصاصی سازمان حاوی اطلاعات طبقه بندی شده باشد لازم است به نحو مناسب رمزگذاری شوند، به نحوی که در صورت دستیابی افراد غیرمجاز به آنها دستیابی به محتوای آنها غیرممکن شود.

- کنترل دسترسی به داده ها، بانک های اطلاعاتی، پایگاه دانش، نرم افزارهای کاربردی و نرم افزارهای بنیادی مورد استفاده برای مدیریت اینگونه داده ها باید مطابق با سه سطح کنترل دسترسی عام، کنترل دسترسی خاص و کنترل دسترسی ممتاز تعریف شود.

- حتی الامکان لازم است محل نگهداری داده های سیستم های اطلاعاتی اختصاصی سازمان، جدا از محل نصب نرم افزارهای مدیریت و بهره برداری مربوطه باشد به نحوی که در صورت فروپاشی نظام کنترل دسترسی یکی از آنها، نتوان به دیگری دست یافت. به عنوان مثال لازم است نرم‌افزار AutoCAD جدا از محل نگهداری فایل های تولید شده توسط آن نصب شود.

---

[1] - Back Up
[2] - Disaster Recovery
[3] - Business Continuity Plan

- لازم است حتی الامکان (و در مراکز حساس و حیاتی الزاماً) هر سیستم اطلاعاتی روی یک سرویس دهنده جداگانه (با رعایت الزام قبلی) نصب شود. به عنوان مثال اگر در یک سازمان یک بانک اطلاعاتی از اطلاعات شخصی مشتریان و یک بانک از اطلاعات گردش حساب نگهداری می شود باید این اطلاعات روی دو ماشین جداگانه نصب شود تا در صورت فروپاشی نظام کنترل دسترسی یا تخریب یک ماشین، امنیت بقیه اطلاعات مورد تهدید واقع نشود.

- نصب نرم افزارهای بنیادی مدیریت داده ها و بانک های اطلاعاتی(مانند SQL، Oracle، DB2،...) روی ایستگاه کاربران عادی یا کاربرانی که نیازی به آن ندارند ممنوع است.

- تمام مراحل کار با فایل های داده، بانک های اطلاعاتی، پایگاه دانش، نرم افزارهای کاربردی، ابزار بنیادی و فایل های پیکربندی مربوط به آنها باید ثبت(Log برداری) و به نحو مناسب نگهداری شود. اطلاعات ثبت شده فوق باید در فواصل زمانی مناسب به منظور کشف موارد مشکوک بازبینی شوند.

- در مواقعی که نوع بهره برداری از اطلاعات مستلزم تجمیع آنها و یا بهره برداری از آنها از طریق یک سیستم نرم افزاری جامع خریداری شده (مانند ERP، نرم افزارهای Core Banking، نرم افزارهای نظام جامع اختصاصی مثل بیمه ای، ثبت احوال، قضایی، انتظامی،...)باشد لازم است:

الف- الزامات امنیتی مورد نظر سازمان که حداقل باید شامل نظام کنترل دسترسی، رمزنگاری و تبادل کلید، تهیه نسخه پشتیبان، احیای سیستم، طرح تداوم عملیات و آموزش پرسنل باشد، تحت عنوان پیوست امنیتی به صورت جداگانه در قرارداد درج شده و چگونگی پاسخ گویی به آنها معلوم شود.

ب- هنگام تحویل قرارداد و قبل از عملیاتی سازی آن باید بازبینی کد منبع[1] انجام و از عدم وجود راه‌های نفوذ مخفی[2] در آن اطمینان حاصل شود.

- کنترل دسترسی ممتاز به فایل های پیکربندی سیستم های اطلاعاتی اختصاصی سازمان در مراکز حساس باید از طریق استفاده از نشانه های سخت افزاری[3] و یا علائم بیومتری[4] و در مراکز حیاتی باید از طریق استفاده از این دو روش به علاوه تایید مقام بالاتر و یا حضور شخص همراه تقویت شود.

- در صورتی که فایل داده، بانک اطاعاتی یا پایگاه دانش اختصاصی سازمان حاوی اطلاعات کنترل دسترسی به سایر سیستم ها باشد لازم است از نگهداری آنها بر روی ماشین هایی که فاقد استانداردهای لازم برای HSM[5] هستند خودداری شود.

فرآیند:

گردآوری، تولید و تبادل داده ها و اطلاعات دلیل اصلی به کارگیری سخت افزار، نرم افزار و سیستم های اطلاعاتی است. همانطور که گفته شد حفظ امنیت اطلاعات ضروری و در بسیاری اوقات حیاتی است. از آنجا که این کار مستلزم انجام فعالیت های متعدد و رعایت نکات دقیق است لازم است برای اجرای آن از روش های هدفمند و فرآیندگرا استفاده شود. هرچند ممکن است داده ها و اطلاعات دارای ماهیت های جداگانه باشند (مثل داده های تشکیل دهنده یک فایل اجرایی، داده های تشکیل دهنده یک پایگاه دانش و

[1] - Source Code Review
[2] - Back Door
[3] - Hardware Token
[4] - Biometrics
[5] - Hardware Security Module

یا داده های تشکیل دهنده یک فایل اطلاعاتی یا پیکربندی)، روش های حفاظت از آنها مشابه یکدیگر می باشد که در قالب فرآیند زیر قابل خلاصه سازی می باشد:

- شناسایی ماهیت داده، اطلاعات و نتایج حاصل از بهره برداری از آنها
- شناسایی آسیب پذیری های ذاتی
- شناسایی عواملی که ممکن است از آسیب پذیری ها بهره برداری کرده و اطلاعات یا داده ها را تخریب کرده یا بهره برداری از آنها را با مشکل مواجه نمایند. این عوامل به عنوان تهدیدات دسته بندی می شوند.
- اولویت بندی تهدیدات
- انتخاب روشهایی برای حذف قطعی تهدیدات یا محدود سازی اثر تهدید در صورت عدم امکان حذف قطعی. این روش ها به عنوان روش های امن سازی یا مکانیزم های کنترلی شناخته می شوند.
- کنترل دائم اجرای روش های امن سازی و مکانیزم های کنترلی برای اطمینان از صحت ماهیت و اجرای آنها
- بهبود فرآیند بر اساس نتایج حاصل از کنترل دائم اجراء

توضیحات:

سیستم های عامل، بانک های اطلاعاتی و برنامه های کاربردی که دارای ماهیت داده ای می باشند را به دو روش عمده می توان مورد حفاظت قرار داد. این دو روش به ترتیب اولویت عبارتند از:

۱ -پشتیبان گیری

۲ -کنترل دسترسی

روش ها مختلفی برای پشتیبان گیری وجود دارد. صرف نظر از الگوهای تهیه و فناوری مورد استفاده برای پشتیبان گیری، قابلیت بازیابی نسخه پشتیبان، مهمترین قابلیتی است که باید مورد توجه قرارگیرد. به عبارت دیگر لازم است پس از پشتیبان گیری، صحت نسخه تهیه شده کنترل شود.

همچنین الگوهای مختلفی برای کنترل دسترسی وجود دارد. این الگوها را می توان از دیدگاه مفهومی و تکنیکی مورد تحلیل قرار داد. انتخاب الگوی مفهومی بر الگوی تکنیکی اولویت دارد. به عبارت دیگر ابتدا باید نیاز کنترل دسترسی از دیدگاه مفهومی مورد توجه قرار گرفته و سپس بر اساس نیاز های شناسایی شده اقدام به انتخاب الگوی تکنیکی شود.

الگوی سه سطحی کنترل دسترسی عام، کنترل دسترسی خاص و کنترل دسترسی ممتاز دیدگاه مفهومی کارایی است که به سادگی قابل پیاده سازی است. کنترل دسترسی عام مبین تعیین و کنترل شرایطی است که کلیه متقاضیان دسترسی باید رعایت کنند. کنترل دسترسی خاص مبین تعیین و کنترل شرایطی است که کلیه متقاضیان دسترسی به بخش خاصی از دارایی های اطلاعاتی باید رعایت کنند. این شرایط بسته به ماهیت و یا کاربرد دارایی اطلاعاتی تعیین می شوند. کنترل دسترسی ممتاز نیز مبین تعیین و کنترل شرایطی است که کلیه متقاضیان دسترسی به فایل های پیکربندی یا تجهیزات کنترل دسترسی یا داراییهای اطلاعاتی حساس یا حیاتی باید رعایت نمایند. با مشخص شدن نیاز های دسترسی هر یک از دارایی های اطلاعاتی، الگوی تکنیکی دسترسی دارایی مشخص شده و بر اساس آن، اجازه دسترسی صادر خواهد شد.