جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

الزامات امنیتی زیرساختهای حیاتی در استفاده از محصولات نرم افزاری سازمانی

نسخه ۱,۰

آبان ماه ۹۸

عادی


بسم الله الرحمن الرحيم

مقدمه

امروزه بکارگیری تکنولوژی، ابزارها و سامانه‌های فناوری اطلاعات در سازمان‌ها با رشد روزافزونی روبه‌رو است. استفاده از این ابزارها و سامانه‌ها در سازمان‌ها به شرط رعایت ملاحظات امنیتی می‌تواند بسیار اثربخش باشد، اما در صورتی که این محصولات دارای ضعف و آسیب‌پذیری امنیتی باشند، به جای اثرگذاری در سازمان‌ها می‌توانند یک تهدید جدی محسوب شده و خسارات جبران‌ناپذیری را به بار آورند. در این مواقع علاوه بر ارائه‌کننده‌ی این گونه محصولات، سازمان بهره بردار نیز در قبال این خسارات مسئول و پاسخگو خواهد بود. هدف از ارائه این سند، تبیین الزامات سازمان‌ها و زیرساخت‌های حیاتی در بهره‌برداری از محصولات نرم‌افزاری سازمانی است و رعایت این الزامات توسط سازمان ضروری است.

۱– قلمرو سند

قلمرو این سند الزامات امنیتی سازمان بهره بردار از محصولات نرم‌افزاری سازمانی در کلیه مراحل انتخاب محصول، عقد قرارداد، نصب، استقرار و پشتیبانی محصول تا پایان قرارداد است. سیستم‌های اتوماسیون اداری، حقوق و دستمزد، اداری مالی، حضور و غیاب، سیستم‌های مدیریت محتوا و یا پورتال‌های سازمانی، از جمله این محصولات نرم‌افزاری سازمانی می‌باشند.

۲–اصطلاحات

سازمان‌ها: تمامی دستگاه‌های اجرایی مشمول ماده ۵ قانون مدیریت خدمات کشوری

ارائه‌کننده محصول: شخصیت حقوقی که محصول را به سازمان ارائه می‌دهد و می‌تواند همان تولیدکننده محصول و یا ارائه‌کننده خدمات نصب و پشتیبانی نیز باشد.

محصول: محصولات نرم‌افزاری سازمانی

محصول داخلی: محصولی است که تولید کننده آن یک شرکت ایرانی است.

۳– الزامات انتخاب محصول

۳-۱ سازمان باید محصولات داخلی را برای بهره برداری انتخاب و خریداری کند مگر در حالتی که ثابت کند محصولات داخلی پاسخگوی نیاز آن سازمان نیست که این امر باید به تایید مرکز افتا

برسد.

۳-۲ سازمان باید محصولات داخلی را انتخاب کند که گواهی ارزیابی امنیتی را از مرکز مدیریت راهبردی افتا مطابق با فرآیند اخذ گواهی ارزیابی امنیتی محصولات دریافت کرده باشد.

تبصره الف. در صورتی که خود سازمان اقدام به تولید نرم‌افزار سفارشی کند و یا به هر نحوی صاحب امتیاز محصول مورد نظر باشد، موظف است برای بهره‌برداری از آن اقدام به اخذ تاییدیه امنیتی از مرکز مدیریت راهبردی افتا[۱] نماید.

۳-۳ سازمان برای انتخاب شرکت ارائه‌دهنده خدمات نصب و پشتیبانی محصول - که ممکن است لزوما تولیدکننده آن نباشد - باید آن دسته از شرکت‌ها را انتخاب کند که پروانه ارائه خدمات نصب و پشتیبانی محصولات نرم افزاری را مطابق با فرآیند اخذ پروانه خدمات دریافت کرده باشند.

۳-۴ سازمان باید محصولی را انتخاب کند که حداقل وابستگی به سکوها و ابزارهای خارجی داشته و در صورت نیاز به استفاده از محصولی دارای ابزارها و اجزای غیر بومی، حتما باید اطمینان حاصل کند که محصول، لایسنس‌های معتبر را دارا است و راهکارهای مناسب را برای تضمین تداوم عملکرد محصول را از ارائه کننده دریافت نماید و نیز آگاهی لازم از وابستگی عملکرد محصول خود به آن‌ها، مخاطرات استفاده از این اجزاء را کسب نماید و و نهایتا راهکارهای اجرایی برای مقابله با این مخاطرات را پیاده سازی نماید.

۴- الزامات زمان عقد قرارداد

۴-۱ مسئولیت تامین هر یک از بخش‌ها، اجزا یا مولفه‌های مستقل نرم‌افزاری محصول، باید در زمان قرارداد تعیین شود و به طور دقیق در قرارداد ذکر گردد. این بخش‌ها می‌تواند شامل سیستم عامل، وب سرور، پایگاه داده و برنامه‌های کاربردی شخص ثالث (مانند فریم ورک‌ها و کتابخانه‌ها)

[۱] http://afta.gov.ir/

باشد.

- ✓ در صورتی که سازمان وظیفه تامین و یا نگهداری هر یک از بخش‌های مستقل نرم‌افزاری را که محصول بر روی آن اجرا می‌شود بر عهده دارد، باید مسئولیت تامین امنیت آن‌ها را بپذیرد و فرآیندهای لازم برای این کار از جمله به‌روزرسانی اجزا، وصله کردن آسیب‌پذیری‌ها، مقاوم‌سازی و پشتیبان‌گیری را انجام دهد.
- ✓ در صورتی که ارائه دهنده محصول وظیفه تامین و یا نگهداری هر یک از بخش‌های مستقل نرم‌افزاری را بپذیرد، سازمان فرآیندهای نظارت و ممیزی امنیت آنها را تدوین و اجرایی نماید.

۴-۲ در محصولاتی که در بستر اینترنت و محلی خارج از مالکیت سازمان جایگذاری می‌شوند، لازم است وظیفه تامین زیرساخت میزبانی و نحوه رعایت دستورالعمل میزبانی امن[۲] خدمات وب در قرارداد به درستی تعیین شود. برخی از ملاحظات امنیتی در این دستورالعمل عبارتند از: ذخیره‌سازی امن داده‌های حساس، اطمینان از گرفتن نسخه پشتیبان دوره‌ای، بروزرسانی و نصب آخرین وصله‌های امنیتی وب‌سرورها

۴-۳ حداقل پارامترهای در دسترس بودن محصول و حداکثر زمان رفع آسیب‌پذیری‌های کشف شده محصول و زمان پاسخگویی و بازیابی در حوادث امنیتی ، متناسب با شدت آن‌ها، در تفاهم‌نامه سطح خدمات[۳] قرارداد تعیین و ذکر گردند.

۴-۴ در زمان قرارداد، کانال مناسب و امنی برای ارتباط سازمان با ارائه‌کننده توافق شود و در قرارداد ذکر گردد. اطلاع‌رسانی و آگاهی‌رسانی به سازمان در خصوص روال کشف و رفع آسیب‌پذیری‌ها از طریق این کانال صورت می‌گیرد.

- ✓ در صورتی که سازمان متوجه وجود آسیب‌پذیری در محصول شود می‌تواند در سریع‌ترین زمان ممکن از طریق این کانال به شرکت اطلاع‌رسانی دقیق نماید.

---

[۲] - این دستورالعمل توسط مرکز افتا منتشر می‌گردد.

[۳] Service-Level Agreement (SLA)

✓ در صورت تغییر اطلاعات سازمان، باید ارائه‌کننده را از این امر مطلع کند تا کانال ارتباطی با آن‌ها برقرار بماند.

۴-۵ سطوح دسترسی مختلف، حقوق دسترسی و چگونگی دسترسی (در محل/دسترسی از راه دور) هر سطح به محصول در مراحل نصب و راهبری توسط ارائه‌کننده و سازمان توافق شود و به طور دقیق در قرارداد ذکر گردد. سطوح دسترسی می‌تواند شامل دسترسی مدیر راهبر محصول، مدیر سیستم عامل و مدیر محصول و حقوق دسترسی حداقل می‌بایست شامل اضافه کردن کاربران، مشاهده داده‌های محرمانه، دسترسی به لاگ‌های ممیزی محصول و تغییر در پیکربندی باشد.

۴-۶ مسئولیت و نحوه پشتیبان‌گیری در سه سطح داده، سطح برنامه کاربردی و سطح سیستم باید توسط سازمان و ارائه‌کننده توافق شود و به طور دقیق در قرارداد ذکر گردد.

۴-۷ سازمان باید آموزش‌های لازم برای بهره‌برداری از تمام قابلیت‌های محصول خریداری شده را در قرارداد خود با ارائه‌کننده محصول قید نماید و کارشناسان بهره‌بردار محصول در سازمان آموزشهای لازم برای استفاده از سامانه را فرا گیرند.

۵- الزامات زمان نصب و استقرار محصول

۵-۱ سازمان باید در زمان نصب محصول اطمینان حاصل کند که نام‌های کاربری و کلمات عبور پیش‌فرض تمامی سرویس‌های مرتبط با محصول از جمله پایگاه داده تغییر کند و نحوه تغییر مجدد آن‌ها را نیز از ارائه‌کننده مطالبه کند و نسبت به تغییر آنها قبل از عملیاتی نمودن سامانه اقدام نماید.

۵-۲ سازمان باید سیاست‌های مربوط به رمز عبور خود را به ارائه‌کننده اعلام کرده و اطمینان حاصل کند که حداقل الزامات امنیتی مربوط به رمزهای عبور محصول (مانند رعایت طول مناسب، پیچیدگی کافی و ذخیره‌سازی به صورت درهم‌سازی شده) رعایت گردد.

۵-۳ سازمان باید هنگام استقرار محصول، محیط عملیاتی و محیط تست مجزایی را در اختیار ارائه‌کننده قرار دهد.

۵-۴ سازمان باید اطمینان حاصل کند که در هنگام نصب محصول، در تمامی اجزای مستقل بکار رفته

در محصول مانند وب‌سرورها و پایگاه داده‌ها از آخرین نسخه‌های پایدار و منطبق با محصول استفاده شده باشد و آخرین وصله‌های امنیتی منتشر شده برای آن‌ها توسط ارائه‌کننده نصب گردد.

۵-۵ سازمان باید پس از نصب محصول، مستندات مورد نیاز از جمله معماری استقرار محصول (نحوه قرار گرفتن محصول در محیط عملیاتی) و اطلاعات دیگر شامل پلتفرم‌ها، تکنولوژی‌ها و وابستگی‌های محصول به نرم‌افزارها، کتابخانه‌های شخص ثالث مورد استفاده در محصول، سرویس‌های اجرایی، پورت‌ها و دسترسی فایل‌ها به هر پورت را جهت راهبری محصول از ارائه‌کننده دریافت کند. پس از آن طبق اطلاعات دریافتی باید تنظیمات لازم برای محدودسازی سرویس‌ها و پورت‌ها انجام شود.

۵-۶ در محصولات تحت وب برای جلوگیری از افشای اطلاعات حساس ، سازمان باید اطمینان حاصل نماید که نمایش جزئیات خطاهای برنامه و اطلاعات نسخه که ممکن است به صورت پیش‌فرض در صفحات وب (مانند header ، banner،footer) موجود باشد، غیرفعال و یا حذف شوند.

۵-۷ سازمان باید پس از استقرار محصول و قبل از عملیاتی نمودن آن نسبت به مقاوم سازی آن اقدام نماید و نیز اطمینان حاصل نماید که پلاگین‌ها و قابلیت‌های کارکردی محصول و زیرساخت‌های مرتبط به آن را که خارج از نیاز سازمان است غیرفعال باشند.

۵-۸ پس از نصب و راه‌اندازی محصول، سازمان باید آموزش‌های لازم برای بهره‌برداری از تمام قابلیت‌های محصول خریداری شده را از ارائه کننده محصول مطالبه نماید.

۵-۹ پس از نصب و راه‌اندازی محصول باید صورتجلسه تحویل محصول با ذکر تمامی قابلیت‌های ارائه شده، مسئولیت‌های طرفین در قبال آن‌ها تنظیم شده و به تایید طرفین برسد.

۶- الزامات پشتیبانی

۶-۱ سازمان باید آسیب‌پذیری‌های کشف شده در محصول و اجزای مستقل آن را از طریق کانال ارتباطی مشخص شده در قرارداد از ارائه‌کننده دریافت کرده و حداکثر ظرف ۷۲ ساعت راهکارهای کوتاه مدتی را برای پیشگیری از بروز خرابی یا حملات احتمالی ناشی از آسیب‌پذیری کشف شده

از ارائه کننده دریافت و اعمال کند. در ادامه لازم است وصله‌های امنیتی منتشر شده توسط ارائه‌کننده را نیز نصب و اعمال کند. علاوه بر این باید خود اقدام به رصد آسیب‌پذیری‌های اجزای مستقل نرم‌افزاری محصول کرده و از نصب وصله‌های امنیتی منتشر شده‌ی آن‌ها اطمینان حاصل کند.

۶-۲ سازمان باید فرآیند مجوزدهی پرسنل سازمان برای دسترسی‌های مدیریتی و راهبری (شامل دسترسی مستقیم به پایگاه داده و محتوی، دسترسی تغییر مجوز کاربران) این سامانه‌ها را به درستی تعیین کند و دسترسی به پرسنل شرکت ارائه دهنده به این سامانه‌ها جهت خدمات پشتیبانی (بروزرسانی و یا عیب‌یابی) حتما با نظارت پرسنل دارای مجوز و دانش فنی مناسب صورت گیرد.

۶-۳ سازمان تا حد امکان، اتصال به این سامانه‌ها را برای پشتیبانی از راه دور فراهم نکند و در صورت نیاز ضروری، با حفظ ملاحظات امنیتی از جمله تایید نشست از راه دور توسط سازمان، تعیین زمان و تاریخ مشخص برای پشتیبانی از راه دور، رمزنگاری نشست‌های از راه دور، استفاده از احراز هویت قوی و دو عامله، ثبت تمامی فعالیت‌های پشتیبانی از راه دور و اطمینان از بسته شدن نشست‌ها پس از اتمام فرآیند پشتیبانی صورت گیرد و با استفاده از مکانیزم‌های مدیریت دسترسی این ارتباطات را مدیریت و پایش نماید.

۶-۴ سازمان باید هر سطح از پشتیبان‌گیری محصول را که طبق قرارداد به ایشان محول شده است به طور مرتب انجام دهد. ضمنا به منظور اطمینان از پشتیبان‌گیری صحیح، در مابقی سطوح پشتیبان‌گیری نیز بررسی به صورت دوره‌ای صورت گیرد و از قابل بازیابی بودن آنها اطمینان حاصل نماید.

۶-۵ سازمان باید در زمان ارائه بروزرسانی‌ها، وصله‌های امنیتی و تغییرات پیکربندی، ابتدا تغییرات را در محیط تست سازمان پیاده سازی نموده و پس از اطمینان از صحت عملکرد آن، در محیط عملیاتی سازمان اعمال نماید.

۶-۶ سازمان در محصولات پورتال‌های سازمانی و سیستم مدیریت محتوی، مکانیزم تشخیص حملات Deface را تا حد امکان و مکانیزم جلوگیری از تغییر در فایلها و پایگاه داده را از ارائه کننده

محصول دریافت نماید.

۷- الزامات پایان قرارداد

۷-۱ در هنگام اتمام قرارداد سازمان باید اطمینان حاصل کند تمامی دسترسی‌های ارائه‌کننده به محصول قطع شود.

۷-۲ سازمان برای ارائه خدمات پشتیبانی، رفع آسیب پذیری‌ها و بروزرسانی تمام سامانه های نرم‌افزاری سازمانی فعال خود، سازوکار مناسب از قبیل عقد قرارداد پشتیبانی با شرکت ارائه دهنده محصول را اجرایی نماید. مسئولیت مخاطرات ناشی از عدم پشتیبانی و بروزرسانی سامانه‌های مذکور بر عهده سازمان می باشد.