بسمه تعالی

توصیه‌نامه‌ی امن‌سازی سامانه‌های فناوری اطلاعات برای مقابله با تهدیدات احتمالی

مرکز ماهر

فهرست مطالب

مقدمه

به منظور افزایش سطح امنیت و پیشگیری حداکثری از حوادث سایبری در صورت افزایش سطح تهدیدات و مرتبط با فضای تحریم‌های کشورهای متخاصم علیه جمهوری اسلامی ایران، اقدامات پیشگیرانه این مستند جهت بررسی و بکارگیری در سطح سازمان‌ها و دستگاه‌ها ارائه می گردد. این پیشنهادات بصورت کلی تدوین شده و جزییات اجرا و بکارگیری آنها می‌تواند توسط کارشناسان تعیین گردد.

۱ به‌روزرسانی سیستم‌عامل و نرم‌افزارها

نرم‌افزارهایی مانند سیستم‌عامل، برنامه‌های کاربردی و کتابخانه‌های چارچوب نرم‌افزاری[۱]، با نقاط ضعف امنیتی شناخته‌شده به‌ویژه آن‌هایی که در بستر وب و یا دیگر اجزای در تماس با اینترنت نصب می‌شوند به مراتب بیشتر در معرض حملات سایبری هستند. لذا توصیه می‌گردد:

- یک فهرست به‌روز و جامع از تمامی نرم‌افزارها و نسخ آنها شامل سیستم‌عامل، برنامه‌ها و کتابخانه‌ها و همچنین firmware های تجهیزات داشته باشید.
- به اخبار امنیتی توجه کرده و اطلاعات مربوط به آن مانند به‌روزرسانی نرم‌افزار و هشدارهای امنیتی را با اشتراک در سامانه اطلاع‌رسانی تامین‌کننده نرم‌افزار به دست آورید.
- همه نرم‌افزارها و firmware های خود را بروز نگه‌دارید.
- اگر هیچ بروزرسانی برای حل مشکل آسیب‌پذیری یکی از نرم‌افزارها وجود ندارد، شما باید خطرات امنیتی را ارزیابی کرده و معیارهای امنیتی جایگزین همچون غیرفعال کردن عملکرد آسیب‌پذیر نرم‌افزار و یا استفاده از یک نرم‌افزار امن‌تر را اتخاذ کنید.
- اطمینان حاصل نمایید که همه سرورها و رایانه‌ها با دیواره‌آتش و نرم‌افزار ضد بدافزار محافظت می‌شوند.

[۱] Framework

۲ تهیه و نگهداری نسخ پشتیبان

به منظور پیشگیری از هرگونه آسیب جدی به دارایی‌ها و اطلاعات، لازم است نسخ پشتیبان از هر گونه اطلاعات ارزشمند بصورت مداوم تهیه و نگهداری گردند. در این خصوص لازم است به نکات زیر توجه گردد:

- نسخه‌های پشتیبان حتما بصورت غیربرخط[۲] نگهداری گردد
- بروزرسانی نسخ پشتیبان در فواصل زمانی مناسب (با در نظر گرفتن ماهیت و اهمیت اطلاعات) صورت گیرد.
- نسخه‌های پشتیبان مختلف از نظر زمانی تا چند دوره حفظ گردند
- پیش از تهیه پشتیان، از صحت و سلامت اطلاعات اطمینان حاصل گردد.
- در خصوص اطلاعات و دارایی‌های مهم تنها به یک نسخه فیزیکی پشتیبان اکتفا نگردد.

۳ بهره‌گیری از رمزنگاری مناسب درتبادل اطلاعات

عدم استفاده از رمزنگاری مناسب در تبادل اطلاعات امکان دسترسی مهاجمین به محتوای ارتباطات را فراهم می‌آورد. لازم است استفاده از کانال‌های رمزنگاری قوی در بسترهای ارتباطی بصورت جدی در دستورکار قرار گیرد. در این خصوص می‌توان به نکات زیر نیز اشاره کرد:

- هر بستری در خارج از شبکه سازمان یا دستگاه ذاتا ناامن محسوب می‌گردد. از جمله شبکه اینترانت کشور که به اشتباه از سوی بسیاری از مدیران شبکه امن درنظر گرفته می شود. لازم است در ارتباطات خارج از سازمان حتما از کانال‌های رمزنگاری مناسب استفاده گردد.
- بهره‌گیری از رمزگذاری اطلاعات و احراز اصالت صفحات وب با بهره‌گیری از مجوزهای HTTPS ضروری است. در این خصوص می توان به موارد امنیتی زیر اشاره نمود:
  - درخصوص بهره‌گیری از HTTPS در وب‌سایت‌ها، از نمایش هر دو محتوای امن (HTTPS) و ناامن (HTTP) در یک صفحه وب شامل اطلاعات حساس پرهیز کنید؛

[۲] offline

چراکه محتوای ناامن (به‌عنوان مثال اسکریپت) ممکن است بتواند به اطلاعات محتوای امن دسترسی پیدا کند.

- رمزنگاری و پروتکل‌های قوی، همچون TLS 1.2 و AES 256 bit باید در تنظیمات وب سرور اولویت بالاتری داشته باشد و الگوریتم های ضعیف و آسیب‌پذیر غیرفعال گردند. در این زمینه از ابزار آزمون SSL ارائه شده در درگاه مرکز ماهر(www.certcc.ir) که بصورت رایگان ارائه می شود استفاده نمایید.

۴ اتخاذ راه‌حل برای دسترسی ایمن از راه‌دور برای مدیریت سرویس‌ها و زیرساخت‌ها

اکیدا ضروری است که هرگونه دسترسی مدیریتی و یا دسترسی به به سامانه‌های داخلی شبکه از طریق بسترهای کنترل شده‌ی امن و با بهره‌گیری از رمزنگاری مناسب صورت پذیرد. دسترسی آزادانه بر بستر شبکه‌های عمومی اینترنت و اینترانت کشور نظیر سرویس‌های RDP ویندوز، SSH تجهیزات و سیستم‌های عامل، ILO در سرورهای HP، صفحات وب مدیریت تجهیزات و ... به هیچ عنوان امن نبوده و مجاز نمی‌باشد لازم است این دسترسی‌ها محدود به شبکه داخلی و یا ارتباطات امن بر بستر VPN مناسب گردد. علاوه بر این، نکات زیر نیز لازم است در نظر گرفته شود:

- از رمز عبور قوی استفاده کنید.
- در صورت امکان مکانیزم های احراز هویت قوی همچون احراز هویت براساس گواهی الکترونیکی و تأیید دومرحله‌ای، استفاده کنید.
- دسترسی کاربر را پس از تلاش‌های زیاد ناموفق در ورود به سیستم را به‌صورت خودکار قطع کنید.
- از پروتکل‌های رمزگذاری امن همچون HTTPS، SFTP و SSH v2 استفاده کنید.
- امکان اتصال از راه‌دور را تنها برای آدرس‌ّای مبدا خاص از اینترنت فراهم کنید.
- براساس اصل حداقل اختیارات، برای هر کاربر یک حساب کاربری منحصر به فرد با حداقل اختیارات ایجاد کنید.

۵ اتخاذ مکانیزم احراز هویت و رمز عبور قوی

لازم است در کلیه سامانه‌های نرم‌افزاری و سخت‌افزاری مکانیزم‌های احراز هویت قوی ومناسب بکار گرفته شود. از سوی دیگر لازم است الزامات سخت‌گیرانه‌ای در انتخاب و استفاده از رمزهای عبور پیچیده اعمال گردد:

- در صورت امکان مکانیزم‌های احراز هویت قوی همچون احراز هویت براساس گواهی الکترونیکی و تأیید دومرحله‌ای، استفاده کنید.
- دسترسی کاربر را پس از تلاش‌های زیاد ناموفق در ورود به سیستم را به‌صورت خودکار قطع کنید.
- سیاست رمزعبور سخت‌گیرانه‌ای را توسعه‌داده و اعمال کنید.

۶ جمع‌آوری، نگهداری و بررسی رخدادنماها

لازم است رویدادها و هشدارهای ایجاد شده در سطح همه‌ی سیستم‌ها را فعال‌کرده و آن‌ها را بصورت دائمی جهت شناسایی تهدیدات احتمالی مورد بررسی قرار دهید

- ✓ فرایندهای رصد و مدیریت حوادث امنیتی، شامل پروسه‌های متعادل‌سازی و مکانیزم‌های کارآمد به منظور گزارش، شناخت، اطلاع‌رسانی و مدیریت حوادث امنیتی را توسعه دهید.
- ✓ اطلاعات رویدادها با جزئیات کافی مانند زمان ورود و خروج، شناسه کاربر، مدت‌زمان فعالیت و جزئیات فعالیت از حساب کاربران و افراد دارای مجوز تهیه و نگهداری کنید.
- ✓ رویدادهای ثبت‌شده باید به‌طور منظم بازبینی شود تا حوادث مشکوک تشخیص داده شوند.
- ✓ دسترسی به رویدادها باید به افراد دارای مجوز محدود شود.

۷ جلوگیری از نشت اطلاعات سازمانی از طریق شبکه‌های اجتماعی

در صورت عدم رعایت نکات امنیتی توسط کارکنان، اطلاعات داخلی و حساس می‌تواند از طریق شبکه‌های اجتماعی و موتورهای جستجوی عمومی ذخیره شود. با سواستفاده از این امکان مهاجمین ممکن است با سهولت بیشتری به سیستم‌ها نفوذ نمایند. لازم است عموم کارمندان در این خصوص توجیح گردند.

۸ جلوگیری از نشت اطلاعات فنی وب سایت‌ها از طریق موتورهای جستجو

برخی از فایل‌های قرارگرفته و جامانده بر روی وب سرورها ممکن است حاوی اطلاعات حساس و قابل سواستفاده توسط مهاجمین از طریق موتورهای جستجو باشد. بمنظور شناسایی و حذف این اطلاعات ابزارهایی وجود دارد که کارکرد آن‌ها تشخیص فایل‌های بلااستفاده (فایل‌های اضافی باقی‌مانده پس از

حذف نرم‌افزار)، لینک‌های خراب و بررسی امکان نمایه‌گذاری و کش‌شدن وب‌سایت شما یا یک فایل از آن، توسط موتور جست‌وجوگر عمومی است. در زیر به چند مورد از این موارد اشاره می‌شود:

- Web Link Validator (Free Trial) (شناسایی فایل‌های بلااستفاده و لینک‌های خراب)
- Google Advanced Search (لیست کردن صفحات وب نمایه‌گذاری و کش شده)
- Yahoo Advanced Search (لیست کردن صفحات وب نمایه‌گذاری و کش شده)

۹ انجام اسکن آسیب‌پذیری‌های امنیتی (تست نفوذ)

وجود آسیب پذیری‌های شناخته شده و نقایص امنیتی ساده در سیستم‌ها و شبکه‌ها، به ویژه سیستم‌های متصل به شبکه عمومی، از مهمترین راه‌های نفوذ مهاجمین است. ارزیابی امنیتی در سطوح مختلف توسط کارشناسان مورد اعتماد نقش مهمی در پیشگیری از وقوع تهدیدات و حوادث سایبری دارد. در این‌خصوص می توان به موارد زیر اشاره نمود:

- لازم است ارزیابی‌های امنیتی بصورت دوره‌ای انجام پذیرد
- ارزیابی‌ها باید از مبادی مختلف (اینترنت، شبکه داخلی، دسترسی‌های راه دور و ..) و با سطوح دسترسی متفاوت در سیستم‌ها و سامانه‌ها صورت پذیرد

۱۰ اعمال سیاست‌های امن‌سازی (Hardening)

لازم است زیرساخت‌های نرم‌افزاری و سخت‌افزاری، شبکه، سیستم‌های عامل، و اپلیکیشن‌های سرویس دهنده بر اساس مستندات و راهنماهای معتبر مورد امن‌سازی قرار گیرند. چنین مستنداتی توسط مراکز امنیتی، شرکت های تولیدکننده محصولات و مرکز ماهر منتشر شده اند. این مستندات عموما تحت عنوان ((مستندات مرجع امن‌سازی)) و یا Security/configuration Best Practice شناخته می‌شوند. توصیه‌می گردد همه سیستم‌ها و سامانه‌ها با استناد به مستندات مشابه مورد بررسی و امن‌سازی دقیق قرار گیرند و این فرایند بصورت دوره‌ای تکرار گردد.