جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

الزامات امنیتی عملیاتی زیرساختهای حیاتی - پایه

عادی

فهرست مطالب

مقدمه

با توجه به حساسیت حوزه های پولی و مالی، ارتباطات و انرژی و تاثیرات گسترده و با سرعت بالای آن بر جامعه و با توجه به شرایط خاص کشور در برهه فعلی و رویکرد همیشگی دشمنان در خصوص انجام حملات سایبری بر علیه این زیرساخت ها، مرکز مدیریت راهبردی افتا در راستای افزایش میزان آمادگی دستگاههای مربوطه در این بخش‌ها در مقابل این حملات و افزایش پاسخ دهی موثرتر به این حوادث محتمل، اقدام به تهیه این مستند نموده است. متولیان امنیت فناوری اطلاعات سازمان موظف به رعایت دقیق و کامل این الزامات در شبکه های فناوری اطلاعات و صنعتی خود می‌باشند. همچنین لازم است گزارش وضعیت اجرای این الزامات در سازمان را به مرکز مدیریت راهبردی افتا ارسال نمایند.

در این سند الزامات امنیتی عملیاتی پایه، در دسته‌های ذیل آورده شده است.

۱. اقدامات پیشگیرانه
۲. اقدامات مقابله‌ای
۳. اقدامات مدیریتی و غیرفنی

۱- اقدامات پیشگیرانه

۱-۱- اشراف بر دارایی‌ها

۱. تهیه لیست بروز از سرویس‌های حیاتی سازمان و وابستگی‌های سخت‌افزاری و نرم‌افزاری مربوط به هر سرویس و اولویت‌بندی آن‌ها براساس ارزشیابی مخاطرات و تحلیل اثر بر کسب وکار سازمان
۲. تهیه لیست بروز از پروتکل‌ها و برنامه‌های کاربردی مجاز بر اساس سیاست های سازمانی
۳. تهیه لیست بروز از آدرس آی‌پی‌های معتبر سازمان بر بستر اینترنت و مشخص نمودن سرویس‌های فعال بر روی آن‌ها
۴. تهیه فهرستی از مشخصات و اطلاعات کامل متولیان تامین و نگهداری سرویس‌ها و سامانه‌های سازمان و تامین کنندگان امنیت آن‌ها
۵. تهیه فهرستی از اماکن استقرار سامانه‌ها، سرویس‌ها و تجهیزات حیاتی سازمان (اماکن حساس)
۶. تهیه مستندات کامل و بروز از معماری و توپولوژی منطقی و فیزیکی شبکه‌های ارتباطی سازمان
۷. تدوین پیوست امنیتی کامل و نقشه راه دستیابی به آن به منظور تأمین امنیت سایبری سرویس‌ها، تجهیزات و دارایی‌های سازمان

۱-۲- امن‌سازی

۱. اطمینان از وجود سازوکار اثر بخش و تمهیدات مناسب
   - ✓ مدیریت، کنترل و نظارت بر دسترسی فیزیکی به اماکن حساس شناسایی شده
   - ✓ مدیریت، کنترل و نظارت بر دسترسی کاربران به منابع و سرویس‌ها بر اساس اصل حداقل دسترسی (شامل ایجاد، فعال‌سازی و غیرفعال‌سازی، حذف و تغییرسطح دسترسی)
   - ✓ مدیریت، کنترل و نظارت بر دسترسی مشاوران، پیمانکاران و کارکنان موقت به شبکه و سیستم های اطلاعاتی
   - ✓ ناحیه‌بندی[1] شبکه‌ها و مدیریت ارتباطات، اعمال کنترل دسترسی بین ناحیه‌های مختلف و نظارت بر آن‌ها
   - ✓ مدیریت لاگ شامل جمع‌آوری، نگهداری، ذخیره‌سازی و اطمینان از صحت عملکرد آن‌ها (ذخیره‌سازی برای بازه زمانی حداقل یکساله در نظر گرفته شود).
   - ✓ جلوگیری از دسترسی غیرمجاز و دستکاری لاگ‌های ذخیره شده و نسخه‌های پشتیبان و نگهداری نسخه‌های پشتیبان سامانه‌ها و سرویس‌های حیاتی در محیط ایزوله
   - ✓ همگام‌سازی زمانی تمامی تجهیزات، سامانه‌ها و لاگ‌ها
   - ✓ مدیریت، کنترل و نظارت بر دسترسی‌های راه‌دور[2] و محدودسازی زمانی، مکانی آن‌ها و حتی‌المقدور محدود نمودن دسترسی‌های راه‌دور خارج از کشور

[1] Zoning
[2] Remote-Access

- ✓ احراز هویت چندعامله و قابلیت عدم‌انکار[3] در تمامی سرویس‌ها و سامانه‌های حیاتی به منظور تصدیق هویت کلیه کاربران
- ✓ پایش، کنترل و نظارت بر پروتکل ها و برنامه های کاربردی در حال استفاده در سازمان به منظور مطابقت آن‌ها با لیست مجاز تهیه شده
- ✓ استفاده از تجهیزات قابل حمل شامل رسانه‌های ذخیره‌ساز، تجهیزات سایبری سازمانی و شخصی
- ✓ استفاده از گذرواژه‌ها با پیچیدگی و تعداد کاراکترهای مناسب، تغییرات دوره‌ای اجباری و سازوکار نگهداری امن آن‌ها
- ✓ افزایش دسترس‌پذیری سرویس‌های حیاتی از طریق راهکارهای توزیع بار[4]، HA[5] و غیره

۲. عدم انتشار سرویس‌های غیرضروری بر بستر اینترنت
۳. غیرفعال کردن سامانه‌ها، سرویس‌ها و تجهیزات بلا استفاده و غیرضروری
۴. جداسازی شبکه متصل به اینترنت از شبکه ارایه سرویس‌های سازمانی بصورت فیزیکی و یا منطقی (در صورت امکان)
۵. جداسازی محیط‌های تست، توسعه و عملیاتی سامانه‌ها از یکدیگر
۶. جداسازی سرور پایگاه داده از سرور برنامه کاربردی، محدودسازی و کنترل دسترسی به آن
۷. مقاوم سازی سیستم‌های عامل، پایگاه‌داده، وب‌سرور، برنامه‌های کاربردی و سایر سرویس‌ها بر اساس اسناد مقاوم سازی منتشر شده توسط تولید کننده
۸. استفاده از دیواره‌های آتش و سامانه مدیریت تهدیدات یکپارچه دارای مجوز در لبه شبکه و سامانه DLP[6] (برای کنترل دسترسی، کنترل ترافیک ورودی و خروجی، جلوگیری از نفوذ و جلوگیری از نشت اطلاعات)
۹. اطمینان از نصب، فعال و به‌روز بودن نسخه تأیید شده سامانه‌های ضد بدافزار و ضدباج افزار روی سرویس‌ها و سامانه‌های حیاتی
۱۰. استفاده از پروتکل‌های امن و ابزارهای رمزنگاری برای حفظ محرمانگی و یکپارچگی داده‌ها و اطلاعات حساس در حین انتقال، پردازش و ذخیره سازی
۱۱. عدم دسترسی آدرس آی‌پی‌های خارجی به سرویس‌هایی که برای استفاده سرویس‌گیرندگان داخل کشور انتشار یافته‌اند.
۱۲. به‌روز رسانی و مدیریت وصله‌های تمامی سیستم عامل‌ها، سرویس‌ها و سامانه‌های حیاتی به صورت مستمر
۱۳. عدم استفاده از نرم‌افزارهای کرک شده در سرور سامانه‌های حیاتی
۱۴. اعمال محدودیت در استفاده از شبکه‌های بیسیم، امن‌سازی و مقاوم‌سازی آن‌ها
۱۵. اطمینان از تغییر تمامی تنظیمات و پیکربندی‌های پیش‌فرض، در نرم‌افزارها و تجهیزات
۱۶. اطمینان از پیکربندی امن سامانه‌ها، تجهیزات، سرویس‌ها و پروتکل‌ها

[3] Non-repudiation
[4] Load balancer
[5] High Availability
[6] Data Leakage Prevention

۱۷. میزبانی تمامی سرویس‌ها و سامانه‌های حیاتی در داخل کشور
۱۸. داشتن SLA مناسب با فراهم کننده زیرساخت در زمینه دسترس‌پذیری و تامین امنیت سرویس
۱۹. اطمینان از به‌روز بودن مستندات مربوط به پیکربندی تجهیزات، سرویس‌ها و سامانه‌ها
۲۰. تدوین و به‌روز رسانی طرح‌های تداوم کسب و کار و بازیابی از فاجعه
۲۱. انجام مانور سایبری بصورت دوره‌ای برای اطمینان از اثربخشی و کارا بودن طرح‌های تداوم کسب و کار و بازیابی از فاجعه و همچنین عملکرد سایت‌های پشتیبان با امکان سوئیچ در کوتاهترین زمان ممکن

تبصره:

- برای عملیاتی نمودن موارد فوق الذکر اولویت با محصولات و خدمات بومی و داخلی بوده و برای استفاده از محصولات و خدمات خارجی مربوطه؛ در صورت احراز عدم وجود محصول و خدمت داخلی مشابه (جهت رفع نیازمندی دستگاه)، می‌بایست ضمن استعلام از مراجع ذیصلاح، فرآیند انجام پشتیبانی توسط شرکتهای داخلی دارای گواهی مرکز افتا، صورت پذیرد.

۲- اقدامات مقابله‌ای

۲-۱- الزامات تشخیص و مقابله با رخداد

۱. اطمینان از پایش رویدادهای امنیتی دارایی‌ها حداقل شامل سرویس‌ها و سامانه‌های حیاتی
۲. پایش مستمر رویدادهای امنیتی، تشخیص حوادث و تعیین سطح آن، اعلام هشدار و مدیریت حوادث سایبری
۳. مدیریت آسیب‌پذیری‌های شامل پویش و رفع آسیب‌پذیری‌های سرویس‌ها و سامانه‌های حیاتی به صورت مستمر
۴. ثبت و بهره‌برداری از درس‌های آموخته شده حوادث به‌منظور جلوگیری از تکرار حوادث مشابه
۵. وجود وبگاه پشتیبان از وبگاه رسمی دستگاه با حداقل دسترسی و امکان تغییر لحظه‌ای در مواقع بحرانی
۶. اطمینان از وجود سازوکار مستمر پشتیبان‌گیری از تمامی سامانه‌های درگیر در ارایه سرویس‌های حیاتی، داده‌های عملیاتی و حساس به‌همراه آخرین تراکنش‌ها، آخرین نسخه پیکربندی تجهیزات و سامانه‌ها، همچنین صحت نسخه‌های پشتیبان و امکان بازیابی صحیح آن‌ها
۷. اطمینان از وجود تمامی سامانه‌های حیاتی در سایت پشتیبان با عملکرد صحیح، آخرین پیکربندی‌های و داده‌های اطلاعاتی

۳- الزامات مدیریتی و فرآیندی

۱. استفاده از شرکت‌های مشاور امنیتی دارای مجوز و گواهی خدمت امن‌سازی و مقاوم‌سازی زیرساخت‌ها از مرکز مدیریت راهبردی افتا و نظارت بر کیفیت خدمات
۲. استفاده از محصولات و سامانه‌های دارای گواهی ارزیابی امنیتی مورد تایید مرکز افتا
۳. ضرورت هماهنگی قبلی با مرکز افتا و اطلاع‌رسانی به مشتریان در صورت نیاز به هرگونه قطعی سرویس‌های حیاتی
۴. عدم استفاده از افراد دو تابعیتی در امورات مرتبط با امنیت و مشاغل حساس و ارسال اسامی و سمت افراد دو تابعیتی در جایگاه مدیریتی و کارشناسی به حراست سازمان
۵. در نظر گرفتن تمهیدات لازم در خصوص مدیریت صحیح منابع انسانی به‌منظور جلوگیری از نارضایتی نیروهای موثر
۶. حتی المقدور ممنوعیت مرخصی‌ها در بازه بحران و یا مرخصی با برنامه‌ریزی متناسب با شرایط
۷. وجود فرایندهای تعاملی بین واحدهای امداد سایبری با متولیان سرویس‌ها و سامانه‌ها
۸. ایجاد تیم مدیریت بحران، تعیین نقش‌ها و مسئولیت‌ها و شرح وظایف مشخص و مکتوب
۹. به اشتراک گذاری اطلاعات حوادث سایبری با مرکز افتا
۱۰. آموزش افراد کلیدی و اعضای تیم مدیریت بحران به منظور مقابله و برخورد مناسب با حوادث سایبری
۱۱. معرفی نماینده تیم مدیریت بحران به‌عنوان مدیر پاسخگویی به رخداد سایبری به‌منظور تعامل و اطلاع‌رسانی حوادث سایبری به مرکز افتا
۱۲. تدوین و اجرای برنامه های فرهنگ سازی و آگاه سازی کلیه کارکنان در حوزه امنیت سایبری
۱۳. آموزش و آگاهی رسانی پرسنل در حوزه سیاست‌های امنیتی سازمان و مقابله با مهندسی اجتماعی