مرکز مدیریت راهبردی افتا

الزامات اتصال امن کاربران جهت استفاده از شبکه، سرویس‌ها و سامانه‌های داخلی سازمان(دورکاری در شرایط خاص)

اسفند ۱۴۰۴

نسخه۱.۱

فهرست

مقدمه

هدف این سند، تعیین الزامات فنی و امنیتی برای برقراری ارتباط از راه دور با شبکه و سامانه‌های داخلی سازمان در شرایط خاص است. رعایت این موارد توسط تمامی کاربران (اعم از کارمند، راهبر، پیمانکار) الزامی بوده و عدم امکان اجرای هر یک از بندها باید به بالاترین مقام سازمانی اطلاع‌رسانی شود.

تأییدیه کمیته امنیت دستگاه

تمامی دسترسی‌های از راه دور به سامانه‌ها، سرورها و منابع داخلی سازمان، صرفاً بر اساس **مصوبه کتبی کمیته امنیت دستگاه** قابل برقراری است. این مصوبه باید به‌صورت مشخص موارد زیر را تعیین نماید:

- **فهرست دقیق سامانه‌ها و سرورهایی** که اجازه دسترسی از راه دور به آنها وجود دارد،
- **نوع دسترسی مجاز** برای هر یک (نظیر مطالعه، ویرایش، مدیریت)،
- **شرایط زمانی و مکانی** دسترسی
- **مسئول تأییدکننده نهایی** در کمیته.

هرگونه تغییر در این فهرست یا اضافه‌شدن سامانه جدید، منوط به تأیید مجدد کمیته بوده و می‌بایست در صورتجلسه مکتوب یا سامانه مصوبات مستند گردد.

۱ .معماری و استقرار سرویس دسترسی از راه دور

۱.۱ .ناحیه مورد اتصال در شبکه

- سرویس دسترسی از راه دور VPN یا Gateway باید در ناحیه **DMZ** شبکه مستقر شود.
- این ناحیه باید **از لحاظ فیزیکی یا حداقل منطقی** از شبکه داخلی، سرور فارم و سایر نواحی دارای زیرساخت جدا باشد تا ترافیک ورودی پیش از ورود به شبکه داخلی کنترل گردد.

۱.۲ .امن سازی پیکربندی

- راهکار انتخابی **نباید با تنظیمات پیش‌فرض** راه‌اندازی شود. پیکربندی نهایی باید مبتنی بر:

- توصیه‌های مقاوم‌سازی شرکت سازنده
- استانداردهای بین‌المللی امنیتی مانند CIS Benchmarks و الزامات ابلاغی مرکز افتا صورت گیرد.

۱.۳ .به‌روزرسانی و مدیریت وصله (در صورت امکان)

- سرویس دسترسی از راه دور باید **پس از انتشار وصله‌های امنیتی**، به‌روزرسانی شود.
- وصله‌ها تنها از **مرجع اصلی** دریافت و پس از تهیه نسخه پشتیبان و **تست در محیط غیرعملیاتی** (در صورت امکان) اعمال گردند.

۱.۴ .پشتیبان‌گیری و تداوم سرویس

- پس از نهایی‌سازی تنظیمات، **نسخه پشتیبان کامل** از پیکربندی تهیه و به صورت امن در مکانی در دسترس نگهداری شود.
- بسته به بحرانی بودن سرویس، **برنامه تداوم کسب‌وکار (BCP)** برای آن تدوین و تمهیدات لازم جهت حفظ سرویس در شرایط بحران پیش‌بینی گردد.

۱.۵ .همگام‌سازی زمان

- زمان سرویس باید به‌طور **مستمر، دقیق و امن** با سرور زمان شبکه داخلی (NTP) همگام‌سازی شود. پایداری این همگام‌سازی با تمهیدات افزونگی تضمین گردد.

۲ .الزامات امنیتی دروازه دسترسی

۲.۱ .پروتکل و رمزنگاری

- برای اتصال از راه دور باید از پروتکل‌های استاندارد با **بالاترین سطح رمزنگاری** مانند **IPSec**، **WireGuard**یا راهکارهای امن مشابه (مبتنی بر استانداردهای بین‌المللی) استفاده شود.

۲.۲ .پایش ترافیک

- تمام ترافیک ورودی به دروازه دسترسی از راه دور باید به‌طور مستمر توسط **سیستم شناسایی و پیشگیری از نفوذ (IDS/IPS)** به صورت **Inline** پایش شود.

۲.۳ .محدودیت‌های دسترسی سطح شبکه

- ترافیک ورودی به دروازه فقط برای **آدرس‌های IP از پیش تعیین‌شده** (مانند محدوده شرکای تجاری یا کاربران ثابت) و فقط روی **پورت و پروتکل مشخص سرویس** مجاز باشد.

۲.۴ .مدیریت دسترسی‌های مدیریتی(PAM)

- هرگونه دسترسی مدیریتی به تجهیزات زیرساخت، سرویس‌ها و سامانه‌های داخلی (اعم از راهبران یا پیمانکاران با سطح دسترسی ادمین/روت) **باید فقط از طریق سرویس مدیریت دسترسی ممتاز (PAM)** انجام شود.
- **دسترسی مستقیم** از اینترنت به پروتکل‌هایی نظیر **SSH، RDP، VNC** و مانند آن **تحت هیچ شرایطی مجاز نیست.**

۳ .احراز هویت و کنترل دسترسی کاربران

۳.۱ .حساب‌های کاربری

- تمام حساب‌های کاربری استفاده‌کننده از سرویس دورکاری باید:
  - دارای **نام کاربری یکتا و مشخص** برای هر فرد باشند.
  - رمز عبور آنها **پیچیده، غیرقابل حدس و حداقل ۱۴ کاراکتر** باشد.
  - رمز عبور این سرویس با رمز سایر سرویس‌های داخلی یکسان نباشد.

۳.۲ .احراز هویت چندعاملی(MFA[1])

- برای تمام کاربران، **احراز هویت چندعاملی (MFA) الزامی** است. روش انتخابی باید از نوع **مقاوم در برابر فیشینگ** مانندFIDO[2] ، کلیدهای امنیتی سخت‌افزاری، یا گواهی‌های دیجیتال باشد.

۳.۳ .مجوزدهی بر اساسLDAP/Active Directory

- پس از اتصال، کاربران باید با استفاده از سرویس‌های احراز هویت مرکزی مانند **LDAP، (Active Directory)** مبتنی بر سیاست **AAA** احراز هویت شوند.

[1] Multi Factor Authentication

- سطح دسترسی هر کاربر بر اساس **پروفایل شغلی** و **اصل کمترین امتیاز** تعیین و اعمال گردد.

۳.۴ .مدیریت نشست

- نشست‌های فعال کاربران راه دور حداکثر پس از **۳ ساعت** ملزم به احراز هویت مجدد هستند.
- در صورت **عدم فعالیت به مدت ۲۰ دقیقه**، اتصال باید به‌طور خودکار قطع شود.

۴ .الزامات امنیتی دستگاه کاربر (کلاینت)

۴.۱ .سیستم‌عامل و به‌روزرسانی

- سیستم‌عامل دستگاه کاربر باید:
  - **در صورت امکان به‌روز** بوده و آخرین وصله‌های امنیتی (تنها از مرجع اصلی) روی آن نصب شده باشد.
  - مطابق استانداردهای امنیتی **مقاوم‌سازی** شده باشد.

۴.۲ .محافظت در برابر بدافزار و نفوذ

- بر روی دستگاه باید **ضد بدافزار سازمانی** با آخرین تعاریف و حداکثر تنظیمات امنیتی فعال باشد.
- وجود قابلیت **تشخیص نفوذ در سطح میزبان (HIDS/HIPS)** با پیکربندی به‌روز و سختگیرانه الزامی است.

۴.۳ .دیواره آتش میزبان

- **دیواره آتش (Host Firewall)** روی دستگاه فعال بوده و قوانین آن به‌صورت امن پیکربندی شود.

۴.۴ .شبکه و اتصال

- کاربران **نباید** از طریق **شبکه‌های عمومی** به سازمان متصل شوند و لازم است از APN اختصاصی در ارتباط استفاده شود.

۴.۵ .حساب کاربری محلی

- روی دستگاه باید یک **حساب کاربری محلی** با نام کاربری مشخص و رمز عبور پیچیده (حداقل ۱۴ کاراکتر) برای استفاده‌کننده ایجاد شده باشد.

۵ .لاگ‌برداری، پایش و واکنش به رویداد

۵.۱ .ثبت رویدادها

- سرویس دسترسی از راه دور باید **تمامی رویدادها** شامل موارد زیر را ثبت کند:
  - احراز هویت‌ها (موفق و ناموفق)
  - تلاش‌های دسترسی
  - تغییرات پیکربندی
  - آدرس IP و پورت مبدأ، پروتکل استفاده شده و سایر فراداده‌های نشست
- لاگ‌ها باید به‌صورت **امن** ذخیره شده و از دستکاری یا حذف غیرمجاز محافظت شوند.

۵.۲ .ارسال بهSIEM

- تمامی رویدادهای ذخیره‌شده باید به‌طور **خودکار و امن** به سامانه **مدیریت رویدادهای امنیتی (SIEM)** سازمان ارسال گردند.

۵.۳ .پایش و واکنش

- لاگ‌های ارسالی باید به‌صورت **لحظه‌ای** پایش شوند. در صورت تشخیص **رویداد مشکوک یا رخداد امنیتی**، اقدامات زیر در دستور کار قرار گیرد:
  - بررسی و تحلیل (شامل جرم‌یابی سایبری در صورت نیاز)
  - اعمال محدودیت‌های لازم برای کاهش ریسک (مانند قطع دسترسی یا مسدودسازی موقت)

۶ .مدیریت ریسک و اطلاع‌رسانی

- چنانچه به هر دلیل (کمبود نیروی انسانی، منابع، بودجه، دانش فنی، نبود لایسنس و ...) امکان اجرای **هر یک از بندهای این سند** وجود نداشته باشد **ریسک آن بند باید به بالاترین مقام سازمانی اطلاع رسانی و تصمیم گیری در خصوص آن به صورت مکتوب اخذ شود.**