دستورالعمل اجرایی

الزامات امن سازی زیرساخت شبکه

از سری اسناد سازمان اورژانس کشور

اداره فناوری اطلاعات و ارتباطات

دی ماه ۱۴۰۲

نسخه ۱.۱

در عصر حاضر تمامی سازمان ها و شرکت ها اهمیت فناوری اطلاعات را درک کرده و آن را قسمتی از بدنه سازمان خود قبول کرده اند امروزه تمامی سازمان‌های سرویس‌دهنده و سرویس‌گیرنده از انواع خدمات و نرم افزارهای تحت شبکه استفاده کرده و خدماتی نظیر خدمات درمانی و ثبت نام های آنلاین ، خدمات آموزشی و ... در این بستر به راحتی قابل ارائه است. سازمان ها واداره ها برحسب نوع سرویس ها و خدمات قابل ارائه خود ،تعدادپرسنل وافراد مراجعه کننده و بزرگی مجموعه از تجهیزات شبکه ای مختلفی از قبیل سرورها و سوئیچ ها و روترها و ... استفاده می نمایند که ایجاد دسترسی های امن به تجهیزات شبکه ای از عوامل مهم و تاثیرگذار در پیشبرد اهداف امنیتی یک سازمان می باشند . به همین جهت برای حفظ امنیت اطلاعات سازمان و جلوگیری از ورود و نفوذ افراد سودجو و ... دستورالعمل یکپارچه توسط اداره فاوا سازمان اورژانس کشور به شرح ذیل تهیه و تنظیم شده است تا مورد بهره‌برداری مراکز فوریت‌های پیش‌بیمارستانی قرار گیرد.

❖ امنیت کاربر نهایی

۱. مدیریت و ممانعت از اتصال حافظه های قابل حمل
۲. تهیه آنتی ویروس لایسنس شده برای سرورها و کلاینت ها و نظارت بر به روزرسانی خودکار آن
۳. توجیه و آگاه سازی پرسنل و افزایش هوشیاری در خصوص گزارش هرگونه مورد مشکوک

❖ پایداری سرویس

۴. تامین افزونگی (Redundancy) در ارتباطات و منابع به تناسب اهمیت و ضرورت سرویسها
۵. پشتیبان گیری امن و بلادرنگ و دوره ای از داده ها و بانک های اطلاعاتی و نگهداری آن در ناحیه امن
۶. ایجاد سرویسهای متقارن برای خدمات ضروری و برای استفاده در زمان بحران

❖ مدیریت دسترسی

۱. احراز هویت دستگاه های منحصر به فرد متصل به شبکه
۲. کنترل دسترسی های مدیریتی به منابع اطلاعات و خدمات شبکه
۳. اعمال کنترل دسترسی برروی فایروال و روتر بصورتی که از دسترسی به سرویس ها و پورت های غیرمجاز جلوگیری نماید

۴. محدودسازی مراجعات و دسترسی های پیمانکاران و افزایش کنترل و نظارت بر اقدامات آنها
۵. محدودسازی دسترسی به خدمات پرکاربرد که نیازمند ارتباطات بین المللی نمی باشند از داخل کشور
۶. بازبینی مجدد دسترسی کاربران به سرویس های لایه کاربرد و حذف دسترسی‌های غیرضروری
۷. اعمال سیاست های امنیتی برای محدودسازی فعالیت کلاینت ها در ساعات مجازی اداری
۸. تغییر متناوب و دوره ای رمز عبور کلیه حساب های کاربری دارای سطح دسترسی بالا در سامانه ها و تجهیزات شبکه با رعایت پیچیدگی و ملاحضات امنیتی
۹. عدم استفاده از حساب کاربری مشترک بین کارشناسان و غیرفعال سازی حساب کاربری بلااستفاده
۱۰. محدود سازی پورت های حساس در زمان های بلااستفاده (SSH , RDP , …)
- لازم به ذکر است پورت Telnet برروی همه تجهیزات و سرویس ها همیشه باید بسته باشد.

❖ مدیریت لاگ

۱. ذخیره سازی لاگ تمامی عناصر شبکه (حداقل یک سال)
۲. ثبت و رصد کامل ترافیک شبکه بوسیله سرویس مانیتورینگ

❖ معماری امن

۱. تفکیک شبکه با درنظر گرفتن جداسازی دسترسی به سرورها کلاینت ها و تجهیزات زیرساختی
۲. عدم استفاده از شبکه های مبتنی بر Wirless در بستر شبکه داخلی و استفاده از مکانیزم های رمزنگاری و اصالت سنجی کلیه داده ای تبادلی در ارتباطات بی سیم
۳. جداسازی گروه های مختلف در لایه های دو ، سه و هفت (طبق استاندارد لایه هایOSI)
۴. ارائه سرویس اینترنت صرفاً در قالب یک سرویس در ناحیه Untrusted و به صورت جدا از سایر نواحی شبکه Trust
۵. اعمال قواعد جدید جهت ایجاد محدودیت برای دسترسی به Vlan های شبکه در سوئیچ ایجاد شده و محدودیت دسترسی به زیرشبکه ها در روتر
۶. فعال سازی Secure Boot در ماشین های مجازی

۷. محدود شدن دسترسی به شبکه Out Of Band[۱] فقط توسط مدیران شبکه و از طریق یک کلاینت محلی مستقل

❖ مستندات

۱. تهیه نقشه از اتصالات logical[۲] دستگاه های شبکه مشتمل بر :

- ✓ محل قرار گیری تجهیزات ارتباطی شبکه.
- ✓ مسیر کابل کشی.
- ✓ محل قرار گیری نودها در اتاق ها.
- ✓ شماره گذاری و Label گذاری بر روی نقاط ابتدایی و انتهایی کابل ها

۲. تهیه شناسنامه برای شبکه هریک از ساختمانها

- ✓ نام ساختمان، کاربری، درجه اهمیت و....
- ✓ لیست تجهیزات Passive وActive و پیکربندی های انجام گرفته.

پایان

[۱] Out Of Band : شبکه مستقل کاملا فیزیکی

[۲] Logical : منطقی