نکات امنیتی دسترسی به دیدگاه

با توجه به اینکه بروز اختلالات عملکردی و رخدادهای امنیتی می‌تواند کل فرایندهای سازمانی و سرویس‌های سامانه را متوقف یا دچار اختلال کند، نگهداری صحیح سرورها و کاهش ریسک‌های امنیتی از مسئولیت‌های حیاتی راهبران، کارشناسان امنیت و فناوری اطلاعات سازمان است.

در همین راستا، مجموعه اقدامات زیر باید به‌صورت دوره‌ای، مستند، قابل ردیابی و تحت نظارت ادمین/مدیر/راهبر مسئول سامانه بررسی و اجرا شوند.

امنیت مجموعه نرم‌افزاری دیدگاه صرفاً وابسته به خود نرم‌افزار نیست؛ بلکه حاصل مجموعه‌ای از **مسئولیت‌های مشترک میان تولیدکننده نرم‌افزار و سازمان بهره‌بردار** در حوزه‌های زیرساخت، شبکه، سیستم‌عامل، پایگاه داده، مدیریت دسترسی، پایش امنیتی و فرآیندهای عملیاتی است. رعایت توصیه‌های زیر می‌تواند نقش مؤثری در کاهش ریسک‌های امنیتی، افزایش پایداری سامانه و جلوگیری از سوءاستفاده‌های احتمالی داشته باشد:

۱ـ مدیریت دسترسی (Access Management)

- اصل حداقل دسترسی (Least Privilege) برای تمام کاربران، راهبران و سرویس‌ها رعایت شود.

- حتی‌الامکان از استفاده روزمره از حساب Administrator خودداری شود.
- عضویت کاربران در گروه‌های Local Administrators به صورت دوره‌ای بازبینی شود.
- حساب‌های بلااستفاده، قدیمی و اشتراکی شناسایی و غیرفعال شوند.
- دسترسی کاربران پس از تغییر سمت یا خروج از سازمان بازبینی و حذف شود.
- دسترسی Remote Administrator صرفاً برای افراد مجاز فعال باشد.

۲ـ امنیت سیستم عامل

- غیرفعال بودن سرویس‌های غیرضروری Windows
- غیرفعال بودن SMBv1
- فعال بودن Windows Defender یا EDR معتبر
- فعال بودن Microsoft Defender Exploit Protection
- فعال بودن BitLocker برای سرورهای فیزیکی در صورت امکان
- بررسی سلامت فایل‌های سیستمی
- حذف نرم‌افزارهای بلااستفاده از سرور
- به‌روزرسانی مداوم سیستم‌عامل و پایگاه داده

۳ـ امنیت شبکه

- قرارگیری سرور در VLAN مناسب

- محدود بودن دسترسی به پورت‌های مدیریتی
- عدم نیاز و دسترسی اینترنت به سرور
- عدم انتشار غیرضروری RDP
- استفاده از VPN امن برای دسترسی راهبران
- محدودسازی دسترسی بر اساس IP
- استفاده از IDS/IPS در مرز شبکه
- جداسازی شبکه کاربران از شبکه سرورها

۴- امنیت SQL Server

- غیرفعال بودن حساب‌های بلااستفاده
- حذف Loginهای غیرضروری
- محدود بودن دسترسی Sysadmin
- بازبینی دوره‌ای Permissionها
- فعال بودن SQL Audit
- بررسی دوره‌ای Loginهای ناموفق
- نصب آخرین Cumulative Updateهای SQL Server
- رمزنگاری ارتباطات (SQL Server (TLS

۵- امنیت IIS

- عدم اضافه نمودن سایت‌های متفرقه و حذف سایت‌های غیر از مورد استفاده دیدگاه
- حذف Virtual Directoryهای بلااستفاده
- غیرفعال بودن Directory Browsing
- استفاده از HTTPS
- استفاده از TLS 1.2 یا TLS 1.3
- غیرفعال بودن SSLهای قدیمی
- استفاده از گواهی معتبر
- بازبینی دوره‌ای Bindingها

۶- مدیریت آسیب‌پذیری‌ها

- انجام Vulnerability Assessment به‌صورت دوره‌ای
- بررسی CVEهای منتشرشده مرتبط با:
  - Windows
  - SQL Server
  - IIS
  - .NET
  - Redis

- رفع آسیب‌پذیری‌های بحرانی در کوتاه‌ترین زمان ممکن
- اولویت‌بندی Patchها بر اساس شدت ریسک

۷ـ امنیت Active Directory

اگر سرور عضو Domain است.

- بازبینی دوره‌ای گروه‌های Domain Admins
- استفاده از LAPS یا Windows LAPS
- محدودسازی دسترسی Domain Admin
- استفاده از حساب جداگانه برای مدیریت
- ثبت و بررسی Loginهای مدیریتی

۸ـ امنیت نسخه پشتیبان

- تست دوره‌ای بازیابی Backup
- نگهداری حداقل یک نسخه Offline
- نگهداری حداقل یک نسخه خارج از سایت
- محافظت Backup در برابر حذف یا رمزگذاری توسط باج‌افزار
- رمزنگاری فایل‌های Backup

۹ـ ثبت و پایش رخدادها

- فعال بودن Windows Audit Policy
- جمع‌آوری Security Log
- بررسی لاگ‌های:
  - SQL Server
  - IIS
  - Windows
  - Application
- ارسال Logها به SIEM
- تعریف Alert برای رخدادهای مهم

مانند:

- Login ناموفق متعدد
- ایجاد Administrator جدید
- حذف فایل‌های سیستمی
- توقف سرویس‌ها
- تغییر Policyها

۱۰ـ امنیت تجهیزات جانبی

- محدودسازی استفاده از USB
- کنترل اتصال هارد اکسترنال
- جلوگیری از اجرای AutoRun
- محدودسازی نصب نرم‌افزار

۱۱ـ امنیت Endpoint

- نصب EDR یا Antivirus معتبر
- به‌روزرسانی روزانه Signatureها
- فعال بودن Real-Time Protection
- جلوگیری از غیرفعال شدن Antivirus توسط کاربران

۱۲ـ امنیت و به‌روزرسانی مداوم مجموعه نرم‌افزاری دیدگاه

- بازبینی دوره‌ای کاربران Admin سامانه
- حذف کاربران بلااستفاده
- بازبینی سطح دسترسی نقش‌ها
- فعال بودن HTTPS

- بررسی گزارش‌های امنیتی مانند Loginهای موفق و ناموفق
- بررسی تغییرات کاربران دارای دسترسی بالا
- بازبینی دوره‌ای تنظیمات امنیتی سامانه

۱۳ـ آمادگی در برابر رخدادهای امنیتی

- تعریف فرآیند Incident Response
- مشخص بودن مسئول پاسخگویی
- ثبت رخدادهای امنیتی
- اطلاع‌رسانی سریع در صورت مشاهده آلودگی
- داشتن سناریوی بازیابی پس از باج‌افزار

۱۴- آموزش کاربران

- آموزش دوره‌ای کاربران
- آموزش شناسایی ایمیل‌های Phishing
- آموزش مهندسی اجتماعی
- آموزش استفاده ایمن از رمز عبور
- آموزش گزارش رخدادهای امنیتی