خدمات تخصصی هاردنینگ و امن‌سازی زیرساخت (Server Hardening)

در دنیای دیجیتال امروز، امنیت یک ویژگی جانبی یا یک انتخاب نیست؛ بلکه ضرورتی انکارناپذیر و بخشی جدایی‌ناپذیر از چرخه حیات سرویس‌هاست. هاردنینگ (Hardening) یا مقاوم‌سازی، فرآیندی است که شالوده‌ای قوی، استاندارد و ایمن را برای میزبانی و اجرای نرم‌افزارهای حیاتی سازمان شما فراهم می‌کند.

ما با تکیه بر استانداردهای جهانی نظیر **CIS (Center for Internet Security)** و **NIST**، لایه‌های امنیتی زیرساخت شما را در سه سطح حیاتی **سیستم‌عامل**، **پایگاه داده** و **وب‌سرور** تقویت می‌کنیم تا با خیالی آسوده بر رشد کسب‌وکارتان تمرکز کنید.

چرا هاردنینگ سرورها ضروری است؟

امن‌سازی پیش‌فرض‌ها (Default Configurations) بزرگ‌ترین نقطه‌ضعف هر سیستم است. خدمات هاردنینگ ما با هدف **کاهش سطح حمله (Attack Surface)** طراحی شده است تا:

1. **ریسک نفوذ و نشت اطلاعات** را به حداقل برساند.
2. **پایداری و Uptime** سرویس‌ها را افزایش دهد.

3. انطباق با قوانین امنیتی (**Compliance**) را تضمین کند.

۱. امن‌سازی سیستم‌عامل (Windows Server Hardening)

سیستم‌عامل ویندوز سرور به عنوان میزبان اصلی سرویس‌های شما، **اولین خط دفاعی** است. ما با اعمال **بیش از ۵۰ تنظیم امنیتی دقیق**، "دژ مستحکم" زیرساخت شما را بنا می‌کنیم.

اقدامات کلیدی:

مدیریت دسترسی و هویت (Identity & Access Management):

- پیاده‌سازی اصل **"کمترین سطح دسترسی"** (Least Privilege).
- غیرفعال‌سازی حساب‌های کاربری پیش‌فرض (مانند **Guest** و **Administrator** پیش‌فرض).
- اجرای سیاست‌های پیچیده رمز عبور و تنظیمات **Account Lockout** برای جلوگیری از حملات **Brute Force**.

پیکربندی سرویس‌ها و پروتکل‌ها:

- غیرفعال‌سازی سرویس‌های غیرضروری و بلااستفاده برای سبک‌سازی و ایمن‌سازی.

• غیرفعال‌سازی پروتکل‌های قدیمی و ناامن (مانند **SMBv1, NetBIOS**).

امنیت شبکه و فایروال:

• پیکربندی دقیق **Windows Firewall** با قوانین **Inbound/Outbound** سخت‌گیرانه.
• ایمن‌سازی دسترسی **RDP** (تغییر پورت پیش‌فرض، محدودسازی IP و الزام استفاده از **VPN**).

مدیریت آپدیت و Patch:

• برنامه منظم برای نصب وصله‌های امنیتی (**Security Patches**) بحرانی.

Audit & Logging:

• فعال‌سازی لاگ‌برداری پیشرفته برای ردیابی تغییرات سیستمی، تلاش‌های ورود ناموفق و دسترسی به فایل‌های حساس.

۲. امن‌سازی وب‌سرور (IIS Hardening)

وب‌سرور **IIS** دروازه ورود کاربران (و هکرها) به اپلیکیشن‌های شماست. تنظیمات پیش‌فرض IIS برای **"راحتی استفاده"** طراحی شده‌اند، نه **"امنیت حداکثری"**. ما این رویکرد را تغییر می‌دهیم تا تجربه کاربری در بستری کاملاً امن و مقاوم صورت پذیرد. هدف ما ایجاد تعادل دقیق بین دسترسی آسان کاربران و مسدودسازی مهاجمین است.

اقدامات کلیدی:

مدیریت هدرهای امنیتی (HTTP Security Headers):

- پیاده‌سازی هدرهای حیاتی مانند **X-XSS-Protection**، **X-Frame-Options**، **HSTS** و **Content-Security-Policy** برای مقابله با حملات **XSS** و **Clickjacking**.
- حذف هدرهای افشاگر اطلاعات سرور (مانند **X-Powered-By** و **Server Banner**).

پیکربندی SSL/TLS:

- غیرفعال‌سازی پروتکل‌های منسوخ (**SSL 2.0/3.0, TLS 1.0/1.1**) و فعال‌سازی **TLS 1.2** و **1.3**.
- استفاده از **Cipher Suite**های قدرتمند و امن.

فیلترینگ درخواست‌ها (Request Filtering):

- محدودسازی نوع فایل‌های قابل آپلود.
- نصب و کانفیگ ماژول **URL Rewrite** برای ایجاد قوانین امنیتی سفارشی.

ایزولاسیون Application Pool:

- اجرای هر وب‌سایت با **هویت (Identity)** اختصاصی و محدودشده.

• محدود کردن دسترسی‌های **Write** و **Execute** در دایرکتوری‌های وب.

۳. امن‌سازی پایگاه داده (SQL Server Hardening)

داده‌ها، ارزشمندترین دارایی سازمان شما هستند. **SQL Server** به عنوان مخزن این داده‌ها، نیازمند **بالاترین سطح حفاظت** است تا از سرقت یا دستکاری اطلاعات جلوگیری شود.

اقدامات کلیدی:

احراز هویت و سطوح دسترسی:

• الزام به استفاده از **Windows Authentication** در صورت امکان.
• غیرفعال‌سازی یا تغییر نام کاربری حساب **sa** و اجبار به استفاده از حساب‌های **Named User**.
• بررسی و حذف دسترسی‌های سطح بالا (**sysadmin**) از کاربران عادی.

امنیت ارتباطات و شبکه:

• تغییر پورت پیش‌فرض **۱۴۳۳** (برای جلوگیری از اسکن‌های خودکار).
• رمزنگاری ارتباطات دیتابیس (**Force Encryption**).
• مخفی کردن **Instance** دیتابیس از دید سرویس **SQL Browser**.

رمزنگاری داده‌ها (Encryption):

- پیاده‌سازی **TDE (Transparent Data Encryption)** برای رمزنگاری فایل‌های دیتابیس روی دیسک (**Data at Rest**).
- رمزنگاری ستون‌های حساس (مانند **کد ملی**، **شماره موبایل**) با **Always Encrypted**.

ممیزی و رصد (Auditing):

- فعال‌سازی **SQL Server Audit** برای ثبت تمامی لاگین‌ها (موفق و ناموفق) و کوئری‌های حساس.
- جلوگیری از اجرای رویه‌های ذخیره‌شده خطرناک (مانند **`xp_cmdshell`**).

فرآیند اجرایی ما

ما امنیت را **به صورت اتفاقی ایجاد نمی‌کنیم، بلکه آن را مهندسی می‌کنیم:**

1. **ارزیابی اولیه (Assessment):** اسکن وضعیت فعلی سرورها و شناسایی شکاف‌های امنیتی.
2. **تدوین طرح امن‌سازی:** ارائه **چک‌لیست اختصاصی** بر اساس معماری نرم‌افزار شما.
3. **اجرا و اعمال تنظیمات:** پیاده‌سازی تغییرات با **کمترین میزان اختلال (Downtime)**.
4. **مستندسازی:** ارائه گزارش کامل از تغییرات اعمال‌شده و **وضعیت امنیتی جدید**.