نمونه‌ای از یک چک‌لیست امنیتی ویندوز سرور

امنیت سازمانی

- ✓ برای هر سرور رکوردی از موجودی‌های آن داشته باشید. این رکورد، حداقل‌های پیکربندی را به‌شکل مستند مشخص و هر تغییر در سرور را ثبت می‌کند.
- ✓ پیش از اعمال هر تغییری در سخت‌افزار یا نرم‌افزار سرور، آن تغییر را کاملا بیازمایید و ارزشیابی کنید.
- ✓ مرتبا ریسک‌ها را برآورد کنید. برای به‌روزرسانی برنامه مدیریت ریسک، از نتایج این برآورد بهره ببرید. فهرستی اولویت‌بندی شده از همه سرورها داشته باشید تا اطمینان یابید که ضعف‌های امنیتی طبق برنامه زمانی ترمیم می‌شوند.
- ✓ همه سرور را در سطح بازبینی یکسان نگه دارید.

آماده‌سازی ویندوز سرور

- ✓ تا زمانی که سیستم‌عامل نصب و تقویت شود، کامپیوترهای تازه نصب شده را از ترافیک شبکه متخاصم
- ✓ (hostile network traffic) محافظت کنید. همه سرورهای جدید در شبکه DMZ را که به اینترنت وصل نیستند، تقویت کنید.
- ✓ برای بایوس/سفت‌افزار پسورد تعیین کنید تا از تغییرات غیرمجاز در تنظیمات استارت‌آپ سرور جلوگیری شود.
- ✓ لاگین کردن خودکار با اکانت مدیریتی در کنسول بازیابی (ریکاوری) را غیرفعال کنید.
- ✓ ترتیب بوت دستگاه‌ها را طوری تنظیم کنید که به‌طور غیرمجاز و خودکار از رسانه‌های دیگر بوت نشوند.

نصب ویندوز سرور

- ✓ مراقب باشید سیستم طی فرآیند نصب خاموش نشود.
- ✓ برای پیکربندی سیستم براساس یک نقش (role) خاص، از Security Configuration Wizard استفاده کنید.
- ✓ مراقب باشید همه وصله‌های مناسب، ترمیم‌های فوری و سرویس‌پک‌ها به‌درستی اعمال شوند. وصله‌های امنیتی، ضعف‌های شناخته‌شده‌ای را که مهاجمان برای نفوذ به سیستم ممکن است از آن‌ها بهره ببرند، ترمیم می‌کنند. پس از نصب ویندوز سرور، بلافاصله آن را به‌وسیله WSUS یا SCCM با جدیدترین وصله‌ها آپدیت کنید.
- ✓ قابلیت اعلام خودکار انتشار وصله‌های جدید را فعال کنید. هرگاه وصله‌ای منتشر شد، آن وصله باید فورا با استفاده از WSUS یا SCCM تحلیل، تست و نصب شود.

تقویت امنیت حساب کاربری

- ✓ مطمئن از استاندارد بودن و قوی بودن پسوردهای مدیریتی و سیستمی‌تان اطمینان حاصل کنید. مخصوصا مراقب باشید که در پسورد اکانت‌های ممتاز (اکانت‌هایی که سطح دسترسی بالایی دارند)، از کلمات معنادار یا لغت‌نامه‌ای استفاده نشود. هر پسورد باید دست‌کم ۱۵ کاراکتر داشته و ترکیبی از حرف، عدد، علائم خاص و کاراکترهای نامرئی (مثل CTRL) باشد. همه پسوردها را هر ۹۰ روز یک‌بار عوض کنید.
- ✓ سیاست‌های گروهی (Group Policy) جهت مسدودسازی اکانت‌ها را طبق بهترین شیوه‌های پیشنهادشده تنظیم کنید.
- ✓ اجازه ندهید کاربران، اکانت مایکروسافتی ایجاد کنند و با آن در کامپیوترها لاگین کنند.
- ✓ اکانت میهمان (Guest account) را غیرفعال کنید.
- ✓ نباید اجازه دهید به کاربران ناشناس، مجوز Everyone اعطا شود.
- ✓ برای شمارش اکانت‌ها و داده‌های به‌اشتراک‌نهاده شده SAM به‌صورت ناشناس، مجوز صادر نکنید.
- ✓ ترجمه SID/Name به‌صورت ناشناس را غیرفعال کنید.
- ✓ حساب‌های کاربری بلااستفاده را فورا غیرفعال یا حذف کنید.

پیکربندی امنیت شبکه

- ✓ دیواره آتش (فایروال) ویندوز را در همه پروفایل‌ها (دامنه‌ها، خصوصی، عمومی) فعال و طوری پیکربندی کنید که به‌طور پیش‌فرض ترافیک ورودی را بلوکه کند.
- ✓ مسدودسازی پورت را در سطح تنظیمات شبکه فعال کنید. دریابید که کدام پورت‌ها باید باز باشند. دسترسی به تمام دیگر پورت‌ها را محدود کنید.
- ✓ تنظیمات‌تان طوری باشد که فقط کاربران احراز هویت شده بتوانند از شبکه به هر کامپیوتری دسترسی یابند.
- ✓ به هر کاربری مجوز act as part of the operating system اعطا نکنید.
- ✓ به اکانت‌های میهمان اجازه ندهید با مجوز سرویس (Log on as a service)، رشته وظایف (log on as a batch job)، به‌صورت محلی (log on locally) یا از طریق RDP لاگین کنند.
- ✓ اگر از RDP استفاده می‌شود، سطح رمزنگاری اتصال RDP را بالا ببرید.
- ✓ گزینه Enable LMhosts lookup را حذف کنید.
- ✓ گزینه NetBIOS over TP/IP را غیرفعال کنید.
- ✓ گزینه ncacn_ip_tcp را حذف کنید.
- ✓ هم Microsoft Network Client و هم Microsoft Network Server را طوری پیکربندی کنید که همیشه ارتباطات‌شان را دیجیتالی امضا کنند.
- ✓ ارسال پسوردهای رمزنگاری نشده به سرورهای SMB طرف سوم را غیرفعال کنید.
- ✓ اجازه ندهید کاربر به‌صورت ناشناس به داده‌های اشتراکی‌شده دسترسی یابد.
- ✓ به سیستم محلی (Local System) اجازه دهید برای NTLM از هویت کامپیوتر استفاده کند.
- ✓ Local System NULL session fallback را غیرفعال کنید.
- ✓ انواع رمزنگاری‌های ممکن برای کربروس را پیکربندی کنید.
- ✓ مقادیر LAN Manager hash را ذخیره نکنید.
- ✓ سطح احراز هویت LAN Manager را طوری تنظیم کنید که فقط NTLMv2 را بپذیرد و LM و NTLM را رد کند.
- ✓ امکان به‌اشتراک‌گذاری فایل و پرینتر از شبکه را حذف کنید. به‌اشتراک‌گذاری فایل و پرینتر به هر کسی اجازه می‌دهد تا به یک سرور متصل شود و بدون نیاز به شناسه کاربری یا پسورد به داده‌های مهم دسترسی یابد.

پیکربندی امنیتی رجیستری ویندوز سرور

- ✓ تمهیدی بیاندیشید تا همه مدیران برای درک جامع نحوه عملکرد رجیستری و هدف هر یک از کلیدهای مختلف آن وقت بگذراند. در سیستم‌عامل ویندوز بسیاری از ضعف‌ها را می‌توان با تغییر کلیدهای خاص رجیستری ترمیم کرد. در ادامه به برخی از آن‌ها اشاره خواهدشد.
- ✓ مجوزهای رجیستری را پیکربندی کنید. رجیستری را از دسترس کاربران ناشناس دور نگه دارید. اگر دسترسی راه دور به رجیستری را لازم ندارید، برایش مجوز صادر نکنید.
- ✓ مقدار MaxCachedSockets (REG_DWORD) را روی 0 تنظیم کنید.
- ✓ مقدار SmbDeviceEnabled (REG)DWORD را روی 0 تنظیم کنید.
- ✓ مقدار AutoShareServer را روی 0 تنظیم کنید.
- ✓ مقدار AutoShareWks را روی 0 تنظیم کنید.
- ✓ همه مقادیر داده درون کلید NullSessionPipes را پاک کنید.
- ✓ همه مقادیر داده درون کلید NullSessionShares را پاک کنید.

تنظیمات امنیتی عمومی

- ✓ سرویس‌هایی را که لازم ندارید غیرفعال کنید. در اکثر سرورها سیستم‌عامل با تنظیمات پیش‌فرض نصب شده است. در تنظیمات پیش‌فرض، اغلب سرویس‌های اضافی که سیستم نیازی به آن‌ها ندارد نیز روشن هستند که این به بروز ضعف‌های امنیتی منجر می‌شود. پس همه سرویس‌های نالازم حتما باید از سیستم حذف شوند.
- ✓ اجزا یا کامپیوننت‌های نالازم ویندوز را حذف کنید. اجزای غیرضروری ویندوز باید از سیستم‌های مهم حذف شوند تا سرورها امن بمانند.
- ✓ با انتخاب NTFS یا BitLocker در ویندوز سرور، قابلیت رمزنگاری سیستم فایل (EFS) بومی ویندوز را فعال کنید.
- ✓ اگر ایستگاه کاری (workstation) حافظه رم زیادی دارد، swapfile ویندوز را غیرفعال کنید. این کارف بازده و امنیت را افزایش می‌دهد زیرا هیچ داده مهمی نمی‌تواند روی هارددیسک نوشته شود.
- ✓ از AUOTORUN استفاده نکنید؛ در غیر این‌صورت کدهای نامطمئن می‌توانند بدون اطلاع مستقیم کاربر اجرا شوند؛ مثلا مهاجم می‌تواند از روی سی‌دی اسکریپت خودش را اجرا کند.
- ✓ سیستم را طوری پیکربندی کنید که پیش از لاگین کردن کاربر، پیغامی رسمی به وی نمایش داده شود. متن پیغام برای مثال می‌تواند چنین باشد: «استفاده غیرمجاز از این کامپیوتر و منابع شبکه ممنوع است...»
- ✓ برای لاگین کردن تعاملی، استفاده از کلیدهای ترکیبی Ctrl + Alt + Del را الزامی کنید (در لاگین تعاملی، کاربر نه از راه دور بلکه به‌صورت محلی در کامپیوتر لاگین می‌کند).
- ✓ برای بیکار ماندن کامپیوتر، محدودیت زمانی تعیین کنید تا جلسه‌های تعاملی بلااستفاده (idle interactive sessions) محافظت شوند.
- ✓ مراقب باشید همه فضاهای ذخیره‌سازی (volume) از سیستم فایل NTFS استفاده کنند.
- ✓ مجوزهای Local File/folder را پیکربندی کنید. از دیگر اقدام امنیتی مهم که عمدتا مغفول می‌ماند، مسدودسازی مجوزهای سطح فایل (file-level) برای سرور است. به‌طور پیش‌فرض، ویندوز روی همه فایل‌ها یا فولدرهای محلی محدودیت‌های خاصی اعمال نمی‌کند؛ در اکثر کامپیوترها به گروه Everyone مجوزهای کامل اعطا می‌شود. گروه Everyone را حذف و در عوض براساس نقش کاربران، گروه‌های مختلف تعریف کنید. به یاد داشته باشید مجوز و سطح دسترسی هر گروه فقط باید به‌اندازه‌ای باشد که بتواند وظایفش را انجام دهد و نه بیشتر. سپس بر پایه همین اصل، به گروه‌ها مجوز دسترسی به فایل و فولدر اعطا کنید. گروه‌های Guest و Everyone و نیز قابلیت لاگین کردن به‌صورت ناشناس را با جدیت از فهرست مجوزهای کاربر حذف کنید. ویندوز با این پیکربندی، امن‌تر خواهدشد.
- ✓ تاریخ/زمان سیستم را تنظیم و آن را طوری پیکربندی کنید که با تایم‌سرورهای دامنه هماهنگ باشد.
- ✓ یک محافظ صفحه‌نمایش (screensaver) پیکربندی کنید تا هرگاه کنسول بی‌کار بود، صفحه نمایش کنسول به‌طور خودکار قفل شود.

تنظیمات Audit Policy

- ✓ Audit Policy را به‌درستی در ویندوز فعال کنید. شما با Audit Policy مشخص می‌کنید که چه نوع رویدادهایی باید ردگیری و در بخش Security log ویندوز سرور ثبت شوند.
- ✓ روش ذخیره‌سازی مستمر Event log را طوری پیکربندی کنید که در صورت نیاز نونویسی شود. اندازه آن را تا ۴ گیگابایت تعیین کنید.
- ✓ به‌منظور مانیتورینگ، کپی روی‌دادهای ثبت شده را به SIEM (مخفف Security Information and Event Management) ارسال کنید (log shipping).

راهنمای امنیت نرم‌افزار

- ✓ نرم‌افزار ضدویروس نصب و آن را فعال کنید. آن را طوری پیکربندی کنید که روزانه آپدیت شود.
- ✓ نرم‌افزار ضدجاسوس‌افزار نصب و آن را فعال کنید. آن را طوری پیکربندی کنید که روزانه آپدیت شود.
- ✓ نرم‌افزاری نصب کنید که یکپارچگی فایل‌های مهم سیستم‌عامل را بررسی کند. ویندوز قابلیتی موسوم به Resource Protection دارد که فایل‌های مهم خاص را به‌طور خودکار بررسی و هر کدام را که معیوب بود با نسخه سالم جایگزین می‌کند.

پایان کار

- ✓ با استفاده از GHOST یا Clonezilla از سیستم‌عامل‌های‌تان ایمیج بگیرید تا همه آنچه روی سیستم‌عامل نصب شده است و نیز همه تنظیمات امنیتی آن در فایل ایمیج کپی شود. در این‌صورت اگر برای مثال لازم شد که ویندوز سرور را از نو نصب کنید، همه برنامه‌ها و تنظیمات امنیتی پیشین از روی فایل ایمیج روی ویندوز پیاده می‌شود و دیگر لازم نیست پس از نصب ویندوز همه نرم‌افزارها و تنظیمات امنیتی موردنیازتان را دوباره یک به یک اعمال کنید.
- ✓ کلید لایسنس ویندوز سرورتان را باتوجه به نسخه آن (2019/2016/2012/2008/2003) وارد کنید.
- ✓ سرور را به دامنه متصل کنید و سیاست‌های موردنیاز گروه دامنه (domain group) را اعمال کنید.