مدیریت WFAS از طریق Group Policy در ویندوز سرور 2019

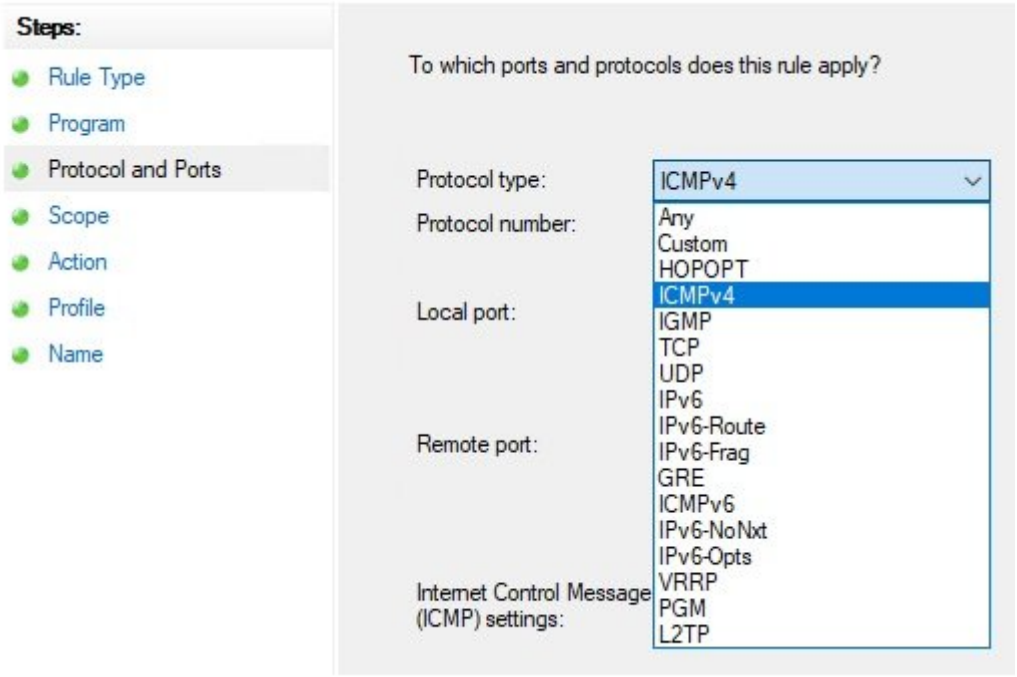
در اغلب موارد، مجبور هستیم قاعده‌ای برای تعیین وضعیت پروتکل ICMP ایجاد کنیم. به عبارت دیگر، در برخی موارد مجبور هستیم دیوارآتش را به شکلی روی سرور تنظیم کنیم که توانایی پاسخ‌گویی به درخواست‌ها پینگ وجود داشته باشد. در برخی از شرکت‌ها کارشناسان شبکه مجبور هستند ICMP را در سرور جدید شرکت فعال کنند تا کلاینت‌ها هر زمان یک پینگ انجام دادند پاسخ را دریافت کنند. هنگامی که نیاز به تعریف و ایجاد یک قانون جدید داریم تا اجازه دهیم پینگ‌ها با موفقیت انجام شوند، قاعده موردنیاز را مشابه با قاعده‌ای که برای RDP ایجاد کردیم، تعریف می‌کنیم با این تفاوت که باید به نکته مهمی دقت کنیم.

برای مطالعه قسمت قبل آموزش رایگان **ویندوز سرور 2019 اینجا** کلیک کنید.

تعریف یک قاعده دیوارآتش برای پروتکل ICMP برای پیاده‌سازی موفقیت‌آمیز پینگ

در برخی از شرکت‌ها کارشناسان شبکه مجبور هستند ICMP را در سرور جدید شرکت فعال کنند تا کلاینت‌ها هر زمان یک پینگ انجام دادند پاسخ را دریافت کنند. هنگامی که نیاز به تعریف و ایجاد یک قانون جدید داریم تا اجازه دهیم پینگ‌ها با موفقیت انجام شوند، قاعده موردنیاز را مشابه با قاعده‌ای که برای RDP ایجاد کردیم، تعریف می‌کنیم، اما باید به نکته مهمی دقت کنیم. اگر به صفحه اول که Rule Type نام دارد و در آن باید نوع قاعده‌ای که در حال ساخت آن هستیم را مشخص کنیم، مراجعه کنید، مشاهده می‌کنید که هیچ گزینه یا پیش تعریفی برای ICMP وجود ندارد. به نظر من این مسئله عجیب است، زیرا این یک قاعده معمولی است که از سوی بیشتر کارشناسان شبکه استفاده می‌شود و بهتر بود گزینه آن در منوی کرکره‌ای قرار می‌گرفت تا گزینه ICMP به سادگی انجام شود. اکنون که چنین گزینه‌ای در دسترس نیست، شما باید یک قاعده ورودی جدیدی ایجاد کنید، درست مشابه کاری که برای RDP انجام دادیم، اما در اولین صفحه اطمینان حاصل کنید گزینه Custom را انتخاب کرده‌اید.

در مرحله بعدی گزینه پیش‌فرض All programs را قبول کنید و دکمه Next را کلیک کنید. در صفحه بعد باید از طریق منویی کشویی نوع پروتکل را مشخص کنید. روی کادر کلیک کرده و گزینه ICMP را برای مدیریت ترافیک این پروتکل انتخاب کنید. همان‌گونه که در شکل زیر مشاهده می‌کنید، بسته به نوع ترافیک شبکه گزینه ICMPv4 یا ICMPv6 در دسترس قرار دارد. طبیعی است گزینه ICMPv4 را مشاهده خواهید کرد که باید آن‌را انتخاب کنید.



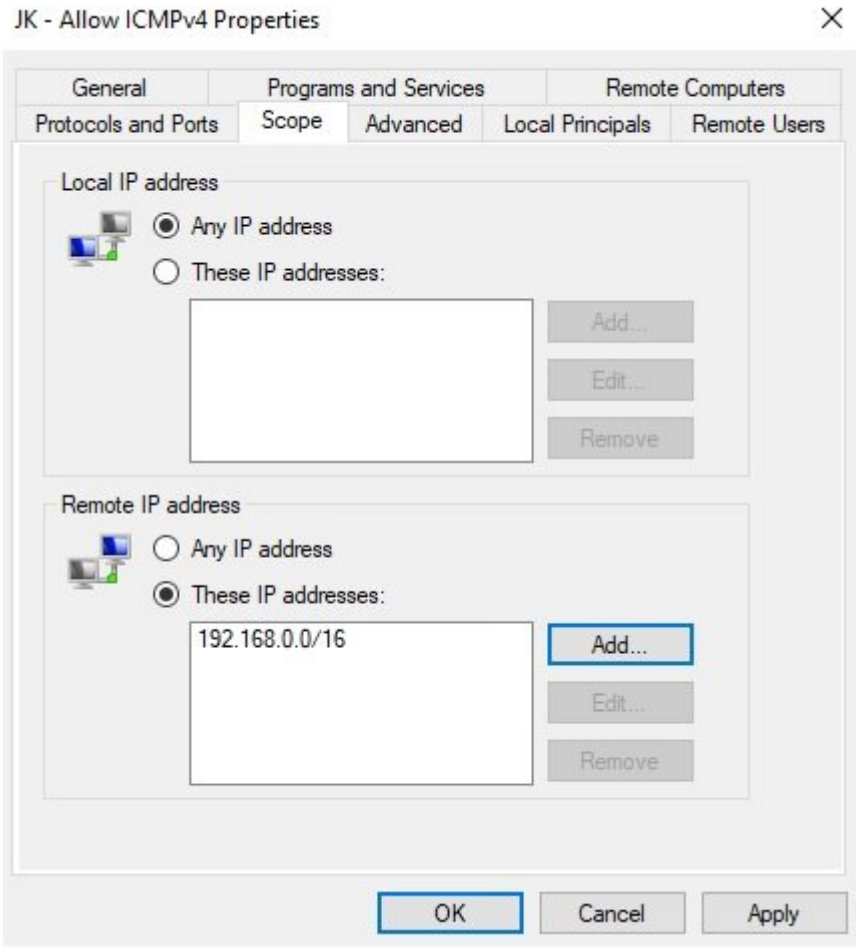
سایر کارهایی که باید انجام دهید، مشابه با زمانی است که در حال تعریف قاعده RDP بودیم. در این‌جا نیز باید نوع حالت اجازه دادن یا مسدود کردن ترافیک برای پروفایل دیوارآتش را مشخص کنیم که طبیعی است گزینه Allow را انتخاب خواهیم کرد. پس از اتمام کار، قاعده جدید ICMPv4 بلافاصله اجرایی می‌شود و اگر قاعده را در حالت Allow تعیین کرده باشید، سرور جدید به‌طور خودکار به درخواست‌های پینگ پاسخ می‌دهد:

```
PS C:\Users\administrator.CONTOSO> ping ra1

Pinging ra1.contoso.local [10.10.10.13] with 32 bytes of data:
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
```

اگر نیاز به تغییر یک قاعده یا ویرایش یک قاعده در دیوارآتش داشتید باید به سراغ تنظیمات پیشرفته یک قاعده بروید. برای این منظور کافی است به صفحه Inbound Rules بروید، روی هر قاعده دیوارآتش مدنظر راست کلیک کنید و گزینه Properties را انتخاب کنید. درون زبانه‌های نشان داده شده، امکان ویرایش جزییات وجود دارد. به عنوان مثال، می‌توانید پورت‌های اضافی را مشخص کنید تا پروفایل دیوارآتش روی آن پورت‌ها اعمال شود یا حتا می‌توانید آدرس‌های آی‌پی که باید این قاعده روی آن‌ها اعمال شود را از طریق زبانه Scope مشخص کنید.

این قابلیت به شما این امکان را می‌دهد تا قاعده دیوارآتش خود را فقط در ارتباط با ترافیک یا بخش خاصی از شبکه یا یک زیر مجموعه خاص از ماشین‌ها اعمال کنید. به عنوان مثال، در اینجا من زبانه Scope را ویرایش کردم تا قاعده جدی تنها روی ترافیکی که از زیرشبکه 192.168.0.0/16 وارد می‌شود اعمال شود:

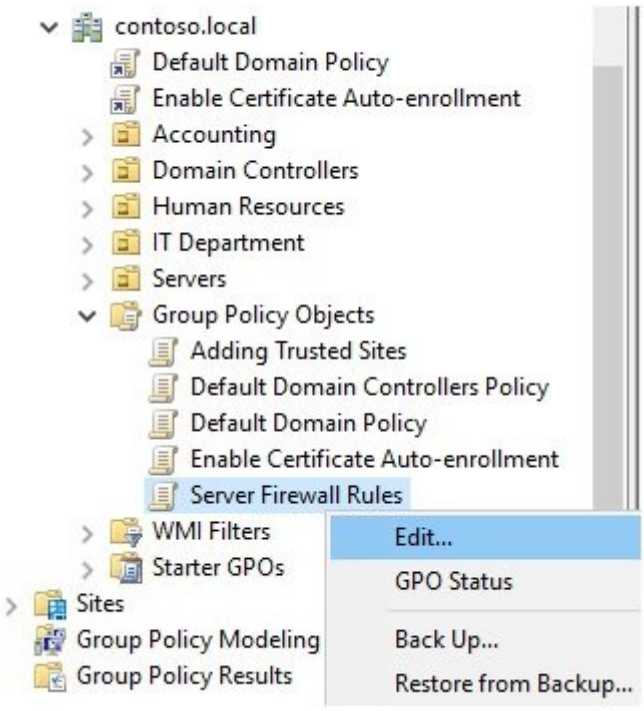


مدیریت WFAS از طریق Group Policy

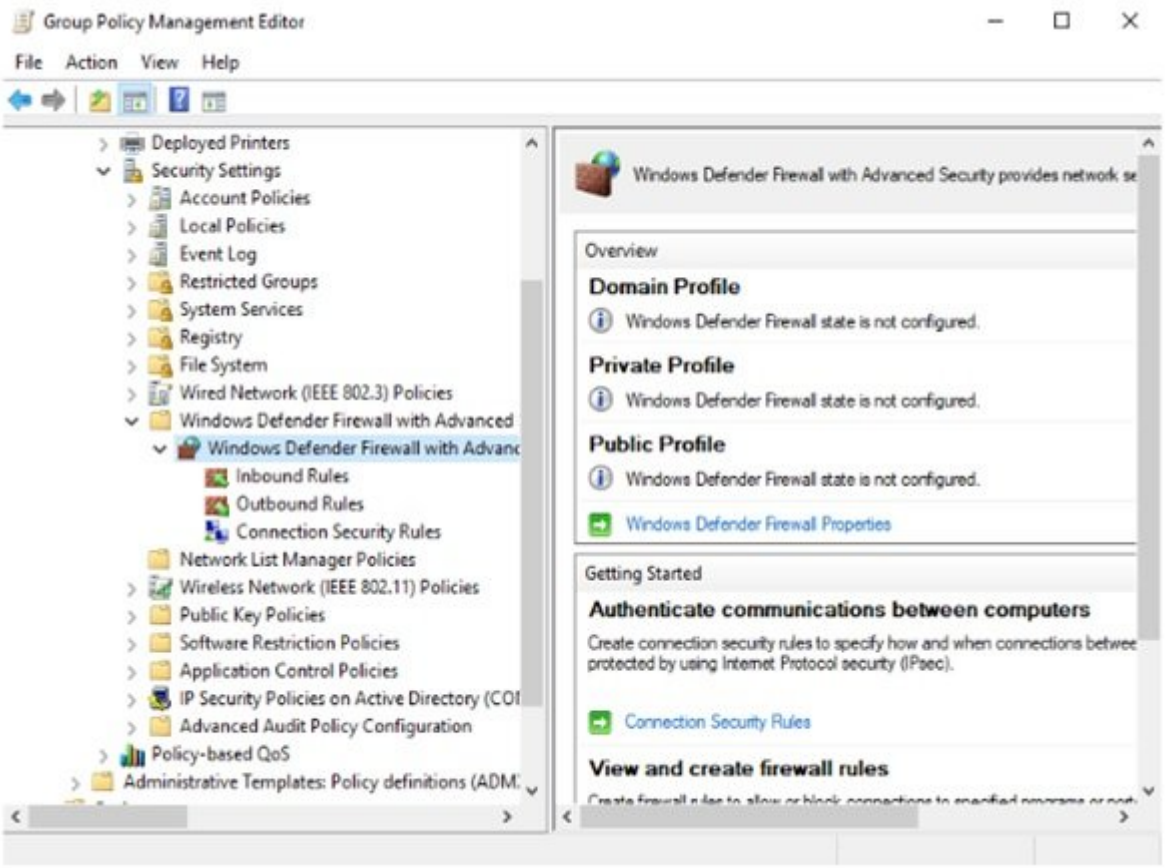
مدیریت قواعد دیوارآتش روی سرورها و کلاینت‌ها می‌تواند گامی بزرگ در جهت ایجاد یک محیط امن‌تر باشد. لازم به توضیح است که فناوری فوق در کلاس سازمانی است، در نتیجه مایکروسافت تمهیداتی در نظر گرفته تا اگر قرار است یک قاعده روی ماشین‌های خاصی اعمال شود، کارشناسان مجبور نشوند یک به یک به سراغ ماشین‌ها بروند و یک قاعده خاص را روی آن‌ها اعمال کنند.

برای حل این مشکل باید از راهکار خط‌مشی گروهی (GPO) سرنام Group Policy Object استفاده کنید. همانند اکثر تنظیمات و عملکردهای موجود در سیستم‌عامل ویندوز مایکروسافت، تنظیم یک خط‌مشی دیوارآتش روی همه دستگاه‌هایی که متصل به دامنه هستند اعمال می‌شود. البته شما می‌توانید خط‌مشی‌های خود را به چند مجموعه تقسیم کنید تا یک GPO تنها روی کلاینت‌ها اعمال شود، در حالی که یک GPO جداگانه قواعد دیوارآتش را روی سرورها اعمال کند. نکته‌ای که لازم است به آن دقت کنید این است که شما می‌توانید ماشین‌ها را گروه‌بندی کنید و برای هر گروه مجموعه قوانین GPO ایجاد کنید و به‌طور خودکار قاعده ساخته شده را در ارتباط با ماشین‌هایی که عضو یک GPO هستند اعمال کنید.

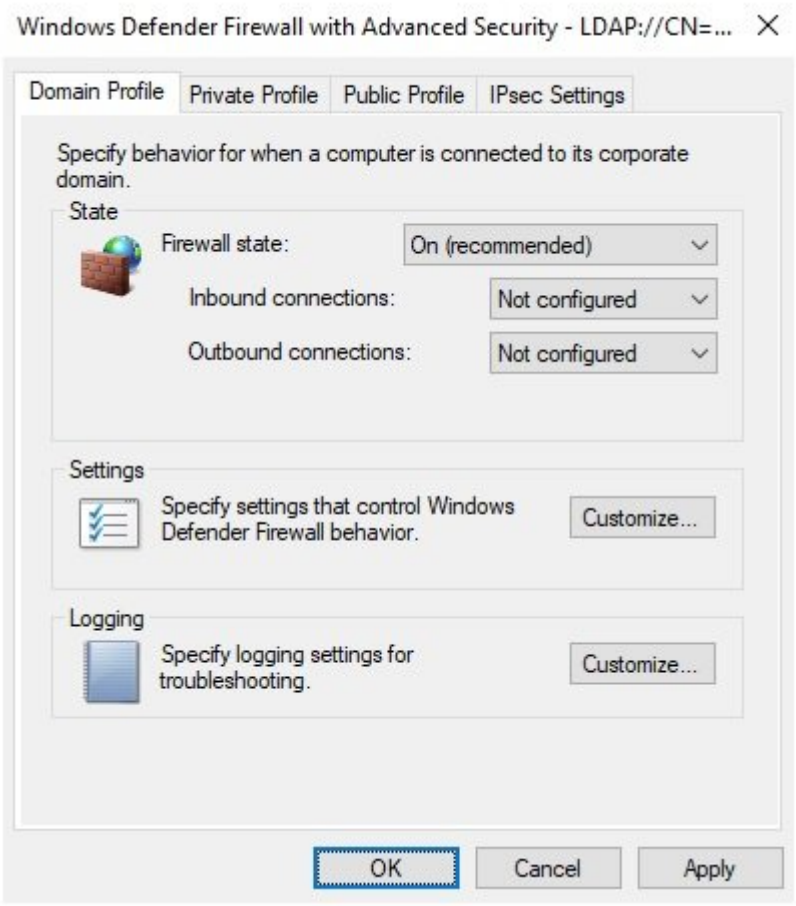
شما قبلاً با نحوه ساخت GPO آشنا شده‌اید، بنابراین یک GPO که قرار است تنظیمات دیوارآتش را شامل شود ایجاد کنید. GPO را لینک کرده و فیلتر کنید تا فقط دستگاه‌های مدنظر تنظیمات را دریافت کنند. شاید ایده بدی نباشد که فرآیند فوق را با OU آزمایش کنید تا اطمینان حاصل کنید تمام قواعدی که می‌خواهید داخل GPO قرار دهید به خوبی در کنار هم قرار گرفتند و با خط‌مشی‌های امنیتی سازمان سازگار باشند. پس از ایجاد GPO جدید، از داخل Console Management Policy Group روی آن راست کلیک کنید و سپس Edit ... را انتخاب کنید:



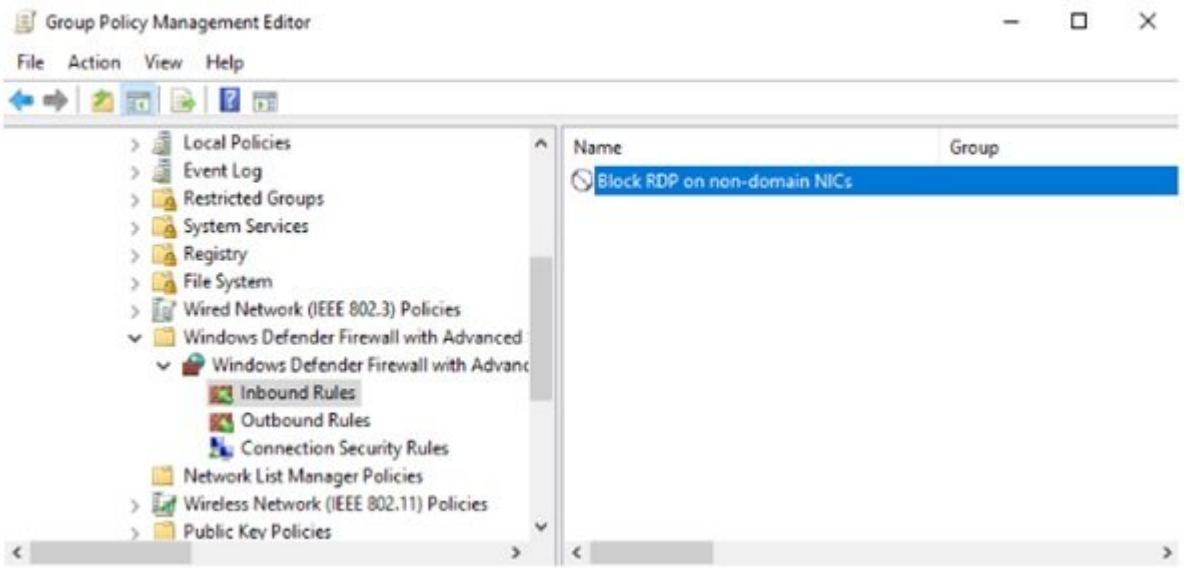
اکنون زمان آن رسیده است تا به درون GPO جدیدی که ایجاد کرده‌ایم نگاهی داشته باشیم. نکته مهمی که باید درباره آن اطلاع داشته باشیم این است چه مکان برای ساخت قواعد جدید دیوارآتش مناسب است. هنگامی که به قواعد دیوارآتشی که درون ماشین محلی خودمان قرار دارد نگاه می‌کنیم، مشاهده می‌کنیم که همه چیز تحت عنوان Windows Defender Firewall with Advanced Security فهرست شده‌اند و در مسیر Computer Configuration | Policies | Windows Settings | Security Settings | Windows Defender Firewall with Advanced Security | Windows Defender Firewall with Advanced Security قرار دارند.



هنگامی که می‌خواهید اطمینان حاصل کنید که پروفایل‌های خاص دیوارآتش یا به‌طور کلی خود دیوارآتش ویندوز چه وضعیتی دارند، مکان فوق بهترین نقطه‌ای است که اطلاعات لازم را ارائه می‌کند. بنابراین ، این همان مکانی است که در صورت لزوم اجازه می‌دهد دیوارآتش ویندوز برای برای هر کاربری غیرفعال کنید. با کلیک روی ویژگی‌های Windows Defender Firewall، پیوندی ظاهر می‌شود که اجازه می‌دهد وضعیت هر پروفایل را به‌طور جداگانه بررسی کنید.



پس از آن‌که پروفایل مدنظر را مطابق با نیازهای خود پیکربندی کردید روی دکمه ok کلیک کنید و به بخش WFAS متعلق GPO بازگردید. درست مشابه با کنسول محلی WFAS، برای قواعد ورودی و خروجی گروه‌بندی‌هایی وجود دارد. کافی است روی Inbound Rules راست‌کلیک کنید و گزینه New Rule را انتخاب کنید. با این ویزاد از قبل و زمانی که در حال ساخت یک قاعده در کنسول محلی WFAS بودید، آشنا شده‌اید، مراحل را به ترتیب کامل کنید، زمانی‌که کار به اتمام رسید، قاعده دیوارآتش شما در GPO نشان داده می‌شود. این قاعده دیوارآتش از قبل در اکتیو دایرکتوری ساخته شده و روی سرورها و ماشین‌هایی که شما در خط‌مشی‌ها به آن‌ها اشاره کردید، نصب شده است.



فناوری‌های رمزنگاری

یک فناوری که همه سازمان‌های بزرگ و هم مردم به آن نیازی مبرمی دارند، رمزگذاری است. بیشتر ما سال‌های متمادی است از سایت‌هایی که با فناوری HTTPS کار می‌کنند، استفاده می‌کنیم، اما هنوز هم استثنائاتی وجود دارد که برخی از شرکت‌های نه چندان مطرح از تکنیک ساده انتقال اطلاعات استفاده می‌کنند که رویکرد فوق بسیار وحشتناکی است، زیرا هر چیزی که اکنون با استفاده از HTTP معمولی یا از طریق یک ایمیل محافظت نشده با الگوهای رمزنگاری از طریق اینترنت ارسال می‌شود ممکن است توسط شخص دیگری خوانده شود. شاید نسبت به این موضوع حساس نباشید و شاید تصور کنید که هیچ فردی در حال رهگیری و خواندن ترافیک شما نیست، اما باید بدانید که اگر به بازدید از وب‌سایتی می‌پردازید که از HTTP استفاده می‌کند یا اگر از هر یک از سرویس‌های ایمیل رایگان برای تبادل اطلاعات استفاده می‌کنید که داده‌ها بدون هیچ‌گونه رمزنگاری ارسال می‌شوند، این احتمال وجود دارد که فردی در نیم کره دیگر زمین در حال خواندن اطلاعات شما است.

در حالی که ما در محافظت از ترافیک مرورگرهای اینترنتی بهتر و بهتر می‌شویم، با این وجود به‌طور سنتی هنوز به داده‌هایی که در پشت دیوارهای شبکه سازمانی قرار دارند چندان توجه نمی‌کنیم و نکات ایمنی در مورد آن‌ها را رعایت نمی‌کنیم. توجه داشته باشید که هکرها انسان‌های کندذهنی نیستند و مجموعه‌ای بسیار بزرگ از ابزارهای پیشرفته را همراه با ترفندهای مهندسی اجتماعی به خدمت می‌گیرند تا به شبکه هر سازمانی نفوذ کنند. وقتی داخل شدند به دنبال چه خواهند بود؟ در بیشتر موارد به سراغ حساب‌های کاربری یا کامپیوترها می‌روند، زیرا اطلاعات اصلی در حساب‌های کاربری قرار دارد. خوشبختانه فناوری‌های مختلفی در **ویندوز سرور 2019** قرار دارند که برای محافظت از داده‌ها و مقابله با حملات هکری قادر به محافظت از مراکز داده هستند. اجازه دهید به این فناوری‌های رمزنگاری اطلاعات از نزدیک نگاهی داشته باشیم.

BitLocker و TPM مجازی

BitLocker یک فناوری است نام آشنا است، زیرا در بیشتر سیستم‌های کلاینتی مجهز به ویندوز قرار گرفته است. بیت‌لاکر می‌تواند یک درایو را به‌طور کامل رمزگذاری کند و این اطمینان را بدهد که داده‌های ما در لپ‌تاپ‌ها یا کامپیوترهای شخصی مصون از سرقت خواهند بود. در چنین شرایطی اگر لپ‌تاپ به سرقت برود، هکرها موفق نخواهند شد به داده‌ها دست پیدا کنند، زیرا تمامی اطلاعات رمزگذاری شده‌اند. خوشبختانه این امکان وجود دارد که از بیت‌لاکر برای محافظت از سرورهای خود استفاده کنیم.

با گسترش روزافزون استفاده از رایانش ابری و منابع ابرمحور، لزوم به‌کارگیری فناوری‌های رمزنگار همچون بیت‌لاکر روی سرورها دوچندان شده است. هنگامی که درباره ابر صحبت می‌کنیم، آن‌چه واقعا به آن نیاز داریم دسترسی به بیت‌لاکر روی ماشین‌های مجازی (سرور یا کلاینت) است. مهم نیست ماشین‌های مجازی (VMs) خود را در یک فضای ابری واقعی که توسط یک سرویس دهنده خدمات عمومی ابر ارائه می‌شود ذخیره می‌کنید یا از ابر خصوصی خود استفاده می‌کنید که به مشترکان اجازه می‌دهید ماشین‌های مجازی خود را در محیط ابر ایجاد کرده و آن‌ها را مدیریت کنند، در هر دو حالت اگر از فناوری رمزگذاری روی درایوهای مجازی استفاده نکرده باشید، فایل‌های VHD و VHDX و همچنین داده‌ها در امنیت قرار ندارند. زیرا هر فردی که مجوز مدیریتی مرتبط با بستر میزبانی مجازی را در اختیار داشته باشد، به راحتی قادر است به داده‌هایی که روی هارددیسک‌های سرور ذخیره شده‌اند دسترسی داشته باشد، حتا بدون آن‌که به شبکه یا حساب‌های کاربری روی دامنه دسترسی داشته باشد. تنها کاری که چنین فردی باید انجام دهد این است که یک کپی از فایل VHDX که شامل تمامی محتویات درایو سرور است را به دست آورده، آن‌را روی یک حافظه فلش کپی کرده، به خانه آورده و هارددیسک مجازی را روی ماشین خود اجرا کند تا محتویات درون آن‌را مشاهده کند. بدون شک این مشکل بزرگی در ارتباط با امنیت داده‌ها است.

در شماره آینده آموزش رایگان ویندوز سرور 2019 مبحث فوق را ادامه خواهیم رفت.

برای مطالعه تمام بخش‌های آموزش **ویندوز سرور 2019** روی لینک زیر کلیک کنید:

آموزش رایگان ویندوز سرور 2019

تاریخ انتشار:
25 آبان 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16265/%D9%85%D8%AF%DB%8C%D8%B1%DB%8C%D8%AA-wfas-%D8%A7%D8%B2-%D8%B7%D8%B1%DB%8C%D9%82-group-policy-%D8%AF%D8%B1-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019