چه قابلیت‌های امنیتی از ویندوز سرور 2019 محافظت می‌کنند؟

امنیت داده‌ها، امنیت شبکه، امنیت اطلاعات و موضوعات مشابه به یکی از دغدغه‌های اصلی کسب‌وکارهای بزرگ تبدیل شده، اما همیشه ابزارها و فناوری‌های جدیدی وجود دارد که برای مقابله با هکرها به سازمان‌ها کمک می‌کنند. ویندوز سرور 2019 به عنوان یکی از تاثیرگذارترین سیستم‌عامل‌های حال حاضر به بهترین و پیشرفته‌ترین قابلیت‌های امنیتی تجهیز شده است. قابلیت‌هایی که امنیت را هم برای کلاینت‌ها و هم برای مدیران سرور به ارمغان آورده است.

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

یک مکانیزم امنیتی محکم و یکپارچه

امنیت داده‌ها، امنیت شبکه، امنیت اطلاعات و موضوعات مشابه به یکی از دغدغه‌های اصلی کسب‌وکارهای بزرگ تبدیل شده، اما همیشه ابزارها و فناوری‌های جدیدی وجود دارد که برای مقابله با هکرها به سازمان‌ها کمک می‌کنند. ویندوز سرور 2019 یکی از امن‌ترین سیستم‌عامل‌های مایکروسافت است که ابزارها و مکانیسم‌های امنیتی قدرتمندی در آن قرار گرفته است.

از مهم‌ترین فناوری‌های امنیتی که ویندوز سرور 2019 به به آن‌ها تجهیز شده است به موارد زیر می‌توان اشاره کرد که قصد داریم در شماره آینده به بررسی آن‌ها بپردازیم.

Windows Defender Advanced Threat Protection

Windows Defender Firewall

Encryption technologies

Banned passwords

Advanced Threat Analytics

General security best practices

Windows Defender Advanced Threat Protection

ویندوز دیفندر چند سالی است در پشت صحنه از سامانه‌های کاربران در برابر تهدیدات امنیتی دفاع کرده است. در چند سال اخیر مایکروسافت یکسری مشکلات آن‌را برطرف کرده و قابلیت‌های مفیدی به آن افزوده است. اولین بار این مولفه امنیتی همراه با سیستم‌عامل ویندوز 8 و به عنوان یک ضد ویروس رایگان داخلی ساخته شد، اما چندان مورد توجه قرار نگرفت. با این حال، ویندوز دیفندر به سرعت پیشرفت کرد و امروزه به ندرت سیستم‌عامل ویندوز 10 را پیدا می‌کنید که ضد ویروس دیفندر یا دیوارآتش روی آن غیر فعال شده باشد. این ابزارها در سیستم‌عامل به‌صورت پیش‌فرض فعال هستند و یکپارچگی و سرعت پاسخ‌گویی دقیق و سریعی دارند که باعث شده‌اند فروشندگان ثالث به سختی بتوانند محصولی یکسان با آن‌ها به بازار عرضه کنند. کارشناسان شبکه زمانی که ضدویروس ثالثی را روی سرور نصب می‌کنند ممکن است بارها و بارها نشتی حافظه را پیدا کنند و سرور آن‌ها به شکل تصادفی راه‌اندازی مجدد شود که چنین موضوعی در دنیای سرورهای امروزی قابل قبول نیست. برخی از متخصصان شبکه هنوز هم بر این باور هستند که قابلیت‌های ضدویروس دینفدر چندان قدرتمند نیستند، زیرا بیت‌دینفدر به شکل رایگان در اختیار کاربران قرار دارد، اما تجربه شخصی من نشان داده که یکپارچگی دیفندر با ویندوز عملکرد آن‌را دوچندان کرده است.

نسخه جدیدتر و خاص‌تر این محصول امنیتی که (ATP) سرنام Windows Defender Advanced Threat Protection نام دارد، مجموعه‌ای از قابلیت‌ها و ابزارهای مرتبط با یکدیگر را برای محافظت از دستگاه‌های ویندوزی به کار می‌گیرد. ضدویروس/ضدبدافزار تنها یکی از این قابلیت‌های این بسته امنیتی است. ویندوز سرور 2016 اولین سیستم‌عامل سروری بود که دیفندر ضدویروس از پیش ساخته شده آن بود. امروزه برخی از شرکت‌های کوچک و بزرگ در سراسر جهان هنوز هم از ویندوز سرور 2019 سرویس پک 2 استفاده می‌کنند که فاقد دیفندر است، با توجه به پیشرفت‌ها و برطرف شدن یکسری از ایرادات ویندوز دیفندر شاید بد نباشد این شرکت‌ها به ویندوز سرور 2019 مهاجرت کنند. در این سری آموزشی، ما زمان کافی در اختیار نداریم تا تمامی ویژگی‌های مختلف Windows Defender ATP که به‌طور مداوم بهبود پیدا می‌کنند را بررسی کنیم. کاری که قصد انجام آن‌را داریم این است که برخی از رابط‌ها را بررسی کنیم، اطمینان حاصل کنیم در مورد متداول‌ترین مولفه‌ها که بدون نیاز به تغییر خط‌مشی‌های امنیتی قادر به استفاده از آن‌ها هستید اطلاعات لازم را به دست آورید و سطح دانش خود در مورد ویژگی‌های پیشرفته‌تر را بهبود بخشید.

نصب ضدویروس ویندوز دینفدر

ویندوز دیفندر به‌طور پیش‌فرض در ویندوز سرور 2019 نصب شده است. اگر تنظیمات ویندوز دیفندر را تغییر نداده باشید، ضدویروس دیفندر نیز روی سیستم شما نصب شده است و به محض نصب سیستم‌عامل به‌طور خودکار از سیستم شما محافظت می‌کند. برای اطمینان از این موضوع، Server Manager را باز کنید و روی گزینه Add roles and features کلیک کرده و سپس به صفحه انتخاب ویژگی‌ها بروید. در این صفحه باید تیک مربوط به ضدویروس ویندوز دینفدر را مشاهده کنید.

نگاهی نزدیک به رابط کاربری ویندوز دینفدر

رابط کاربری ویندوز دیفندر در سرور 2019 همانند سیستم‌عامل ویندوز 10 است، اما اگر هنوز به سراغ این ابزار نرفته‌اید، در این بخش نگاهی گذرا به رابط کاربری خواهیم داشت. برای شروع کار روی دکمه Start کلیک کنید و برنامه Settings را باز کنید و روی گزینه Update & Security کلیک کنید در صفحه ظاهر شده روی گزینه Windows Security در سمت چپ صفحه کلیک کنید. در صفحه ظاهر شده نمایی کلی از مؤلفه‌های مختلف دینفدر که برای محافظت از سیستم طراحی شده‌اند را مشاهده می‌کنید. دقت کنید شما هیچ کاری برای فعال‌سازی این قابلیت‌ها نکرده‌اید و همگی به شکل پیش‌فرض فعال هستند.

با کلیک بر روی هر یک از گزینه‌های نشان داده شده، توضیحات مفصل‌تری درباره عملکرد هر یک از آن‌ها مشاهده می‌کنید و همچنین گزینه‌های بیشتری برای فعال یا غیرفعال کردن مکانیسم‌های محافظتی در اختیارتان قرار می‌گیرد. اگر روی گزینه Virus & threat protection کلیک کنید، اطلاعات مختصری در ارتباط با ضدویروس دیفندر مشاهده می‌کنید، به‌طور مثال، هر زمان فایل‌ها به‌روزرسانی می‌شوند ضدویروس آن‌ها را پویش می‌کند و.... اگر روی پیوند Manage کلیک کنید به گزینه غیرفعال کردن ضدویروس دیفندر همراه با سایر گزینه‌هایی که برای فعال یا غیر فعال کردن بخش‌های مختلف ارائه شده‌اند، دسترسی خواهید داشت. در این قسمت قصد داریم سه گزینه مهم این رابط کاربری را بررسی کنیم، زیرا در مقاله‌های آینده اشاراتی به این گزینه‌های خواهیم داشت. هنگامی‌که در مورد بخش ATP دیفندر صحبت می‌کنیم با سه گزینه زیر روبرو می‌شویم:

غیرفعال کردن Windows Defender

همان‌گونه که اشاره شد ضدویروس دینفدر به‌طور پیش‌فرض و همانند سایر ابزارهای خانواده دیفندر روی ویندوز فعال است. با فشار دکمه رادیویی که در شکل بالا مشاهده می‌کنید ضدویروس به‌طور موقت غیر فعال می‌شود. اگر تصمیم خود را گرفتید که ضدویروس دیفندر را به‌طور کامل غیرفعال کنید، زیرا ضدویروسی که قبلا هزینه آن‌را پرداخت کرده‌اید عملکرد بهتری دارد، دو گزینه وجود دارد. ضدویروس دیفندر به گونه‌ای طراحی شده که در صورت نصب ضدویروس دیگری به‌طور خودکار غیرفعال می‌شود. به عبارت دقیق‌تر تمام آن کاری که باید انجام دهید، این است که ضدویروس ثالث را نصب و سرور را راه‌اندازی مجدد کنید تا ضدویروس دیفندر غیرفعال شود و ضدویروس ثالث اجازه دهد بدون ایجاد مشکل کار خود را انجام دهد. نکته مهمی که برخی از متخصصان کامپیوتر به آن توجه نمی‌کنند این است که چند برنامه ضدویروس را روی یک سیستم اجرا می‌کنند که این‌کار واقعا به دور از عقل است! تضب ضدویروس‌های مختلف روی یک سیستم باعث ب وجود آمدن تضادهای بسیاری می‌شود، حافظه اصلی سیستم را بیهوده مصرف می‌کند که کندی سرعت را به همراه دارد و در نهایت باعث می‌شود، سیستم رفتارهای عجیبی از خود نشان دهد. اگر تصمیم دارید از ضدویروس خود استفاده کنید و به‌طور کامل دیفندر را غیرفعال کنید، باید دینفدر را به‌طور کامل از روی سرور حذف کنید. این‌کار به راحتی و توسط پاورشل و اجرای دستور زیر انجام می‌شود:

```
Uninstall-WindowsFeature -Name Windows-Defender
```

ATP چیست؟

به سختی می‌توان تعریف دقیقی برای ATP ارائه کرد، زیرا یکی از مولفه‌های اصلی دیفندر ویندوز است. مکانیزم‌های امنیتی ویندوز دیفندر در تعامل با یکدیگر از کلاینت‌ها و سرورها در برابر تهدیدات امنیتی محافظت می‌کنند.
ضدویروس، قابلیت دیوارآتش، محافظت از سخت‌افزار و حتا محافظت در برابر باج‌افزارها در ترکیب با یکدیگر و در تعامل با بخش Windows Security ویندوز سرور 2019 همگی تحت عنوان ATP شناخته می‌شوند.

نکته جالبی که در ارتباط با ویندوزدیفندر وجود دارد به رویکرد مایکروسافت در قبال به‌کارگیری فناوری ابری باز می‌گردد. مایکروسافت از فناوری ابری و محاسبات ابرمحور به منظور بهبود عملکرد ضدویروس بیت‌دیفندر استفاده می‌کند. ممکن است به این موضوع دقت نکرده باشید، اما اکثر دستگاه‌های ویندوزی (10) متصل به اینترنت با گزارش‌دهی آسیب‌پذیری‌ها و فعالیت‌های مخرب جدید به مایکروسافت، موفق شده‌اند به بهبود عملکرد بیت‌دینفدر و کاهش تهدیدات امنیتی کمک کنند. اطلاعاتی که توسط این ماشین‌ها تولید می‌شود با استفاده از فناوری یادگیری ماشین تجزیه‌وتحلیل می‌شود و اطلاعات پالایش شده به تمامی دستگاه‌های مبتنی بر ویندوز ارسال می‌شود تا یک بدافزار ناشناخته موفق نشود به سرعت طیف گسترده‌ای از سامانه‌ها را قربانی کند.

امروزه میلیون‌ها کاربر در سراسر جهان ایمیل خود را از طریق آفیس 365 چک می‌کنند. جالب آن‌که برخی از کاربران هیچ‌گاه متوجه نمی‌شوند، اما آفیس 365 برای شناسایی و مسدود کردن سوءاستفاده‌ها یک پردازش امنیتی روی داده‌ها انجام می‌دهد. به عنوان مثال، اگر یک آدرس ایمیل در یک شرکت به‌طور ناگهانی ایمیلی برای گروه بزرگی از مردم ارسال کند و آن ایمیل حاوی یک سند ورد با قابلیت اجرای ماکروها باشد، کاری نیست که یک کاربر به‌طور عادی انجام دهد. آفیس 365 می‌تواند به سرعت این موضوع را تشخیص داده و سند را به بخش امنیتی که در وضعیت آفلاین قرار دارد ارسال می‌کند، آن‌را باز می کند(آن‌را اجرا یا اگر ضمیمه‌ای با قابلیت اجرایی در آن قرار داشته باشد، آن‌را در منطقه امن اجرا می‌کند) و بررسی می‌کند که آیا این فایل به بدافزاری آلوده شده است یا خیر. اگر این‌گونه باشد، آفیس 365 فایل را بلوکه می‌کند و مانع شیوع این رفتار فاجعه‌بار می‌شود. تمامی این‌کارها بدون دخالت کاربر یا کارمندان فناوری‌اطلاعات انجام می‌شود. اگر یکی از کارمندان شرکت بدافزار جدید را دریافت کرد و این موضوع توسط مایکروسافت شناسایی شد، به سرعت ایمیل و فایل آلوده را بلکوه می‌کند تا سایر مشتریانی که ایمیل آن‌ها توسط فناوری ابرمحور مایکروسافت میزبانی می‌شود قربانی نشوند. این راهکار شگفت‌انگیز است.

این ایده در مورد ضدویروس دیفندر نیز صادق است، به‌طوری که شما به دیفندر اجازه می‌دهید با منابع ابری مایکروسافت ارتباط برقرار کند و اطلاعات را ارسال کند.

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:

13 آبان 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16238/%DA%86%D9%87-%D9%82%D8%A7%D8%A8%D9%84%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%A7%D8%B2-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF%D8%9F