ویندوز Server Core 2019 چیست و چرا نقش مهمی در آینده خواهد داشت؟

یکی از دلایل دور شدن از رابط گرافیکی افزایش قابلیت‌های خودکارسازی و گسترش‌پذیری است. هنگامی که همه سرورهای ما به شکل یکسان طراحی شوند به ما قدرت مانور بیشتری شبیه به سرویس‌های ابری می‌دهند. به‌کارگیری حداقلی منابع، کارکرد ساده‌تر و عدم نیاز به مراجعه به پنجره‌های مختلف و کلیک کردن روی گزینه‌های مختلف باعث شده، Server Core به تدریج جای خود در بازار را پیدا کند. مایکروسافت می‌گوید: «در آینده کسب‌وکارها به سراغ سرورهایی می‌روند که فاقد رابط گرافیکی (GUI) هستند.»

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

تجزیه و تحلیل تهدید پیشرفته

یکی از جالب‌ترین ویژگی‌های امنیتی که طی چند سال گذشته مایکروسافت ارائه کرده ویژگی (ATA) سرنام Advanced Threat Analytics است. به عبارت دقیق‌تر ATA یک ویژگی یا عملکردی نیست که برای سیستم‌عامل ویندوز سرور ساخته شده باشد، بلکه یک مولفه داخلی است که برای ایمن‌سازی محصولات مایکروسافت ارائه شده است. ATA بر تمامی ترافیک اکتیو دایرکتوری نظارت می‌کند و در مورد رفتارهای مخاطره‌آمیز یا رفتارهای غیرعادی به شکل بلادرنگ هشدارهایی برای مدیر شبکه ارسال می‌کند.

عملکرد ATA به راحتی قابل درک است و به همین دلیل باعث شده مورد توجه مدیران شبکه قرار گیرد. مولفه فوق در پس‌زمینه فرآیندها و پردازه‌ها وارد می‌شود و سعی می‌کند اطلاعاتی در مورد عملکرد پردازه‌ها به‌دست آورد که در نوع خود جالب توجه است. شما شبکه خود را پیکربندی می‌کنید تا تمام ترافیکی که به کنترل‌کننده دامنه وارد یا از آن خارج می‌شود را بررسی کنید. مطمئن‌ترین راه برای تحقق این موضوع در سطح شبکه پیاده‌سازی حالت قرینه‌ای پورت است تا تمامی بسته‌هایی که به کنترل‌کننده دامنه وارد می‌شود توسط ATA بررسی شوند، اما در سطحی که یک مهاجم قادر به مشاهده آن نباشد. به این ترتیب ، حتی اگر یک هکر یا فرد خاطی در شبکه شما باشد و در جست‌وجوی مکانیزم‌های امنیتی باشد که از شبکه محافظت می‌کنند، بازهم ATA قابل مشاهده نخواهد بود. با این وجود ، قرینه‌سازی درگاه برای نظارت بر ترافیک کاری نیست که شرکت‌های کوچک قادر به انجام آن باشند، زیرا راه‌اندازی آن پیچیده است و دوم آن‌که نصب یک عامل ATA روان که بدون مشکل روی کنترل‌کننده دامنه اجرا شود فرآیند ساده‌ای نیست. این عامل باید اطلاعات لازم را به سرورهای پردازشی ATA ارسال کند.

سرورهای پردازشی ATA تمامی داده‌ها را دریافت می‌کنند و سپس شروع به پیدا کردن الگوها می‌کنند. اگر کارمند A از رایانه رومیزی به‌نام BETTY-PC و تبلتی به‌نام BETTY-TABLET استفاده کند، ATA این الگو را خواهد دید و حساب کاربری وی را با آن دستگاه‌ها مرتبط می‌کند. رویکرد فوق قادر است از الگوهای ترافیک عادی نیز مراقبت

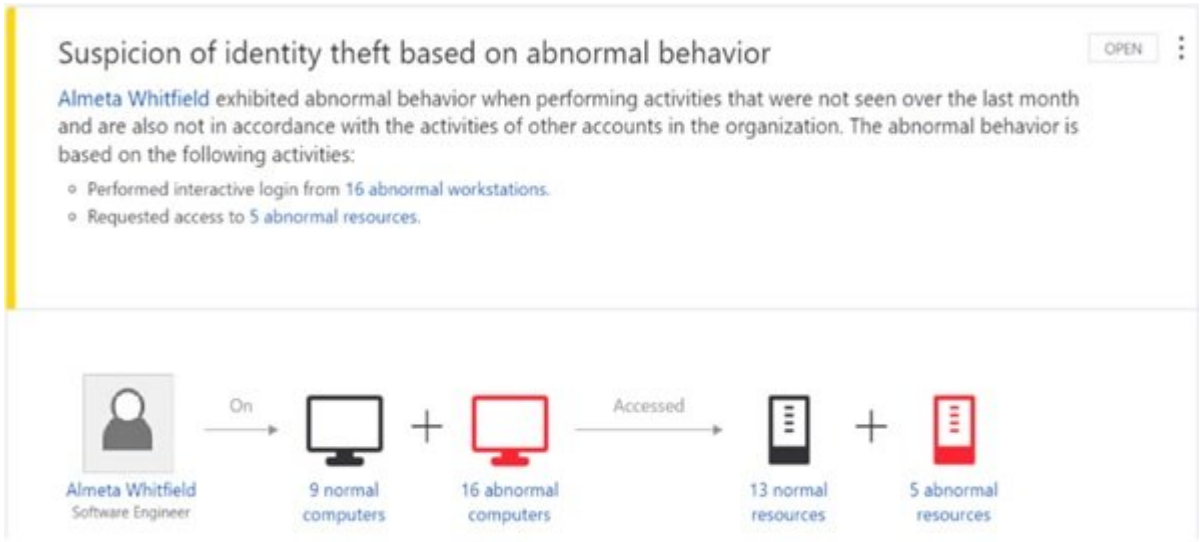
کند. کارمند A معمولا حدود ساعت 8 صبح کار را آغاز می‌کند و ترافیک کاری او حدود ساعت 5 بعد پایان می‌یابد. او به‌طور معمول به چند سرور فایل و یک سرور SharePoint دسترسی دارد. بعد از گذشت یک هفته از جمع‌آوری و نظارت بر داده‌ها، ATA ایده خوبی در ارتباط با عملکرد کارمند A پیدا می‌کند.

یک شب اتفاقی می‌افتد. ATA می‌بیند، یکسری اتفاقات غیر معمول در ارتباط با گذرواژه حساب‌های کاربری کارمند A در حال انجام است. این موضوع به خودی خود ممکن است مشکل خاصی نباشد، اما پس از گذشت مدت زمانی و به شکل ناگهانی ترافیکی از سوی کارمند A وارد ترمینال یک سرور می‌شود که در حالت عادی نباید این اتفاق رخ دهد، زیرا اعتبارنامه کارمند A برای دسترسی به کنترل‌کننده دامنه استفاده می‌شود. به وضوح مشخص است که حمله‌ای در حال انجام است. ابزارهای از پیش ساخته شده در اکتیو دایرکتوری نمی‌توانند اطلاعات دقیقی در اختیار ما قرار دهند. ما ممکن است با بررسی رخدادها و گزارش‌ها تنها شکست در ورود گذرواژه‌ها برای دسترسی به حساب‌های کاربری را مشاهده کنیم اما دلیل بروز این مشکل را پیدا نمی‌کنیم. این موضوع می‌تواند سرآغازی بر یک نقض بسیار بزرگ باشد که هرگز اطلاعاتی در مورد آن به دست نخواهیم آورد. در حالی که عملکرد ATA در این زمینه متفاوت است.

رابط مدیریتی ATA عملکردی شبیه به فیدهای یک رسانه اجتماعی دارد که به شکل بلادرنگ به‌روزرسانی می‌شوند. یک مدیر شبکه با نگاه کردن به فید رسانه‌ای ATA قادر است همه اتفاقات را مشاهده کند و به سرعت تشخیص دهد که یک حساب کاربری هک شده یا گذرواژه حساب لو رفته و برای دسترسی به کنترل‌کننده دامنه استفاده شده است. هیچ ابزاری نیست که به خوبی ATA بتواند ترافیک اکتیو دایرکتوری را رصد کند و نکاتی در ارتباط با الگوها و رفتارهای غیرعادی به دست آورد.

ATA هنوز هم یک فناوری جدید است و باید برخی از ویژگی‌های آن بهبود پیدا کند. در شکل زیر رابط وب ATA را مشاهده می‌کنید که چگونه فیدهای آن به سبک رسانه‌های اجتماعی تصویری روشن ارائه می‌کنند. در تصویر زیر یک حمله فرضی را مشاهده می‌کنید که به شکل هدفمند توکن Kerberos یک کاربر سرقت رفته و سپس برای دسترسی به برخی از فایل‌های محرمانه که تنها کاربر دمی آلبوز می‌توانست به آن‌ها دسترسی داشته باشد روی یک کامپیوتر دیگر استفاده شده است. در حالی که ATA این فعالیت را متوقف نکرد، اما به سرعت و در عرض چند ثانیه در یک فید هشداردهنده نشان می‌دهد یک حمله Pass-the-Ticket رخ داده است.

مثال دیگری در این زمینه به کاربری به نام آلماتا وایتفیلد اشاره دارد که به‌طور ناگهانی به 16 رایانه دسترسی پیدا می‌کند که معمولا به آن‌ها دسترسی ندارد، پرچم قرمز بزرگ دیگری که مرتبط با حساب کاربری او است توسط ATA نشان داده می‌شود.



برای کسب اطلاعات بیشتر و به‌کارگیری ATA پیشنهاد می‌کنم به **این آدرس** مراجعه کنید.

بهترین الگوهای عمومی امنیتی

برخی اوقات برای بهبود امنیت سامانه‌های خود باید به جای اعتماد به پردازه‌ها و عملکردهای سیستم‌عامل فقط به خودمان اعتماد کنیم. از آن جمله به موارد زیر می‌توان اشاره کرد: آیا کلیه کارمندان فناوری‌اطلاعات مجوزهای مدیریتی در اختیار دارند؟ آیا هیچ یک از کارمندان فناوری‌اطلاعات به گذرواژه حساب مدیر دامنه داخلی دسترسی دارند؟ آیا کارمندانی دارید که برای ورود به سیستم مجوز مدیریتی داشته باشند؟ اگر پاسخ شما به این پرسش‌ها مثبت است، بهتر است یک بازنگری جدی در خط‌مشی‌های امنیتی داشته باشید.

متأسفانه، در بیشتر شبکه‌ها یک چنین دسترسی‌هایی وجود دارد. هنوز هم مهندسان برای پیکربندی سرورهای جدید از حساب دامنه مدیر استفاده می‌کنند. این بدان معنا است که آن‌ها نه تنها به مهم‌ترین حساب کاربری شبکه دسترسی دارند و از این مجوز برای انجام کارهای روزانه استفاده می‌کنند، بلکه بدان معناست که اگر مشکلی پیش آمد یک نفر واحد پاسخ‌گو نخواهد بود. وقتی من سرور جدیدی را تنظیم می‌کنم یا با استفاده از حساب اصلی مدیر تغییراتی در سرور موجود ایجاد می‌کنم و مشکل بزرگی رخ می‌دهد هیچ کس نمی‌تواند ثابت کند که من این کار را انجام داده‌ام. استفاده از حساب‌های کاربری عمومی روشی مطمئن برای روشن کردن فردی است که مشکلی را به وجود آورده است. در ارتباط با سمت کلاینت، آیا کاربران برای دسترسی به سامانه‌های خود به مجوز مدیریتی نیاز دارند؟ در حالت کلی کاربران عادی و کاربرانی با مجوز دسترسی بالا هر یک ممکن است شکافی در مکانیزم‌های امنیتی به وجود آورند که به ویروس‌ها اجازه می‌دهند خودشان را روی سامانه‌ها نصب کنند.

هیچ‌گاه برای وب‌گردی در اینترنت از ویندوز سرور استفاده نکنید

سرپرستان شبکه بیشتر اوقات خود را در سرور سپری می‌کنند و خیلی اوقات مجبور می‌شوید از مرورگر وب برای بررسی موضوع استفاده کنید. از آن‌جایی که اینترنت اکسپلورر در ویندوز سرورها وجود دارد، گاهی اوقات سریع‌ترین و ساده‌ترین راه به‌کارگیری کنسول سرور برای ورود به اینترنت است. پیشنهاد می‌کنم چنین کاری را انجام ندهید، زیرا بیشتر دستگاه‌های تحت شبکه بدون محافظت از ضدویروس استفاده می‌شوند. همین موضوع در ارتباط با فیلترهای اینترنت صدق می‌کند. ما همیشه فکر می‌کنیم ترافیک کلاینت از طریق پروکسی به شبکه سازمانی وارد می‌شود و در نتیجه این موضوع را بررسی نمی‌کنیم که آیا ترافیک سرور به همان روش به سمت خارج حرکت می‌کند یا خیر. لازم است به این نکته دقت کنید که همواره یک حمله مرد میانی ممکن است از طریق سایت‌ها به راحتی برای سرور شما دردسرساز شود.

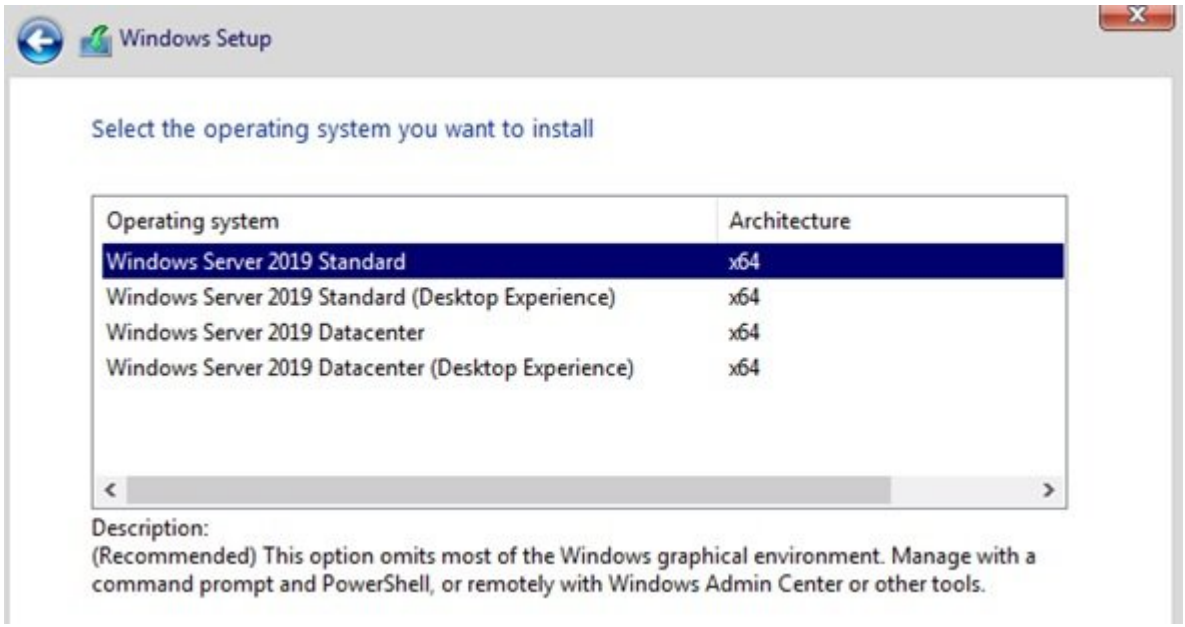
نکات دیگری نیز در ارتباط با رعایت نکات ایمنی همچون حساب‌های کاربری، تنظیم آن‌ها مجوزهای مدیریتی، کنترل دسترسی مبتنی بر نقش نیز وجود دارد که ما تحقیق در ارتباط با این موضوعات را به شما واگذار می‌کنیم و به سراغ مبحث Server Core می‌رویم.

Server Core

در 20 سال گذشته، شاهد پیشرفت‌های زیادی در ارتباط با سیستم‌عامل‌های مایکروسافت بودیم. پیشرفت نکات مثبت و منفی دارد. نکات مثبت می‌توانند ویژگی‌ها و پیشرفت‌های جدیدی باشد که زندگی را برای ما آسان‌تر می‌کند و نکات منفی می‌تواند رابط‌های گرافیکی که حافظه را سریع مصرف می‌کنند و ساختارهای فایلی پیچیده باشند.
خوشبختانه هر نسخه جدیدی که عرض می‌شود تنها به مقدار کمی توان محاسباتی بیشتر و کمی فضای هارددیسک نسبت به نسخه قبلی نیاز دارد. مایکروسافت برای برخی از شرکت‌ها که حیطه کاری آن‌ها گسترده نیست یک نسخه کوچکتر از ویندوز سرور 2019 ارائه کرده که Server Core نام دارد. البته Server Core مدت زمان مدیدی است که وجود دارد و برای کسب‌وکارهایی آماده شده که به دنبال اجرای روان یک نسخه کوچک‌تر، روان‌تر، کارآمد و ایمن از ویندوز سرور هستند.

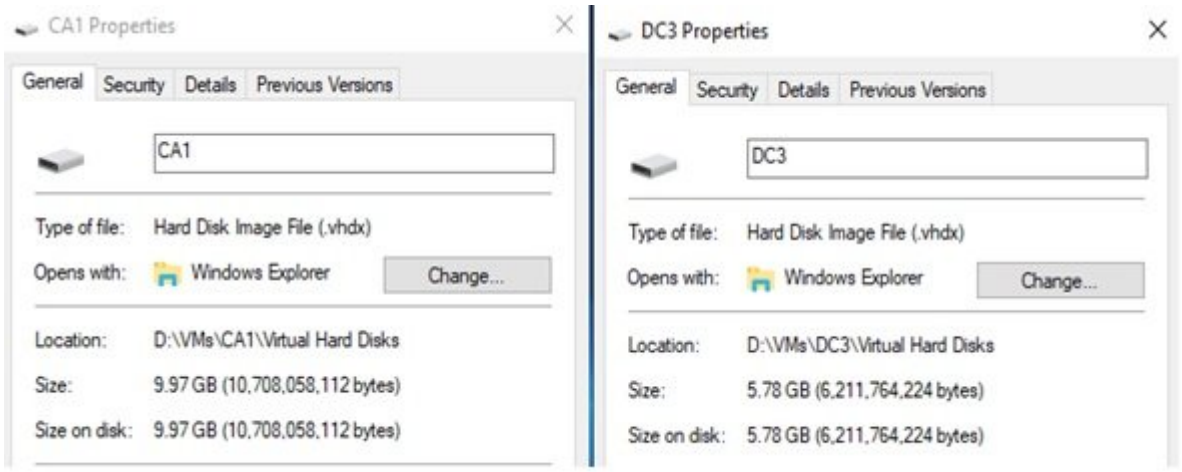
چرا از سرور هسته استفاده می‌کنیم؟

چرا باید به Server Core توجه کنیم؟ Server Core مدلی از ویندوز سرور است که در اختیار کسب‌وکارها قرار دارد، هرچند بیشتر سرپرستان شبکه از اعتماد کردن به آن هراس دارند. بیشتر کسب‌وکارها ترجیح می‌دهند از مدل دارای رابط گرافیکی یا همان Desktop Experience استفاده کنند. همه شرکت‌ها می‌دانند که Server Core چیست، اما تعدا کمی از آن استفاده می‌کنند. چرا ما نیاز به استفاده از Server Core داریم؟ مایکروسافت می‌گوید: «در آینده کسب‌وکارها به سراغ سرورهایی می‌روند که فاقد رابط گرافیکی (GUI) هستند. در زمان نصب ویندوز سرور، پنجره نصب گزینه‌های زیر را در اختیارتان قرار می‌دهد:



یکی از دلایل دور شدن از رابط گرافیکی افزایش قابلیت‌های خودکارسازی و گسترش‌پذیری است. هنگامی که همه سرورهای ما به شکل یکسان طراحی شوند به ما قدرت مانور بیشتری شبیه به سرویس‌های ابری می‌دهند.
به‌کارگیری حداقلی منابع، کارکرد ساده‌تر و عدم نیاز به مراجعه به پنجره‌های مختلف و کلیک کردن روی گزینه‌های مختلف باعث شده، Server Core به تدریج جای خود در بازار را پیدا کند.

مزایای دیگری نیز در ارتباط با Server Coreوجود دارد. عدم نیاز به فضای ذخیره‌سازی زیاد، کاهش مصرف حافظه و کاهش سطح حملات در مقایسه با نمونه سنتی از ویژگی‌های شاخص این گونه از ویندوز سرور است. به همین دلیل است که مایکروسافت Server Core را آینده می‌داند. اجازه دهید تفاوت در حجم را با ذکر مثالی روشن کنیم.
ویندوز سرور 2019 مبتنی بر رابط گرافیکی در حال اجرا به چیزی در حدود 10 گیگابایت فضای هارد دیسک نیاز دارد (در شکل زیر CA1)، اما در مقابل Server Core تنها 5.8 گیگابایت فضای ذخیره‌سازی نیاز دارد که به عبارت دقیق‌تر یک کاهش 40٪ فضا را نشان می‌دهد (DC3).



امکان سوییچ کردن به عقب و جلو دیگر وجود ندارد

اگر تجربه کار با ویندوز سرور Windows Server 2012 R2 را داشته باشید به خوبی می‌دانید که امکان سوییچ کردن وجود داشت. شما می‌توانستید یک سرور جدید مبتنی بر یک دسکتاپ کامل ایجاد کرده و در ادامه به حالت Server Core سوییچ کنید. برعکس این قضیه نیز صادق بود و امکان سوییچ از Server Core به حالت گرافیکی وجود داشت، اما دیگر این‌گونه نیست. از این پس نمی‌توانید میان سیستم‌عامل‌های سوییچ کنید. بنابراین باید در هنگام نصب سیستم‌عامل به دقت موضوعات را سنجیده باشید. اگر یک سرور را به عنوان Server Core پیاده‌سازی می‌کنید، سرور باید تا انتها از Server Core استفاده 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:

06 آذر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16336/%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-2019-server-core-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%86%D8%B1%D8%A7-%D9%86%D9%82%D8%B4-%D9%85%D9%87%D9%85%DB%8C-%D8%AF%D8%B1-%D8%A2%DB%8C%D9%86%D8%AF%D9%87-%D8%AE%D9%88%D8%A7%D9%87%D8%AF-%D8%AF%D8%A7%D8%B4%D8%AA%D8%9F