بهبود سطح ایمنی شبکه‌های نرم‌افزار محور و ابر ترکیبی

امنیت در شبکه‌های نرم‌افزارمحور با ویندوز سرور 2019

در عصری که محاسبات مدرن ابری توانسته‌اند بهره‌وری و سرعت انجام کارها را افزایش دهند، کسب‌وکارهای بیشتر و بیشتری به دنبال آن هستند تا فعالیت‌های خود را به سمت ابرهای عمومی، خصوصی یا ترکیبی انتقال دهند.
شرکت‌ها تنها زمانی با خیال آسوده به سراغ فناوری‌های ابرمحور می‌روند که اطمینان حاصل کنند داده‌های آن‌ها به بهترین شکل محافظت شده و نشتی اطلاعات، کسب‌وکار آن‌ها را تهدید نمی‌کند. بر همین اساس، نگرانی امنیتی را باید یکی از عوامل بازدارنده عزیمت کسب‌وکارها به فناوری‌های ابری در نظر بگیریم. مدیران ارشد سازمان‌ها اغلب این پرسش‌ها را مطرح می‌کنند که ابر چقدر برای انجام فعالیت‌های کوچک و بزرگ آن‌ها ایمن است؟ مکانیزم‌های امنیتی ابر می‌توانند به درستی مانع سرقت اطلاعات و جاسوسی‌های صنعتی شوند؟ آیا فناوری‌های ابرمحور می‌توانند بدون مشکل با پروتکل IPv6 کار کنند؟

شبکه نرم‌افزارمحور ویندوز سرور 2019 ویژگی‌های متعددی برای بهبود سطح اعتماد مشتریان ارائه کرده است. قابلیت‌هایی که تضمین می‌کنند سازمان‌ها می‌توانند در هر دو حوزه انجام فعالیت‌های درون سازمانی یا ارائه خدمات برون‌سازمانی به مشتریان خود، بدون نگرانی از بابت نشتی اطلاعات، فعالیت‌های روزانه را انجام دهند.
اکنون، این پیشرفت‌های امنیتی با پلت‌فرم جامع **شبکه نرم‌افزارمحور** مایکروسافت یکپارچه شده و در اختیار کسب‌وکارها قرار گرفته است.

رمزگذاری زیر شبکه‌ها

چه تعداد از برنامه‌هایی که روی شبکه شما اجرا می‌شوند از رمزگذاری استفاده می‌کنند؟ چه تعداد از این برنامه‌های کاربردی از روش‌های رمزنگاری که هنوز هم ایمن هستند استفاده می‌کنند؟ به احتمال زیاد برخی از این برنامه‌های کاربردی آلوده به آسیب‌پذیری‌هایی هستند که باعث به سرقت رفتن یا نشتی اطلاعات می‌شوند.
مدیر یک شبکه می‌تواند برنامه‌های کاربردی که تحت شبکه اجرا می‌شوند را پیدا کرده، الگوهای رمزنگاری برنامه‌ها را تجزیه و تحلیل کرده و آن‌ها را به‌روز کند، اما به جای این فرآیند زمان‌بر و خسته کننده، بهتر نیست رمزگذاری در سطح **شبکه نرم‌افزارمحور** انجام شود؟ با رمزگذاری زیرشبکه در یک شبکه نرم‌افزارمحور مبتنی بر سیستم‌عامل ویندوز سرور 2019، هر بسته‌ای که ماشین مجازی را ترک می‌کند، به‌طور خودکار رمزگذاری شده و به ایمن‌ترین شکل به مقصد یا سایر نقاط پایانی درون همان شبکه تحویل داده می‌شود. یک چنین سازوکاری در برابر آسیب‌پذیری‌ها سطح بالایی از امنیت را ارائه می‌کند، به این دلیل که اگر یک آسیب‌پذیری شناسایی شود، فرآیند به‌روزرسانی در سریع‌ترین زمان انجام می‌شود و همه برنامه‌های کاربردی به شکل خودکار وصله‌های امنیتی را دریافت خواهند کرد. رویکرد فوق در ارتباط با هر زیرشبکه‌ای در یک شبکه مجازی با تعیین یک گواهی رمزنگاری برای استفاده از ویژگی فوق و تظیم Encryption در وضعیت فعال قابل استفاده است. رند موریمتو، مدیرعامل اجرایی شرکت Convergent Computing می‌گوید: «سازمان‌ها به دنبال مکانیزم‌های محافظتی از طریق کنترل‌های

نرم‌افزارمحور و حذف پیچیدگی‌ها هستند و این درست همان نقطه‌ای است که رمزگذاری شبکه مجازی به میزان قابل توجهی به این نیاز آن‌ها پاسخ داده و اجازه می‌دهد سازمان‌ها به ساده‌ترین شیوه ممکن امنیت کسب‌وکار خود را بهبود بخشند.»

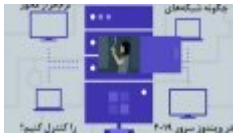
مطلب پیشنهادی

آموزش رایگان ویندوز سرور منطبق با سرفصل‌های بین المللی – 19
آشنایی با انواع و نحوه کار گواهی‌نامه‌های SSL در ویندوز سرور 2019

Firewall logging

Microsegment راهکاری برای ساخت نواحی ایمن در مراکز داده و استقرارهای ابری است که به شرکت‌ها اجازه تفکیک فعالیت‌ها و کارهای مهم از یکدیگر را داده و به ایمن‌سازی جداگانه هر یک از فرآیندهای کاری می‌پردازد. این راهکار به منظور بهبود امنیت در سطح شبکه انجام می‌شود. microsegment با ایجاد کرانه‌های ایمن سعی می‌کند از شبکه در برابر حملات محافظت کند. به نظر می‌رسد راهکار فوق جامع و قدرتمند است، اما چگونه می‌توان اطمینان حاصل کرد راهکار فوق به درستی کار می‌کند؟ در زمان بروز یک حمله هکری چگونه این مسئله باید گزارش شود؟ اگر یک نقض داده‌ای رخ داد، چگونه فرآیند تجزیه و تحلیل پس از حمله انجام می‌شود و چقدر طول می‌کشد؟ Firewall logging ویندوز سرور 2019 برای پاسخ‌گویی به یک چنین پرسش‌هایی طراحی شده است.
در **ویندوز سرور 2019، شبکه نرم‌افزارمحور** به میزبان Hyper-V اجازه می‌دهد، گزارش‌های دیوارآتش سازگار با قالب Azure Network Watcher را تولید کند. راهکار فوق اکوسیستمی از ابزارهای مرتبط با مولفه Network Watcher است که اجازه می‌دهد فرآیند پیاده‌سازی شبکه نرم‌افزارمحور مبتنی بر ویندوز سرور به ساده‌ترین شکل پیاده‌سازی شود.
ویژگی فوق به دور از هرگونه پیچیدگی است، به این دلیل که تنها با یک‌بار اعمال پیکربندی روی یک کنترل‌کننده شبکه، شما می‌توانید فرآیند ورود فردی به شبکه را در مجموعه قواعد Access Control List وارد کنید. در این حالت مولفه‌هایی که هماهنگ با این قواعد هستند به‌طور خودکار به سیستم وارد می‌شوند. رند موریمتو، مدیرعامل اجرایی شرکت Convergent Computing می‌گوید: «تنظیمات شبکه نرم‌افزارمحور ویندوز سرور 2019 دارای یک مولفه بسیار جالب در ارتباط با حسابرسی دیوارآتش است که قادر است همه ارتباطات درون شبکه نرم‌افزارمحور را ثبت و ضبط کرده و گزارش کاملا دقیقی را ارائه کند.»

مطلب پیشنهادی



آموزش رایگان ویندوز سرور منطبق با سرفصل‌های بین المللی – 32
چگونه شبکه‌های نرم‌افزار محور در ویندوز سرور 2019 را کنترل کنیم؟

Fabric ACLs

ویندوز سرور 2016 به منظور بهبود امنیت شبکه‌های مجازی راهکار مبتنی بر خودکارسازی به‌کارگیری فهرست‌های کنترل دسترسی (ALCs) به ماشین‌های مجازی (VM) برای اتصال به زیرشبکه‌های مجازی را فراهم کرد. ویندوز سرور 2019 این قابلیت را به شبکه‌های fabric گسترش داد تا مدیران شبکه بتوانند دسترسی به ماشین‌های زیرساخت را محدود کنند تا فرآیند مدیریت و خودکارسازی با اضافه کردن فهرست‌های کنترل دسترسی به زیرشبکه‌های منطقی ساده‌تر شود. این حرف به معنا این است که هر ماشین مجازی مدیریت شده با **شبکه نرم‌افزارمحور** متصل به یک شبکه محلی مجازی قادر است به شکل خودکار فهرست کنترل دسترسی را دریافت کرده و از آن استفاده کند.

Virtual Network Peering

اولین مکانیزم امنیتی یک شبکه نرم‌افزارمحور که به‌نام کرانه امنیتی اولیه شبکه نرم‌افزارمحور شناخته می‌شود، ایزوله‌سازی است که شبکه مجازی آن‌را ارائه می‌کند، اما گاهی اوقات لازم است کرانه برداشته شود تا دو شبکه مجازی بتوانند با یکدیگر ارتباط برقرار کنند. به‌طور مثال، یک پایگاه داده در یک شبکه مجازی مستقر کرده‌اید، اما در نظر دارید از طریق برنامه‌های دیگری که درون یک شبکه مجازی جداگانه قرار دارند به پایگاه داده دسترسی پیدا کنید. Virtual Network Peering برای چنین مواقعی طراحی شده است. قابلیت فوق به روترهای مجازی در شبکه‌های مجازی اجازه می‌دهد با یکدیگر در ارتباط باشند، بدون آن‌که لزومی داشته باشد این ارتباط از طریق یک گیت‌وی انجام شود. راهکاری که توان عملیاتی را افزایش داده و تاخیر زمانی میان شبکه‌های مجازی را کاهش می‌دهد.

فیلیپس موس، مدیر اجرایی Acuutec می‌گوید: «Virtual Network Peering راهکاری برای ساده‌سازی استقرار، مدیریت و حذف هزینه‌های اضافی است. سناریوهای مختلفی بر پایه این قابلیت مفید قابل اجرا هستند. پس از ادغام شدن دو شبکه مجزا با هدف اتصال به یکدیگر، دو شبکه فوق به صورت یک شبکه واحد نشان داده می‌شوند.

یکسان‌سازی شبکه‌های مجازی مزایای متعددی به همراه دارد که همتا به همتا شدن ترافیک میان ماشین‌های مجازی در شبکه‌های مجازی که فقط از طریق زیرساخت ستون فقرات (Backbone) و با اتکا بر آدرس‌های آی‌پی خصوصی هدایت می‌شوند، اتصال با کمترین زمان تاخیر و دسترسی به حداکثر پهنای باند میان منابع در شبکه‌های مجازی مختلف، برقراری ارتباط میان منابع موجود در یک شبکه مجازی با منابعی که درون شبکه مجازی دیگر قرار دارند و عدم وجود زمان غیرفعال (Downtime) در زمان ایجاد ارتباط نظیر به نظیر میان منابع شبکه‌های مجازی موجود، گوشه‌ای از توانایی‌های قابلیت فوق است.»

مطلب پیشنهادی

آموزش رایگان ویندوز سرور منطبق با سرفصل‌های بین المللی – 09
آموزش ویندوز سرور: با User Accounts و Security Groups در ویندوز سرور 2019

پشتیبانی از IPv6

در مقطع فعلی ممکن است کسب‌وکار شما به IPv6 نیازی نداشته باشد، اما برای برخی از کسب‌وکارها به ویژه در خارج از ایران اضافه شدن پشتیبانی از IPv6 به شبکه نرم‌افزار محور یک قابلیت ارزشمند است. در حالی که ویژگی فوق یک قابلیت امنیتی نیست، اما همراه با ویندوز سرور 2019، شبکه نرم‌افزارمحور می‌تواند از IPv6 برای فضاهای آدرس شبکه مجازی، آی‌پی‌های مجازی و شبکه‌های منطقی استفاده کند. تمامی قابلیت‌های امنیتی شبکه نرم‌افزار محور با آدرس‌های IPv6، زیر شبکه‌ها و همچنین فهرست‌های کنترل دسترسی و مسیریابی تعریف شده توسط کاربر کار می‌کنند.

اگر هنوز هم از بیلدهای پیش‌نمایش یا نسخه‌های آزمایشی ویندوز سرور 2019 استفاده می‌کنید، لازم است آن‌ها را کنار گذاشته و نسخه رسمی ویندوز سرور 2019 را استفاده کنید تا بتوانید از ویژگی فوق استفاده کنید. پس از نصب بدون مشکل می‌توانید از زیرشبکه Ipv6 روی زیرشبکه مجازی خودتان استفاده کرده و آدرس‌های Ipv6 را به ماشین‌های مجازی اختصاص دهید. درست به همان شکلی که از IPv4 استفاده می‌کنید.

مطلب پیشنهادی

معرفی مفاهیم شبکه به زبان ساده - ip address
آشنایی کامل با انواع آدرس آی‌پی - IPv4 و IPv6

کلام آخر

همان‌گونه که مشاهده کردید، مایکروسافت روی مبحث محافظت از شبکه‌های نرم‌افزارمحور و بهبود سطح و قابلیت‌های امنیتی در ویندوز سرور 2019 سرمایه‌گذاری‌های قابل توجهی انجام داده است. خلاصه‌ای از اقدامات مایکروسافت در خصوص **شبکه‌های نرم‌افزارمحور** و امنیت آن‌ها در **ویندوز سرور 2019** عبارتند از:

شما می‌توانید داده‌ها را با استفاده از رمزنگاری شبکه مجازی انتقال داده و مانع به سرقت رفتن اطلاعات یا جاسوسی‌های صنعتی شوید.
شما می‌توانید ترافیک روی میزبان را ثبت و ضبط کنید تا برای عیب‌یابی، حسابرسی یا انجام یک تجزیه و تحلیل ساده از آن استفاده کنید.
اکنون می‌توانید فهرست‌های کنترل دسترسی امنیتی را برای شبکه‌های فیزیکی fabric استفاده کنید.
شما می‌توانید ارتباط امن و با عملکرد بالا بین شبکه‌های مجازی را فعال کنید
شما می‌توانید از فرآیند آدرس‌دهی مبتنی بر IPv6 برای شبکه‌های مجازی خود استفاده کنید
تمامی این پیشرفت‌ها و قابلیت‌ها با هدف جلب اعتماد مشتریان در زمان انجام فعالیت‌های مبتنی بر ابر ترکیبی انجام شده است. بدون شک کاربران سیستم‌عامل ویندوز سرور 2019 می‌توانند مطمئن باشند که فعالیت‌های آن‌ها در ویندوز سرور 2019 به ایمن‌ترین شکل انجام می‌شود.

برای مطالعه تمام بخش‌های آموزش ویندوز سرور 2019 تهیه شده در سایت ماهنامه شبکه اینجا کلیک کنید.

تاریخ انتشار:

14 آذر 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16185/%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%AF%D8%B1-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%86%D8%B1%D9%85%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1%D9%85%D8%AD%D9%88%D8%B1-%D8%A8%D8%A7-%D9%88%DB%8C%D9%86%D8%AF%D9%88%D8%B2-%D8%B3%D8%B1%D9%88%D8%B1-2019