معیارهای انتخاب یک ضدویروس مناسب چیست؟

همواره یکی از مهم‌ترین پرسش‌هایی که مدیران شبکه از خودشان می‌پرسند، این است: **"کدام آنتی‌ویروس مناسب شبکه من است؟"**

شمار پاسخ‌هایی که برای این پرسش می‌توان یافت، گاهی به اندازه ای فراوان است که از تعداد شرکت‌های تولید کننده آنتی‌ویروس‌ها بیشتر می‌شود! از این روی روند گزینش آنتی‌ویروس، گاهی چنان پیچیده می‌شود که شاید مدیر شبکه را به جایی برساند که از خیر آن بگذرد و هرآنچه دم دست است را موقتی هم که شده در شبکه راه بیاندازد.

اینکه کدام یک از آنتی‌ویروس‌ها به راستی نیاز ما را پوشش می‌دهند یا توان کدام یک از آنها واقعاً ارزش بهایی که بابت آن پرداخت می‌شود را دارد، نیاز به بررسی‌های موشکافانه‌ای دارد.

در زیر پرسش‌هایی گردآوری شده است که می‌تواند در این راه کارشناسان را یاری رساند:

۱- مهم است نقش Firewall را بهتر اجرا کند یا محافظت از فایل‌های موجود؟

آگاه باشید که سازمان‌های گوناگون، تجمع اطلاعاتی متفاوت و البته مسیرهای ورود و خروج اطلاعاتی متفاوتی دارند. بیمارستان‌ها، کارخانه‌ها و سازمان‌های نظامی نوع اندوختن اطلاعاتشان و روش ورود و خروج داده‌هایشان از شبکه با هم فرق دارند.

۲- میزان درآمد سازمان چه اندازه است؟

درآمد سازمان، سقف سرمایه‌گذاری امنیتی را تعیین می‌کند. به گویش دیگر معین می‌کند که تا چه اندازه باید برای امنیت پول پرداخت کرد و این سیستم امنیتی باید از چه اندازه سرمایه پاسداری کند.

۳- سازمان به راستی چه اندازه بر روی امنیت سرمایه گذاری خواهد کرد؟

گاهی سرمایه‌ای که سازمان می‌خواهد برای امنیت کنار بگذارد، برابر با توان یا نیاز آنها نیست. گاهی حتی ممکن است برای امنیت وادار به دریافت وام هم شود، و البته گاهی هم ممکن است که بسیار کمتر از نیاز واقعی و توان پرداختی اش سرمایه‌گذاری کند.

۴- این آنتی‌ویروس باید امنیت چندین کاربر را تامین کند؟

شمار کم یا بسیار کاربر، گزینه‌های متفاوتی از آنتی‌ویروس را نیاز دارد. گاهی یک سیستم امنیتی بسیار پیچیده و بزرگ، برای یک شبکه کوچک تا اندازه ای دست و پا گیر می‌شود که شبکه را تا اندازه از کار افتادن آسیب‌پذیر می‌کند. و یا برعکس، گزینش یک آنتی‌ویروس ساده برای شبکه ای با شمار بسیار بالای کاربر، به هنگام بروز مشکل در شبکه یا حتی نیاز به یک تنظیم خاص، مدیر شبکه را به پریشانی بکشاند!

۵- سازمان در آینده چند کاربر خواهد داشت؟

آینده نگری در گزینش آنتی‌ویروس، مدیر شبکه را از تلاش‌های دوباره و دوباره کاری‌ها در آینده نجات می‌دهد.

۶- شبکه در کدام شهر و کشور واقع است؟

این که شبکه در کدام موقعیت جغرافیایی قرار دارد، میزان اهمیت امنیتی و در نتیجه کیفیت آنتی‌ویروس را معین می‌کند. امنیت در چین، هند، سوئیس، برزیل و ایران و یا شهرهای تهران، بندرعباس، زاهدان و عسلویه حال و هوایی کاملاً متفاوت دارد.

۷- کدام توانایی آنتی‌ویروس بیشتر نیاز است؟ فایروال، IPS، امنیت فایل ها، امنیت ایمیل‌ها یا حتی Messaging و چت؟

برخی از آنتی‌ویروس‌ها، بسیار گران‌تر از برخی دیگر هستند. گاهی این بهای گزاف، برای توانایی‌هایی است که به راستی شبکه به آنها نیازی ندارند. و البته برعکس، گاهی هم ناخن خشکی در هنگام گزینش آنتی ویرس، شبکه و سازمان را از برخی لایه‌های بسیار با ارزش امنیت بی‌بهره می‌گذارد.

۸- داد و ستد اطلاعاتی سازمان و شبکه آن، تا چه اندازه ایست؟ درون شهری، کشوری یا جهانی؟

۹- چقدر زمان برای شروع در اختیار دارید؟ چند روز تا چند هفته؟ چند ماه؟ یا یک روز؟

سفارش دادن یک آنتی‌ویروس زمان بر است، همچنین نصب و راه اندازی هرکدام زمان خودش را نیاز دارد. برنامه زمانبندی در امنیت، گاهی تاثیرات عجیبی در تصمیم‌گیری‌ها می‌گذارد.

۱۰- آنتی‌ویروس باید از چند Segment پشتیبانی کند؟

باید آگاه بود که برخی از آنتی‌ویروس ها توانایی پشتیبانی از چندین سگمنت را ندارد.

۱۱- فعالیت سازمان چیست؟ تولیدی؟ بیمارستانی؟ نظامی؟

هر دسته از سازمان ها، نحوه زخیره‌سازی اطلاعاتی خاص خودش را دارد. مثلاً تولیدی‌ها سیستم‌های پایگاه داده حجیمی برای انبار داری دارند در حالی که شرکت‌های فروش، بیشتر مواردات اطلاعاتی سنگینی را در Gateway و با بیرون از شرکت و اینترنت دارند.

۱۲- کدام گزینه مهم است: امکان Customize کردن و کسب دانش مدیریت سیستم توسط کارشناسان فنی سازمان، یا پشتیبانی سریع و بهتر توسط شرکت تولید کننده آنتی‌ویروس؟

آموختن برخی از آنتی‌ویروس ها، بسیار مشکل و زمانبر است. همچنین برخی از شرکت‌های ارائه کننده اصولاً سیستم آموزشی خوبی ندارند و برخی دیگر آنها پشتیبانی خوبی ندارند! برای همین در هنگام گزینش آنتی ویرس، لازم است بررسی شود که قرار است که خود سازمان مدیریت سیستم را به عهده بگیرد تا سرعت واکنش و مدیریت رویدادها بیشتر شود، یا قرار است این کار برای دستیابی به تنظیمات حرفه‌ای‌تر و دقیق‌تر و البته بی‌دردسرتر توسط شرکت فروشنده انجام شود.

۱۳- آیا قرار است این آنتی‌ویروس جایگزین آنتی‌ویروسی دیگر شود؟

برخی از شرکت ها، خدمات جایگزینی را به صورت رایگان ارائه می‌کنند. برخی دیگر اصولاً این کار در لیست خدمات آنها نیست. پاک کردن بعضی از آنتی‌ویروس ها با جان کندن تمام می‌شود! و بعضی دیگر به سادگی آب خوردن با یک کلیک.

۱۴- ساختار شبکه چیست؟ Windows، Novell، Unix یا Linux یا آمیخته ای از یک یا دوتا از آنها؟

برای گروهی از سازمان‌ها بسیار مهم است که تمام سیستم‌ها محافظت شوند، و البته هستند سازمان‌هایی که قید امنیت تعدادی از سیستم‌هایشان را می‌زنند تنها به این دلیل که آنتی‌ویروس ارزانتر، از آن پشتیبانی نمی‌کند!

۱۵- نرم‌افزارهایی که در شرکت استفاده می‌شوند از چه نوعی هستند؟ مبادلات بزرگ اطلاعاتی با پایگاه داده دارند یا صفحات HTML و وبسایت را پردازش می‌کنند؟

اینکه سازمان مبتنی بر چه گروهی از نرم افزارها فعالیت می‌کند، در گزینش آنتی‌ویروس تاثیرگذار است. نرم افزارهایی که با پایگاه داده کار می‌کنند، با نرم افزارهای وب سایت و حتی آن دسته از نرم افزارها که به صورت سرویس کار می‌کنند، رفتارهای متفاوتی را با آنتی‌ویروسها، و البته آنتی‌ویروسها با آنها دارند.

۱۶- چه فناوری‌هایی در شبکه فعال است: XML، HTTP، EE۲J، Net. و یا سرویس‌های وب؟

آنتی‌ویروس‌های مختلف در پردازش فناوری‌های متفاوت سرعت و دقت متفاوتی دارند که لازم است مد نظر قرار گیرد.

از آنجا که هر شبکه ویژگی‌های خودش را دارد و گزینه‌هایی که باید مورد توجه قرار گیرند تنها تنها محدود به میزان فشار آنتی‌ویروس بر روی شبکه نیست، مقایسه آنتی‌ویروس‌ها نمی‌تواند خیلی موفق باشد. روی هم رفته می‌توان گفت که میزان بزرگی سازمان و شبکه‌ای که آنتی‌ویروس در آن بکار گرفته می‌شود، در بیشتر مواقع نقش مهمی در تصمیم گیری برای انتخاب آنتی‌ویروس دارد.