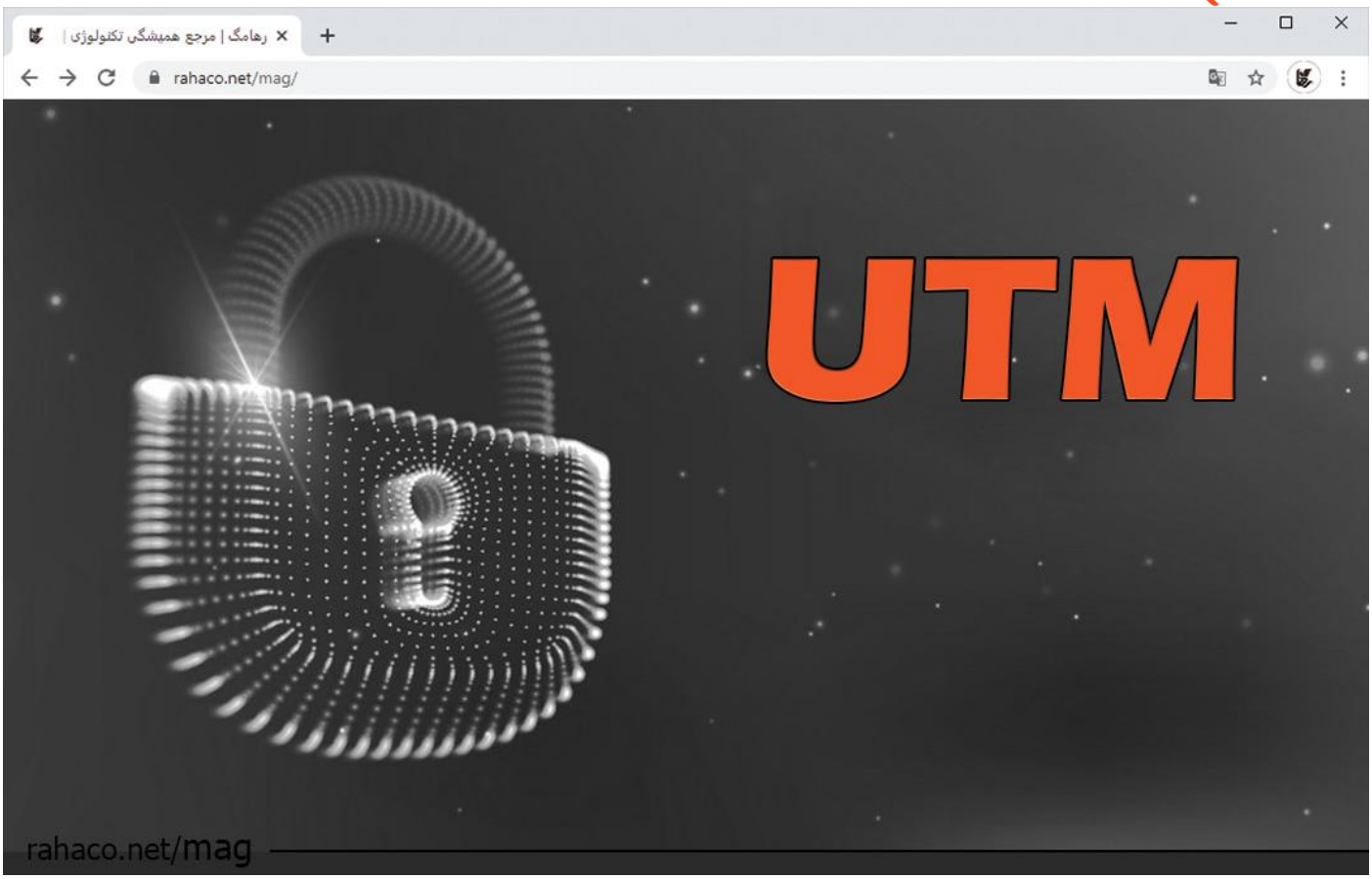
utm یا سامانه مدیریت یکپارچه تهدیدات؛ ایده‌ای جدید برای مقابله با تهدیدات شبکه

شرکت رهاکو

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

حملات سایبری از سال ۲۰۱۹ تاکنون دو برابر شده است و انواع جدیدی از تهدیدات مانند سرقت رمزارزها هر روز در حال افزایش است. اگرچه این تهدیدات روند رو به رشد شبکه‌ها را متوقف نمی‌کنند، اما اختلال در امنیت شبکه هزینه‌های جبران ناپذیری را برای مشاغل در پی دارد و به طور جدی بر آینده کسب و کارها تاثیرگذار است.

هکرها اغلب کسب‌وکارهای کوچک را هدف قرار می‌دهند، چرا که زیرساخت امنیتی آن‌ها نسبت به شرکت‌های بزرگ بسیار ساده‌تر است. معمولا اهداف این حملات دسترسی به دیتاهای مهم یا هک کردن کارت‌های اعتباری است که در دارک وب فروخته می‌شوند. مهم نیست به چه علتی از ابزارها و سرویس‌های امنیتی استفاده می‌کنید، یک زیرساخت امنیتی ضعیف می‌تواند هزینه هنگفتی را برای سازمان شما به همراه داشته باشد.

یکی از بهترین دروازه‌های امنیتی در برابر حملات بدافزار استفاده از فایروال یا سامانه مدیریت تهدیدات (UTM) است. فایروال UTM چندین لایه امنیتی را در یک راه حل واحد ترکیب می‌کند و برای جلوگیری از ورود حملات به شبکه شما روی چندین نقطه از زیرساخت شبکه تمرکز می‌کند. همچنین، سامانه مدیریت یکپارچه شبکه و تهدیدات زمان مدیریت را کاهش می‌دهد و معمولا هزینه کم‌تری در مقایسه با خرید هر راهکار به صورت جداگانه ارائه می‌دهد.

UTM چیست و چگونه کار می‌کند؟

عملکرد فایروال UTM با روش‌های مختلفی انجام می‌شود. روش‌های مبتنی بر جریان و مبتنی بر پروکسی از اصلی‌ترین استراتژی‌های این سرویس می‌باشند. شروع مبتنی بر جریان داده‌ها را در یک دستگاه UTM جمع آوری می‌کند تا بررسی کند آیا اختلالی در جریان داده وجود دارد یا اینکه مشکل از جای دیگریست؟

راه اندازی مبتنی بر پروکسی نیز به روشی مشابه کار می‌کند. تنها تفاوت این است که به عنوان یک پروکسی، تهدیدات امنیتی احتمالی را بررسی می‌کند و اگر محتوای بررسی شده عاری از بدافزار باشد، برای کاربر ارسال خواهد شد.

اگر خطری شبکه شما را تهدید کند، بلافاصله شناسایی می‌شود و در اسرع وقت از سیستم حذف خواهد شد. اولین و مهم‌ترین وظیفه این سرویس نصب ایمن نرم افزار در یک سیستم است. پس از آن پروکسی حملات احتمالی را شناسایی کرده و از ورود آن‌ها به سیستم جلوگیری می‌کند.

فایروال و عملکردهای آن

در مقاله‌های قبلی عملکرد و اهداف فایروال را مورد بحث قرار دادیم. فایروال داده‌های ورودی و خروجی را اسکن می‌کند، محتوای نامناسب یا مخرب را تشخیص می‌دهد و سپس آن را مسدود می‌سازد. فایروال‌های نسل 3 در مقایسه با برنامه‌های فایروال معمولی کمی فراتر می‌روند. این فایروال‌ها علاوه بر بررسی داده‌های ورودی، کارهای دیگری نیز انجام می‌دهند. این وظایف شامل شبکه‌سازی هوشمند اپلیکیشن، ورود ایمن، سیستم یکپارچه پیشگیری از حملات، شناسایی تهدیدات و غیره است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

هدف از مدیریت یکپارچه تهدیدات چیست؟

UTM مزایای منحصر به فردی برای بهبود امنیت شرکت‌های کوچک و بزرگ به ارمغان می آورد. UTM پیچیدگی سیستم امنیتی یک شرکت را به حداقل می‌رساند. به همین ترتیب، سطح آموزش ارائه شده به حداقل می‌رسد و مدیریت آسان برنامه‌ها در آینده فراهم خواهد شد. هم چنین، در دراز مدت می‌توانید به جای خرید تجهیزات جدید و اضافی، در هزینه خود صرفه جویی کنید.

سیستم‌های UTM برای سازمان‌های بزرگتر مزایای بیشتری به همراه می‌آورند و از شبکه‌ها در برابر تهدیدات محافظت می‌کند. این تهدیدات شامل بدافزارها و حملات متعددی است که بخش‌هایی از شبکه را به طور همزمان هدف قرار می‌دهند.

اگر برای ساختن هر دیوار امنیتی از دستگاه‌های مختلف استفاده می‌کنید، این حملات اجتناب ناپذیر خواهند بود. به این دلیل که هر دیوار امنیتی باید به طور جداگانه اجرا شود تا تهدیدات امنیتی همیشه به روز باشد. از آنجایی که UTM یک نقطه دفاعی منحصر به فرد ایجاد می‌کند، مقابله با تهدیدات بسیار ساده می‌شود.

محافظت از شبکه در برابر تهدیدات با UTM

تلاش برای مقابله با تهدیدات سایبری مختلف که شرکت‌ها با آن مواجه می‌شوند باعث می‌شود صاحبان کسب‌وکار به برنامه‌های متعددی از جمله آنتی ویروس، فایروال، محافظت از وب و غیره روی بیاورند.

کاری که فایروال UTM انجام می‌دهد این است که تمام ویژگی‌های محصول را در یک برنامه واحد ترکیب می‌کند. به همین ترتیب، مدیریت آسان‌تر شده و از تمام لایه‌های زیرساخت شبکه محافظت می‌شود. در ادامه چندین مورد از مزایای استفاده از فایروال UTM برای امنیت شبکه را می‌خوانید.

مدیریت ساده

به جای کار با چندین پنل مدیریتی، یک فایروال UTM امکان مدیریت آسان را برای شما فراهم می‌کند. از طریق این سیستم امنیتی می‌توانید شبکه‌ها را برای اعمال سیاست‌های امنیتی نظارت کنید و از هرگونه تهدیدی آگاه باشید.

کار با برنامه‌های ابری

شما می‌توانید از طریق فایروال UTM به برنامه‌های ابری خود دسترسی داشته باشید. این بدان معناست که دسترسی‌های امنیتی تمام برنامه‌های ابری خود را می‌توانید کنترل کنید.

مقابله یادگیری عمیق با تهدیدات پیچیده

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

UTM های امروزی از هوش مصنوعی و deep learning برای تشخیص الگوهای رفتاری استفاده می‌کنند که بیشتر مورد هدف حمله قرار می‌گیرند. حتی به کمک این فایروال‌ها می‌توانید ویروس‌های ناشناخته را شناسایی کنید و همیشه یک قدم از آخرین بدافزارها و حملات سایبری جلوتر باشید.

امنیت وب

فایروال‌های UTM بطور جامع از سیستم شما در فضای وب محافظت می‌کنند. فایروال‌ها از بازدید تصادفی یک وبسایت مخرب و آلوده کردن سیستم شما به ویروس یا سایر کدهای خطرناک جلوگیری می‌کنند.

محافظت از ایمیل

ایمیل‌های اسپم و فیشینگ دو مشکل بزرگ برای صندوق ورودی کاربران ایجاد می‌کنند. یکی از این مشکلات منجر به نقض اطلاعات ایمیل می‌شود. مشکل دیگر باعث می‌شود ساعت‌های بی‌شماری را هدر دهید و صندوق ورودی ایمیل خود را مرتب کنید تا به پیام‌های اصلی و واقعی برسید.

چالش‌های استفاده از UTM

گاهی مزایای استفاده از UTM می‌تواند بزرگترین ضعف آن باشد. وقتی تمام قابلیت‌های امنیتی شرکت در یک دستگاه متمرکز شود، مسلما به یک نقطه ضعف تبدیل خواهد شد. یعنی هکرها فقط باید UTM را هدف حمله قرار بدهند تا کل سیستم امنیتی سازمان را از بین ببرند.

شرکت هایی که از UTM استفاده می‌کنند، خطر قرار دادن تمام «تخم مرغ» امنیتی شان در یک سبد را می‌پذیرند. این خطر باید جدی گرفته شود و مزایا و معایب احتمالی آن‌ها هنگام تجزیه و تحلیل راهکارهای امنیتی به درستی بررسی شود.

UTM یا فایروال: کدام را انتخاب کنیم؟

مدیریت یکپارچه UTM تمام عملکردهای فایروال نسل بعد را در بر می‌گیرد و خدمات بسیاری ارائه می‌دهد. (شاید به همین دلیل است که بسیاری از افراد، از جمله مدیران امنیت شبکه، از این دو اصطلاح به جای یکدیگر استفاده می‌کنند!)

از نظر قیمت، UTM و فایروال هم در یک محدوده قرار می‌گیرند. بنابراین، تصمیم گیری و انتخاب هرکدام از آن‌ها باید بر اساس اولویت باشد. از آنجایی که تمام عملکردهای فایروال در UTM گنجانده شده است، می‌توانید فایروال های نسل بعد را انتخاب کنید. در غیر این صورت، اگر به خدمات اضافی UTM نیاز دارید، سامانه مدیریت یکپارچه تهدیدات UTM رهاکو تمام راه حل های ممکن را به شما ارائه می‌دهد.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

چه زمانی باید از یک سیستم مدیریت یکپارچه تهدید استفاده کنیم؟

سیستم مدیریت تهدید یکپارچه لزوما راه حل نهایی نیست. با این حال، هنوز هم جزء ارزشمندی از سیستم امنیتی شما خواهد بود. مهم نیست که این سیستم UTM سازمان شما چقدر قوی باشد، در شرایط مختلف بخش مفیدی از یک استراتژی امنیت سایبری را تشکیل می‌دهد. قبل از شروع کار با این سیستم باید آن را به طور کامل ارزیابی کنید و از خود بپرسید:

- چگونه این سیستم با حفاظت‌های امنیتی سایبری سازمان شما مطابقت دارد؟
- چگونه با فرآیندهای کسب و کار شما هماهنگ است؟
- آیا سازمان شما برای استفاده از این سیستم به تغییرات عمده ای نیاز دارد؟
- آیا در حال حاضر ابزاری دارید که عملکردهای مشابهی را انجام دهند؟
- اگر چنین است، آیا UTM این عملکرد را بهتر از ابزارهای انجام می‌دهد؟

UTM لزوما نباید جایگزین ابزارهای امنیت سایبری شود، اما می‌توان از آن برای تقویت دروازه‌های حفاظتی استفاده کرد. از سوی دیگر، اگر محصولات امنیتی شما منسوخ شده باشد، استفاده از UTM می‌تواند یک جایگزین منطقی برای آن‌ها باشد. در مفهوم جامع، UTM فقط یکی دیگر از ابزارهای امنیت سایبری است؛ راهکاری که باید در زمان و مکان مناسب مورد استفاده قرار گیرد؛ درست مانند هر راهکار امنیتی دیگر.

نتیجه گیری

در حال حاضر سامانه مدیریت یکپارچه تهدیدات UTM بدون شک یکی از بهترین راهکارهای امنیتی است. این سرویس به لطف بسیاری از ویژگی‌های امنیتی مختلف، از سازمان‌ها در برابر طیف گسترده‌ای از تهدیدات محافظت می‌کند. علاوه بر این، سرویس‌های زیادی مانند: VPN و فیلترینگ وب نیز می‌توانند در استراتژی امنیت داده‌ها با UTM ادغام شوند. با این سرویس امنیت و آرامش بیشتری را به سازمان خود می‌بخشید.

برای ادغام سیستم مدیریت تهدیدات در استراتژی امنیت سایبری سازمان خود به کمک نیاز دارید؟ با کارشناسان رهاکو تماس بگیرید تا در مورد چالش‌های امنیتی شبکه به شما کمک کنند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net