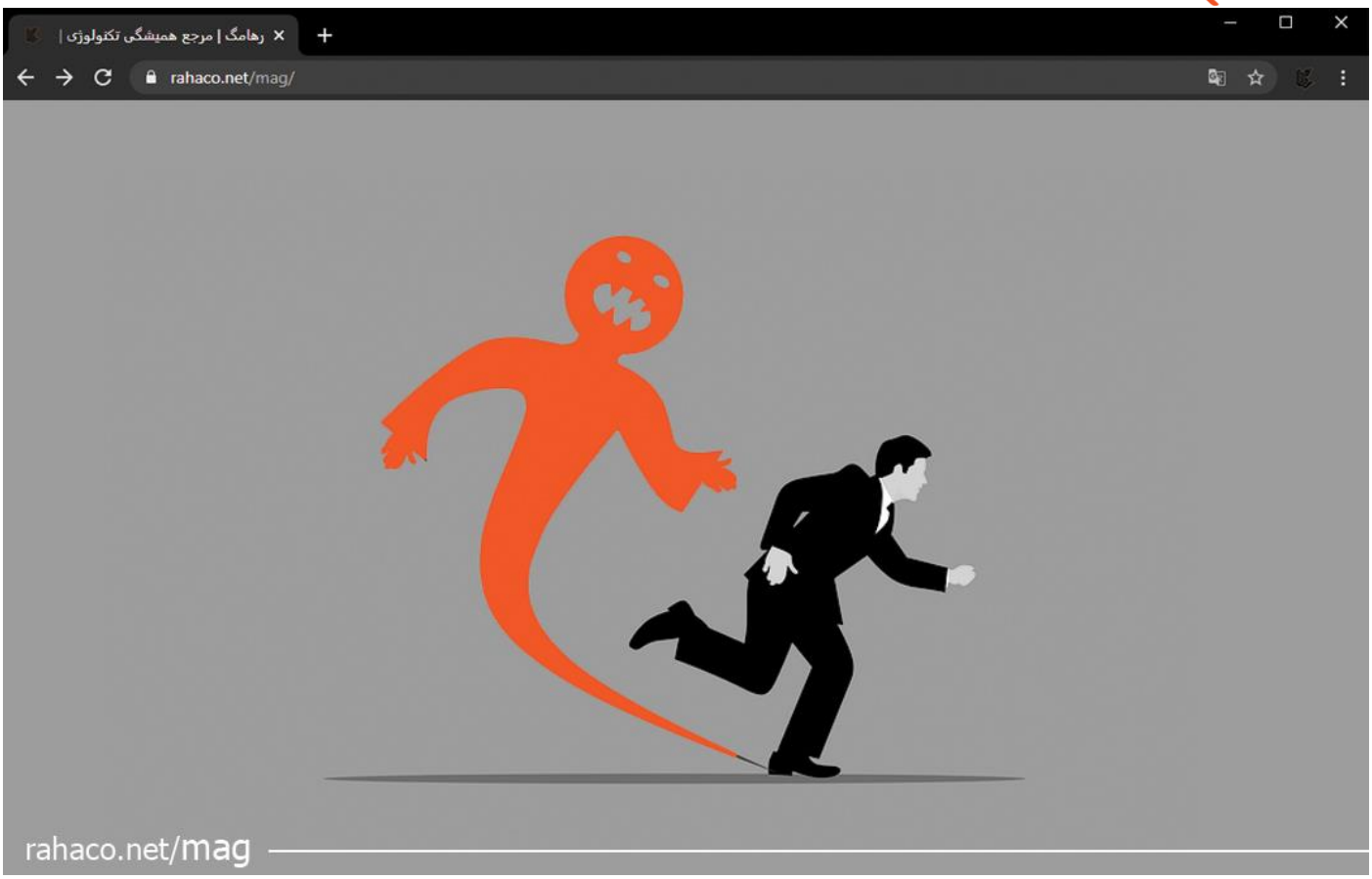
امنیت utm، یک سیستم مقرون به صرفه و یکپارچه برای محافظت از اطلاعات شبکه

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

سامانه مدیریت یکپارچه شبکه و تهدیدات یک پلتفرم امنیتی مدرن و یکپارچه را برای سازمان ها فراهم کرده است که از زیرساخت فناوری اطلاعات محافظت می‌کند .یک جایگزین خوب برای سیستم‌های امنیتی محسوب می شود و برای سازمان‌هایی که به کارایی، انعطاف‌پذیری و رشد ارزش می‌دهند، مزایایی را ارائه می‌دهند. حملات سایبری روز به روز بیشتر می‌شود و عواقب زیانبار مالی و اعتباری را به دنبال دارد. شما برای محافظت بهتر از سازمان و مهم‌تر از آن از مشتریان خود به یک روش دفاعی مناسب نیاز دارید! نگران نباشید، چندین راه حل در اختیار شما است و یکی از آن‌ها مدیریت یکپارچه تهدیدات (UTM) است.
مدیریت یکپارچه تهدیدات یک راهکار قوی است که می‌توانید به راحتی در سازمان خود پیاده سازی کنید. این سامانه قدرت فایروال نسل بعد (NGFW) و دیگر ابزارهای امنیتی را با هم ترکیب کرده و در خود جای می‌دهد. در مقاله امنیتUTM ، می آموزید که مدیریت تهدید یکپارچه چیست؟ چگونه کار می‌کند و بهترین ابزارهای UTM در بازار امروز کدامند؟ مثل همیشه، اجازه دهید با یک تعریف ساده شروع کنیم، آماده‌اید؟

مدیریت یکپارچه تهدیدات یا امنیت UTM چیست؟

مدیریت یکپارچه تهدید (UTM) یک سیستم امنیتی است که در برابر تهدیدات امنیت سایبری مانند: ویروس‌ها، بدافزارها، جاسوس افزارها و غیره محافظت می‌کند .UTM سیستم‌های امنیتی و مدیریتی را در یک پلتفرم واحد ادغام می‌کند. در نتیجه، مدیریت آن بسیار آسان تر خواهد بود. راهکار UTM در درجه اول برای محافظت از شبکه های سازمانی بزرگ طراحی شده است، اما برای کسب و کارهای کوچک و متوسط نیز مفید خواهد بود. قابلیت‌ها و ویژگی‌های مفید این سامانه در دراز مدت سود زیادی برای شرکت‌ها به دنبال دارد. حال بیایید ویژگی‌های سیستم مدیریت تهدیدات یکپارچه را با هم بررسی کنیم.

سه ویژگی ضروری سیستم امنیت utm

در این بخش، به طور خلاصه در مورد مهم‌ترین ویژگی‌هایی که باید در هر سیستم UTM وجود داشته باشد صحبت می‌کنیم. هر سیستم امنیت UTM باید این ویژگی ها را داشته باشد، اما برخی ممکن است فاقد این قابلیت‌ها باشند. اگر اینطور است، به جستجو ادامه دهید! به طور کلی سه ویژگی ضروری در هر سیستم مدیریت تهدیدات یکپارچه وجود دارد.

1. فایروال شبکه

فایروال پایه و اساس امنیت است و به حفظ امنیت شبکه در سازمان‌ها کمک می‌کند. شما قطعا به یک فایروال در سیستم مدیریت تهدید یکپارچه خود نیاز دارید. اگر سیستم UTM مورد نظرتان فایروال ارائه نمی‌دهد همچنان به جستجو ادامه دهید تا زمانی که فایروال را پیدا کنید!

2. سیستم تشخیص نفوذ(IDS)

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

برنامهIDS ، شبکه و سیستم‌های شما را برای تشخیص فعالیت‌های مشکوک نظارت می‌کند. اگر این سیستم مشکلی را تشخیص دهد، گزارش آن را به تیم امنیتی یا سیستم مدیریت رویداد سازمان شما ارسال می‌کند.

3. سیستم پیشگیری از نفوذ(IPS)

IPSیک سرویس فعال است که نفوذها را شناسایی کرده و اقدامات مناسب را برای جلوگیری از وقوع آن‌ها انجام می‌دهد IPS .این کار را با بررسی ترافیک، جستجوی ناهنجاری‌ها و در راستای سیاست‌های سازمان انجام می‌دهد. استفاده از IDS وIPS ، شبکه ها و سیستم‌ها را غیر قابل نفوذ می‌کند. این‌ها سه ویژگی ضروری هستند که باید قبل از انتخاب یکی از راهکارهای امنیت utm در نظر بگیرید. در ادامه فهرستی از چندین ویژگی دیگر را که باید به آن‌ها توجه کنید، در اختیار شما قرار می‌دهیم.

سایر ویژگی‌های مهمی که باید در نظر بگیرید

ویژگی‌های ذکر شده در بالا اصلی‌ترین ویژگی‌هایی هستند که در سامانه UTM وجود دارند. اما ویژگی‌های دیگر نیز همچنان مهم هستند. البته این قابلیت‌ها در تمام سیستم های UTM یافت نمی‌شوند و ممکن است بسته به نیاز سازمان خود به آن‌ها نیاز نداشته باشید.

- درگاه آنتی ویروس
- فایروال لایه برنامه (لایه 7)
- بازرسی عمیق
- پروکسی وب و فیلتر محتوا
- فیلتر ایمیل به منظور جلوگیری از حملات هرزنامه و فیشینگ
- پیشگیری از از دست دادن داده ها(DLP)
- اطلاعات امنیتی و مدیریت رویداد(SIEM)
- شبکه مجازی خصوصی(VPN)
- کنترل دسترسی به شبکه
- خدمات امنیتی اضافی در برابر حملات(DoS)

امیدوارم این لیست به شما کمک کند تا سیستم UTM خود را بهتر انتخاب کنید. در ادامه نحوه عملکرد یک سیستم مدیریت تهدید یکپارچه را بررسی می‌کنیم.

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

سیستم‌های امنیت UTMچگونه کار می‌کنند؟

هدف سیستم UTM شناسایی هر گونه ضعف در شبکه سازمان شماست. به همین ترتیب، تیم امنیتی می‌تواند به راحتی تمام آسیب‌پذیری‌ها را برطرف کند. و این کار را به دو روش زیر انجام می‌دهد:

1. بررسی مبتنی بر جریان

در بازرسی مبتنی بر جریان سیستم UTM از داده‌های وارد شده به شبکه شما نمونه می‌گیرد و آن‌ها را بررسی می‌کند. در این فرایند سیستم به دنبال ویروس‌ها و سایر حملات مخرب می‌گردد. اگر چیز مشکوکی پیدا کند هشدارها یا اقدامات خودکار را برای محافظت از شبکه فعال خواهد کرد.

2. بررسی مبتنی بر پروکسی

بازرسی مبتنی بر پروکسی یک روش امنیتی شبکه است که در آن سیستم امنیت UTM محتویات بسته‌های داده ورودی را از طریق فایروال، VPNو غیره بررسی می‌کند. پس از آن، از یک دستگاه امنیتی به عنوان پروکسی برای کنترل داده‌های ورودی به دستگاه استفاده می‌کند. سیستم امنیت UTM تشخیص می‌دهد که کدام داده‌ها مضر هستند و از ورود آن‌ها به شبکه جلوگیری می‌کند. دانستن نحوه کار سیستم UTM یک قدم خوب است، اما کافی نیست. در ادامه بهترین روش‌های مدیریت تهدیدات برای دفاع از شبکه را مشاهده می‌کنید.

بهترین روش‌های امنیتی UTM

علاوه بر داشتن جدیدترین سخت افزارها یا نرم افزارها باید سازمان خود را با بهترین شیوه های مدیریت تهدیدات منطبق کنید. شرکتی که بهترین دفاع را داشته باشد می‌تواند به سرعت به هر تهدیدی پاسخ دهد. در اینجا بهترین روش ها را معرفی کرده ایم:

دیدگاه شبکه یکپارچه

تیم فناوری اطلاعات باید از هرگونه تهدید احتمالی مانند: بدافزار، فیشینگ و غیره آگاهی کامل داشته باشد. همه باید برای جلوگیری از این تهدیدات با یکدیگر همکاری کنند. همچنین تیم‌های امنیتی سازمان باید به همه چیز در سیستم دسترسی داشته باشند. این امر به طور کلی مدیریت امور را آسان‌تر می‌کند. جمع آوری داده‌های دقیق یکی از مزایای بزرگی است که سیستم مدیریت تهدید یکپارچه ارائه می‌دهد.

استفاده از ابزارهای تحقیق مناسب

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

برای بررسی شبکه و تجزیه و تحلیل داده‌ها باید از ابزارهای مناسب استفاده کنید. علاوه بر این، سیستم امنیت UTMباید بتواند به طور خودکار تهدیدات سطح پایین را مدیریت کند تا متخصصان چالش‌های بزرگ‌تر را انجام دهند. یک سیستم مدیریت تهدید یکپارچه این ویژگی‌ها را دارد.

حفظ نرخ پاسخ موثر

پاسخ‌های سریع و اقدامات خودکار بهترین رویکرد برای حفظ امنیت است. با این حال، یک برنامه قوی راهی عالی برای جمع آوری تیم‌ها در بخش های مختلف می‌باشد. نرخ پاسخ موثر کلید کاهش آسیب های احتمالی است. تاکنون سیستم مدیریت تهدید یکپارچه، ویژگی‌ها و نحوه عملکرد و برخی از بهترین روش‌ها برای مدیریت تهدیدات را بررسی کردیم. حالا زمان آن رسیده است که بهترین راهکارهای UTM را مورد بحث قرار دهیم.

بهترین برنامه های مدیریت تهدیدات یکپارچه

راهکار نرم افزار اختصاصی UTM برای هر شرکتی که به دنبال افزایش قدرت سیستم‌های امنیتی است، تفاوت بزرگی ایجاد می‌کند. در ادامه با سه مورد از بهترین راهکارهای موجود در بازار آشنا خواهید شد.

Kerio Control

برای مشاغل کوچک و متوسطی که به دنبال افزایش نیازهای امنیتی خود هستند KerioControl یک نرم افزار UTMمناسب محسوب می‌شود. این برنامه شامل یک فایروال نسل بعد (NGFW) و یک سیستم مدیریت تهدید یکپارچه است. این برنامه برای شرکت‌هایی که به دنبال راهکارهای امنیتی هستند یک گزینه ایده آل محسوب می‌شود.

امکانات:KerioControl

- فایروال
- سیستم حفاظت از نفوذ(IPS)
- فیلتر محتوای وب و برنامه
- VPN

Change Tracker Gen7

ابزار Change Tracker Gen7 با نظارت دقیق خیالتان را راحت می‌کند. ویژگی‌های این نرم افزار تمام تغییرات فایل‌های شما را تجزیه و تحلیل می‌کنند. به طور کلی، این راهکار نرم افزاری تضمین می‌کند که تغییرات سیستم شما سازگار و ایمن هستند.

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

امکانات:Change Tracker Gen7

- پیشگیری از اختلال
- تشخیص اختلال
- نظارت فوری بر یکپارچگی فایل
- مدیریت آسیب پذیری و نظارت مستمر

Alert Logic

این نرم افزار قابلیت‌های عالی سیستم امنیت UMT را در اختیار شما قرار می‌دهد. سرویس تشخیص و پاسخ مدیریت شده آن نظارت دقیق در محیط را فراهم می‌کند و به شما و تیمتان کمک می‌کند تا اقدامات درست را برای رفع مشکل انجام دهید.

امکانات:Alert Logic

- سرعت
- امنیت بهبود یافته
- صرفه جویی

نتیجه گیری

موارد بالا 3 مورد از بهترین راهکارهای نرم افزاری UTM هستند که امروزه سازمان‌های زیادی از آن‌ها استفاده می‌کنند. استفاده از یک سیستم مدیریت تهدید یکپارچه راهی عالی برای محافظت از سازمان‌هاست. راهکارهای امنیت UTM دارای ویژگی‌های زیادی مانند IDS و IPS هستند که به راحتی سیستم امنیتی سازمان شما را تقویت می‌کنند. در این مقاله، بهترین شیوه های مدیریت تهدیدات را در اختیار شما قرار دادیم و اشاره کردیم که داشتن یک راهکار نرم افزاری مانند KerioControl می‌تواند در راستای حفظ امنیت به شما کمک کند. امروزه بیش از هر زمان دیگری نیاز دارید تا برای محافظت از سازمان خود در برابر حملات سایبری اقدامات لازم را انجام دهید. پس از شناخت بهترین نرم افزار امنیتی پیاده سازی و اجرای آن بسیار حائز اهمیت خواهد بود پس همین حالا برای محافظت از شرکت و مشتریان خود با ما تماس بگیرید. 02154521 شماره تماس شرکت رها برای دریافت مشاوره رایگان و تخصصی از کارشناسان متخصص حوزه فناوری اطلاعات است.

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