عنوان مقاله: راهکارهای حفاظت از SQL Server در برابر حملات DDoS

نویسنده مقاله: تیم فنی نیک‌آموز

تاریخ انتشار: ۲۰ خرداد ۱۴۰۳

منبع: https://nikamooz.com/protecting-sql-server-against-ddos-attacks/

حفاظت از SQL Server در برابر حملات DDos امری بسیار حیاتی است؛ زیرا SQL Server به‌عنوان پایگاه داده اصلی برای بسیاری از سیستم‌ها و برنامه‌ها عمل می‌کند. این حفاظت نه‌تنها امنیت داده‌ها و اطلاعات برنامه‌ها را فراهم می‌کند، بلکه مانع ازدست‌رفتن اطلاعات مهم و آسیب‌های جدی می‌شود. در این مقاله قصد داریم به بررسی روش‌های حفاظت از این پایگاه داده در برابر حملات دیداس بپردازیم تا مانند یک سپر فولادی از دیتابیس خود محافظت کنید.

تعریف حملات DDoS

قبل از آنکه به روش‌های حفاظت از SQL Server در برابر حملات DDos بپردازیم، بهتر است به‌صورت ریشه‌ای با این مفهوم آشنا شوید. دقیقاً منظور از حمله دیداس چیست؟

به زبان ساده، حمله دیداس، یکی از حملات هکری است که با هدف غیرقابل دسترس‌کردن یک سایت، برنامه یا سرویس آنلاین برای کاربران واقعی، انجام می‌شود. مهاجمان در این حملات، با کمک شبکه‌ای از دستگاه‌های آلوده به بدافزار (که به آن‌ها Botnets گفته می‌شود) یا ارسال حجم عظیمی از ترافیک جعلی، سرور هدف را غرق در ترافیک می‌کنند. این ترافیک اضافی باعث می‌شود تا سرور یا شبکه هدف، قادر به پاسخگویی به درخواست‌های واقعی کاربران نباشد و درنتیجه، از دسترس خارج شود.

تأثیرات مخرب حملات DDoS بر روی SQL Server

حملات دیداس می‌توانند برای کسب‌وکارها بسیار مخرب باشند و منجر به ازدست‌رفتن درآمد، آسیب به اعتبار و حتی اختلال در عملیات شوند. به همین دلیل، مهم است که برای مقابله با این نوع حملات، اقدامات امنیتی مناسب را اتخاذ کنید و با راه حل‌های حفاظت از SQL Server در برابر حملات DDos آشنا باشید. ازجمله تأثیرات دیداس روی SQL Server می‌توان به موارد زیر اشاره کرد:

- **کاهش عملکرد SQL Server:** سیل عظیمی از ترافیک جعلی به سمت SQL Server، باعث اشباع منابع سیستم مانند CPU، حافظه و پهنای باند می‌شود. این وضعیت، درنهایت پردازش کوئری‌ها را به‌شدت کند می‌کند و باعث تأخیر در پاسخگویی می‌شود.
- **کاهش دسترس‌پذیری:** این حملات می‌تواند SQL Server را در برخی موارد، از دسترس خارج کند. با از دسترس خارج‌شدن پایگاه داده، خسارت مالی زیادی متوجه صاحبان سایت می‌شود.
- **کاهش امنیت و خطرات بزرگ‌تر:** در برخی موارد، حملات دیداس درحقیقت یک حمله اولیه و آمادگی برای یک حمله بزرگ‌تر بوده و ممکن است هکرها اهداف بدتری مانند سرقت اطلاعات را دنبال کنند.
- **هزینه‌های اضافی:** حفاظت از SQL Server در برابر حملات DDos می‌تواند پرهزینه باشد. این هزینه‌ها شامل هزینه‌های مربوط به راه‌اندازی و نگهداری راه حل‌های امنیتی، استخدام متخصصان امنیتی و جبران خسارات ناشی از حملات می‌شود.

برای در امان ماندن از اثرات مخرب بالا، ادامه مطلب را از دست ندهید!

روش های تشخیص حملات DDoS

بارزترین نشانه یک حمله دیداس، کندشدن یا عدم دسترسی ناگهانی به یک وب‌سایت یا سرویس است. اما از آنجایی که دلایل متعددی مانند افزایش واقعی ترافیک، می‌تواند مشکلات عملکردی مشابهی ایجاد کنند، معمولاً نیاز به تحقیقات بیشتری است. برای حفاظت از SQL Server در برابر حملات DDos، روش‌ها و ابزارهای مختلفی ظهور کرده‌اند که هرکدام، ویژگی‌ها و قابلیت‌های منحصربه‌فردی دارند. در ادامه، ۴ مورد از این ابزارها را باهم مقایسه می‌کنیم.

SolarWinds Security Event Manager (SEM)

سامانه SEM یا مدیریت رویداد امنیتی سولار ویندوز، یک پلتفرم مدیریت امنیت جامع است که با قابلیت‌های منحصربه‌فرد خود می‌تواند حملات DDos را تشخیص دهد. این ابزار، یکی از بهترین ابزارها برای تشخیص دیداس است.

مزایا:

- مانیتورینگ فوری
- یکپارچه‌سازی با هوش تهدید (اعلام هشدار برای تهدیدات خارجی سایت)
- هشدارهای قابل تنظیم

معایب:

- پیچیدگی در پیاده‌سازی و مدیریت

Sucuri Website Firewall (WAF)

یک فایروال وب مبتنی‌بر ابر (Cloud) که به‌عنوان یکی از بهترین ابزارها برای حفاظت از SQL Server در برابر حملات DDos محسوب می‌شود.

مزایا:

- پیاده‌سازی آسان
- کارآمدی بالا دربرابر حملات مبتنی‌بر وب

معایب:

- ممکن است برای زیرساخت‌های یک شبکه پیچیده، مناسب نباشد.

StackPath Web Application Firewall (WAF)

یک فایروال وب که حفاظت از SQL Server در برابر حملات DDos و امنیت برنامه برای برنامه‌های وب ارائه می‌دهد.

مزایا:

- الگوریتم‌های رفتاری برای تشخیص حملات
- آستانه‌های قابل تنظیم دیداس

معایب:

- دید محدود به ترافیک شبکه

سرویس حفاظت DDoS مبتنی بر ابر Link11

یک سرویس ابری برای تشخیص و کاهش تهدیدات در زمان واقعی است.

مزایا:

- مقیاس‌پذیری خوب
- مقرون‌به‌صرفه
- محافظت برای زیرساخت ابری

معایب:

- سفارشی‌سازی محدود در مقایسه با راه حل‌های درون‌سازمانی

راهکارهای پیشگیری از حملات دیداس

جلوگیری از حملات دیداس، به‌خصوص در دوره‌های ترافیک بالا یا در یک شبکه گسترده با توزیع جغرافیایی زیاد، می‌تواند چالش‌برانگیز باشد. در ادامه، چند راهکار طلایی برای پیشگیری از حملات و همچنین حفاظت از SQL Server در برابر حملات DDos معرفی می‌کنیم.

Firewalls

فایروال‌ها می‌توانند با بررسی بسته‌های IP و مسدودکردن ترافیک‌هایی که با معیارهای امنیتی از پیش تعیین‌شده مطابقت ندارند، به‌عنوان دروازه‌بان عمل کنند. این امر می‌تواند شامل مسدودکردن ترافیک از منابع شناخته‌شده مخرب، آدرس‌های IP جعلی یا درخواست‌هایی باشد که از الگوهای حمله دیداس شناخته‌شده پیروی می‌کنند.

Switches

سوئیچ‌ها، دستگاه‌های شبکه‌ای هستند که وظیفه مسیریابی ترافیک بین دستگاه‌های متصل به یک شبکه محلی (LAN) را برعهده دارند. درحالی‌که سوئیچ‌ها به‌طور خاص برای حفاظت از SQL Server در برابر حملات DDos طراحی نشده‌اند، می‌توان از آن‌ها به روش‌های مختلف برای افزایش امنیت شبکه و کاهش خطر این حملات استفاده کرد. برای مثال، سوئیچ‌ها می‌توانند برای جداسازی ترافیک شبکه به بخش‌های مختلف استفاده شوند.

Application Front End Hardware

این سخت‌افزار، درحقیقت یکی از قوی‌ترین ابزارها برای حفاظت از SQL Server در برابر حملات DDos است. برای استفاده از این ابزار، آن را در مسیر ترافیک ورودی به سرور نصب می‌کنند. این سخت‌افزار به‌صورت زیر کار می‌کند:

- **بررسی و آنالیز ترافیک:** تمام بسته‌های ارسالی به سمت سرور ابتدا توسط این سخت‌افزار، بررسی و آنالیز می‌شوند. این کار به‌منظور شناسایی و مسدودکردن ترافیک مخرب، مانند بدافزار، حملات دیداس و سایر تهدیدات امنیتی انجام می‌شود.
- **اولویت‌بندی ترافیک:** باتوجه‌به نوع ترافیک، سخت‌افزار می‌تواند به‌طور هوشمندانه ترافیک را اولویت‌بندی کند. به‌عنوان‌مثال، ترافیک حیاتی برای کسب‌وکار می‌تواند در اولویت قرار گیرد تا درصورت ازدحام شبکه، به‌طور کامل و بدون وقفه به سرورها برسد.
- **افزایش عملکرد:** این سخت‌افزار، با توزیع بار ترافیک بین چندین سرور و استفاده از تکنیک‌های کش، می‌تواند به‌طور قابل توجهی عملکرد برنامه‌ها را افزایش دهد.

پیاده سازی اقدامات امنیتی در SQL Server

حفاظت از SQL Server در برابر حملات دیداس امری مهم است که باید همواره به آن توجه کرد. برای افزایش امنیت، ضروری است که اقداماتی را انجام دهید تا بتوانید امنیت این پایگاه داده را تضمین کرده و از وقوع حملات جلوگیری کنید. از مهم‌ترین اقدامات امنیتی که برای حفاظت از SQL Server در برابر حملات DDos می‌توانید انجام دهید عبارت‌اند از:

- استفاده از سرویس‌های DDoS Protection
- استفاده از سیستم‌های حفاظتی IDS
- حفظ امنیت هسته سیستم‌عامل
- محافظت از سرویس PHP سرور
- محافظت از اسکریپت‌های تحت Perl
- توجه به امنیت و پایداری اسکریپت‌های تحت python
- محافظت از سرور با آنتی شل
- کمک‌گرفتن از آنتی‌ویروس قوی با کانفیگ استاندارد برای بررسی سرور

استفاده از شبکه های توزیع محتوا (CDN) و سرویس های ابری برای مقابله با دیداس

خوب است بدانید که استفاده از یک شبکه تحویل و توزیع محتوا (CDN) برای ذخیره منابع می‌تواند فشار روی سرورهای یک سازمان را کاهش دهد و باعث شود دسترس‌پذیری سامانه بهبود پیدا کند. برای این کار، از ذخیره‌سازها کمک گرفته می‌شود. ذخیره‌سازها، کپی‌هایی از محتوای درخواستی را ذخیره می‌کنند تا درخواست‌های کمتری توسط سرورهای اصلی سرویس‌دهی شود.

علاوه‌براین، سرویس‌های ابری، حفاظت از SQL Server در برابر حملات DDos را ارائه می‌دهند. این سرویس‌ها به سازمان‌ها کمک می‌کنند تا قبل از رسیدن حملات به برنامه‌ها، شبکه‌ها و زیرساخت‌های هدف، آن‌ها را نظارت، پیشگیری و کاهش دهند. برخی از مزایای کلیدی دفاع چندلایه عبارتند از:

- **مسیریابی و تسریع ترافیک:** سرویس ابری، به پخش‌شدن ترافیک‌های ناگهانی در سراسر شبکه شما برای به‌حداقل‌رساندن تأخیر و تراکم کمک می‌کند.
- **کاهش خودکار و دائمی حملات DDoS:** این قابلیت می‌تواند ترافیک مخرب را در کمتر از سه ثانیه تشخیص داده و مسدود کند.
- **فایروال وب نسل بعدی (WAF):** این فایروال محدودیت سرعت پیشرفته، مجموعه قوانین سفارشی و پیشگیری انعطاف‌پذیر از تهدیدات را ارائه می‌دهد.

تکنیک های بهینه سازی عملکرد SQL Server برای مقاومت در برابر DDoS

ازجمله تکنیک‌های بهینه‌سازی عملکرد و حفاظت از SQL Server در برابر حملات DDos می‌توان به موارد زیر اشاره کرد:

- **حافظه:** میزان حافظه اختصاص‌یافته به SQL Server را به‌طور مناسب تنظیم کنید. کمبود حافظه می‌تواند منجر به کندشدن کوئری‌ها و افزایش احتمال حملات دیداس شود.
- **CPU:** تعداد هسته‌های CPU اختصاص‌یافته به SQL Server را براساس حجم کاری خود تنظیم کنید.
- **فضای دیسک:** از فضای دیسک کافی برای ذخیره‌سازی داده‌ها و فایل‌های log استفاده کنید. کمبود فضای دیسک می‌تواند منجر به کندشدن کوئری‌ها و افزایش احتمال از کار افتادن SQL Server در هنگام حملات DDoS شود.
- **کوئری‌های ناکارآمد را شناسایی و اصلاح کنید:** کوئری‌های ناکارآمد می‌توانند به‌طور قابل‌توجهی بر عملکرد SQL Server تأثیر بگذارند و آن را در برابر حملات دیداس آسیب‌پذیرتر کنند.
- **از ابزارهای نظارت برای رصد عملکرد SQL Server خود استفاده کنید:** این ابزارها می‌توانند به شما در شناسایی و رفع مشکلات قبل از اینکه به حملات DDoS منجر شوند، کمک کنند.

پروتکل ها و سیاست های واکنش به حملات DDoS

پس از حفاظت از SQL Server در برابر حملات DDos ، اقدامات مهمی برای بازیابی کامل سیستم و جلوگیری از تکرار حملات در آینده وجود دارد که باید انجام دهید. این اقدامات شامل موارد زیر است:

- برای شروع بررسی کنید که چه سیستم‌ها و سرویس‌هایی تحت تأثیر قرار گرفته‌اند؟ چه مقدار داده یا عملکرد از دست رفته است؟
- هکران ممکن است از فرصت سواستفاده کرده و بدافزار نصب یا به داده‌های حساس دسترسی پیدا کرده باشند. این موارد را به‌خوبی شناسایی کنید.
- جزئیات مربوط به حمله را ثبت کنید؛ ازجمله زمان شروع و پایان، نوع حمله، منابع حمله، حجم ترافیک، اقدامات انجام‌شده برای مقابله با حمله و نتایج این اقدامات.
- فایروال‌ها، سیستم‌های تشخیص نفوذ (IDS) و سیستم‌های پیشگیری از نفوذ (IPS) خود را برای اطمینان از پیکربندی صحیح و به‌روز بودن آن‌ها بررسی کنید.

جمع بندی : راهکارهای حفاظت از SQL Server در برابر حملات DDoS

در این مقاله سعی کردیم به بررسی کامل مفهوم دیداس و همچنین روش‌های مهم حفاظت از SQL Server در برابر حملات DDos بپردازیم. همان‌طور که اشاره شد، حفاظت از SQL Server دربرابر حملات بسیار مهم است؛ زیرا این پایگاه داده حاوی اطلاعات بسیار مهمی است که ازدست‌رفتن آن‌ها می‌تواند آسیب‌های جبران‌ناپذیری را وارد کند. اما با استفاده از از روش‌ها و راه‌حل‌های امنیتی مختلفی که وجود دارد، می‌توان از SQL Server در برابر این حملات محافظت کنیم.

به نظر شما چه روش‌هایی تأثیر بهتری در مقابله با این حملات دارند؟ آیا سایت شما هم موردحمله قرار گرفته است؟ اگر این‌طور است، می‌توانید خیلی سریع از طریق راه‌های ارتباطی سایت با کارشناسان متخصص ارتباط گرفته و مشکلات خود را مطرح کنید.