KASPERSKY DDOS PROTECTION

Schützen Sie Ihr Unternehmen mit Kaspersky Lab vor DDoS-Angriffen

CYBERKRIMINELLE HABEN ES AUF UNTERNEHMEN ABGESEHEN

Wenn Ihr Unternehmen bereits einen Distributed-Denial-of-Service-Angriff (DDoS) erlitten hat, wissen Sie, dass die Kosten und Rufschäden verheerend sein können. Doch selbst wenn Ihr Unternehmen das Glück hatte, bisher von den Angriffen der Cyberkriminellen und Hacker verschont zu bleiben, können Sie sich in Zukunft nicht darauf verlassen.

DIE ANZAHL UND DIE SCHWERE DER ANGRIFFE STEIGEN

In den vergangenen Jahren ist es für Cyberkriminelle erheblich günstiger geworden, einen DDoS-Angriff durchzuführen. Zugleich sind die Angriffe heute komplexer und so umfangreich, dass sie die Kommunikationsbandbreite des angegriffenen Unternehmens in Sekundenschnelle einnehmen können, wodurch beinahe sofort entscheidende interne Geschäftsabläufe lahmgelegt werden und die Onlinepräsenz des angegriffenen Unternehmens abgeschaltet wird.

Da sich Unternehmen aller Größenordnungen auf ihre IT-Infrastruktur und Webseite verlassen, um ihre geschäftskritischen Vorgänge zu unterstützen, sind längere Ausfallzeiten, zum Beispiel durch einen DDoS-Angriff, nicht akzeptabel. Angesichts der Häufigkeit, des Umfangs und der Schwere moderner Angriffe ist es für Unternehmen nicht ausreichend, sich erst dann um den Schutz vor DDoS-Angriffen und um die Risikobegrenzung zu kümmern, wenn ihre Infrastruktur bereits angegriffen wird. Stattdessen müssen sich Unternehmen – und öffentliche Einrichtungen – der Bedrohungen bewusst sein und angemessene Verteidigungsmechanismen gegen DDoS-Angriffe einrichten.

„GEFAHR ERKANNT, GEFAHR GEBANNT“

Jedes Unternehmen muss über eine Anti-DDoS-Strategie verfügen – und bereit sein, diese umzusetzen, wenn ein Angriff erkannt wird. Im Falle eines Angriffs kann das Unternehmen den Schaden dann sofort begrenzen. Dazu gehört:

- Minimieren der Ausfallzeiten für geschäftskritische Infrastrukturen und Abläufe
- Sicherstellen, dass Kunden weiterhin Zugriff auf Online-Services haben
- Aufrechterhaltung der Produktivität der Mitarbeiter
- Minimierung der Rufschädigung

DDOS-ANGRIFFSMETHODEN

Cyberkriminelle und Hacker verwenden verschiedene Techniken, um DDoS-Angriffe zu implementieren, die die IT-Infrastruktur des anvisierten Unternehmens lahmlegen oder überlasten.

ÜBERLASTUNGSANGRIFFE

Diese Angriffe nehmen immer weiter zu. Indem ein Datenverkehrsaufkommen erzeugt wird, das die verfügbare Bandbreite des Unternehmens übersteigt, wird bei dem Angriff die Kapazität der Internetverbindung des angegriffenen Unternehmens ausgelastet – wodurch alle anderen Online-Aktivitäten deaktiviert oder verzögert werden.

ANGRIFFE AUF DER PROGRAMMEBENE

Mit Angriffen auf der Programmebene sollen Server lahmgelegt werden, die wichtige Programme bereitstellen, z. B. die Web-Server, von denen die Onlinepräsenz eines angegriffenen Unternehmens abhängt.

ANDERE INFRASTRUKTURANGRIFFE

Angriffe, die darauf abzielen, die Netzwerkgeräte und/oder Server-Betriebssysteme zu deaktivieren, können den gesamten Betrieb wichtiger Geschäftsabläufe vollständig anhalten.

HYBRIDANGRIFFE

Cyberkriminelle führen auch komplexe Angriffe aus, die mehrere Methoden kombinieren – Überlastungsangriffe, Angriffe auf der Programmebene und Angriffe auf die Infrastruktur.

OPTIMALE LÖSUNG FÜR VERTEIDIGUNG UND RISIKOBEGRENZUNG

Kaspersky DDoS Protection bietet einen umfassenden, integrierten Schutz vor DDoS-Angriffen und eine Lösung zur DDoS-Minimierung, die alle Maßnahmen für den Schutz Ihres Unternehmens abdeckt. Kaspersky DDoS Protection bietet alles, damit sich Ihr Unternehmen vor allen Arten von DDoS-Angriffen schützen und ihre Auswirkungen minimieren kann – von kontinuierlicher Analyse über Warnungen bezüglich möglicherweise erfolgende Angriffe bis hin zum Empfang Ihres umgeleiteten Datenverkehrs, der Bereinigung Ihres Datenverkehrs und der Weiterleitung des bereinigten Datenverkehrs an Sie.

KASPERSKY DDOS PROTECTION UMFASST:

- Kaspersky Lab Sensorsoftware – innerhalb Ihrer IT-Infrastruktur
- Die Dienste unseres globalen Netzwerks an Cleaning Center für Datenverkehr
- Unterstützung von unseren Security Operations Center- und DDoS-Sicherheitsexperten
- Detaillierte Angriffsanalysen und -Reporting

SO FUNKTIONIERT KASPERSKY DDOS PROTECTION

Die Sensorsoftware von Kaspersky Lab erfasst Informationen über Ihren gesamten Kommunikationsverkehr – ganzjährig rund um die Uhr. Der Sensor ist so nah wie möglich an der Ressource installiert, die Sie schützen möchten – und erfasst kontinuierlich Informationen über Ihren Datenverkehr:

- Kopfzeilendaten
- Protokolltypen
- Anzahl von gesendeten und erhaltenen Byte
- Anzahl von gesendeten und erhaltenen Paketen
- Aktivitäten und Verhalten – von jedem Besucher auf Ihrer Webseite
- Alle Metadaten über Ihren Datenverkehr

Diese gesamten Informationen werden an die Cloud-basierten Server von Kaspersky Labs weitergeleitet und dort analysiert, damit wir Profile des Verhaltens von typischen Besuchern und Ihres typischen Datenverkehrs erstellen können. Dabei wird auch berücksichtigt, wie der Datenverkehr nach Tageszeit und Wochentag abweichen kann und wie sich besondere Ereignisse auf die Muster des Datenverkehrs auswirken. Aufgrund dieser detaillierten Einblicke in Ihren "normalen" Datenverkehr“ und das „normale Besucherverhalten“ können unsere Cloud-basierten Server Ihren Datenverkehr in Echtzeit und akkurat ermitteln und schnell Anomalien identifizieren, die darauf hindeuten, dass Ihr Unternehmen angegriffen wird.

Zudem überwachen unsere Experten kontinuierlich die DDoS-Bedrohungslage, um neue Angriffe zu identifizieren. Dank dieses Expertenwissens kann Kaspersky Lab sicherstellen, dass Sie von einer schnellen Reaktion auf Angriffe profitieren.

VERMEIDEN VON FEHLALARMEN … UND BEREINIGUNG IHRES DATENVERKEHRS

Sobald ein möglicher Angriff auf Ihr Unternehmen von unseren Servern oder Sicherheitsexperten festgestellt wurde, erhält das Kaspersky Lab Security Operations Center eine Warnung. Um falsche Warnmeldungen – und damit überflüssige Geschäftsunterbrechungen – zu vermeiden, überprüfen Experten von Kaspersky Lab, ob die Anomalie im Datenverkehr oder das verdächtige Verhalten aus einem DDoS-Angriff resultiert. Dann treten unsere Experten sofort mit Ihrem Unternehmen in Kontakt, um Ihnen die Weiterleitung Ihres Datenverkehrs an unser Netzwerk von Cleaning Center zu empfehlen.

Wenn während des Angriffs Ihr gesamter Datenverkehr durch eines unserer Cleaning Center geleitet wird:

- wird Ihre Infrastruktur nicht mehr durch die schiere Menge an „Datenmüll“ überlastet
- entfernt unser Bereinigungsprozess den gesamten Datenmüll
- wird legitimer Datenverkehr von unserem Netzwerk an Cleaning Center zurück an Sie geleitet

… und der gesamte Vorgang ist für Ihre Mitarbeiter und Kunden vollständig transparent.

SCHNELLE UND EINFACHE EINRICHTUNG DES SCHUTZES

Wenn Sie sich für Kaspersky DDoS Protection entscheiden, müssen Sie einige Konfigurationen vornehmen, bevor Ihre Rund-um-die-Uhr-Überwachung – und Ihre Kommunikationskanäle für Live-Angriffe – eingerichtet werden. Kaspersky Lab und seine Partner übernehmen den Konfigurationsvorgang, soweit Sie das wünschen.

Wenn Sie eine Komplettlösung benötigen, können Kaspersky Lab und seine Partner die Mehrheit von Konfigurationsprozessen abdecken, einschließlich:

- Installation der Sensorsoftware und -hardware an Ihrem Standort
- Einrichtung der Umleitung des Datenverkehrs in in unsere Cleaning Center
- Einrichtung der Bereitstellung des bereinigten Datenverkehrs für Ihr Unternehmen

… dann müssen Sie dem Sensor nur noch eine separate Internetanbindung zur Verfügung stellen, sodass Kaspersky DDoS Protection weiterhin Daten erfassen kann, wenn Ihre Internetanbindung durch einen Angriff gestört wurde.

DER SENSOR – MIT ÜBERWACHUNG RUND UM DIE UHR

Die Sensorsoftware von Kaspersky Lab wird mit einem standardmäßigen Ubuntu Linux-Betriebssystem geliefert. Da die Sensorsoftware auf einem standardmäßigen x86-Server ausgeführt wird – oder auf einer virtualisierten Maschine * – müssen Sie keine spezielle Hardware warten.

Der Sensor ist mit dem SPAN-Port (Switched Port Analyzer) verbunden, damit Sie die bestmögliche Übersicht über den gesamten Datenfluss in und aus der zu schützenden Ressource erhalten.

Sobald der Sensor mit Ihrer Infrastruktur verbunden ist, beginnt er damit, Daten aus Ihrem eingehenden und ausgehenden Netzwerkverkehr zu erfassen. Er analysiert die Kopfzeilendaten jedes Pakets und sendet Informationen an die Cloud-Server von Kaspersky DDoS Protection, wo wir statistische Profile des normalen Verkehrsverhaltens und normalen Besucherverhaltens für Ihr Unternehmen erstellen.

Damit Ihre Kommunikation privat bleibt und um Ihre Compliance-Verpflichtungen zu erfüllen, erfasst der Sensor keine Inhalte von Nachrichten in Ihrem Kommunikationssystem. Der Sensor erfasst nur Informationen über Ihren Datenverkehr, sodass die Vertraulichkeit Ihrer Nachrichten durch die Prozesse von Kaspersky DDoS Protection niemals verletzt wird.

*Die virtualisierte Maschine muss die von Kaspersky Lab festgelegten Mindestanforderungen an die Leistung erfüllen.

UMLEITUNG DES DATENVERKEHRS

Unter normalen Bedingungen – während die Cloud-basierten Kaspersky DDoS Protection-Server Ihren Datenverkehr auf Anzeichen eines DDoS-Angriffs überwachen – wird Ihr Datenverkehr direkt an Ihr Unternehmensnetzwerk geleitet. Ihr Datenverkehr wird erst dann an die Cleaning Center unseres globalen Netzwerks geleitet, wenn ein Angriff erkannt wurde und Ihr Unternehmen bestätigt hat, dass der Datenverkehr umgeleitet werden soll.

Kaspersky DDoS Protection bietet Ihnen eine Auswahl an Umleitungsmethoden:

- Border Gateway Protocol (BGP)
- Domain Name System (DNS)

VIRTUALISIERTE "GENERIC ROUTING ENCAPSULATION (GRE)-TUNNEL"

Unabhängig davon, welche Umleitungsmethode sich am besten für Ihr Unternehmen eignet, werden virtualisierte GRE-Tunnel für die Kommunikation zwischen Ihrem Border Gateway – oder Router – und jedem relevanten Kaspersky DDoS Protection-Cleaning Center verwendet.

Im Falle eines DDoS-Angriffs auf Ihr Unternehmen wird Ihr gesamter Datenverkehr an eines unserer Cleaning Center weitergeleitet. Die virtualisierten GRE-Tunnel werden dann verwendet, um den bereinigten Datenverkehr von unseren Cleaning Center an Ihr Unternehmen zu übertragen.

▶ ENTSCHEIDUNG ZWISCHEN BGP UND DNS

Ob Sie Ihren Verkehr über BGP oder DNS umleiten, hängt größtenteils von der Art Ihrer IT-Systeme und ihrer Kommunikations-Infrastruktur ab:

- Für BGP benötigen Sie:
  - Ein anbieterneutrales Netzwerk, welches die Ressourcen beinhaltet, die Sie schützen möchten
  - Ein autonomes System

  … und die meisten großen Unternehmen können diese Kriterien erfüllen.

- Für DNS müssen Sie in der Lage sein:
  - Ihre eigene Domain-Zone für die Ressourcen zu verwalten, die Sie schützen möchten
  - das Time to Live (TTL) für DNS-Aufzeichnungen auf 5 Minuten einzustellen

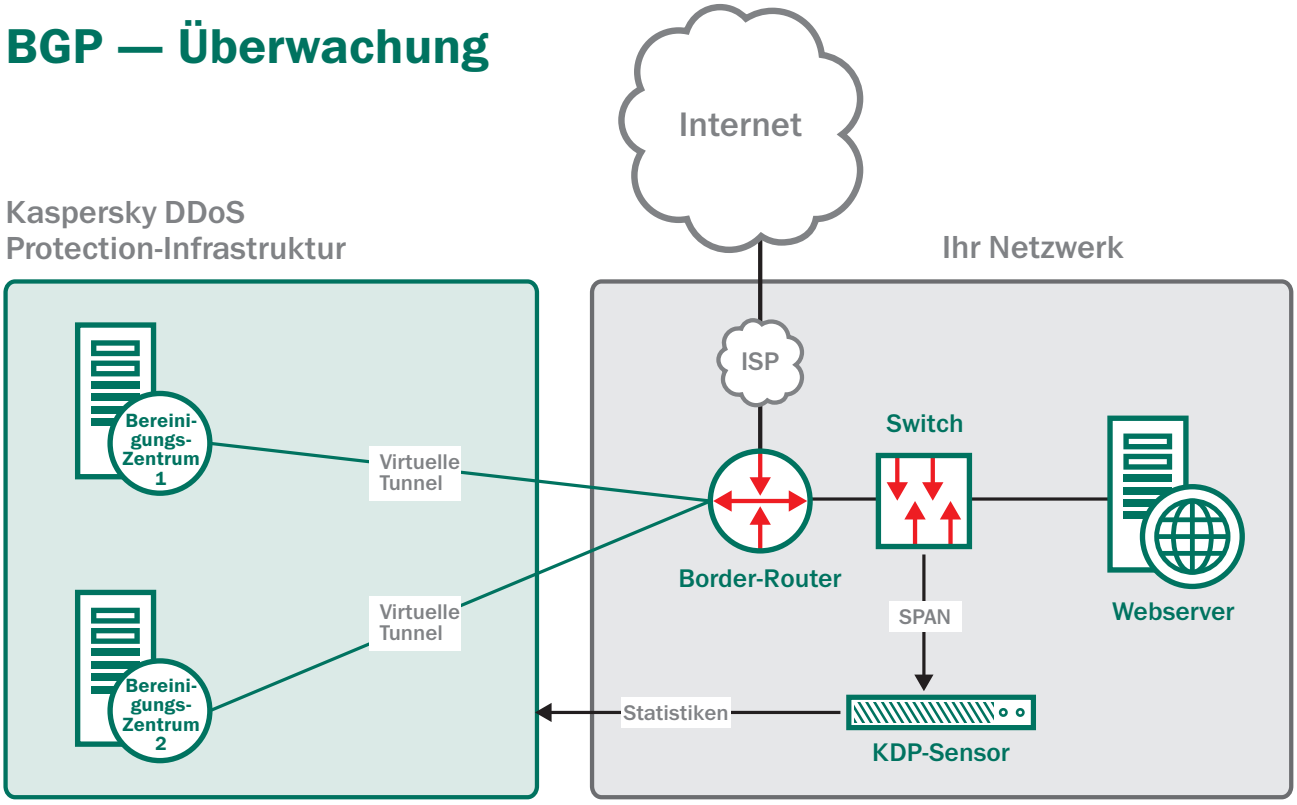
Während eines Angriffs wird mit der BGP-Methode in der Regel eine schnellere Umleitung des Verkehrs ermöglicht. Daher ziehen die meisten Unternehmen BGP vor.

FUNKTIONSWEISE DER BGP-UMLEITUNG

ÜBERWACHUNG

Im Überwachungsmodus wird Ihr gesamter Datenverkehr direkt an Ihr Unternehmen geleitet. Jedoch befinden sich die virtualisierten GRE-Tunnel im „Live"-Betrieb, wobei Ihre Router und unsere BGP-Router häufig Statusinformationen austauschen, sodass die Kaspersky Cleaning Center jederzeit bereit sind, Ihren umgeleiteten Datenverkehr zu empfangen, falls dies erforderlich wird.

BGP — Überwachung

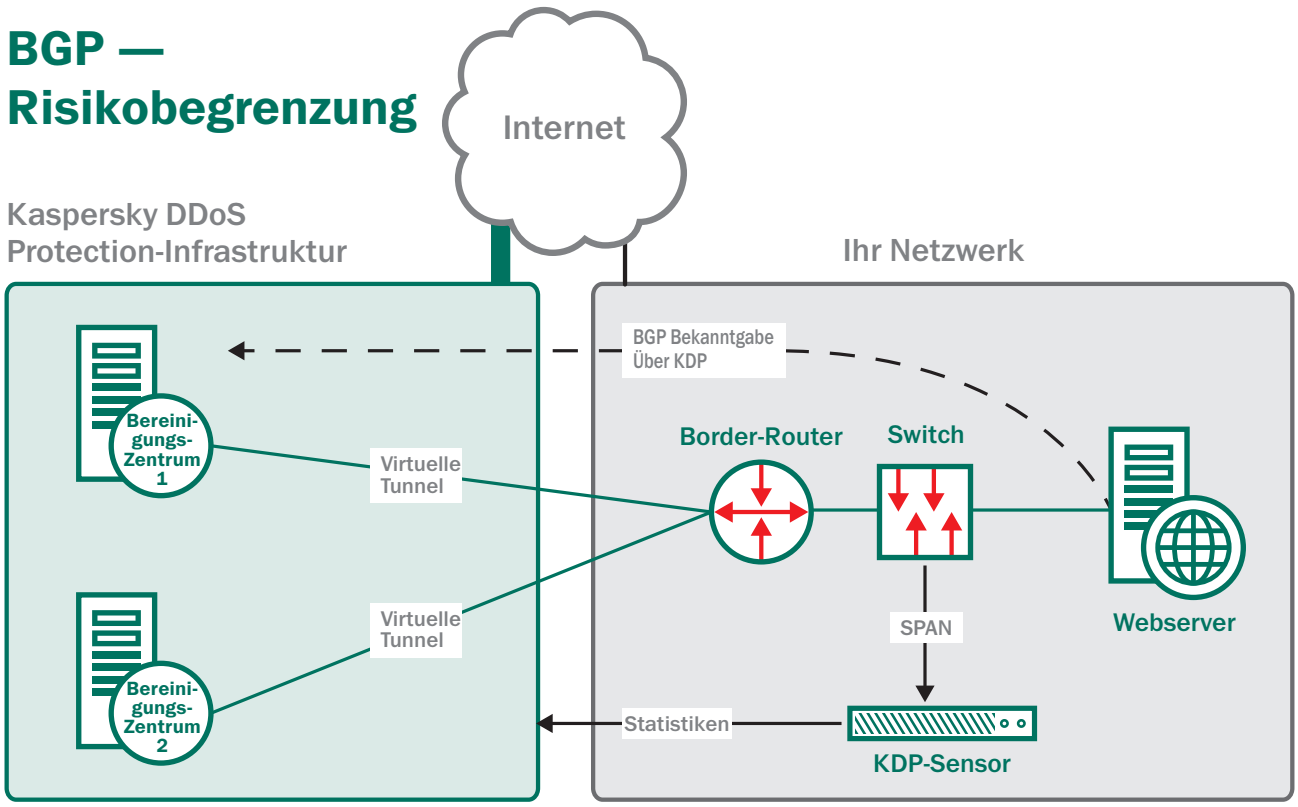


WÄHREND DES ANGRIFFS

Wenn der Sensor von Kaspersky Lab eine Anomalie im Datenverkehr feststellt und die Experten von Kaspersky Lab den Beginn eines Angriffs bestätigen, können Sie sich dafür entscheiden, Ihren gesamten Datenverkehr an ein Kaspersky Cleaning Center umzuleiten.

Während des gesamten Angriffs erfasst der Sensor von Kaspersky Lab weiterhin Daten und sendet sie zur Analyse an die Cloud-basierten Kaspersky DDoS Protection-Server.

BGP — Risikobegrenzung



NACH DEM ANGRIFF

Wenn der Angriff vorbei ist, wird Ihr Datenverkehr wieder direkt an Ihr Unternehmen geleitet. Der Sensor erfasst weiterhin Informationen über Ihren Datenverkehr und leitet diese Daten kontinuierlich an unsere Cloud-basierten Server weiter, damit wir unsere Verhaltensprofile Ihrer normalen Verkehrsbedingungen fortlaufend verfeinern können.

Die virtualisierten Tunnel bleiben weiterhin im Live-Betrieb. Sie tauschen Statusinformationen zwischen Ihren Routern und den Routern von Kaspersky Lab aus, sodass Kaspersky DDoS Protection sofort einsatzbereit ist, wenn ein Angriff gegen Ihr Unternehmen gestartet wird und Sie sich erneut dafür entscheiden, Ihren Datenverkehr umzuleiten.

Die Experten von Kaspersky Lab stellen Ihnen nach dem Angriff zudem eine detaillierte Analyse zur Verfügung, die Berichte zu Folgendem umfasst:

- Was während des Angriffs geschah
- Wie lange der Angriff dauerte
- Wie genau ist Kaspersky DDoS Protection mit dem Angriff umgegangen?

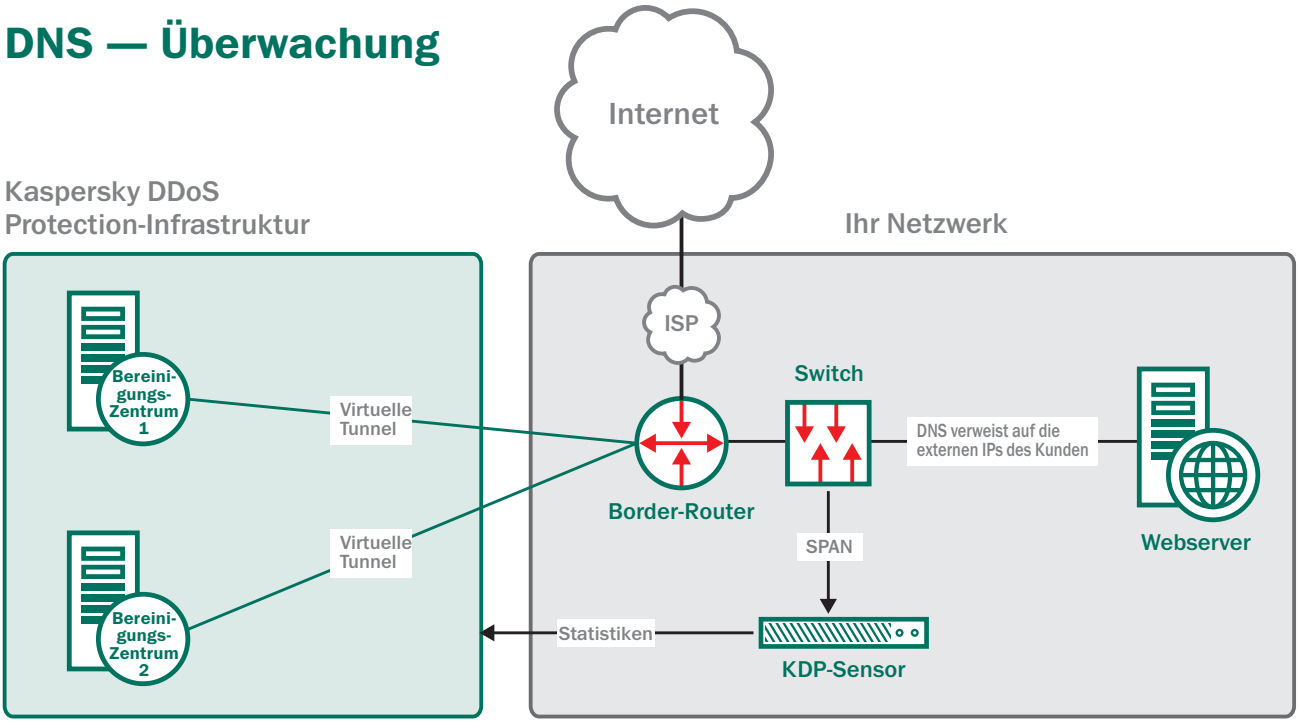
FUNKTIONSWEISE DER DNS-UMLEITUNG

ÜBERWACHUNG

Während der Erstinstallation weist Kaspersky Lab Ihrem Unternehmen eine seiner Kaspersky DDoS Protection IP-Adressen zu. Diese Adresse kommt im Falle eines Angriffs zum Einsatz.

Im Überwachungsmodus wird Ihr gesamter Datenverkehr direkt an Ihr Unternehmen geleitet – über die normale(n) IP-Adresse(n). Jedoch befinden sich die virtualisierten GRE-Tunnel im „Live"-Betrieb, wobei Ihre Router und unsere BGP-Router häufig Statusinformationen austauschen, sodass die Kaspersky DDoS Protection-Cleaning Center jederzeit bereit sind, Ihren umgeleiteten Datenverkehr zu empfangen, falls dies erforderlich wird.

DNS — Überwachung

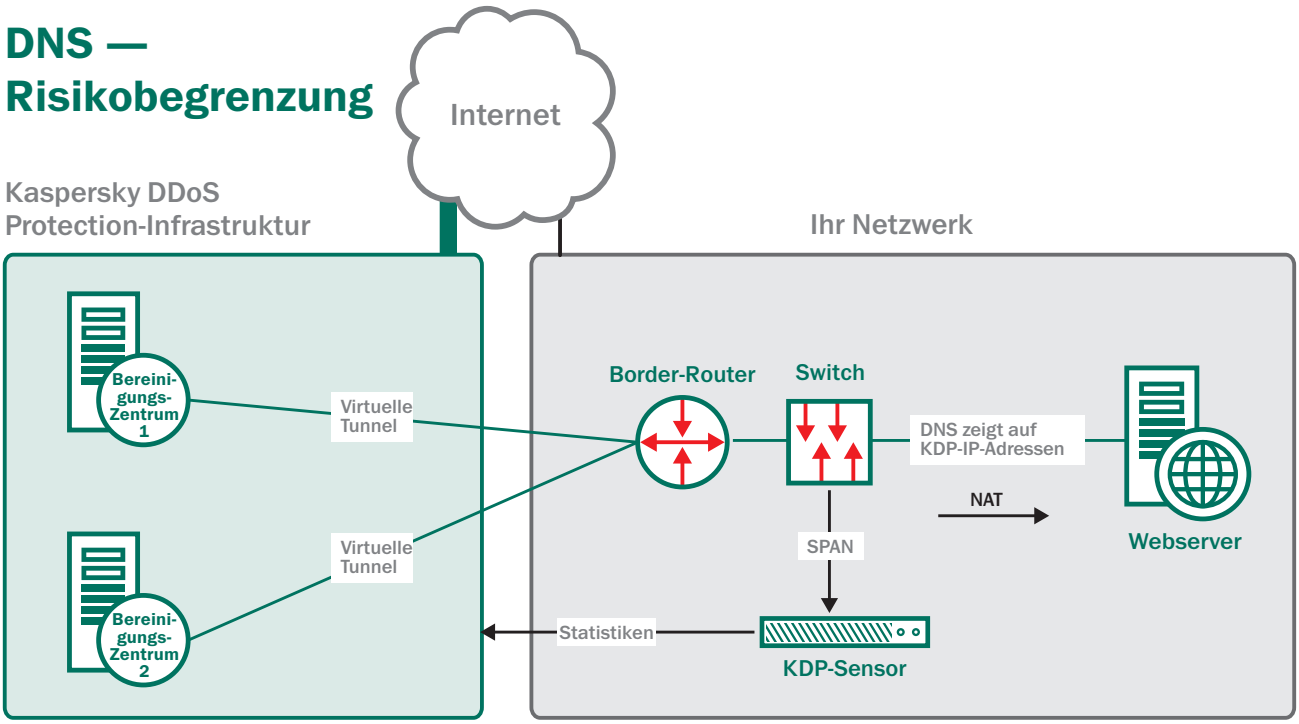


WÄHREND DES ANGRIFFS

Wenn der Sensor von Kaspersky Lab eine Anomalie im Datenverkehr erkennt und die Experten von Kaspersky Lab den Beginn eines Angriffs bestätigen, ändern Sie einfach die IP-Adresse Ihres Unternehmens im DNS-Eintrag, sodass Ihr Unternehmen nun die IP-Adresse von Kaspersky DDoS Protection verwendet, die ihm bei der Erstinstallation zugewiesen wurde. Da Hacker Ihre IP-Adresse direkt angreifen können, muss Ihr ISP außerdem den gesamten Datenverkehr an Ihre ursprüngliche IP-Adresse blockieren – mit Ausnahme der Kommunikation mit der DDoS Protection-Infrastruktur von Kaspersky Lab.

Nachdem Sie Ihre IP-Adresse geändert haben, wird Ihr gesamter Datenverkehr an die Cleaning Center von Kaspersky Lab umgeleitet. Dann wird der bereinigte Datenverkehr von unseren Cleaning Center über die virtualisierten GRE-Tunnel zurück an Ihr Unternehmen geleitet.

DNS — Risikobegrenzung



NACH DEM ANGRIFF

Wenn der Angriff vorbei ist, können Sie Ihre ursprüngliche IP-Adresse im DNS-Eintrag wieder freigeben, damit Ihr Datenverkehr wieder direkt an Ihr Unternehmen gesendet wird.

Der Sensor von Kaspersky Lab erfasst weiterhin Informationen über Ihren Datenverkehr und leitet diese Daten kontinuierlich an unsere Cloud-basierten Server weiter, damit wir unsere Verhaltensprofile Ihrer normalen Verkehrsbedingungen fortlaufend verfeinern können.

Die virtualisierten Tunnel bleiben weiterhin im Live-Betrieb. Sie tauschen Statusinformationen zwischen Ihren Routern und den Routern von Kaspersky Lab aus, sodass Kaspersky DDoS Protection sofort einsatzbereit ist, wenn ein Angriff gegen Ihr Unternehmen gestartet wird und Sie sich erneut dafür entscheiden, Ihren Datenverkehr umzuleiten.

Die Experten von Kaspersky Lab stellen Ihnen nach dem Angriff zudem eine detaillierte Analyse zur Verfügung, die Berichte zu Folgendem umfasst:

- Was während des Angriffs geschah
- Wie lange der Angriff dauerte
- Wie genau ist Kaspersky DDoS Protection mit dem Angriff umgegangen?

BEDROHUNGSINFORMATIONEN – FÜR EINEN NOCH BESSEREN SCHUTZ

Kaspersky DDoS Protection umfasst eine weitere wichtige Verteidigungskomponente.

Kaspersky Lab ist einer der ersten Anbieter von Anti-Malware-Software, der eine Lösung zum Schutz vor DDoS-Angriffen bietet. Kaum ein anderer Anti-DDoS-Anbieter verfügt über unsere Fachkenntnisse und eine interne Sicherheitsabteilung und -Infrastruktur in vergleichbarer Größe.

Im Rahmen ihrer Arbeit an wegweisenden IT-Sicherheitslösungen überwachen unsere Experten kontinuierlich die Bedrohungslage, um neue Malware und noch unbekannte Internetbedrohungen zu identifizieren. Dieselben Experten überwachen mit gleichermaßen fortschrittlichen Methoden die DDoS-Bedrohungslage. Dank dieser Fachkenntnisse können wir DDoS-Angriffe früher erkennen, damit Ihr Unternehmen von schnellerem Schutz profitiert.

MEHRSTUFIGER SCHUTZ

Indem wir eine einzigartige Kombination von statistischer Analyse, Verhaltensanalyse und proaktivem Expertenwissen über DDoS-Angriffe bieten, stellen wir einen gründlicheren Schutz vor DDoS-Angriffen bereit.

DataSheet_DDoS/August14/Global