KASPERSKY DDOS PROTECTION

Erfahren Sie, wie Kaspersky Lab Ihr Unternehmen gegen DDoS-Angriffe schützt

UNTERNEHMEN IM VISIER DER CYBER-KRIMINELLEN

Falls Ihr Unternehmen jemals Opfer eines Angriffs durch Distributed Denial of Service (DDoS) wurde, wissen Sie bereits, dass die damit einhergehenden finanziellen Verluste und der Imageschaden verheerend sein können. Aber selbst wenn Ihr Unternehmen bisher in der glücklichen Lage war, der Aufmerksamkeit und den Angriffen der Cyber-Kriminellen und Hacker zu entgehen, so sind die Aussichten, auch in Zukunft von diesem Übel verschont zu bleiben, weitaus weniger positiv.

DDOS ANGRIFFE STEIGEN RASANT

Leider ist der finanzielle Aufwand zur Durchführung von DDoS-Angriffen in den vergangenen Jahren deutlich gesunken. Dies hat zu einem beträchtlichen Anstieg der Angriffe geführt. Zugleich nehmen die Angriffe immer mehr an Komplexität zu und übersteigen mittlerweile eine Größenordnung, die die Kommunikation des angegriffenen Unternehmens binnen Sekunden zum Erliegen bringen kann. Dabei werden wichtige Geschäftsprozesse beeinträchtigt und die Online-Präsenz des Unternehmens lahmgelegt.

Da Unternehmen jeder Größe zur Aufrechterhaltung geschäftskritischer Abläufe auf eine jederzeit funktionierende IT-Infrastruktur und den ungehinderten Zugang zu ihren Online-Ressourcen angewiesen sind, können Ausfallzeiten in Folge eines DDoS-Angriffs keinesfalls akzeptiert werden. Zweifellos können Unternehmen, angesichts des Volumens, der Reichweite und der zunehmenden Schwere der DDoS-Angriffe, die Einrichtung einer angemessenen Abwehr und das Ergreifen geeigneter Maßnahmen zur Eindämmung dieser Bedrohungen nicht bis zum Zeitpunkt des Angriffs auf ihre Infrastruktur aufschieben. Stattdessen müssen sich Unternehmen und öffentliche Institutionen der Risiken von DDoS-Angriffen bewusst werden und ausreichende Vorkehrungen zur Abwehr dieser Gefahren treffen.

„GEFAHR ERKANNT, GEFAHR GEBANNT“

Jedes Unternehmen braucht eine Anti-DDoS-Strategie, die bei Entdeckung eines Angriffs jederzeit angewendet werden kann. Zur Eindämmung der negativen Auswirkungen kann das Unternehmen dann im Ernstfall unverzüglich die folgenden Maßnahmen ergreifen:

- Minimieren von Ausfallzeiten geschäftskritischer Infrastrukturen und Prozesse
- Sicherstellen des Zugriffs von Kunden auf Online-Dienste
- Aufrechterhalten der Produktivität von Mitarbeitern
- Minderung des Imageschadens

▶ SZENARIO EINES DDOS-ANGRIFFS

Zur Ausführung eines DDoS-Angriffs auf die IT-Infrastruktur eines Unternehmens bedienen sich Cyber-Kriminelle und Hacker den verschiedensten Methoden, die das Zielsystem überlasten oder dessen Verfügbarkeit außer Kraft setzen.

VOLUMENANGRIFFE

Bei diesen Attacken werden Datenvolumen erzeugt, die von der verfügbaren Bandbreite des angegriffenen Firmennetzwerks nicht mehr bewältigt werden können. Schließlich kommt die Internetverbindung dadurch vollständig zum Erliegen, und die vorhandenen Online-Ressourcen können nicht oder nur mehr eingeschränkt genutzt werden.

ANGRIFFE AUF DIE ANWENDUNGSSCHICHT

Bei Angriffen auf die Anwendungsschicht wird versucht, Server, auf denen geschäftskritische Anwendungen laufen wie beispielsweise die Webserver, auf denen die Online-Präsenz des Opfers basiert, zum Absturz zu bringen.

ANDERE ANGRIFFE AUF DIE NETZWERKINFRASTRUKTUR

Angriffe, die darauf abzielen, Netzwerkgeräte und/oder Server-Betriebssysteme zu deaktivieren, können zum vollständigen Stillstand zentraler Geschäftsprozesse führen.

HYBRIDE ANGRIFFE

Cyber-Kriminelle führen auch komplexe Angriffe durch, bei denen sie gleichzeitig mehrere Methoden zum Einsatz bringen. Die dabei verwendeten Techniken zielen entweder auf die Netzwerkverbindungen, die Anwendungen oder die Infrastruktur ab.

UMFASSENDE LÖSUNG ZUR ABWEHR UND SCHADENSBEGRENZUNG

Kaspersky DDoS Protection ist eine integrierte Komplettlösung zur Abwehr und Schadensminderung von DDoS-Angriffen, die alle gefährdeten Bereiche in Ihrem Unternehmen abdeckt. Von der kontinuierlichen Analyse Ihres Online-Datenverkehrs über die Alarmierung im Falle eines möglichen Angriffsversuchs bis hin zu der dadurch erforderlichen Umleitung, Bereinigung und anschließenden Rückleitung des „sauberen“ Datenverkehrs bietet der DDoS-Schutz von Kaspersky alles, was Sie in Ihrem Unternehmen benötigen, um sich gegen alle Arten von DDoS-Angriffen zu verteidigen und vorhandene Risiken zu mindern.

IM LEISTUNGSUMFANG VON KASPERSKY DDOS PROTECTION ENTHALTEN:

- Die Sensor-Software von Kaspersky Lab – ein integraler Bestandteil Ihrer IT-Infrastruktur
- Die Leistungen des globalen Netzwerks unserer „Zentren zur Bereinigung des Datenverkehrs“
- Unterstützung durch unser Sicherheitsüberwachungszentrum und unsere Experten für den Schutz gegen DDoS-Angriffe
- Detaillierte Analysen und Berichte

FUNKTIONSWEISE VON KASPERSKY DDOS PROTECTION

Die Sensor-Software von Kaspersky Lab sammelt rund um die Uhr alle Informationen über Ihren Datenverkehr. Der Sensor wird möglichst dicht an der zu schützenden Ressource installiert. Dort erfasst er u. a. folgende Daten über Ihre Kommunikation:

- Header-Daten
- Protokolltypen
- Anzahl der gesendeten und empfangenen Bytes
- Anzahl der gesendeten und empfangenen Pakete
- Aktivitäten und Verhalten von jedem Besucher auf Ihrer Website
- Alle Metadaten über Ihren Datenverkehr

Alle erfassten Informationen werden an die Cloud-Server von Kaspersky Lab weitergeleitet und analysiert. Die daraus erstellten Profile geben Aufschluss über das Verhalten durchschnittlicher Besucher sowie die Eigenschaften des typischen Verkehrs. Zudem lassen sich Aussagen darüber treffen, inwieweit der Traffic je nach Tageszeit und Wochentag variiert und wie außergewöhnliche Ereignisse das Muster Ihres Datenverkehrs beeinflussen können. Anhand dieser detaillierten Kenntnisse über die „Bedingungen bei normalem Datenverkehr“ und das „normale Besucherverhalten“ können unsere Cloud-Server die aktuelle Situation Ihres Datenverkehrs präzise und in Echtzeit einschätzen und innerhalb kürzester Zeit potenzielle Auffälligkeiten und Abweichungen erkennen, die einen Angriff auf Ihr Unternehmen vermuten lassen.

Darüber hinaus überwachen unsere Sicherheitsexperten permanent die DDoS-Bedrohungslandschaft und können dadurch das Risiko bevorstehender Angriffe sofort erkennen. Durch diese zielgenaue Ermittlung des Angriffspotenzials können Kunden von Kaspersky Lab entstehende Bedrohungen bereits im Frühstadium erkennen und angemessen darauf reagieren.

VERMEIDEN VON FEHLALARMEN MIT ANSCHLIESSENDER BEREINIGUNG DES DATENVERKEHRS

Sobald unsere Server oder Sicherheitsexperten einen potenziellen Angriff auf Ihr Unternehmen erkennen, wird im Sicherheitsüberwachungszentrum von Kaspersky Lab ein Alarm ausgelöst. Um Fehlalarme und unnötige Störungen in Ihrem Betriebsablauf zu vermeiden, überprüfen die Techniker von Kaspersky Lab zunächst, ob der Datenverkehr tatsächlich Unregelmäßigkeiten aufweist oder das verdächtige Verhalten von einem DDoS-Angriff herrührt. Anschließend nehmen unsere Experten sofort Kontakt mit Ihrem Unternehmen auf, um Ihnen die Umleitung des Datenverkehrs auf das Netzwerk unserer Bereinigungszentren zu empfehlen.

Während des Angriffs – wenn Ihr gesamter Datenverkehr unser Bereinigungszentrum durchläuft:

- Verhindern wir die Überschwemmung Ihrer Infrastruktur mit unerwünschtem Datenverkehr
- Bereinigen wir Ihren Datenstrom
- Leiten wir zulässigen Traffic aus dem Netzwerk unserer Bereinigungszentren an Sie zurück

… und der gesamte Prozess ist für Ihre Mitarbeiter und Kunden in allen Phasen vollkommen transparent und nachvollziehbar.

SICHERHEIT EINRICHTEN GEHT SCHNELL UND EINFACH

Wenn Sie sich für Kaspersky DDoS Protection entscheiden, sind nur einige wenige Konfigurationen erforderlich, um eine durchgängige Überwachung und eine jederzeit verfügbare Abwehr von Angriffen auf Ihre Kommunikationskanäle zu gewährleisten. Kaspersky Lab kann in Zusammenarbeit mit seinen Partnern jeden von Ihnen gewünschten Anteil der Konfigurationsaufgaben übernehmen.

Wenn Sie eine schlüsselfertige Lösung bevorzugen, kann Kaspersky Lab in Zusammenarbeit mit seinen Partnern den überwiegenden Teil der erforderlichen Systemkonfigurationen für Sie übernehmen. Dabei führen wir u. a. folgende Aufgaben durch:

- Installieren der Sensor-Software und -Hardware in Ihrem Netzwerk
- Einrichten der Umleitung zu unseren Bereinigungszentren
- Konfigurieren der Bereitstellung von „sauberem“ Datenverkehr in Ihrem Unternehmen

Anschließend müssen Sie nur noch einen gesonderten Internet-Kanal zur Verbindung mit dem Sensor zur Verfügung stellen – damit sind für Kaspersky DDoS Protection alle Voraussetzungen erfüllt, um weiterhin Daten zu sammeln, wenn Ihr Internet-Hauptkanal durch einen Angriff außer Gefecht gesetzt ist.

DER SENSOR – ZUR ÜBERWACHUNG RUND UM DIE UHR

Die Sensor-Software von Kaspersky Lab ist serienmäßig mit einer konventionellen Linux-Distribution („Ubuntu“) ausgestattet. Da die Sensor-Software auf einem Standard-Server mit x86-Architektur oder auf einer virtuellen Maschine* läuft, gibt es keine speziellen Hardware-Komponenten, die von Ihnen gewartet werden müssen.

Der Sensor ist an den SPAN-Port (Switched Port Analyzer) angebunden und hat daher eine ausgezeichnete Sicht auf den gesamten Datenverkehr, der über die zu schützende Ressource geleitet wird.

Sofort nach Anbindung an Ihre Infrastruktur beginnt der Sensor mit der Überwachung des eingehenden und ausgehenden Datenverkehrs. Er analysiert den Header der einzelnen Datenpakete und leitet die erfassten Informationen an die Cloud-Server von Kaspersky DDoS Protection weiter. Daraus entwickeln wir für Ihr Unternehmen individuelle Statistik-Profile des „normalen Verhaltens von Datenverkehr“ sowie des „normalen Verhaltens von Besuchern“.

Um die Vertraulichkeit Ihrer Kommunikationen zu gewährleisten und Sie bei der Einhaltung von Richtlinien und Vorschriften zu unterstützen, erfasst der Sensor nicht den Inhalt des zu überwachenden Nachrichtenverkehrs. Der Sensor erfasst nur Daten über Ihren Netzverkehr. Die Vertraulichkeit Ihrer Mitteilungen und Nachrichten bleibt daher von den von Kaspersky DDoS Protection ausgeführten Prozessen jederzeit gewahrt.

*Die virtuelle Maschine muss die von Kaspersky Lab festgelegten Mindestanforderungen erfüllen.

UMLEITUNG DES DATENVERKEHRS

Während die Cloud-Server von Kaspersky DDoS Protection Ausschau nach Anzeichen eines DDoS-Angriffs halten, wird der Datenverkehr, unter normalen Bedingungen, direkt an Ihr Unternehmensnetzwerk geleitet. Die Umleitung Ihres Verkehrs an das globale Netzwerk unserer Bereinigungszentren erfolgt nur bei Erkennen eines Angriffs und nach Vorliegen Ihrer ausdrücklichen Einwilligung.

Kaspersky DDoS Protection bietet Ihnen eine Auswahl verschiedener Umleitungsmethoden:

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

VIRTUELLE GRE-TUNNEL (GENERIC ROUTING ENCAPSULATION)

Unabhängig vom optimalen Weiterleitungsverfahren für Ihr Unternehmen erfolgt der Aufbau einer sicheren Kommunikation zwischen Ihrem Border-Gateway, oder Router, und des jeweils zuständigen Bereinigungszentrums von Kaspersky DDoS Protection über virtuelle GRE-Tunnel.

Bei einem DDoS-Angriff auf Ihr Unternehmen kann Ihr gesamter Datenverkehr an eines unserer Bereinigungszentren weitergeleitet werden. Aufgabe der virtuellen GRE-Tunnel ist es dann, den „sauberen“ Datenverkehr aus unseren Bereinigungszentren in Ihr Unternehmen zurückzuleiten.

▶ BGP ODER DNS – SIE HABEN DIE WAHL

Ob Sie Ihren Datenverkehr über BGP oder DNS umleiten, hängt in erster Linie von der IT- und Kommunikationsinfrastruktur Ihres Unternehmens ab:

- Bei Datenübertragung über BGP benötigen Sie:
  - Ein anbieterunabhängiges Netzwerk – in das alle zu schützenden Ressourcen einbezogen sind
  - Ein autonomes System

  … Kriterien, die in den meisten größeren Unternehmen erfüllt sind.

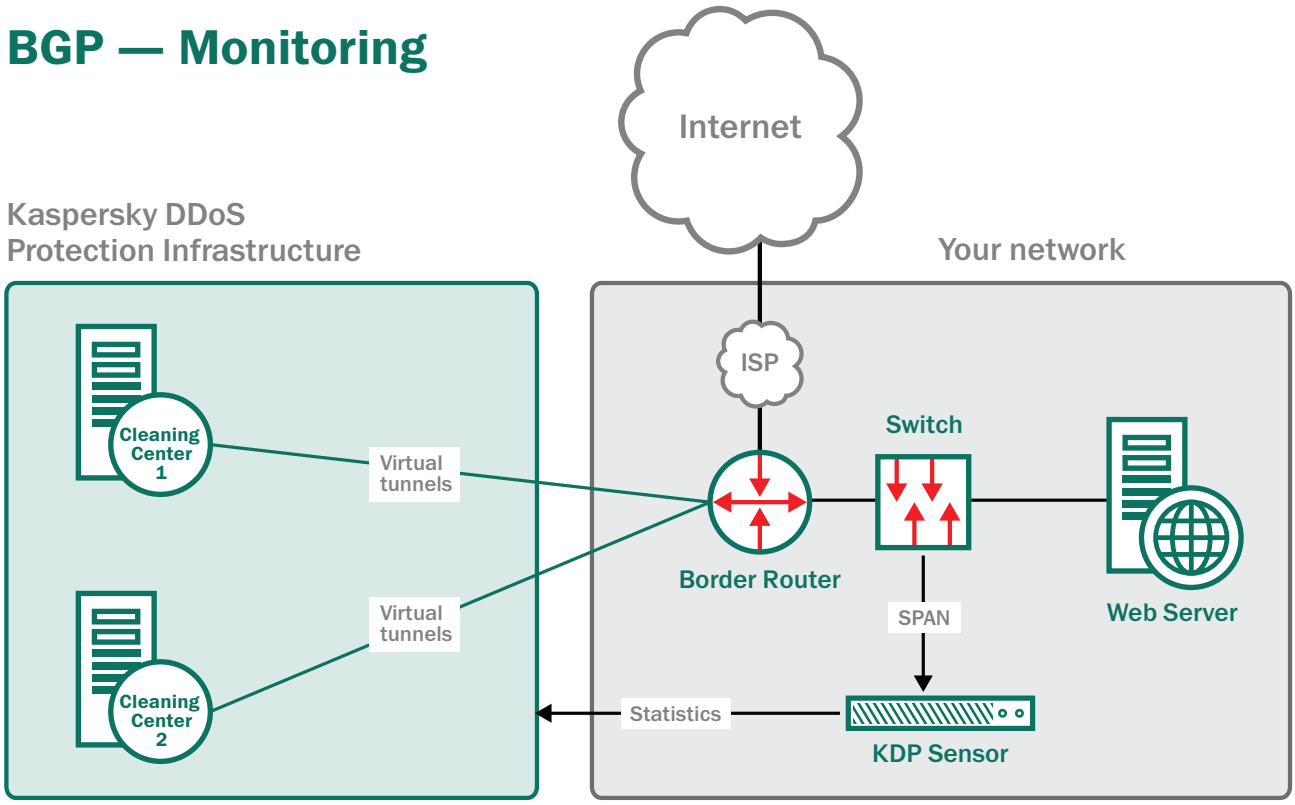
- Bei Datenübertragung über DNS müssen Sie:
  - Für die zu schützenden Ressourcen Ihre eigene Domain-Zone verwalten
  - Die Gültigkeitsdauer (TTL) von DNS-Einträgen auf 5 Minuten einstellen

In der Regel ermöglicht das BGP-Verfahren eine schnellere Umleitung des Datenverkehrs bei Angriffen – die meisten Unternehmen entscheiden sich deshalb zur Datenübertragung für das BGP-Protokoll.

FUNKTIONSWEISE DER BGP-UMLEITUNG

ÜBERWACHUNG

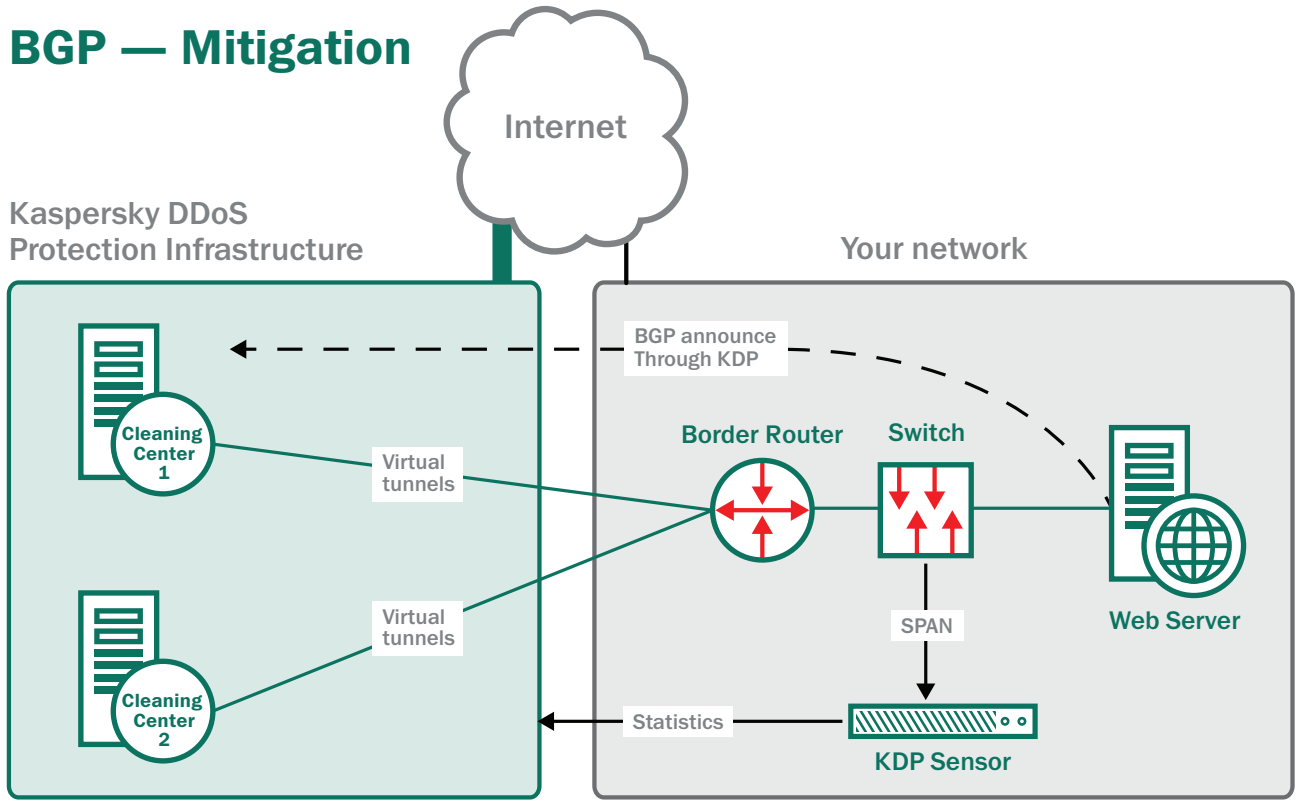
Im Überwachungsmodus wird Ihr kompletter Datenverkehr direkt an Ihr Netzwerk geleitet. Die virtuellen GRE-Tunnel befinden sich allerdings im „Live“-Betrieb, damit zwischen Ihren Routern und unseren BGP-Routern regelmäßig Statusinformationen ausgetauscht werden können und die Bereinigungszentren von Kaspersky DDoS Protection jederzeit bereit sind, um den aus Ihrem Netzwerk umgeleiteten Datenverkehr in Empfang zu nehmen.



WÄHREND EINES ANGRIFFS

Entdeckt der Sensor von Kaspersky Lab Auffälligkeiten oder Abweichungen in Ihrem Netzwerkverkehr und bestätigen die Techniker von Kaspersky Lab den Beginn eines Angriffs, können auf Wunsch sämtliche Datenströme an ein Bereinigungszentrum von Kaspersky DDoS Protection umgeleitet werden.

Während der gesamten Dauer des Angriffs sammelt der Sensor von Kaspersky Lab kontinuierlich Informationen und leitet diese zur Analyse an die Cloud-Server von Kaspersky DDoS Protection weiter.



NACH EINEM ANGRIFF

Nach Beendigung des Angriffs wird Ihr Datenverkehr noch einmal direkt an Ihr Unternehmen geleitet. Der Sensor sammelt weiterhin Daten über Ihren Traffic und leitet diese permanent an unsere Cloud-Server weiter, damit wir die von uns erstellten Verhaltensprofile über die bei Ihnen vorherrschenden Bedingungen bei normalem Netzwerkverkehr schrittweise verfeinern können.

Die virtuellen Tunnel bleiben zum Austausch von Statusinformationen zwischen Ihren Routern und den Routern von Kaspersky Lab fortwährend in Betrieb. Kaspersky DDoS Protection ist dadurch jederzeit in der Lage, bei einem weiteren Angriff auf Ihr Unternehmen unverzüglich zu handeln und nach Rücksprache mit Ihnen den Datenverkehr entsprechend umzuleiten.

Die Experten von Kaspersky Lab liefern Ihnen nach einem Angriff detaillierte Analysen und Berichte mit Angaben zu folgenden Punkten:

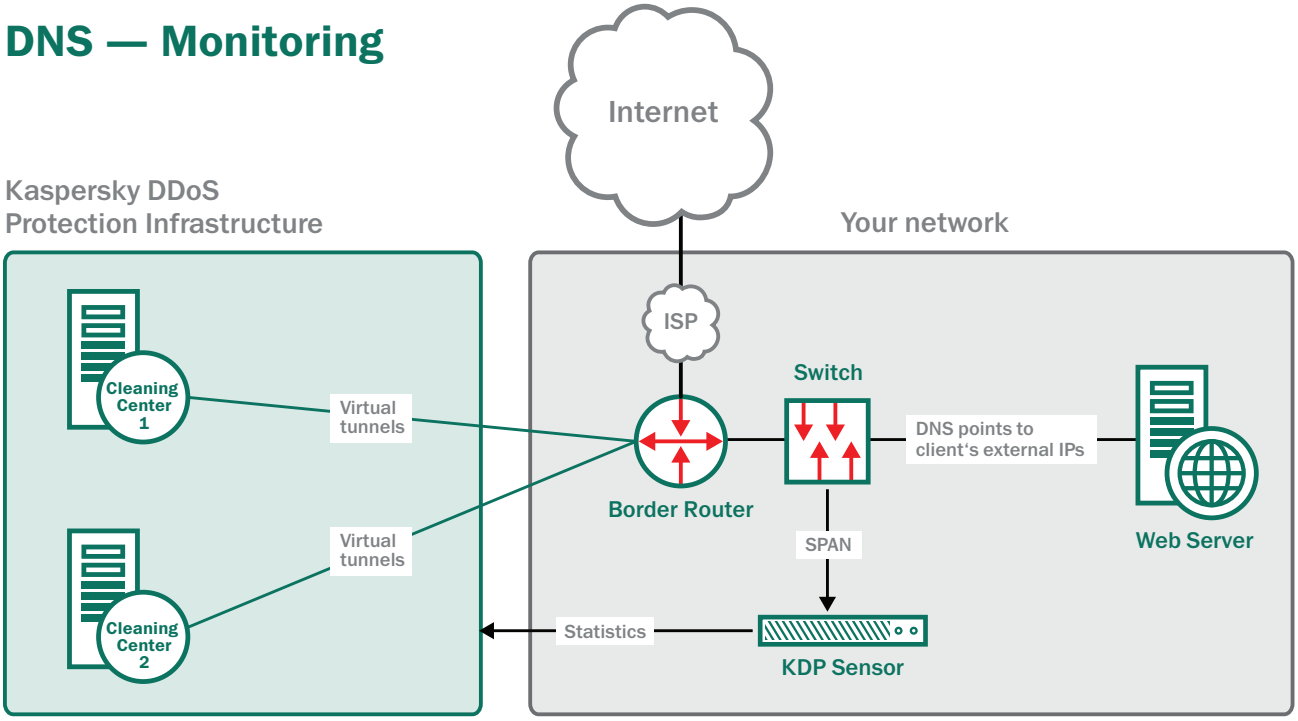
- Verlauf des Angriffs
- Dauer des Angriffs
- Reaktion von Kaspersky DDoS Protection auf den Angriff

FUNKTIONSWEISE DER DNS-UMLEITUNG

ÜBERWACHUNG

Bei der Ersteinrichtung vergibt Kaspersky Lab an Ihr Unternehmen eine Adresse aus einem Pool der in Kaspersky DDoS Protection verfügbaren IP-Adressen. Diese Adresse wird im Falle eines Angriffs genutzt.

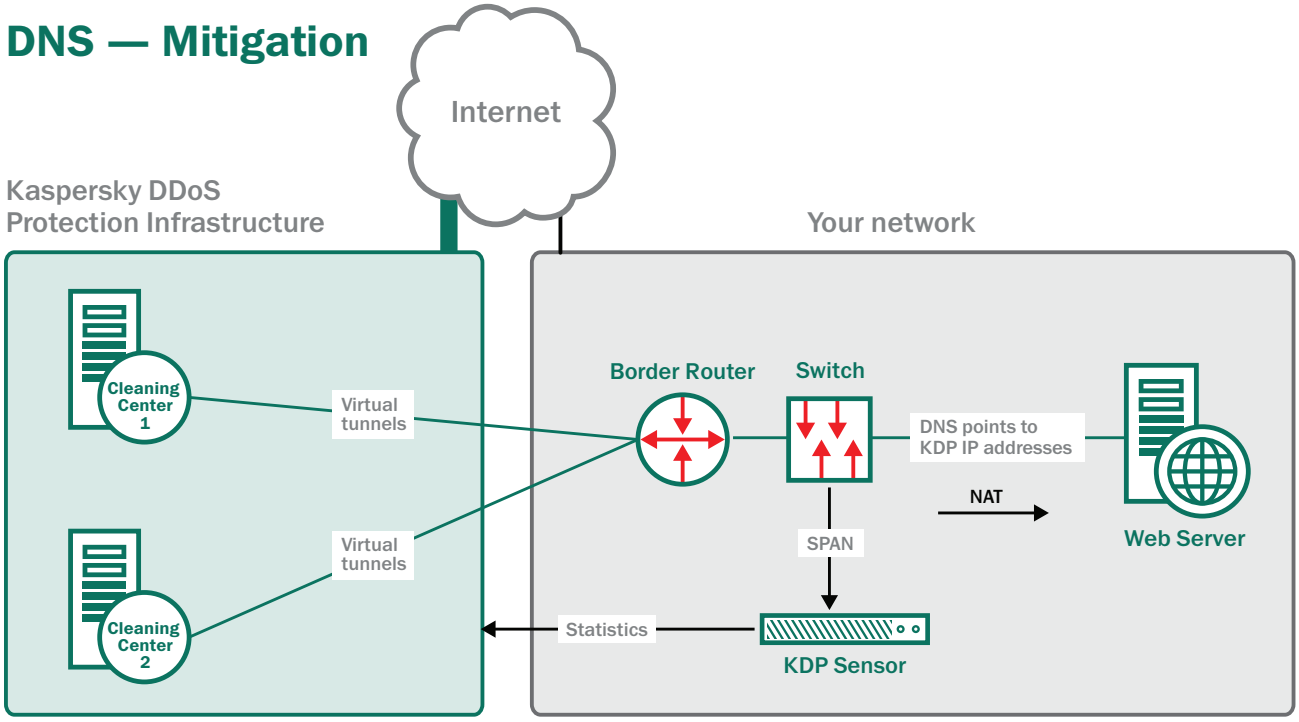
Im Überwachungsmodus wird Ihr kompletter Datenverkehr über die normale(n) IP-Adresse(n) direkt an Ihr Netzwerk geleitet. Die virtuellen GRE-Tunnel befinden sich allerdings im „Live"-Betrieb, damit zwischen Ihren Routern und unseren BGP-Routern regelmäßig Statusinformationen ausgetauscht werden können und die Bereinigungszentren von Kaspersky DDoS Protection jederzeit bereit sind, um den aus Ihrem Netzwerk umgeleiteten Datenverkehr in Empfang zu nehmen.



WÄHREND EINES ANGRIFFS

Entdeckt der Sensor von Kaspersky Lab Auffälligkeiten oder Abweichungen in Ihrem Netzwerkverkehr und bestätigen die Techniker von Kaspersky Lab den Beginn eines Angriffs, ändern Sie einfach die IP-Adresse Ihres Unternehmens im DNS-A-Eintrag Dadurch wird die IP-Adresse verwendet, die Ihnen von Kaspersky DDoS Protection bei der Ersteinrichtung zugewiesen wurde. Da Hacker Ihre IP-Adresse direkt angreifen können, muss Ihr ISP währenddessen den gesamten Datenverkehr – mit Ausnahme der Kommunikation mit der Infrastruktur von Kaspersky DDoS Protection – an Ihre ursprüngliche IP-Adresse sperren.

Da Ihre IP-Adresse geändert wurde, wird Ihr gesamter Datenverkehr an die Bereinigungszentren von Kaspersky Lab umgeleitet. Der „saubere" Datenverkehr wird dann aus unseren Bereinigungszentren über die virtuellen GRE-Tunnel an Ihr Unternehmen zurückgeleitet.



NACH EINEM ANGRIFF

Nach Beendigung des Angriffs können Sie Ihre ursprüngliche IP-Adresse wieder freigeben und den DNS-A-Eintrag ändern, damit Ihr Datenverkehr noch einmal direkt an Ihr Unternehmen geleitet wird.

Der Sensor von Kaspersky Lab sammelt weiterhin Daten über Ihren Traffic und leitet diese permanent an unsere Cloud-Server weiter, damit wir die von uns erstellten Verhaltensprofile über die bei Ihnen vorherrschenden Bedingungen bei normalem Netzwerkverkehr schrittweise verfeinern können.

Die virtuellen Tunnel bleiben zum Austausch von Statusinformationen zwischen Ihren Routern und den Routern von Kaspersky Lab fortwährend in Betrieb. Kaspersky DDoS Protection ist dadurch jederzeit in der Lage, bei einem weiteren Angriff auf Ihr Unternehmen unverzüglich zu handeln und nach Rücksprache mit Ihnen den Datenverkehr entsprechend umzuleiten.

Die Experten von Kaspersky Lab liefern Ihnen nach einem Angriff detaillierte Analysen und Berichte mit Angaben zu folgenden Punkten:

- Verlauf des Angriffs
- Dauer des Angriffs
- Reaktion von Kaspersky DDoS Protection auf den Angriff

BEDROHUNGSANALYSE – ZUR BESSEREN ABWEHR VON RISIKEN

Kaspersky DDoS Protection verfügt über eine weitere wichtige Komponente der Verteidigung

Kaspersky Lab ist der erste Hersteller von Anti-Malware, der auch eine Lösung zum Schutz vor DDoS-Angriffen bietet.

Im Zusammenhang mit der Entwicklung wegweisender IT-Sicherheit überwachen unsere Sicherheitsanalysten kontinuierlich die Bedrohungslandschaft und können dadurch neue Malware und Internet-Bedrohungen bereits in der Phase des Entstehens aufdecken. Diese Experten, mit den gleichen anspruchsvollen Methoden, setzen wir auch zur Überwachung von Bedrohungen durch DDoS-Angriffe ein. Dank dem Wissen dieser Spezialisten können wir DDoS-Angriffe noch früher erkennen und Ihr Unternehmen noch schneller durch geeignete Abwehrmaßnahmen unterstützen.

MEHRSTUFIGER SCHUTZ

Mit einer einzigartigen Kombination aus kontinuierlicher Überwachung des Datenverkehrs, statistischen und verhaltensorientierten Analysen in Verbindung mit der proaktiven Bereitstellung von Daten über DDoS-Angriffe liefern wir DDoS-Schutz, der höchsten Ansprüchen gerecht wird.

g6kma/Stand: September 2014

Kaspersky Labs GmbH
Despag-Straße 3
85055 Ingolstadt
www.kaspersky.de

KASPERSKY lab