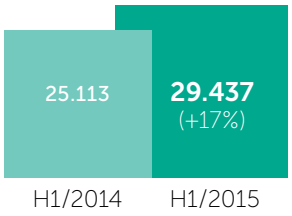
KASPERSKY DDOS PROTECTION

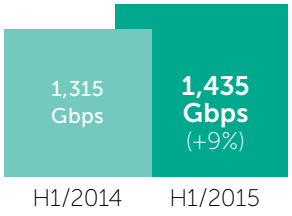
Wenn Ihr Geschäft bereits einem Distributed Denial-of-Service(DDoS)-Angriff ausgesetzt war, dann wissen Sie, wie verheerend der finanzielle Schaden und die Auswirkungen auf zentrale Geschäftsprozesse Ihres Unternehmens sein können. Falls noch nicht, dann ist es nur eine Frage der Zeit, bis DDoS-Attacken eines Tages auch Ihr Unternehmen treffen. Zeit, die Sie nutzen können, um sich vorzubereiten.

Kaspersky DDoS Protection (KDP) ist eine robuste und integrierte Lösung, um die Überlastung Ihrer Online Ressourcen oder Netzwerkinfrastruktur zu verhindern und damit einen kontinuierlichen Ablauf Ihrer online Geschäftsprozesse sowie Schutz zentraler Werte Ihres Unternehmens zu ermöglichen. Von der ständigen Analyse des Datenverkehrs zu Ihren Online Ressourcen, über zeitnahe Warnungen zu potentiellen Attacken, intelligenten Filtertechnologien, bis hin zu leistungsfähigen Rechenzentren mit Sicherheitsexperten und globaler Expertise bietet unsere Lösung alles, was Ihr Unternehmen benötigt, um sich vor allen Arten von DDoS-Attacken und deren Auswirkungen zu schützen.

DDoS Attacken in Deutschland



Durchschnittliche Bandbreite

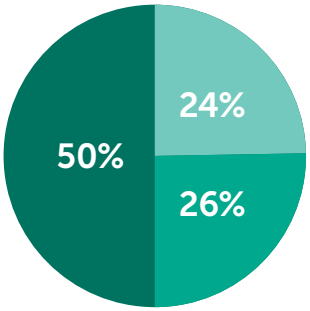


Kaspersky Corporate IT Security Risk Umfrage

- **5500+ Firmen** in 26 Ländern
- **20% der Firmen mit 50+ Mitarbeitern** berichten von DDoS Attacken

50% der DDoS führten zu einer merkbaren

und 24% zu einer vollständigen Unterbrechnung



26% der DDoS Attacken führten zum Verlust von wichtigen Daten

Schnelle Identifizierung von Bedrohungen

Kaspersky Labs Sensor, installiert in der DDoS Protection Cloud oder in Ihrem Netzwerk, analysiert den Datenverkehr, erstellt Profile von typischen Besuchern, deren Verhalten und Datenmustern. Der Datenverkehr wird in Echtzeit überwacht, so dass jede Veränderung, die von einer Attacke verursacht sein könnte, automatisch identifiziert und sofort von unseren Sicherheitsexperten untersucht wird.

Parallel überwachen unsere Kaspersky DDoS Intelligence Experten das weltweite DDoS-Environment und identifizieren neue Muster sowie Technologien von DDoS-Attacken, die schon auf dem Weg in Ihr Netzwerk sein könnten.

Flexible DDoS Mitigation

Sobald eine DDoS-Attacke identifiziert ist, werden unsere Experten im Sicherheitszentrum alarmiert. Mit Kaspersky DDoS Protection Connect und Connect+ werden automatisch Gegenmaßnahmen aktiviert, während gleichzeitig unsere Sicherheitsexperten Tests durchführen, um die optimale Abwehrstrategie abhängig vom Volumen, der Art und Gefährlichkeit der Attacke individuell auf das Sicherheitsprofil Ihres Unternehmens abzustimmen.

Im Fall von Kaspersky DDoS Protection Control entscheiden Sie, wann wir Gegenmaßnahmen entsprechend Ihrer Sicherheitspolitik, Geschäftsziele und Netzwerkinfrastruktur starten sollen. Diese Flexibilität gibt uns die Möglichkeit, die beste Abwehrmethode auf Ihre individuellen Bedürfnisse zuzuschneiden.

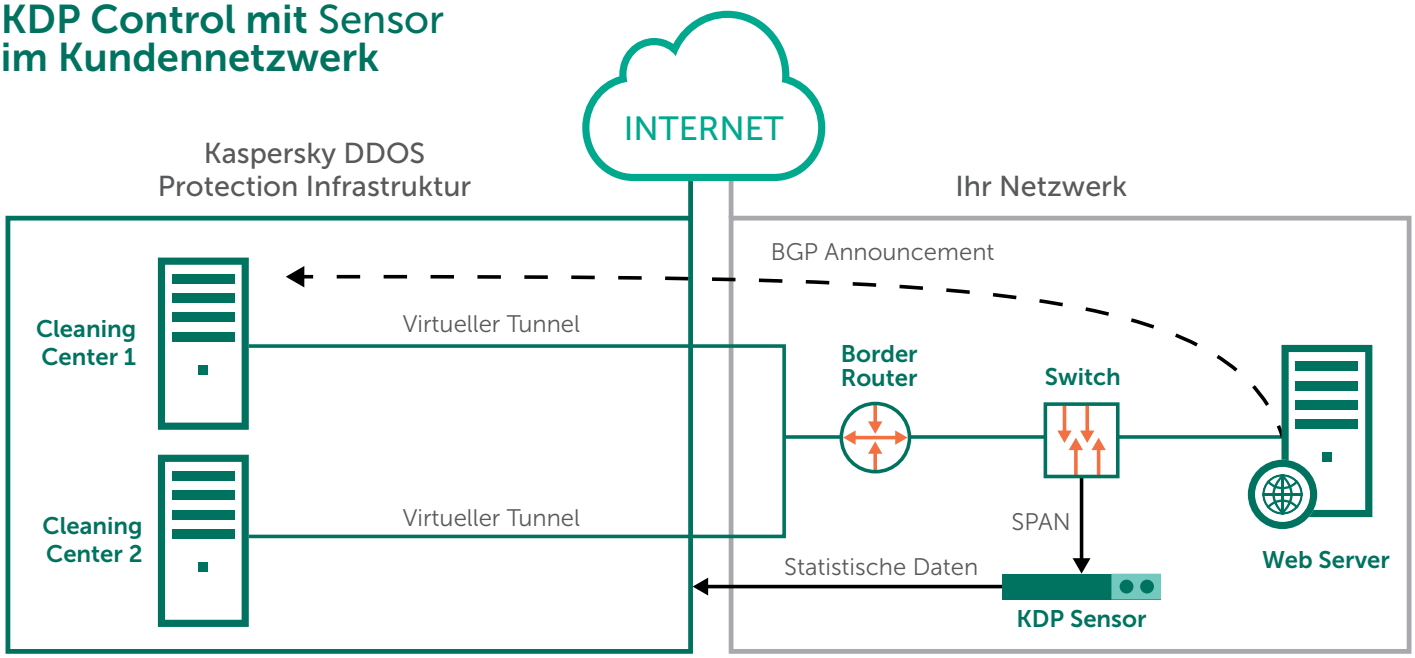
DDoS Attacke und Business As Usual

Während einer Attacke, wenn der gesamte Online Datenverkehr Ihres Unternehmens über die Kaspersky DDoS Service Plattform geleitet ist, werden

- Ihr Online Service, Homepage und Netzwerk nicht von illegitimen Datenverkehr überwältigt,
- dynamische und individuelle Filter- und Schutzmaßnahmen eingesetzt, um Ihren Online Datenverkehr zu überwachen, und
- nur „gesäuberte" Daten an Sie weitergeleitet.

... und das in einem transparenten Prozess, ohne Unterbrechung oder Datenverlust für Ihre Mitarbeiter, Kunden und Partner..

KDP Control mit Sensor im Kundennetzwerk



Richtige Auswahl der DDoS Mitigation

Noch immer sehen viele Unternehmen die Sicherheit ihres Netzwerks, der Online Service und Daten als Angelegenheit der IT-Abteilung. Doch die Erfahrung zeigt, dass der Schutz vor DDoS-Attacken wie jedes andere Cyber-Risiko Chefsache und wichtiges Element eines ausgewogenen Risikomanagements im Unternehmen. Kaspersky Lab bietet zur Auswahl:

KDP Connect – smart und schnell installiert, Ihre Daten werden ständig via DNS und Proxy/GRE über unsere Plattform geleitet,

KDP Control – Stand-by Option, wir schützen im Bedarfsfall Ihre Online Ressourcen via BGP und GRE/MPLS,

KDP Connect+ – Schutz Ihrer Online Ressourcen im /24+ IP Netzwerk, Ihre Daten werden ständig via BGP und GRE/MPLS über unsere Plattform geleitet.

DDoS Intelligence - Proaktiver Schutz

Als der erste globale Cyber-Security Dienstleister mit einer eigenen DDoS Mitigation Lösung können wir auf die Kompetenz und Erfahrung unseres weltweit führenden Security Intelligence Teams zugreifen.

Unsere Experten und unser spezialisiertes Threat Intelligence Team helfen uns, frühzeitig und weltweit neue DDoS-Attacken zu entdecken, so dass wir Ihr Unternehmen proaktiv und schnell schützen können.

KDP Vorteile

- Intelligenter und vollständiger Schutz vor allen DDoS-Attacken
- Keine Einschränkung bei der Abwehr von Volumen-Attacken
- Einzigartige Sensor-Technologie zur Datenüberwachung
- Hoch skalierbare Cleaning Center in Amsterdam und Frankfurt
- Echtzeit global DDoS Intelligence mit Big Data Sicherheitsanalyse
- Schneller Schutz und Support durch unser Emergency Response Team 24/7

Diese einzigartige Kombination aus ständiger Kontrolle des Datenverkehrs, statistischer und verhaltensbasierter Analyse sowie proaktive und globale Überwachung von DDoS-Attacken sind Grundlage für einen robusten Schutz vor DDoS-Attacken.

Mehr Informationen über Kaspersky DDoS Protection und Hinweise, wie Sie sich vor DDoS-Attacken schützen können, finden Sie auf www.kaspersky.com oder rufen Sie einfach Ihren nächsten Kaspersky Lab Partner an.

KDDos-Protection/Version 2/Aprl 2016/DACH