



VERISIGN® INTERNET DEFENSE NETWORK

HÄUFIG GESTELLTE FRAGEN (FAQs)



HÄUFIG GESTELLTE FRAGEN (FAQs)

WAS IST EIN DOS- ODER DDOS-ANGRIFF?

Ein Denial-of-Service-Angriff oder Distributed-Denial-of-Service-Angriff tritt auf, wenn ein einzelner Host (DoS) oder mehrere Hosts (DDoS) legitimen Datenverkehr mit böswilliger Absicht zum Zweck der zeitweiligen oder dauerhaften Unterbrechung einer Anwendung oder eines Service an ein Ziel senden.

Ziele können unter anderem Webserver, DNS-Server, Anwendungsserver, Router, Firewalls sowie Internetbandbreite sein.

WAS BEDEUTET „IN THE CLOUD“?

Der Begriff „Cloud“ wird als Symbol oder Metapher für das Internet verwendet und basiert auf der Darstellung des Internets in Netzwerkdiagrammen. In the Cloud bezieht sich üblicherweise auf einen Service, der für einen Kunden bereitgestellt bzw. durchgeführt wird, bevor er in die Verbindung(en) bzw. die Infrastruktur seines Internetdienstes gelangt.

Im Wesentlichen leitet ein In-the-Cloud-DDoS-Schutz den für ein Unternehmen bestimmten Datenverkehr über ein Internet-Datenzentrum, in dem unerwünschte DDoS-Pakete herausgefiltert werden. Der bereinigte Datenverkehr wird dann an das Unternehmen weitergeleitet.

HANDELT ES SICH BEIM VERISIGN INTERNET DEFENSE NETWORK UM EINEN ERGÄNZENDEN SERVICE ODER WÜRDEN ES UNSERE FIREWALL, UNSER INTRUSION PREVENTION SYSTEM (IPS) BZW. UNSER INTRUSION DETECTION SYSTEM (IDS) UND/ ODER ANDERE SICHERHEITSPRODUKTE IN UNSERER NETZWERKINFRASTRUKTUR ERSETZEN?

Das VeriSign Internet Defense Network ist ein ergänzender Service und kein Ersatz für eine bestehende Sicherheitsinfrastruktur.

ICH VERWENDE MEHRERE VERBINDUNGEN VON VERSCHIEDENEN INTERNETDIENSTANBIETERN (ISP, INTERNET SERVICE PROVIDER). FUNKTIONIERT DAS VERISIGN INTERNET DEFENSE NETWORK MIT MEINER LÖSUNG?

Ja, das VeriSign Internet Defense Network kann DDoS-Angriffe für jeden Internetdiensteanbieter überwachen und die von ihnen ausgehende Gefahr minimieren. Es bietet außerdem gleich hohe Servicequalität für Kunden mit Multi-homed-Netzwerken. Das bedeutet, dass ein Kunde nur ein Team und einen Vorgang zur Beseitigung von Bedrohungen benötigt, um den Angriff abzuwehren. Er muss sich nicht auf mehrere Bandbreitenanbieter verlassen, um im selben Zeitrahmen ähnliche Schlussfolgerungen zu erhalten. Da unsere Lösung netzwerkunabhängig ist, können Sie Ihre Infrastruktur jederzeit an sich ändernde Geschäftsanforderungen anpassen.

WIE LANGE DAUERT ES, DAS VERISIGN INTERNET DEFENSE NETWORK BEREITZUSTELLEN?

Normalerweise dauert es weniger als vierzehn (14) Tage, bis die Überwachungslösung eingerichtet ist und Datenverkehr vom Kunden empfangen werden kann.

WIE LANGE DAUERT ES, BIS ICH ÜBER EINEN DDOS-ANGRIFF AUF MEIN NETZWERK ODER MEINE ANWENDUNG INFORMIERT WERDE? WELCHE ART VON SERVICE LEVEL AGREEMENT (SLA) WIRD MIT DEM VERISIGN INTERNET DEFENSE NETWORK ANGEBOten?

Üblicherweise werden Kunden innerhalb von fünf Minuten über einen möglichen Angriff benachrichtigt, nachdem eine Überwachungswarnung ausgelöst wurde.

Das derzeit angebotene SLA besagt, dass VeriSign den Kunden gemäß seinem Eskalationsplan innerhalb von 15 Minuten nach Eingang einer Überwachungswarnung kontaktieren wird. Bei diesem Kontakt prüft VeriSign gemeinsam mit dem Kunden, ob eine Schadensminimierung erforderlich ist oder ob die Warnung von einer legitimen





HÄUFIG GESTELLTE FRAGEN (FAQs)

Kundenaktivität verursacht wurde. Falls eine Schadensminimierung erforderlich ist, schlägt VeriSign die geeignetste Vorgehensweise vor.

Wenn die Umleitung des Datenverkehrs des Kunden empfohlen wird, wird der Datenverkehr des Kunden zum VeriSign Internet Defense Network umgeleitet, bevor er das Netzwerk des Kunden erreicht. VeriSign wendet auf den zum VeriSign Internet Defense Network umgeleiteten Datenverkehr mehrere Filterungsstufen an, die schrittweise den Datenverkehr blockieren, der die internetbasierten Services des Kunden unterbrechen oder deaktivieren soll. Legitimer Datenverkehr wird anschließend vom VeriSign Internet Defense Network wieder zum Netzwerk des Kunden zurückgeleitet. Wenn der DDoS-Angriff vorbei ist, leitet VeriSign gemeinsam mit dem Kunden entsprechende Schritte ein, damit der normale Geschäftsbetrieb wieder aufgenommen werden kann.

FINDEN BEI EINEM DDOS-ANGRIFF MANUELLE EINGRIFFE IN MEINE INFRASTRUKTUR STATT?

VeriSign richtet Schadensminimierungsverfahren ein, die perfekt zu Ihrem Servicemodell passen. Optimale Lösungen unterscheiden sich unter anderem abhängig von Netzwerkgröße und genutztem Servicetyp.

Falls der Datenverkehr durch unser BGP-Off-Ramping umgeleitet wird, ist kein manueller Eingriff in das Netzwerk des Kunden erforderlich. Falls der Datenverkehr per DNS umgeleitet wird, müssen Ihre „A“-Datensätze auf eine IP-Adresse von VeriSign verweisen und die Time-to-Live (TTL) muss auf die Mindestanzahl an Weiterverbreitungen eingestellt werden.

Nach der Schadensminimierung wird der Datenverkehr wieder an Sie zurückgeleitet.

WIE SIEHT DER ABLAUF BEI EINEM ANGRIFF AUS?

Wenn eine Warnung ausgelöst wird, kontaktiert das VeriSign-Support-Team den Kunden, vergibt eine Vorfalldnummer und beginnt mit der Untersuchung. Sobald feststeht, dass es sich um einen DDoS-Angriff handelt, wird eine Schadensminimierung empfohlen. Unser SLA sieht vor, dass der Kunde innerhalb von 15 Minuten nach Eingang einer

Warnung eine Empfehlung zur Schadensminimierung erhält. Mit Erlaubnis des Kunden leitet VeriSign den Datenverkehr daraufhin zur Schadensminimierung des DDoS-Angriffs an eine entsprechende Einrichtung oder mehrere Einrichtungen um. Das Support-Team des VeriSign Internet Defense Network beginnt dann je nach Bedarf mit der weiteren Untersuchung des Ursprungs des Angriffs bis hin zu den Upstream-Providern, um den Angriff näher an seinem Entstehungspunkt abwehren zu können.

KONTAKTIEREN SIE DEN KUNDEN, NACHDEM DER DOS/DDOS-ANGRIFF GESTOPPT WURDE?

Ja. Einer unserer VeriSign Security Operations-Mitarbeiter setzt sich mit dem im Eskalationsplan angegebenen Unternehmensvertreter in Verbindung, um die Rückleitung des Datenverkehrs in den ursprünglichen Pfad zu besprechen.

KANN ICH MEINEN ROUTER SO EINSTELLEN, DASS EIN DDOS-ANGRIFF VEREITELT WIRD?

Router können keine gefälschten IP-Quellen blocken oder manuell tausende von IP-Adressen zurückverfolgen. Folglich sind Zugriffskontrolllisten gegen DDoS-Angriffe nutzlos.

KANN ICH MEINE FIREWALL SO EINSTELLEN, DASS EIN DDOS-ANGRIFF VEREITELT WIRD?

Firewalls sind nicht zur Schadensminimierung bei DDoS-Angriffen geeignet. Die Verwendung einer Firewall zur Schadensminimierung könnte zum Ausfall der CPU führen und Speicherressourcen belegen. Außerdem können Firewalls keine Anomalien im Datenverkehr erkennen.

KANN ICH MEIN INLINE IPS ODER MEIN IDS SO EINSTELLEN, DASS EIN DDOS-ANGRIFF VEREITELT WIRD?

Ja, aber hierfür sind umfangreiche manuelle Einstellungen erforderlich, die viel Zeit in Anspruch nehmen und dennoch Angriffspunkte bieten können.

Ein IDS befindet sich üblicherweise hinter der Firewall mit einem Uplink zu einem Router oder einem Switch vor der Firewall. Ein IDS löst eine Warnung aus, wenn es eine Anomalie erkennt. Zu diesem Zeitpunkt belegt der Angriff jedoch bereits Ihre Internetbandbreite und kann





HÄUFIG GESTELLTE FRAGEN (FAQs)

die Verbindung saturieren. Dies kann zum Ausfall der CPU führen und Speicherressourcen belegen.

Ein IPS kann durchaus zur Erkennung von Anomalien verwendet werden. Es benötigt jedoch mehrere Wochen, um selbst „normale“ Datenverkehrsmuster verstehen zu können. Außerdem sind häufige manuelle Einstellungen erforderlich, um legitimen Datenverkehr von potenziell gefährlichem oder zu blockierendem Datenverkehr unterscheiden zu können.

ICH STELLE ÜBERMÄSSIG VIEL BANDBREITE ZUR VERFÜGUNG, UM DDoS-ANGRIFFE AUF DIESE WEISE ZU VERHINDERN. WAS KANN DAS VERISIGN INTERNET DEFENSE NETWORK IN DIESEM FALL FÜR MICH TUN?

Diese Methode ist nicht gerade kostengünstig. Wenn sich Ihr üblicher Datenverkehr beispielsweise auf bis zu 15 Mbps beläuft und Sie für den Fall eines DDoS-Angriffs 30 Mbps bereitstellen, dann stellen Sie um 100 Prozent mehr Bandbreite zur Verfügung als nötig und haben Ihre monatlichen Kosten hierfür verdoppelt. Die Angreifer können das Ausmaß ihrer Angriffe jedoch jederzeit problemlos erhöhen. Da einige DDoS-Angriffe inzwischen mit über 40 Gbps erfolgen, könnte die übermäßige Bereitstellung von Internetbandbreite ein sehr kostspieliges Unterfangen darstellen.

WIE SIEHT ES MIT BLACKHOLE-LISTEN FÜR DIE IP-ADRESSEN AUS?

Wenn Sie eine oder mehrere IP-Adressen auf Blackhole-Listen setzen, kann dies dazu führen, dass legitime Datenpakete zusammen mit böswilligem Datenverkehr geblockt werden, was wiederum einen Sieg für den Angreifer bedeutet. Falls ein ISP als Blackhole verwendet wird, muss zuerst die Quelle des Datenverkehrs ermittelt werden, wodurch wertvolle Zeit verloren gehen kann, und es ist nicht sicher, dass legitimer Datenverkehr nicht doch blockiert wird.

WO BEFINDEN SICH DIE DATENZENTREN DES VERISIGN INTERNET DEFENSE NETWORK ZUR SCHADENSMINIMIERUNG?

- Ashburn, Virginia
- San Francisco, Kalifornien
- Amsterdam, Niederlande
- Tokio, Japan

SIND DIE DATENZENTREN DES VERISIGN INTERNET DEFENSE NETWORK IN BEZUG AUF TECHNISCHE AUSSTATTUNG UND KAPAZITÄT ZUR SCHADENSMINIMIERUNG IDENTISCH?

Alle Datenzentren des VeriSign Internet Defense Network sind in Bezug auf die Kapazität (Dual 10 Gigabit Ethernet) identisch. Da wir NICHT an einen bestimmten Hardwareanbieter oder Service Provider gebunden sind, verfügen unsere Datenzentren NICHT über dieselbe technische Ausstattung.

WIE HANDHABT DAS VERISIGN INTERNET DEFENSE NETWORK DIE DATENSPEICHERUNG? FÜR WIE LANGE WERDEN DATEN GESPEICHERT?

Derzeit gestaltet sich unsere Richtlinie zur Datenspeicherung wie folgt:

- bei Schadensminimierung = 1 Jahr
- DoS-Warnung (niedrig) = 30 Tage
- DoS-Warnung (mittel) = 60 Tage
- DoS-Warnung (hoch) = 90 Tage
- Berichte zum Datenverkehr = 60 Tage

Diese Richtlinie kann jederzeit geändert werden und stellt keine Garantie dar. Weitere Informationen erhalten Sie von Ihrem VeriSign-Mitarbeiter.

AUF WELCHEM WEG ERHALTEN DIE KUNDEN BERICHTE ZUM DATENVERKEHR?

Die Berichte zum Datenverkehr können über das Portal erstellt und anschließend in eine XML- oder PDF-Datei exportiert werden.

WELCHE ART VON GERÄTEN BENÖTIGT EIN MÖGLICHER KUNDE IN SEINER EINRICHTUNG?

Das VeriSign Internet Defense Network unterstützt folgende Geräte:





HÄUFIG GESTELLTE FRAGEN (FAQs)

CISCO-ROUTER

Peakflow SP 4.5 unterstützt folgende Cisco-Router

herkömmliche IOS-basierte Cisco-Router mit IOS 12.0 oder höher (Netflow v5 und v9)

Produktfamilie Cisco Catalyst 4500 mit Sup IV oder höher und NFFC (Netflow v5)

Produktfamilie Cisco Catalyst 5500 mit geeignetem Sup und NFFC (Netflow v7)

Produktfamilie Cisco Catalyst 6500 mit Sup 2 oder höher, Hybrid oder Native (Netflow v5 und v7)

Cisco CRS-1 (Netflow v9)

Wichtig: Cisco Catalyst-Router unterstützen keine TCP-Flags.

JUNIPER CFLOWD V9-DATENVERKEHR

Juniper cflowd v9 wird nur für IP-Datenverkehr unterstützt. Cflowd-Daten aus MPLS-basiertem Datenverkehr funktionieren mit der aktuellen JunOS-Software eventuell nicht und Peakflow SP unterstützt diese Daten offiziell nicht.

CISCO-ROUTER

Peakflow SP 4.5 unterstützt folgende Juniper-Router

Juniper T-Serie (cflowd v5 oder v9 mit Services PIC)

Juniper M-Serie mit Internet Processor II (cflowd v5 oder v9 mit Services PIC)

Juniper J-Serie (cflowd v5)

Juniper TX-Serie (cflowd v9)

Juniper MX960 (cflowd v5)

FOUNDRY-ROUTER

Peakflow SP unterstützt Foundry-Router mit sFlow v2, v4 und v5. Foundry unterstützt nicht die Generation von ACL.

FORCE10-ROUTER

Peakflow SP unterstützt Force10-Router mit sflow.

Geräte oder andere Anbieter, die Informationen zum Datenfluss oder IPFIX bereitstellen können, werden fallspezifisch behandelt.

MUSS ICH EINE VERBINDUNG ZUM DATENZENTRUM DES VERISIGN INTERNET DEFENSE NETWORK ERWERBEN, DAMIT MEIN DATENVERKEHR UMGELEITET WERDEN KANN?

Sie können eine Verbindung zu einem der Datenzentren des VeriSign Internet Defense Network erwerben oder wir leiten Ihren Datenverkehr per On-Ramping über einen GRE-Tunnel (häufigste Wahl) oder einen VPN-Tunnel um.

GIBT ES ANFORDERUNGEN IN BEZUG AUF DEN IP-ADRESSRAUM?

Damit VeriSign Ihren Datenverkehr mithilfe von BGP per Off-Ramping umleiten kann, müssen Sie mindestens über /24 oder 254 raumweise kontinuierliche IP-Adressen verfügen. /24 erhalten Sie von Ihrem Internet Service Provider oder von ARIN, APNIC, RIPE, AFRINIC oder LACNIC.

- www.arin.net – Nordamerika
- www.apnic.net – Asiatisch-pazifischer Raum
- www.ripe.net – Europa
- www.afrinic.net – Afrika
- www.lacnic.net – Südamerika und Karibik

IST ES MÖGLICH, MIT DEM VERISIGN INTERNET DEFENSE NETWORK EINEN EINZELNEN WEBSERVER ZU SCHÜTZEN?

Ja, bei einem einzelnen Webserver kann der Datenverkehr über eine DNS-Änderung umgeleitet werden. Sie müssen hierfür jedoch einige Änderungen an Ihrem System vornehmen. Wir stellen Ihnen IP-Adressen von VeriSign zur Verfügung, damit Sie den „A“-Datensatz Ihres verwalteten DNS-Servers (oder Ihres ISP) auf die neu zugewiesene IP-Adresse von VeriSign ändern können.

GIBT ES BEI DER UMLEITUNG DES DATENVERKEHRS PER OFF-RAMPING AN VERISIGN EINE LATENZ, DIE BERÜCKSICHTIGT WERDEN MUSS?

Die Latenz richtet sich nach der Entfernung zwischen der geschützten Einrichtung des Kunden und dem Datenzentrum des VeriSign Internet Defense Network.





HÄUFIG GESTELLTE FRAGEN (FAQs)

VeriSign verfügt über genügend öffentliche und private Peering-Punkte bei den meisten globalen Internet-Austauschknoten. Dadurch sind optimale Routing-Wege durch das Internet möglich. VeriSign verteilt seine Datenzentren außerdem weltweit, um die Latenz zu minimieren. Die Datenzentren befinden sich in der Washington DC Metro Area, in der Silicon Valley/San Francisco Bay Area, in Amsterdam und in Tokio. Kunden in diesen Märkten sollten keine messbare Latenz feststellen können (<5 ms). Des Weiteren müssen Kunden in den USA eventuell mit einer zusätzlichen Latenz von 15 bis 30 ms pro 1.000 Meilen Abstand vom Datenzentrum rechnen. Die Erfahrung hat gezeigt, dass zwischen Ost- und Westküste der USA mit einer Latenz von etwa 30 bis 35 ms zu rechnen ist.

BEIM BORDER GATEWAY PROTOCOL (BGP) KANN ES ÜBER 30 MINUTEN DAUERN, BIS DEM KUNDEN EINE NETZWERKBLOCKADE GEMELDET WIRD. WELCHE MASSNAHMEN WERDEN ZUR VERKÜRZUNG DER KONVERGENZZEIT ERGRIFFEN, BEVOR VERISIGN GELEGENHEIT HAT, DEN DATENVERKEHR ZU FILTERN?

VeriSign hat sich ausführlich mit dem Problem der Konvergenzzeit beim BGP beschäftigt. VeriSign nutzt die Dienste eines Marktführers bei der Überwachung der BGP-Route, der weltweit hunderte von BGP-Sonden mit tausenden von BGP-Feeds verteilt hat. VeriSign verwendet dieses Tool, um die Zeit zu messen, die BGP-Updates für die Verbreitung über das Internet benötigen. Obwohl die Konvergenzzeit nicht vollständig kontrollierbar oder vorhersehbar ist, laufen alle BGP-Feeds üblicherweise innerhalb von zwei (2) Minuten oder weniger auf dem neuen geschützten Pfad zusammen. VeriSign rät seinen Kunden, mit einer Konvergenzzeit von etwa fünf (5) Minuten zu rechnen. Unserer Erfahrung nach ist die Zeit jedoch sehr viel kürzer. VeriSign verwendet schon seit Jahren BGP-Warnungen zur Ausfallsicherung kritischer .com- und .net-Infrastrukturdienste.

INWIEFERN NUTZT VERISIGN SEINE BEZIEHUNGEN ZU ANDEREN INTERNETDIENSTANBIETERN BEI EINEM ANGRIFF, DEN DER KUNDE NICHT SELBST ABWEHREN KANN?

VeriSign verfügt über genügend öffentliche und private Peering-Punkte bei den meisten globalen Internet-Austauschknoten. Dadurch kann VeriSign etwa 60 % des Internets über Peering-Punkte erreichen. Als Anbieter kritischer Infrastrukturen nimmt VeriSign mit den meisten großen Netzwerken an denselben Foren zur Betriebssicherheit teil, die auch Tier-1-, Tier-2- und Tier-3-Anbieter zur Interaktion untereinander nutzen. Wenn ein Kunde ein Problem hat, kann VeriSign diese Beziehungen zur direkten Interaktion mit den Anbietern in denselben Foren und auf dieselbe Weise nutzen, auf die diese Netzwerke untereinander kommunizieren.

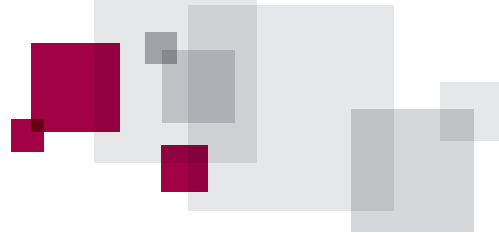
WIE VERFÄHRT VERISIGN MIT VERSCHLÜSSELTEN DATEN (SSL), UM DIE ART EINES ANGRIFFS VERSTEHEN ZU KÖNNEN?

Wenn nur die Nutzdaten verschlüsselt sind und der Kunde den Verschlüsselungscode nicht herausgeben möchte, können wir lediglich die Header oder sämtliche Daten außerhalb der Nutzdaten filtern. Falls der Kunde jedoch bereit ist, den Code herauszugeben, können wir das Datenpaket entschlüsseln, filtern und nach der erneuten Verschlüsselung über einen sicheren Pfad an den Kunden zurückschicken.

IST DAS VERISIGN INTERNET DEFENSE NETWORK IN DER LAGE, MIT DEN IN DER NETZWERKINFRASTRUKTUR DES KUNDEN VERWENDETEN GERÄTEN ZUR ÜBERWACHUNG, SCHADENSMINIMIERUNG ODER KORRELATION ZUSAMMENZUARBEITEN?

VeriSign prüft solche Geräte fallspezifisch und entscheidet dann, ob sie in das VeriSign Internet Defense Network integriert werden können.





HÄUFIG GESTELLTE FRAGEN (FAQs)

UNTERSTÜTZT DAS VERISIGN INTERNET DEFENSE NETWORK IPV6?

Die Unterstützung von IPv6 durch das VeriSign Internet Defense Network wird derzeit getestet. Ein Verfügbarkeitsdatum steht jedoch noch nicht fest.

WEITERE INFORMATIONEN

Weitere Informationen zum VeriSign® Internet Defense Network erhalten Sie von einem VeriSign-Mitarbeiter unter InternetDefenseNetwork@VeriSign.com oder besuchen Sie uns unter www.VeriSign.de.

ÜBER VERISIGN

VeriSign ist der führende Anbieter digitaler Infrastrukturdienste der digitalen Welt. Jeden Tag verlassen sich Unternehmen und Kunden milliardenfach auf unsere Internet-Infrastruktur, um sicher zu kommunizieren und Handel zu treiben.

Weitere Informationen finden Sie auf unserer Website www.VeriSign.de.

