



VERISIGN® INTERNET DEFENSE NETWORK - ÜBERSICHT

Die zunehmende Häufigkeit und Schwere von Distributed Denial of Service- (DDoS-) Angriffen führt zu einer raschen Veränderung bei der Netzwerksicherheit. Diese finanziell, politisch oder technologisch motivierten Angriffe übersteigen regelmäßig die jüngsten Ereignisse der letzten Jahre. Diese Angriffe zu vereiteln, bevor sie das Unternehmen schädigen, ist zu einer teuren und oftmals ineffizienten Lösung geworden. Dadurch hat sich die DDoS-Minimierung zu einem der vorrangigsten Sicherheitsprobleme für Unternehmen entwickelt, die ihre Geschäfte online abwickeln.

Das VeriSign® Internet Defense Network bietet Unternehmen eine zuverlässige und skalierbare DDoS-Schutzstrategie. Als vertrauenswürdiger Partner hilft VeriSign Unternehmen, online zu bleiben, ohne dabei in eine umfangreiche Infrastruktur investieren zu müssen.

DDOS-ANGRIFFE: EINE ZUNEHMENDE BEDROHUNG

DDoS-Angriffe berauben rechtmäßige Benutzer absichtlich ihrer Internetressourcen, indem sie ein Netzwerk üblicherweise mit einer Flut von Datenpaketen aus den verschiedensten Quellen überlasten. Die Angreifer verursachen üblicherweise einen Denial of Service-Zustand, indem sie entweder Serverbandbreite belegen oder den Server selbst beeinträchtigen.

Heutzutage formen böswillige Elemente aus beeinträchtigten Computern sogenannte „Botnetze“, mit denen groß angelegte Angriffe auf nichts ahnende Opfer durchgeführt werden können. Schätzungen zufolge werden zu jedem Zeitpunkt zwischen vier und sechs Millionen Computer aktiv in Botnetzen genutzt. Diese Botnetze nutzen die Rechenleistung und Bandbreite von tausenden beeinträchtigter Computer, um selbst die größten und modernsten Netzwerke zusammenbrechen zu lassen. Einige Berichte schätzen, dass täglich über 10.000 Angriffe stattfinden. Viele ISPs melden Angriffe mit über 10 Gbps (Gigabit pro Sekunde).

ÜBERSICHT

Das VeriSign Internet Defense Network trägt zum Schutz vor katastrophalen DDoS-Angriffen in Unternehmen bei, indem es bösartigen Datenverkehr, der auf eine Störung oder Deaktivierung von Services auf Internetbasis abzielt, erkennt und herausfiltert. Im Gegensatz zu herkömmlichen Sicherheitslösungen filtert das VeriSign Internet Defense Network schädlichen Datenverkehr bereits vor dem Unternehmensnetzwerk – sozusagen "in-the-Cloud" – heraus.

Das VeriSign Internet Defense Network kombiniert die Sicherheit der erstklassigen Plattformen von VeriSign zur Analyse und Erkennung des Datenverkehrs mit der Flexibilität, die Komponenten zur Schadensminimierung nur bei Bedarf einsetzen zu müssen. Wenn ein Vorfall erkannt wird, leitet VeriSign in Zusammenarbeit mit dem Kunden den für den geschützten Service vorgesehenen Internetverkehr an das VeriSign Internet Defense Network um. Die Umleitung geschieht „in-the-Cloud“, um den Angriff auf das Internet Defense Network umzuleiten, bevor das

HAUPTVORTEILE

Enorme Kapazität und hohe Skalierbarkeit

Websites werden ständig aktualisiert und global verteilt, damit sie auch vor den größten DDoS-Angriffen geschützt sind.

Weltweite Beziehungen

Unsere weltweiten Beziehungen mit Netzbetreibern, ISPs und anderen Netzwerkanbietern gewährleisten zusätzliche Sicherheitsmaßnahmen.

24-Stunden-Management, -Überwachung und -Support

Die Sicherheitsanalytiker von VeriSign stehen rund um die Uhr zur Erkennung von Angriffen und zur Schadensminimierung zur Verfügung.

Geringere Kosten

Da keine zusätzliche Ausrüstung vor Ort benötigt wird, sparen Kunden durch betriebliche Effizienz, geringe Support-Kosten und Größenvorteile Zeit und Geld.

Ausgebildete und engagierte Experten

Zertifizierte Sicherheitsexperten absolvieren eine umfassende Sicherheitsausbildung. Außerdem werden sie einer eingehenden Überprüfung unterzogen.





DATENBLATT

Kundennetzwerk übernommen oder anderweitig geschädigt wird. Während VeriSign die Datenverkehrsmuster überwacht, beginnt das rund um die Uhr arbeitende Sicherheitsteam mit der Bereinigung des umgeleiteten Datenverkehrs mithilfe modernster Technologien zur Schadensminimierung. Böartiger Datenverkehr wird stufenweise geblockt und der gefilterte Datenverkehr wird an das Netzwerk des Kunden gesendet. Auf diese Weise kann der normale Geschäftsbetrieb aufrechterhalten werden.

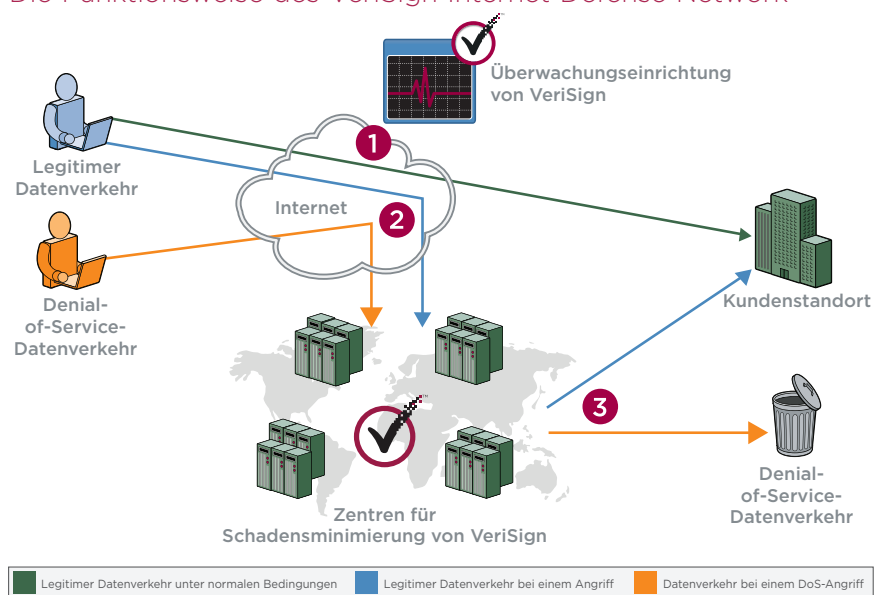
Reaktionsschnelligkeit

Kundenspezifische Eskalationsprozesse werden erarbeitet, um Probleme erkennen und identifizieren sowie ihren potenziellen Schaden minimieren zu können.

Progressive Filterung

Die Netzwerkteams von VeriSign arbeiten mit dem Kunden zusammen, um den Grad der Filterung optimal anzupassen. Wenn die Angriffsvektoren eindeutiger definiert sind, ist eine umfassendere Filterung durch VeriSign möglich.

Die Funktionsweise des VeriSign Internet Defense Network



SERVICEKOMPONENTEN

Überwachung

Die Überwachung des Datenverkehrs des Kunden ist von entscheidender Bedeutung, um Angriffe bereits in der Anfangsphase erkennen und entschärfen zu können. Die Informationen zum Datenfluss sammelt VeriSign über die mit dem Internet verbundenen Router des Kunden. Beispiele für den Internetverkehr des Kunden werden in die Korrelations-Engine von VeriSign zur Bedrohungserkennung, Ausgabe von Warnungen und zur Berichterstellung integriert. Die Häufigkeit des Packet Sampling kann an Größe, Typ und Routerleistung des Kunden angepasst werden.

Die Datenpakete werden durch Korrelation verschiedener, in den Headern der Datenpakete enthaltene Felder klassifiziert und analysiert. Anschließend werden die Datenpakete in Kategorien aufgeteilt und mithilfe moderner Heuristik korreliert, um normale von anormalen Datenverkehrsmustern trennen zu können.





DATENBLATT

Der Datenverkehr des Kunden wird rund um die Uhr vom VeriSign Security Operations Center überwacht. Kundenspezifische Warnungen ermöglichen geschulten Sicherheitsexperten die sofortige Erkennung von im Entstehen begriffenen, potenziellen Bedrohungen. Des Weiteren können die Kunden ihren eigenen Datenverkehr und eventuelle Warnungen über ein sicheres Online-Portal überwachen.

Erkennung von Bedrohungen

Die frühzeitige Erkennung möglicher Bedrohungen ist entscheidend für die Schadensminimierung, bevor sie sich in vollem Umfang auf Unternehmen auswirken können. Aus diesem Grund sucht VeriSign stets nach neuen Methoden zur Erkennung und Klassifizierung bössartiger Aktivitäten. Die Erkennung von Bedrohungen umfasst zwei primäre Komponenten: die Signaturanalyse und das dynamische Profiling.

- **Signaturanalyse** - Bei der Signaturanalyse (oder der Erkennung von Missbrauch) wird nach vordefinierten Abweichungen gesucht, die Anzeichen für einen DDoS-Angriff darstellen. VeriSign nutzt eine Kombination aus Best Practices der Branche und firmeneigenen Technologien, um diese Signaturen zu identifizieren. Da sich die Angriffe stets weiterentwickeln, werden die aus der Schadensminimierung gewonnenen Erkenntnisse in die Forschung und Entwicklung mit einbezogen, um neue Bedrohungssignaturen besser erkennen zu können.
- **Dynamisches Profiling** - Da nicht alle Kunden gleich sind und die Angriffsprofile sich ständig ändern, ist es von entscheidender Bedeutung, dass VeriSign mit den „normalen“ Datenverkehrsmustern jedes einzelnen Kunden vertraut ist. Hierfür arbeitet VeriSign mit dem Kunden zusammen, um ein dynamisches Profil seines Internetverkehrs zu erstellen. Abweichungen von diesem Kundenprofil, die vordefinierte Grenzwerte überschreiten, werden automatisch an die rund um die Uhr arbeitenden Sicherheitsteams von VeriSign übermittelt. Dadurch kann VeriSign schnell auf neue und einzigartige Angriffsprofile reagieren.

Minimierung

VeriSign erarbeitet gemeinsam mit den Kunden für ihr Servicemodell optimierte Verfahren zur Schadensminimierung. Die Minimierung umfasst drei Komponenten: Off-Ramping, Filterung und On-Ramping. Da Pünktlichkeit für den Schutz der Kundenservices von entscheidender Bedeutung ist, arbeitet VeriSign in den anfänglichen Einrichtungs- und Testphasen viel mit den Kunden zusammen, um eine nahtlose Integration aller drei Komponenten sicherstellen zu können.

- **Off-Ramping** - Die Sicherheitsexperten von VeriSign leiten den für den Kundenservice bestimmten Internetverkehr „in-the-Cloud“ an Websites des VeriSign Internet Defense Network um, sodass der Datenverkehr zuerst zu VeriSign gelangt. Off-Ramping wird dann genutzt, wenn ein möglicher Angriff eine Umleitung des Datenverkehrs rechtfertigt.

HAUPTMERKMALE

- Rund-um-die-Uhr-Überwachung
 - On-Demand-Schadensminimierung
 - Einfache Einrichtung und Konfiguration
 - Wahlmöglichkeit zwischen Off-Ramping für DNS- oder BGP-Datenverkehr
 - On-Ramping-Optionen für Tunneling, VPN oder Direct Connect-Datenverkehr*
 - Detaillierte Ereignisberichte und -analysen
 - Sicheres Kundenportal
 - Keine Ausrüstung am Kundenstandort erforderlich**
- * in bestimmten Gegenden verfügbar
** falls VPN nicht erforderlich ist





DATENBLATT

VeriSign bietet verschiedene Methoden für das Off-Ramping des Datenverkehrs an, unter anderem BGP-Meldungen (Border Gateway Protocol) oder Änderungen an DNS-Datensätzen des Kunden. Die optimale Lösung variiert je nach Kunde und ist von der Größe des Kundennetzwerks, dem Servicetyp sowie einer Reihe anderer Überlegungen abhängig.

- **Filterung** - VeriSign arbeitet mit einem mehrschichtigen Ansatz zur Filterung des Datenverkehrs, der die Regeln im Laufe der Zeit schrittweise optimiert. Da das Blockieren des gesamten an den Kunden gerichteten Datenverkehrs zu demselben Ergebnis führt wie ein DDoS-Angriff, sorgt VeriSign dafür, dass legitimer Datenverkehr das vorgesehene Ziel auch wirklich erreicht. Mit der Zeit erhöht Filtertechnologie auf dem neuesten Stand der Technik den Filtergrad, um nach und nach immer mehr böartigen Datenverkehr blockieren zu können.

Filter werden in verschiedenen Schichten des OSI-Modells (Offenes Kommunikationssystem) angewendet. Auch wenn einige Angriffe minimiert werden können, indem man Filter in der Netzwerkschicht einsetzt, erfordern komplexe Angriffe nun eine Analyse und Filterung bis in die Anwendungsschicht. VeriSign kann kommerziell verfügbare Produkte mit benutzerdefinierten, eigenen Entwicklungen zur Erstellung einer erstklassigen Lösung zur Minimierung von DDoS-Angriffen ergänzen.

- **On-Ramping** - Sobald der Datenverkehr bereinigt wurde, leitet ihn VeriSign vom VeriSign Internet Defense Network an das Kundennetzwerk weiter. Die Netzwerkarchitekten von VeriSign erarbeiten gemeinsam mit den Kunden die beste Methode zur Rückleitung des bereinigten Datenverkehrs in das Kundennetzwerk. GRE-Tunneling (Generic Routing Encapsulation), die Einrichtung eines VPN oder eine direkte Verbindung zu einem Standort sind einige Möglichkeiten hierfür.

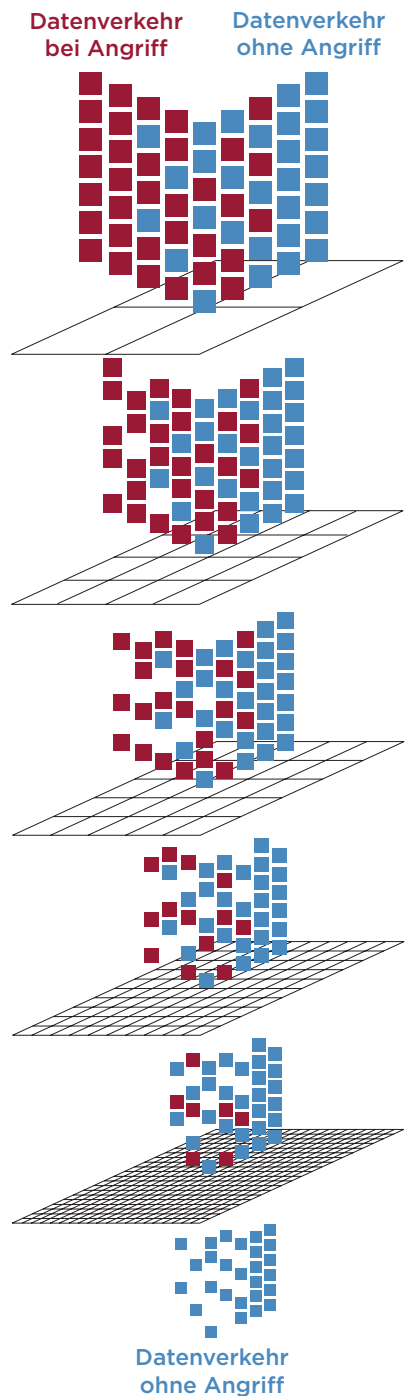
Berichterstellung

Da das Verständnis des Datenverkehrs eines Kunden der erste Schritt zum Schutz wichtiger Services ist, stellt VeriSign detaillierte Statistiken zum Datenverkehr zur Verfügung, um durchdachte Entscheidungen treffen zu können. Beispiele hierfür sind Berichte zum gesamten Datenverkehr und zu Anwendungen, Protokolle sowie Ereignisberichte.

ZUSAMMENFASSUNG

Da böswillige Elemente immer grissener vorgehen, steigen die Bedrohungen für Unternehmensnetzwerke exponentiell an. Aus hunderttausenden von beeinträchtigten Geräten bestehende Botnetze bilden die Basis für Tools, die vernichtende Angriffe durchführen können, die sich nicht nur auf den Umsatz eines Unternehmens auswirken, sondern auch seinen Ruf schädigen und das Kundenvertrauen beeinträchtigen können. Kurz gesagt: Sicherheitslösungen müssen sich mit derselben enormen Geschwindigkeit weiterentwickeln wie die Bedrohungen.

EIN MEHRSCHICHTIGER ANSATZ ZUR FILTERUNG





DATENBLATT

Das VeriSign Internet Defense Network ist ein Ergebnis dieses Sicherheitsfortschritts. Durch die Minimierung von Bedrohungen näher am Kern des Internets kann VeriSign einige der größten Angriffe weltweit effektiv und effizient minimieren. Gleichzeitig kann VeriSign schnell reagieren und entsprechende Gegenmaßnahmen einleiten. Als Marktführer beim Schutz kritischer Internetinfrastrukturen verfügt VeriSign über die Erfahrung und die Technologie, um Unternehmen zu helfen, ihre wertvollen Internet-Vermögenswerte zu schützen.

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 unter www.Verisign.de.

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.

