INDEVIS DDoS PROTECT

KOMPLEMENTÄRER DDoS-SCHUTZ FÜR INDEVIS DATACENTER SERVICES

DDoS-Attacken können dazu führen, dass die Unternehmens-Webseite nicht verfügbar ist und auf wichtige Dateien und Programme nicht zugegriffen werden kann. Schwere wirtschaftliche Schäden für Ihr Unternehmen können die Folge sein. Durch den Schutz vor DDoS-Attacken lassen sich solche Angriffe abwehren und Sie können Ihr Unternehmen vor Arbeitsausfällen, Umsatzeinbußen und Imageverlust bewahren.

Distributed-Denial-of-Service-Angriffe zielen darauf ab, die Netzwerkinfrastruktur mit großen Datenmengen zu überlasten. Über Bot-Netze initiieren Hacker DDoS-Angriffe auf Webseiten oder webbasierte Anwendungen, indem sehr viele unvollständige oder falsche Anfragen beziehungsweise Protokollelemente gesendet werden. So wird die IT-Infrastruktur überlastet und echte Anfragen können nicht mehr bewältigt werden, da die Bandbreite nicht mehr ausreicht. Dadurch werden Dienste in ihrer Funktionalität beeinträchtigt und stehen Nutzern sowie Unternehmen nur eingeschränkt oder überhaupt nicht mehr zur Verfügung. Mit *indevis DDoS Protect* können Sie sich vor Service-Unterbrechungen, die durch DDoS-Angriffe verursacht werden, schützen.

DDoS PROTECT: IHR ADDITIVES SCHUTZSYSTEM

indevis DDoS Protect kann ausschließlich komplementär zu den *indevis Datacenter & Virtualization Services* oder *indevis Web App Secure* eingesetzt werden. Mit *indevis DDoS Protect* schützen Sie Ihr Unternehmen vor volumetrischen Attacken, Transportprotokoll-Anomalien, Angriffen auf Protokolle wie TCP, http oder https/TLS sowie Dienste und Applikationen wie DNS, SIP etc. Ihr Datenverkehr wird permanent überwacht, wobei das DDoS-Schutzsystem Angriffe auf IP-Adressen, IP-Adressbereiche (CIDR) aber auch auf ein Autonomos System (AS) selbständig erkennt.

DIE LEISTUNGEN VON INDEVIS DDoS PROTECT IM ÜBERBLICK

- Blockierung auffälliger Nutzer anhand definierter Schwellwerte
- Filtertechnologie: Verhaltensüberwachung einzelner IP-Adressen, ganzer IP-Adressbereiche (CIDR) oder Autonomer Systeme (AS)
- Protokoll-Verifizierung durch Überprüfung von Nutzern und Protokollstandards
- Bogon-Filter: Überprüfung der Gültigkeit verwendeter IP-Adressen
- Überprüfung der IP-Reputation anhand einer globalen Datenbank
- Schutz vor Flooding Attacken
- Möglichkeit zur individuellen Begrenzung der Datenrate
- GEO-Blocking: Möglichkeit zum Blockieren von Anfragen aus bestimmten Regionen und zur Begrenzung von Verkehr anhand geografischer Herkunft
- Whitelisting/Blacklisting
- Layer 3, 4 & 7 DDoS-Schutz

indevis
Sicherheit in einer vernetzten Welt

Ihre Vorteile

- Komplementärer DDoS-Schutz für *indevis Datacenter & Virtualization Services* oder *indevis Web App Secure*
- Vielschichtiges Schutzsystem mit Alarmierungsfunktion
- Schutz vor volumetrischen Attacken, Transportprotokoll-Anomalien, Angriffen auf Internet-Protokolle und Angriffen auf Dienste und Applikationen
- Optionales grafisches User-Interface (WebUI) mit Realtime-Monitoring und Reporting-Möglichkeiten
- Keine Investition in Hardware, künftige jährliche Software-Wartungsverträge, Consulting oder Trainings
- indevis stellt ein Helpdesk zur Verfügung – und entlastet damit Ihre eigene IT-Abteilung

cloud services
MADE IN GERMANY

SIE WOLLEN
MEHR ERFAHREN?

Ihr persönlicher Ansprechpartner berät Sie gerne und findet mit Ihnen heraus, welches Konzept am besten zu Ihnen passt.

+49 (89) 45 24 24-100
sales@indevis.de
www.indevis.de

DDoS-SCHUTZ FÜR LAYER 3, 4 UND 7

Durch Tracking und eine Alarmfunktion kann das System schon im Übertragungsnetz Anomalien erkennen, sodass die entsprechenden Abwehrmechanismen greifen können.

SCHUTZ AUF PROTOKOLLEBENE 3 UND 4 DES OSI-SCHICHTMODELLS

- Das System kann eine Attacke anhand von Anomalien erkennen, unterstützt durch Tracking und Alarmierung, wenn bestimmte Verkehrsmuster zu einzelnen Hosts außerhalb des normalen Netzwerkverhaltens liegen.
- Diese Verkehrsmuster enthalten: TCP-SYN, TCP-RST, TCP-Null, ICMP, IP-Null, IP-Fragmented, DNS, UDP und IP private address traffic, inklusive Datenverkehr zu und von IPv6 hosts.
- Folgende Protokoll-Anomalien/-Attacken können erkannt werden: Ungültige Pakete und Protokollverletzungen (Invalid Packets), Zombie-Erkennung (Botnetze / Zombie Detection), TCP- SYN Authentication und HTTP- Authentication, DNS Authentication, DNS Malformed, HTTP Malformed, SIP Malformed, TCP Connection Reset (traffic detection only), Baseline Enforcement

LAYER 7 DDOS-SCHUTZ – REAKTIVER SCHUTZ
Anwendunsspezifischer Schutz auf Applikationsebene

- Das System ist in der Lage, dedizierte HTTP-Pakete mit HTTP-Headern entsprechend konfigurierbarer Vorgaben zu verwerfen.
- Das System ist in der Lage, HTTP-Verkehr anhand spezifischen Signaturen mit potenziell bösartigen HTTP-Aktivitäten zu blockieren. Die Signatur-Feeds werden von einer IP-Reputation Datenbank mit weltweitem Zugriff auf Metadaten geliefert.
- Das System ist in der Lage, fehlerhafte HTTP-Pakete zu erkennen und zu verwerfen.
- Das System kann mehrere wählbare Reaktionsmöglichkeiten, gegen fehlerhafte HTTP-Pakete auf verschiedene Gefahrenstufen, bereitstellen.
- Das System kann unabhängig vom Belastungszustand fehlerhafte HTTP-Pakete erkennen und verwerfen, wenn diese nicht standardkonform sind, ungültige Parameter aufweisen oder sich deutlich vom üblichen Verhalten von Clients unterscheiden.
- Das System ermöglicht es, konfigurierbare Schwellwerte (Anzahl der HTTP-Operationen pro Sekunde, pro Zielserver) festzulegen, anhand derer Hosts blockiert werden.
- Das System ermöglicht es, konfigurierbare Schwellwerte (Anzahl der HTTP-Operationen pro URL, pro Sekunde, pro Zielserver) festzulegen, anhand derer Hosts blockiert werden können.
- Das System ist in der Lage, reguläre Ausdrücke (Regular Expressions) zu nutzen, um Beschränkungen und Filter für das HTTP Rate Limiting, zur HTTP Objekt-Erkennung und zur HTTP Header Erkennung festzulegen.
- Das System kann fehlerhafte DNS-Anfragen verwerfen.
- Das System kann DNS Floods von gespooften Adressen beenden.
- Das System kann Angreifer blockieren, die DNS-Anfragen schicken, die oberhalb eines konfigurierten Schwellwertes liegen.
- Das System kann fehlerhafte SSL/TLS-Anfragen blockieren.
- Das System kann fehlerhafte SIP-Pakete blockieren.
- Das System kann Angreifer blockieren, die SIP-Pakete schicken, die oberhalb eines konfigurierten Schwellwertes liegen.

OPTIONAL: KUNDEN USER-INTERFACE (WEB UI) FÜR REALTIME-MONITORING UND REPORTING

Das System besitzt eine grafische Benutzeroberfläche, die über einen Standardbrowser aufgerufen und als zusätzliche kostenpflichtige Option zur Verfügung gestellt werden kann, um online den Status konfigurierbarer Echtzeitdaten des Anschlusses einzusehen.

Sie wollen *indevis DDoS Protect* kennenlernen? Auf Wunsch führen wir Ihnen diesen Service gerne in einer Demo-Session vor und erläutern Ihnen die Vorteile unseres additiven DDoS Schutz-Systems.

Über die indevis GmbH

Die BSI-zertifizierte indevis IT-Consulting and Solutions GmbH bietet seit 1999 IT-Sicherheits-, Datacenter- und Netzwerklösungen für Unternehmen jeder Größe und Branche. Dabei erfüllt indevis sowohl die Anforderungen der Wirtschaft als auch die von öffentlichen Behörden und Hochschulen.

Als einer von Deutschlands führenden Managed Security Service Providern ist indevis der Partner für IT-Sicherheit und Netzwerktechnik für über 1.800 Kunden.

indevis betreibt zwei Niederlassungen: in München und Hamburg. Weitere Mitarbeiter agieren von mehreren Standorten in Deutschland. Insgesamt beschäftigt indevis über 70 Mitarbeiter.

indevis
Sicherheit in einer vernetzten Welt

indevis IT-Consulting and Solutions GmbH

Irschenhauser Straße 10
81379 München

Tel. +49 (89) 45 24 24-100
Fax: +49 (89) 45 24 24-199

sales@indevis.de
www.indevis.de