Leistungs-beschreibung.

DDoS Defense Service.

PŸUR Business

Leistungsbeschreibung.

DDoS Defense Service.

1. Allgemeines

DDoS-Angriffe (Distributed Denial of Service Attacks) zielen darauf ab, Dienste zu beeinträchtigen oder vollständig vom Netz zu nehmen.
Es werden dabei die Dienste, wie eine bestimmte Website, eine Plattform oder ein Webservice massiv mit Traffic überlastet.
Typische Anzeichen für einen DDoS-Angriff sind ein erhöhter Internettraffic und abnehmende Dienstqualität, eine erkennbar überhöhte Auslastung von Ressourcen und eine niedrige Netzwerkleistung.
Diese Art von Cyber-Angriffen können Unternehmen durch hohe Ausfallzeiten oder/und durch Datenverlust hohe finanzielle Schäden zufügen oder/und zur Rufschädigung führen.
Die Infrastruktur der PŸUR Business kombiniert Ansätze am Edge Netzwerk und im Backbone und bietet mit ihrem hohen Datendurchsatz bereits einen Schutz des eigenen Netzwerks gegen Volumenangriffe.
Um die Netzwerke unserer Kunden abzusichern, bietet PŸUR Business ergänzend Dienste als Zubuch-Optionen zu Internetschlüssen an. Sie beinhalten Prozesse und Systeme, die der regelbasierten (DDoS Basic Protection) oder reaktiven Abwehr (DDoS Defense Service) von Angriffen unmittelbar auf Dienste und Infrastruktur unserer Kunden dienen.

2. Leistungs- und Produktvoraussetzungen

Alle DDoS-Schutz-Services sind Zubuch-Optionen, d. h. für die Nutzung des DDoS-Schutzes muss ein Kunde über einen Internetzugang von PŸUR Business verfügen.
Der DDoS Defense Service ist ein reaktiver Service, der ausschließlich kundeninitiiert eingeleitet wird.

3. Leistungen

Folgende Leistungen sind im DDoS Defense Service (kundeninitiierter reaktiver Service) enthalten und können im Angriffsfall eingesetzt werden:

3.1 Mitigation am Edge Router

Mithilfe von BGP-Flowspec-Filterlisten können Regeln manuell zum Edge Router ausgespielt werden. Diese werden nach Beendigung einer Attacke in Absprache mit dem Kunden deaktiviert.

3.2 Durchsatzbegrenzung

Mittels Durchsatzbegrenzung im Netzwerk wird nur ein Teil der IP-Pakete zur Zieladresse geroutet, so dass der attackierte Dienst eingeschränkt erreichbar ist.

3.3 Blackholing

Der gesamte an eine IP-Adresse oder an einen IP-Adressbereich des Kunden adressierte Datenverkehr wird verworfen (Blackholing). Die IP-Adresse oder der IP-Adressbereich ist nicht länger im Internet erreichbar.

3.4 Eingesetzte Technik

Die BGP-Flowspec-Regeln werden bei Aktivierung in Echtzeit innerhalb weniger Sekunden an alle Core-Router verteilt und sind dann sofort aktiv.
Die Deaktivierung der Regeln geschieht nach Vereinbarung ebenfalls in Echtzeit.
Es kann auf temporäre Bedrohungen bezüglich des Datenvolumens reagiert werden und es können in gemeinsamer Abstimmung spezifische Regeln implementiert werden.
Die Abwehr von DDoS-Angriffen findet an den Außengrenzen des PŸUR Business Netzwerks statt und ist daher auf PŸUR Business Anschlüsse begrenzt. Eine Mitigation in fremden Netzen findet nicht statt.

PŸUR Business

Leistungsbeschreibung.

DDoS Defense Service.

4. Serviceleistungen PŸUR Business

4.1 Einrichtung des Service

Zur Klärung der Rahmenbedingungen und Definition des Notfall-Management-Prozess findet vor Aufnahme des DDoS Defense Services ein Workshop mit Teilnahme der verantwortlichen Ansprechpartner des Kunden und PŸUR Business statt.

4.2 Service im Angriffsfall

Die Einleitung von Abwehrmaßnahmen erfolgt ausschließlich nach Kontaktaufnahme und Meldung eines Angriffs und Aufforderung durch den Kunden. Basierend auf der Geschäfts- und Risikoeinschätzung des Kunden muss dieser Kontakt mit unserer Hotline im Operation Maintenance Center (OMC) aufnehmen und Details zu dem Angriff nennen, um Maßnahmen zur Mitigation zu vereinbaren und durchzuführen.
Die Einstellung der Mitigation und Rücknahme von Regeln erfolgt ebenfalls in Abstimmung mit dem Kunden.

4.3 Service-Zeiten

Die PŸUR Business betreibt 24 Stunden am Tag und an 365 Tagen im Jahr ein Operation and Maintenance Center (OMC), um die angebotenen Dienste bereitzustellen.
Das OMC nimmt die Angriffsmeldungen unter der Rufnummer der Störungshotline oder per E-Mail an omc@pyur.com entgegen.

Dem DDoS Defense Service sind folgende Servicezeiten zugeordnet:

- 24/7 h, Montag–Sonntag
- Reaktionszeit: 30 Minuten

Die Reaktionszeit ist die Zeitspanne zwischen dem Eingang der Angriffsmeldung und der Eröffnung des Trouble-Tickets mit der Bekanntgabe der Ticketnummer telefonisch oder per E-Mail.

5. Mitwirkungspflichten des Kunden

Der Kunde ist verpflichtet, die erforderlichen Informationen zur Aufnahme des Dienstes im Rahmen des initialen Workshops an die Mitarbeiter der PŸUR Business zu übergeben. Wichtige Informationen in diesem Zusammenhang sind z. B.:

1. Zahl der Anschlüsse
2. Service IDs der Anschlüsse je mit
   - DNS Name Server
   - DNS Resolver
   - LDAP Dienste
   - Weitere Dienste
3. Besonderheiten
4. Kontaktdaten des verantwortlichen Mitarbeiters und die seiner direkten Vertretung

Darüber hinaus ist es sinnvoll, initial den Normalzustand des Netzwerktraffics aller Dienste festzuhalten:

- Netzwerkbandbreite in bit/s, pps
- Anfragen pro Sekunde oder Workload der Infrastruktur

Im Falle eines Angriffs ist auf die Service ID zu verweisen und eine ergänzende Information zu den vom Angriff betroffenen IP-Adressen zu benennen.

6. Laufzeit

Der Service kann mit einer Frist von 4 Wochen zum Ende eines Kalendermonats, erstmals jedoch zum Ende des 24. Kalendermonats, gerechnet ab entgeltpflichtiger Bereitstellung, gekündigt werden. Der Service endet automatisch, sobald der Kunde nicht mehr über einen Internetanschluss von PŸUR Business verfügt.

PŸUR Business

Leistungsbeschreibung.

DDoS Defense Service.

7. Kombination mit DDoS Basic Protection

DDoS Defense Service lässt sich mit dem regelbasierten DDoS-Schutz (DDoS Basic Protection) kombinieren.

8. Allgemeine Bestimmungen

Alle Leistungen im Rahmen der Inbetriebnahme und des Betriebs werden mit großer Sorgfalt durch speziell ausgebildetes Personal mit großer Projekterfahrung erbracht. Dennoch kann PŸUR Business nicht gewährleisten, dass diese Dienstleistung ununterbrochen zur Verfügung steht oder hundertprozentigen Schutz bietet.
Es gelten ergänzend die Allgemeinen Geschäftsbedingungen für PŸUR Business Telekommunikationsdienstleistungen der HLkomm Telekommunikations GmbH sowie die Preisliste für DDoS-Schutz.

PŸUR Business

Wir sind für Sie da.

HLkomm Telekommunikations GmbH
Nonnenmühlgasse 1, 04107 Leipzig
Telefon: + 49 (3 41) 86 97 0
Telefax: + 49 (3 41) 86 97 4 99
E-Mail: business@pyur.com
www.pyur.com/business

pyur.com/business

PŸUR
Business