Leistungs-beschreibung.

DDoS Defense Service.

PŸUR Business

Leistungsbeschreibung.

DDoS Defense Service.

1. Allgemeines

DDoS-Angriffe (Distributed Denial of Service Attacks) über das Internet zielen darauf ab, Dienste zu beeinträchtigen oder vollständig vom Netz zu nehmen. Es werden dabei der Anschluss oder Server massiv mit Traffic überlastet.
Typische Anzeichen für einen DDoS-Angriff sind ein erhöhter Internet-Traffic 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 ergänzende Dienste zur Eindämmung von DDoS-Attacken (Mitigation) an. Sie beinhalten Prozesse und Systeme, die der Abwehr von Angriffen unmittelbar auf Dienste und Infrastruktur unserer Kunden dienen.
Der DDoS Defense Service kann zur Auto-Mitigation und ergänzend im Angriffsfall zur reaktiven Mitigation genutzt werden.
Falls nicht, kann der Kunde entscheiden, ob er den Kontakt zum Operation and Maintenance Center (OMC) der PŸUR Business zur reaktiven Mitigation aufnehmen möchte.

2. Leistungs- und Produktvoraussetzungen

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.
Ein Kunde muss für die Nutzung des DDoS Defense Services daher über einen Internetzugang von PŸUR Business verfügen.
Vor Einrichtung des Service werden pro zusammenhängender IP-Adressgruppe vom Kunden feste Schwell- und Triggerwerte definiert und für die Auto-Mitigation jeweils dazugehörige einheitliche Abwehrregeln (Managed Objects) abgestimmt.
Diese Schwellwerte, Triggerwerte und Regeln für die Auto-Mitigation bleiben dauerhaft eingerichtet.
Der Kunde hat das Recht, zwei Mal pro Vertragsjahr eine Änderung der Managed Objects zu verlangen.

3. Leistungen

3.1 Auto-Mitigation

Wenn die Auto-Mitigation eingerichtet wurde, wird diese ohne Eingriff des Kunden durch das Überschreiten von Schwell- und Triggerwerten für zuvor festgelegte IP-Adressgruppen ausgelöst.

3.2 Reaktive Mitigation

Im Rahmen der reaktiven Mitigation, welche aktiv vom Kunden durch Kontaktaufnahme über die PŸUR Business Hotline eingeleitet werden muss, werden die Mitigationsregeln zwischen Kunden und PŸUR Business unmittelbar im Angriffsfall abgestimmt und angewendet.
Die Filterregeln werden nach Aktivierung innerhalb weniger Sekunden an die Edge-Router im Netzwerk verteilt und sind sofort aktiv.
Nach Beendigung der Attacke werden die Regeln in Absprache mit dem Kunden deaktiviert.

PŸUR Business

Leistungsbeschreibung.

DDoS Defense Service.

3.3 Blackholing

Entscheidet sich der Kunde für „Blackholing“, wird der gesamte an eine IP-Adresse oder an einen IP-Adressbereich des Kunden adressierte Datenverkehr verworfen. Die IP-Adresse oder der IP-Adressbereich ist dann nicht länger im Internet erreichbar.

3.4 Alarmierung per E-Mail

Für die vorab definierten IP-Adressgruppen findet eine kontinuierliche Überwachung des Netzwerk-Traffics statt. Bei Überschreiten der festgelegten Schwell- und Triggerwerten erfolgt die Alarmierung per E-Mail.

3.5 Zugriff auf Web-App mit Dashboards

Mit der Bereitstellung des Dienstes erhält der Kunde einen dedizierten Zugriff auf die Web-App, die über ein kundenindividuelles Dashboard Informationen zur Analyse von komplexen DDoS-Angriffen anzeigt.
Zugangsrechte für die Web-App werden für einen fest definierten Teilnehmerkreis von maximal 2 (zwei) Ansprechpartnern des Kunden vergeben.

3.6 Monatliche Reports

Dem Kunden wird monatlich ein automatisierter Report per E-Mail im PDF-Format mit Statistiken der letzten 30 Tage zur Verfügung gestellt.
Dieser enthält eine Zusammenfassung des Datenverkehrs, der DDoS-Alarmierungen und TCP/UDP Anwendungsprotokolle.

4. Serviceleistungen PŸUR Business

4.1 Einrichtung des Service

Zur Klärung der Rahmenbedingungen, der Definition des Notfall-Management-Prozess und der Managed Objects für die Auto-Mitigation findet vor Aufnahme des DDoS Defense Service eine Abstimmung zwischen den verantwortlichen Ansprechpartnern des Kunden und PŸUR Business statt.

4.2 Service im Angriffsfall

Die Einleitung von reaktiven Abwehrmaßnahmen erfolgt ausschließlich nach Kontaktaufnahme mit dem Operation Maintenance Center (OMC) und der Aufforderung zur Mitigation durch den Kunden.
Der Kunde teilt seine Service-ID sowie die Details des Angriffs mit, insbesondere die betroffenen IP-Adressen, und stimmt die Maßnahmen zur Mitigation mit PŸUR Business ab.
Die Rücknahme der Mitigation-Maßnahmen erfolgt nach Aufforderung durch den Kunden.

4.3 Service-Zeiten

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
- 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, diejenigen Informationen zur Verfügung zu stellen, welche PŸUR Business für die Leistungserbringung benötigt.

PŸUR Business

Leistungsbeschreibung.

DDoS Defense Service.

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.

7. 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