PFALZKOM
Pfalzwerke Gruppe



DDoS-Schutz bei PFALZKOM: lokal trifft global.

Wenn plötzlich niemand mehr durchkommt: PFALZKOM schützt Unternehmen vor digitalen Massenangriffen und verbindet lokale Abwehr mit den globalen Filterkapazitäten von Marktführer Myra Security.

Ludwigshafen, Oktober 2026 – Die Website ist da. Die Server laufen. Die Daten sind sicher. Und trotzdem kommt niemand mehr durch. Was zunächst widersprüchlich klingt, beschreibt einen DDoS-Angriff. Angreifer schicken so viele künstliche Anfragen gleichzeitig an die digitale Infrastruktur eines Unternehmens, dass für echte Kunden, Mitarbeitende oder Geschäftspartner kein Durchkommen mehr ist.

PFALZKOM erweitert deshalb gemeinsam mit Myra Security, dem deutschen Marktführer für DDoS-Schutz, sein Sicherheitsportfolio um eine neue leistungsstarke Schutzlösung. Diese verbindet lokale Filtertechnik in den PFALZKOM-Rechenzentren mit den globalen Abwehrkapazitäten von Myra Security. Damit erhalten auch mittelständische Unternehmen Zugang zu einer leistungsfähigen, mehrstufigen Abwehr gegen Überlastungsangriffe.

Wenn der digitale Eingang plötzlich blockiert ist

Das Prinzip eines DDoS-Angriffs ist einfach, man stelle sich einen Geschäftseingang vor, vor dem plötzlich Tausende Menschen stehen, die gar nichts kaufen wollen. Sie blockieren Türen und Zufahrten, die echten Kunden bleiben draußen. Im Internet übernehmen diese Rolle sogenannte Botnetze. Sie bestehen aus einer Vielzahl kompromittierter Computer, Server oder vernetzter Geräte, die von Angreifern ferngesteuert werden. Gemeinsam erzeugen sie innerhalb kürzester Zeit enorme Mengen künstlichen Datenverkehrs. Die Folge ist, dass Internetleitungen, Server oder Anwendungen überlastet werden. Websites sind nicht mehr erreichbar, Kundenportale reagieren nicht, Transaktionen brechen ab oder digitale Schnittstellen zu Lieferanten fallen aus.

Anders als bei vielen Cyberattacken müssen dabei nicht einmal Daten gestohlen oder Systeme gehackt werden. Es reicht, den Zugang zu ihnen zu blockieren. Für Unternehmen, deren Geschäftsprozesse vom Internet abhängen, kann aus einem technischen Problem deshalb schnell ein wirtschaftliches werden. Produktions- und Lieferketten können ins Stocken geraten, digitale Umsätze ausfallen und Dienstleistungen nicht mehr erreichbar sein.

Wenn Angriffe wie echte Nutzeranfragen aussehen

Auch DDoS-Angriffe haben sich verändert. Klassische Attacken versuchen vor allem, eine Internetleitung mit möglichst großen Datenmengen zu verstopfen. Moderne Angriffe gehen teilweise subtiler vor. Sie imitieren echte Nutzer und greifen gezielt Anwendungen an. Statt Millionen offensichtlich verdächtiger Datenpakete zu senden, können Angreifer

PFALZKOM GmbH
Wredestraße 35
67059 Ludwigshafen
info@pfalzkom.de
www.pfalzkom.de
presse@pfalzkom.de

beispielsweise immer wieder besonders aufwendige Suchanfragen auf einer Website auslösen. Für klassische Sicherheitssysteme sehen diese zunächst wie normale Besucher aus. Für den Server bedeuten sie jedoch Schwerstarbeit. PFALZKOM setzt deshalb auf mehrere Verteidigungslinien.

Wie eine Wasserfilteranlage für Daten

Das Prinzip dahinter lässt sich mit einer Wasserfilteranlage vergleichen. Bevor das Wasser beim Verbraucher ankommt, durchläuft es verschiedene Filterstufen. Unerwünschte Bestandteile werden herausgefiltert, sauberes Wasser darf passieren. Beim DDoS-Schutz geschieht Ähnliches mit dem Datenverkehr. Systeme analysieren die eingehenden Anfragen und trennen schädlichen von legitimem Traffic. Verdächtige Daten werden verworfen, echte Anfragen gelangen weiter zu den Systemen des Unternehmens. Die erste Verteidigungslinie befindet sich direkt in den PFALZKOM-Rechenzentren. Dort überwachen spezielle Systeme den Datenverkehr kontinuierlich. Registrieren sie ungewöhnliche Muster oder überschrittene Schwellenwerte, kann die Filterung automatisch einsetzen. Der Vorteil der lokalen Lösung ist, dass PFALZKOM den Schutz granular auf die Infrastruktur seiner Kunden abstimmen kann und auch kleinere Netze absichert.

Wenn die Welle zu groß wird

Doch selbst die leistungsfähigste lokale Filteranlage hat physische Grenzen. Bei extrem großen Angriffen können Datenmengen entstehen, die bereits die Internetanbindung eines Rechenzentrums überlasten würden. Dann greift die zweite Verteidigungslinie. Über die Infrastruktur von Myra Security kann der Datenverkehr bereits außerhalb des regionalen PFALZKOM-Netzes gefiltert werden. Die schädliche Datenflut wird abgefangen, bevor sie die eigentliche Infrastruktur erreicht. Erst der bereinigte Verkehr wird weitergeleitet. So entsteht ein hybrides Schutzmodell: kleine und mittlere Angriffe möglichst nah an der eigenen Infrastruktur abfangen, extreme Angriffswellen bereits davor brechen.
„Bei DDoS-Angriffen geht es nicht um Datendiebstahl, sondern darum, Dienste und Anwendungen für Nutzer unerreichbar zu machen. Bereits kurze Ausfälle können erhebliche Auswirkungen auf Unternehmen und Organisationen haben“, sagt Sebastian Brechtel, Produktmanager bei PFALZKOM**.** „Durch die Kombination aus lokaler Abwehr in unserem Rechenzentrumscampus und den globalen Filterkapazitäten von Myra können wir Angriffe unterschiedlicher Größenordnung wirksam abwehren. Damit ermöglichen wir auch kleineren Netzen und einzelnen Internetanschlüssen ein Schutzniveau, das bislang häufig nur großen Unternehmen vorbehalten war. Für unsere Kunden bedeutet das vor allem eines: Websites, Kundenportale, Anwendungen und die dahinterliegenden Geschäftsprozesse bleiben auch im Angriffsfall verfügbar.

Vom Mittelstand bis zur kritischen Infrastruktur

Besonders relevant ist der Schutz für Unternehmen, deren Geschäft unmittelbar von permanent verfügbaren digitalen Diensten abhängt. Dazu gehören beispielsweise Industrieunternehmen mit vernetzten Lieferketten, Onlinehändler und Betreiber von Kundenportalen ebenso wie Energieversorger, Stadtwerke, Gesundheitseinrichtungen und öffentliche Verwaltungen.

Für Betreiber kritischer Infrastrukturen gewinnt die Verfügbarkeit zusätzlich an Bedeutung. Auch regulatorische Anforderungen an Cyberresilienz und Risikomanagement erhöhen den Handlungsdruck.

Der PFALZKOM DDoS Schutz ergänzt als Service das bestehende Portfolio. Unternehmen müssen damit keine eigene zusätzliche DDoS-Abwehrinfrastruktur aufbauen. PFALZKOM und Myra stimmen Schutzmechanismen und Filterregeln auf die jeweilige Infrastruktur und den typischen Datenverkehr des Kunden ab. Dabei lassen sich auch Angriffe auf Webanwendungen gesondert absichern. Ergänzend können unter anderem Zugriffe nach Herkunft gesteuert, ungewöhnlich viele Anfragen einzelner Quellen begrenzt und Angriffe detailliert ausgewertet werden.

Die digitale Tür muss offen bleiben

Mit dem neuen Angebot erweitert PFALZKOM den Schutz seiner Rechenzentrums- und Netzinfrastruktur um eine zusätzliche Sicherheitsebene. Im Mittelpunkt steht dabei ein vergleichsweise einfaches Ziel: echte Nutzer sollen durchkommen, Angreifer nicht. Denn je stärker Unternehmen ihre Prozesse digitalisieren und miteinander vernetzen, desto wichtiger wird neben dem Schutz von Daten auch die Verfügbarkeit der Systeme. Digitale Sicherheit bedeutet heute nicht nur, Angriffe abzuwehren, sondern sicherzustellen, dass Geschäftsprozesse auch unter Angriff weiterlaufen.

PFALZKOM GmbH
Wredestraße 35
67059 Ludwigshafen

info@pfalzkom.de
www.pfalzkom.de
presse@pfalzkom.de