LINK11

5

DINGE, DIE SIE ÜBER DDOS WISSEN SOLLTEN

www.link11.com

HERZLICH WILLKOMMEN

Schön, dass Sie unseren **DDoS-Leitfaden** heruntergeladen haben. Er soll Sie dabei unterstützen, sich präventiv vor **DDoS-Attacken** zu schützen.

Im Fall eines **DDoS-Angriffs** reichen Sekunden aus, um Ihre IT-Infrastruktur lahmzulegen und einen enormen Schaden anzurichten. Warten Sie nicht, bis etwas passiert ist: Mindern Sie das Risiko, nicht erst den Schaden.

So wahrscheinlich ist es....

dass Sie im Lotto gewinnen:	**1:140.000.000**
dass Sie Opfer eines Haiangriffs werden:	**1:4.000.000**
dass Sie vom Blitz getroffen werden:	**1:200.000**
dass Sie beim Golf ein Hole in One landen:	**1:10.000**
dass Sie einen Autounfall haben:	**1:100**

... dass Sie Opfer einer DDoS-Attacke werden: 1:4

Die eigentliche Herausforderung besteht nicht nur darin, über DDoS-Attacken Bescheid zu wissen, sondern auch darin, die Schwachstellen Ihrer Systeme zu verstehen und dieses Wissen in umsetzbare Strategien zu verwandeln. Ein umfassender und kritischer Ansatz ermöglicht die Entwicklung einer Sicherheitslösung, die die Auswirkungen von DDoS-Angriffen antizipiert und abmildert und so eine robuste Verteidigung gegen potenzielle Bedrohungen aufbaut:

1. Das DDoS-Risiko ist real und komplex
2. Kritische Vermögenswerte haben Schwachstellen
3. Präzision und Geschwindigkeit
4. Effektiver DDoS-Schutz braucht Spezialisten
5. Link11 – Empowering your Business Security

DAS DDOS-RISKO IST REAL UND KOMPLEX

DDoS-Angriffe sind nicht nur eine theoretische Bedrohung, sondern eine alltägliche Realität. Sie haben in den letzten Jahren stark zugenommen. Die Gründe dafür sind vielfältig:

- **Politisierung des Cyberraums:** Geopolitische Spannungen und Konflikte führen zu einem Anstieg politisch motivierter Cyberangriffe.
- **Leicht zugängliche Tools:** Die Verfügbarkeit von einfach zu bedienenden DDoS-Tools senkt die Einstiegshürde für Angreifer.
- **Technologischer Fortschritt:** Neue Technologien wie IoT und KI ermöglichen komplexere und effektivere Angriffe.

Cyberkriminelle nutzen immer ausgefeiltere Methoden, um Unternehmen zu attackieren. Durch den Boom von Cybercrime-as-a-Service können selbst kleine Unternehmen zum Ziel werden. Moderne DDoS-Angriffe sind **smart und komplex**. Die zunehmende Geschwindigkeit und Intensität von Attacken, insbesondere die wachsende Zahl von Turboangriffen, die innerhalb weniger Sekunden ihre volle Wucht entfalten, stellen Unternehmen vor neue Herausforderungen.

Im ersten Halbjahr 2024 erreichte bereits über ein Drittel aller Angriffe im Link11-Netzwerk innerhalb der ersten zehn Sekunden ihren Höhepunkt. **Diese Entwicklung zeigt, dass Angreifer ihre Taktiken kontinuierlich verfeinern und Unternehmen ihre Sicherheitsmaßnahmen anpassen müssen, um effektiv geschützt zu sein.**

Gerade DDoS-Angriffe sind immer einfacher und kostengünstig zu bewerkstelligen. Neben der gestiegenen Komplexität war es noch nie so einfach und kostengünstig, DDoS-Angriffe selbst in die Tat umzusetzen – in vielen Fällen benötigt man dazu nicht einmal technisches Verständnis. Schlagkräftige Attacken von gut bestückten Botnetzen können direkt aus dem Internet für überschaubares Geld gebucht werden.

Eine effektive Schutzlösung ist daher unerlässlich. Aber Vorsicht: Ein DDoS-Schutz agiert je nach Angriffsart unterschiedlich effektiv. Es ist daher äußerst wichtig, dass der eingesetzte Schutzmechanismus nicht nur in einer Disziplin effektiv agiert, sondern alle Angriffsmuster zuverlässig mitigiert. Angreifer setzen verstärkt auf KI und Schutztechnologien, die NICHT ebenfalls daraufsetzen, können solchen Angriffen kaum noch standhalten.

Informieren Sie sich regelmäßig im Link11 Cyber-Report zu neuen Angriffsmustern und Trends

Downlaod Report

IHRE VERMÖGENSWERTE IM VISIER

Die Sicherheit von IT-Systemen ist für Unternehmen jedweder Größe von zentraler Bedeutung. Schwachstellen in diesen Systemen führen zu ernsthaften Sicherheitslücken, die von Cyberkriminellen ausgenutzt werden können.

Tag und Nacht suchen bösartige Hacker im Internet nach potenziellen Schwachstellen. Dabei greifen sie auf sogenannte Open Source Intelligence (OSINT) zurück. Aus öffentlichen Quellen wie dem Internet werden frei verfügbare Informationen zusammengetragen und im Anschluss mithilfe von künstlicher Intelligenz analysiert.

Dazu gehören etwa interne Ressourcen wie offene Ports und vernetzte Geräte. Aber auch auf Unternehmenswebseiten und in sozialen Netzwerken können Cyberkriminelle wertvolle Informationen finden, um ihre Angriffe zu planen und später auszuführen.

Umso wichtiger ist es, dass Sie regelmäßige Sicherheitsaudits durchführen, um zu prüfen, ob die Sicherheitsmaßnahmen wie der DDoS-Schutz auf dem neuesten Stand sind. Und dass proaktiv, bevor die potenziellen Angreifer die Sicherheitslücken in geschäftskritischen Anwendungen oder Netzwerken entdeckt haben.

PRÄZISION UND GESCHWINDIGKEIT

Präzision und Geschwindigkeit sind in Kombination entscheidend bei der Abwehr von DDoS-Attacken. Beide Aspekte sollten gleich stark ausgeprägt sein, um Sie effektiv vor Gefahren zu schützen.

Präzise Angriffserkennung: Die Grundlage zur Abwehr
Um die richtigen Gegenmaßnahmen einzuleiten, muss das System zuerst präzise einen Angriff in Ihren Traffic-Mustern erkennen. Gerade sogenannte Zero-Day-Angriffe, die auf unentdeckte Schwachstellen in Ihrer IT-Infrastruktur abzielen, erfordern eine intelligente, selbstlernende Lösung für die erfolgreiche Abwehr.

Schnelle Mitigation: Jede Sekunde zählt:
Bevor es zu Schäden kommt, sollte ein verlässlicher DDoS-Schutz Attacken in Echtzeit abwehren – die Time-to-Mitigate (TTM) sollte hier so schnell wie nur möglich sein. Erfolgt die Mitigation in Echtzeit, können Auswirkungen wie Website-Performance, nicht erreichbare Services, Produktionsausfälle oder Rufschädigung verhindert werden. Dabei zählt jede Sekunde, denn die Kosten eines DDoS-Angriffs können schnell steigen.

Link11 garantiert per
Service Level Agreement
eine Mitigation von maximal

10 Sekunden.

EFFEKTIVER DDOS-SCHUTZ BRAUCHT SPEZIALISTEN

Für viele Unternehmen sind die Verfügbarkeit und Performance von Webseiten oder Web-Applikationen wie z.B. Warenkörbe, Kundenportale oder Online-Zahlungssysteme bei E-Commerce-Shops unverzichtbar. Das Risiko, von einem DDoS-Angriff getroffen zu werden, liegt bei 1:4 und wird häufig unterschätzt.

Umso wichtiger ist es, dass geeignete Schutzmaßnahmen implementiert sind, bevor ein Angriff in vollem Gange ist. Lassen Sie sich von Spezialisten beraten, welcher Schutz in welchem Umfang für Sie der richtige ist.

Die Link11-Experten beschäftigen sich täglich mit der Abwehr von Angriffen und unterstützen Sie von Anfang an. Zu Beginn begleiten spezialisierte Sales Development Representatives und Account Executives Ihren Evaluierungs- und Entscheidungsprozess. Für die technische Umsetzung und Implementierung in Ihr bestehendes IT-System stehen Ihnen erfahrene Solution Engineers während des Onboardings zur Seite und die lösungsorientierten Mitarbeiter im Service Center leisten Ihnen 24/7 Hilfe im Notfall.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstreicht die Bedeutung eines mehrstufigen Schutzansatzes und empfiehlt die Zusammenarbeit mit qualifizierten Sicherheitsdienstleistern. Nur so können Unternehmen sich effektiv vor den zunehmend komplexen und häufigen DDoS-Angriffen schützen. Link11 ist anerkannter Anbieter von DDoS-Schutz für kritische Infrastrukturen und erfüllt die hohen Anforderungen des BSI und bietet Ihnen einen umfassenden Schutz, der auf Ihre individuellen Bedürfnisse zugeschnitten ist.

Was zeichnet einen effektiven DDoS-Schutz aus?

Ein effektiver DDoS-Schutz zeichnet sich durch folgende Merkmale aus:

- Präzise Angriffserkennung: Erkennung von Angriffen in Echtzeit von neuen und unbekannten Bedrohungen
- Schnelle Mitigation: Minimierung der Ausfallzeit durch schnelle Abwehrmaßnahmen
- Skalierbarkeit: Anpassung an wechselnde Bedrohungslagen und Wachstum des Unternehmens
- Transparenz: Detaillierte Berichte und Einblicke in die Angriffsaktivitäten

LINK11 – EMPOWERING YOUR BUSINESS SECURITY

Cybersecurity ist kein Luxus mehr, sondern eine Notwendigkeit. DDoS-Angriffe sind zu einer alltäglichen Bedrohung geworden, die Unternehmen aller Größenordnungen betrifft.

Link11 ist mehr als nur ein Anbieter von DDoS-Schutzlösungen. Seit der Gründung im Jahr 2005 stehen wir an der Seite unserer Kunden, um ihre IT-Infrastruktur zu sichern. Das eigene globale Netzwerk mit KI-basiertem und patentiertem DDoS-Schutz bietet hohe Verfügbarkeit, Multi-Terabit-Kapazität und niedrige Latenzzeiten.

Warum Link11?

- Expertise: 130+ Sicherheitsexperten mit 150+ Jahren DDoS-Expertise sind stets auf dem neuesten Stand der Bedrohungslandschaft.
- Proaktiver Schutz: Wir bieten Ihnen einen umfassenden Schutz vor DDoS-Angriffen und anderen Cyberbedrohungen. 1Mio+ abgewehrte Attacken auf 1+ Mio. IP-Adressen für 500+ Kunden
- Personalisierte Lösungen: Unsere Lösungen passen sich perfekt an Ihre individuellen Anforderungen an. Link11 sichert weltweit bereits mehr als 2 Millionen Assets, verteilt über verschiedene Branchen.
- Rundum-Service: Mit einem hohen Net-Promoter-Score (NPS) stehen wir Ihnen jederzeit zur Seite, um Ihre Fragen zu beantworten und Sie bei der Umsetzung Ihrer Sicherheitsstrategie zu unterstützen.
- Umfassender DDoS-Schutz: Link11 schützt Ihre gesamte IT-Infrastruktur vor Angriffen. Unsere Lösung bietet proaktiven Schutz auf den Netzwerk- und Anwendungsschichten (Layer 3, 4 & 7).

Durch die Zusammenarbeit mit einem **BSI-zertifizierten** Sicherheitsdienstleister wie Link11 können Sie Ihre digitale Infrastruktur effektiv schützen und sich **DSGVO-konform** vor den Folgen von DDoS-Angriffen absichern.

IHR KONTAKT

Stärken Sie Ihre Cyber-Resilienz mit Link11. Über 500 Unternehmen vertrauen bereits auf unsere Expertise und setzen auf unsere maßgeschneiderten DDoS-Schutzlösungen. Wir garantieren Ihnen höchste Verfügbarkeit Ihrer IT-Systeme. Lassen Sie sich von unseren Erfolgsgeschichten inspirieren und erfahren Sie, wie Link11 auch Ihr Unternehmen vor DDoS-Attacken schützen kann. Vereinbaren Sie jederzeit gerne einen unverbindlichen Gesprächstermin, in dem wir Ihnen alle Fragen rund um unseren umfassenden DDoS-Schutz beantworten.

Kontaktieren Sie unsere Experten

LINK11

Link11 GmbH | Lindleystr. 12 | 60314 Frankfurt | www.link11.com