Die Bedeutung von Akamai für den DDoS-Schutz gemäß NIS2 in der deutschen Verwaltung

Inhaltsverzeichnis

Einleitung

Für die deutschen Verwaltung stellen DDoS-Angriffe eine Gefahr für die Cybersicherheit kritischer IT-Anwendungen und damit für deren Stabilität und Arbeitsfähigkeit dar. Entsprechend fordern immer mehr Regulatorien, kritische IT-Anwendungen vor dieser und anderen Cybergefahren zu schützen.

DDoS-Angriffe können potenziell auf verschiedene Organisationen der öffentlichen Verwaltung abzielen, einschließlich Regierungsbehörden, Kommunen oder anderen Verwaltungseinheiten. DDoS-Angriffe auf die deutsche Verwaltung können verschiedene Ziele haben. Ein Ziel könnte darin bestehen, die Online-Dienste einer Behörde oder Institution zu stören, um die Verfügbarkeit von wichtigen Informationen oder Services einzuschränken. Dies kann den reibungslosen Betrieb und die Erreichbarkeit von Regierungswebsites, Online-Diensten für die Bürger oder Kommunikationssystemen beeinträchtigen.

Um solche Angriffe abzuwehren, ist es wichtig, dass die deutsche Verwaltung angemessene Sicherheitsmaßnahmen implementiert. Dazu gehören der Einsatz von Firewalls, Intrusion Detection Systems (IDS), Traffic-Analyse-Tools und DDoS-Mitigation-Systemen. Durch diese Maßnahmen können verdächtiger Netzwerkverkehr erkannt, Angriffe abgewehrt und die Auswirkungen von DDoS-Angriffen minimiert werden.

Akamai ist ein Unternehmen, das Expertise in Content Delivery Network (CDN)-Diensten und Web-Sicherheitslösungen besitzt. Akamai kann die deutsche Verwaltung in Bezug auf das Abwehren von DDoS-Angriffen unterstützen, indem es fortschrittliche DDoS-Mitigationslösungen bereitstellt. Diese Lösungen können große und komplexe Angriffe erkennen und abwehren, um die Infrastruktur der Verwaltung zu schützen. Darüber hinaus bietet Akamai auch Content Delivery Services an, um den Zugriff auf Websites und Online-Dienste zu beschleunigen und blockiert als Bestandteil des Content Delivery Services bösartigen Datenverkehr mittels Web Application Firewall und schützt dadurch Webanwendungen. Zusätzlich dazu kann Akamai Sicherheitsberatungsdienste anbieten, um die deutsche Verwaltung bei der Entwicklung einer umfassenden Sicherheitsstrategie zu unterstützen, einschließlich Risikobewertungen und Empfehlungen zur Verbesserung der Sicherheit der deutschen Verwaltung.

Dieses Positionspapier beschreibt die Möglichkeiten von Akamai, einem führenden Anbieter von DDoS-Schutzlösungen, für die deutsche Verwaltung Sicherheitsmaßnahmen, inklusive deren technischer Implementierung, zu ergreifen. Es werden ebenfalls Aspekte des Datenschutzes, der technischen Implementierung und der Akamai Technologie-Partner mit betrachtet.

Aufgabenstellung

1. **Die NIS2-Richtlinie und ihre Bedeutung für die deutsche Verwaltung**

- Die NIS2-Richtlinie, als ein Regulatorium, um kritische IT-Anwendungen vor Cybergefahren zu schützen, hat das Ziel, die Netzwerk- und Informationssicherheit in der Europäischen Union zu stärken.
- Sie legt Anforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste fest, um vorbeugende Maßnahmen gegen Cyberangriffe, einschließlich DDoS-Angriffen, zu ergreifen.
- Die deutsche Verwaltung ist verpflichtet, die Vorgaben der NIS2-Richtlinie umzusetzen, um die Sicherheit ihrer Netzwerke und Informationssicherheits-Dienste zu gewährleisten.

2. **DDoS-Angriffe und ihre Bedrohung für die deutsche Verwaltung**

- DDoS-Angriffe zielen darauf ab, Netzwerke und Online-Dienste durch Überlastung zu beeinträchtigen, indem sie eine große Anzahl von Anfragen generieren.
- Diese Angriffe können erhebliche Auswirkungen auf die Verfügbarkeit von Diensten der deutschen Verwaltung haben und den ordnungsgemäßen Betrieb kritischer Systeme gefährden.
- Eine effektive Abwehr von DDoS-Angriffen ist daher von großer Bedeutung, um die Dienstkontinuität und den Schutz sensibler Daten sicherzustellen.

3. **Die Rolle von Akamai im DDoS-Schutz gemäß NIS2**

- Akamai ist ein renommierter Anbieter von DDoS-Schutzlösungen und verfügt über umfangreiche Erfahrung und Expertise in diesem Bereich.
- Die Akamai Lösungen bieten fortschrittliche Technologien zur Erkennung und Abwehr von DDoS-Angriffen in Echtzeit.
- Akamai verfügt über ein globales Netzwerk von Verteidigungsinfrastrukturen, das es ermöglicht, den Datenverkehr zu filtern und legitime Anfragen von schädlichem Datenverkehr zu unterscheiden.
- Durch die leistungsstarken Akamai Schutzmechanismen und ihre Fähigkeit, sich schnell an neue Angriffsmuster anzupassen, bietet Akamai einen zuverlässigen Schutz vor DDoS-Angriffen für die deutsche Verwaltung.

4. Vorteile der Zusammenarbeit mit Akamai

- Die Zusammenarbeit mit Akamai ermöglicht es der deutschen Verwaltung, auf die Erfahrung und Expertise eines etablierten Unternehmens zurückzugreifen, das sich auf DDoS-Schutz spezialisiert hat.
- Akamai bietet proaktive Überwachung, um potenzielle Bedrohungen frühzeitig zu erkennen und darauf zu reagieren.
- Durch die Nutzung der Dienste von Akamai kann die deutsche Verwaltung die Auswirkungen von DDoS-Angriffen minimieren und die Verfügbarkeit ihrer Online-Dienste sicherstellen.

Technische Darstellung

Die technische Lösung von Akamai für den DDoS-Schutz basiert auf einer Kombination fortschrittlicher Technologien und einem globalen Netzwerk von Verteidigungsinfrastrukturen. Hier sind einige Schlüsselelemente der technischen Lösung:

1. DDoS-Erkennung

- Akamai nutzt eine Kombination aus Echtzeitüberwachung und maschinellem Lernen, um DDoS-Angriffe frühzeitig zu erkennen.
- Durch Analyse von Netzwerkdaten, Traffic-Mustern und Verhaltensmerkmalen identifiziert Akamai verdächtigen Datenverkehr, der auf einen DDoS-Angriff hinweisen könnte.

2. Traffic-Filterung

- Sobald ein DDoS-Angriff erkannt wird, leitet Akamai den Datenverkehr durch seine Verteidigungsinfrastrukturen.
- Diese Infrastrukturen verfügen über fortschrittliche Filtermechanismen, um schädlichen Datenverkehr von legitimen Anfragen zu trennen.
- Durch die Anwendung von Heuristiken, Whitelists, Blacklists und anderen Algorithmen sorgt Akamai dafür, dass nur legitime Anfragen an die geschützten Dienste weitergeleitet werden.

3. Skalierbarkeit und globale Verteidigung

- Akamai betreibt ein weltweit verteiltes Netzwerk von Servern, das eine hohe Skalierbarkeit und Flexibilität bietet.
- Dies ermöglicht es, selbst bei massiven DDoS-Angriffen den bösartigen Datenverkehr zu blockieren, die Dienste vor Überlastung zu schützen und weiterhin für legitime Anfragen zur Verfügung zu stellen.
- Das globale Netzwerk von Akamai verteilt den Datenverkehr geografisch, um eine optimale Performance und Ausfallsicherheit zu gewährleisten.

4. Anpassungsfähigkeit und Echtzeit-Reaktionsfähigkeit

- Akamai aktualisiert seine DDoS-Schutzmechanismen kontinuierlich, um auf neue Angriffsmuster und -techniken reagieren zu können.
- Durch Echtzeit-Analysen und automatisierte Systeme kann Akamai schnell auf sich entwickelnde Bedrohungen reagieren und entsprechende Schutzmaßnahmen ergreifen.
- Bei einem DDoS-Angriff passt sich das System von Akamai dynamisch an die aktuellen Angriffsmerkmale an, um die Angriffe zu blockieren und die Dienste zu schützen.

Produktübersicht

Akamai bietet eine Reihe von Produkten und Lösungen zum Schutz vor DDoS-Angriffen an. Hier sind einige Schlüsselprodukte:

- **"App and API Protection”**
  Dies ist ein robuster Web Application Firewall (WAF) Dienst, der vor DDoS-Angriffen und anderen webbasierten Bedrohungen schützt. Der Dienst erkennt und blockiert schädlichen Datenverkehr, und lässt nur legitime Anfragen auf die Anwendungen und Websites der deutschen Verwaltung zu. Dadurch schützt der Dienst die kritischen IT-Anwendung der deutschen Verwaltung.

- **"Prolexic Routed"**
  Dieser Service bietet DDoS-Mitigation für Netzwerke und Infrastrukturen. Akamai leitet den Netzwerkverkehr über seine Cloud-Infrastruktur, in der legitime Anfragen an die Netwerke und Infrastruktur der deutschen Verwaltung weitergeleitet werden und bösartiger Datenverkehr blockiert wird. .

- **"Cloud Security Solutions"**
  Akamai bietet eine Suite von Cloud-Sicherheitslösungen an, die den Schutz vor DDoS-Angriffen verbessern. Dies umfasst DDoS-Mitigation, Web Application Firewalling, Bot-Management und Schutz vor anderen Web-basierten Bedrohungen.

- **"Prolexic SSL Inspection"**
  Dieser Service ermöglicht die sichere Inspektion von SSL-verschlüsseltem Datenverkehr. Dies ist wichtig, um versteckten schädlichen Datenverkehr zu erkennen und zu blockieren, der sich hinter verschlüsselten Verbindungen verbirgt.

Diese Produkte von Akamai werden kontinuierlich weiterentwickelt und an die sich verändernden Bedrohungslandschaften angepasst. Sie bieten einen umfassenden Schutzmechanismus gegen DDoS-Angriffe, um die Verfügbarkeit, Integrität und Sicherheit der Infrastruktur der deutschen Verwaltung zu gewährleisten.

Datenschutz

Akamai nimmt den Datenschutz sehr ernst und setzt sich aktiv für die Sicherheit und den Schutz der Daten seiner Kunden ein. Die Akamai implementiert umfangreiche Sicherheitsmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten. Dazu gehören physische Sicherheitsvorkehrungen, Zugriffskontrollen und Verschlüsselungstechnologien. Akamai verarbeitet personenbezogene Daten gemäß den geltenden Datenschutzgesetzen und hält sich an die Prinzipien der Datenminimierung und Zweckbindung. Das bedeutet, dass sie nur die Daten erheben, die für den vereinbarten Zweck erforderlich sind, und sie nur für den notwendigen Zeitraum speichern. Unsere Kunden können sich auf Vertraulichkeitsvereinbarungen verlassen, die Akamai mit ihnen abschließt, um den Schutz ihrer Daten sicherzustellen. Darüber hinaus verfügt Akamai über klare Datenschutzrichtlinien und informiert transparent über die Art der gesammelten Daten, den Zweck der Verarbeitung und die Rechte der Kunden in Bezug auf ihre Daten. Akamai arbeitet kontinuierlich daran, die Einhaltung der Datenschutzstandards sicherzustellen und unterzieht sich regelmäßigen Audits und Prüfungen. Datenschutz ist jedoch eine gemeinsame Verantwortung, und Kunden sollten auch ihre eigenen Datenschutzrichtlinien und -verfahren überprüfen, um sicherzustellen, dass sie ihre Daten angemessen schützen, wenn sie Dienste von Akamai nutzen.

Die DDoS-Schutzlösungen von Akamai erfüllen einschlägige Datenschutzbestimmungen und unterstützen darüber hinaus dabei, einschlägige Sicherheitsanforderung an kritische IT-Anwendungen enthalten zu können. Entsprechende Informationen sind in dem Privacy Trust Center von Akamai, https://www.akamai.com/legal/compliance/privacy-trust-center, abrufbar.

Partner

Akamai hat in Deutschland verschiedene Partner und Kunden, mit denen sie zusammenarbeiten, um ihre Dienstleistungen anzubieten. Einige der bekannten Partner von Akamai in Deutschland sind:

Systemintegratoren und Beratungsunternehmen:

- Bechtle
- Computacenter
- Controlware
- Accenture
- Deloitte

Telekommunikationsunternehmen:

- Deutsche Telekom
- NTT
- Vodafone

Hosting- und Cloud-Service-Provider:

- Plusserver
- Boreus
- Noris Networks
- Akquinet

Schlussfolgerung

Der Schutz vor DDoS-Angriffen ist von entscheidender Bedeutung, um die Netzwerk- und Informationssicherheit in der deutschen Verwaltung gemäß den einschlägigen Regularien, wie die NIS2-Richtlinie und ihre Umsetzungsgesetze zu gewährleisten. Die Zusammenarbeit mit einem erfahrenen Anbieter wie Akamai bietet die Möglichkeit, fortgeschrittene DDoS-Schutzlösungen zu implementieren und den Schutz vor solchen Angriffen zu optimieren. Indem die deutsche Verwaltung auf die Expertise von Akamai zurückgreift, kann sie ihre Netzwerke und Dienste effektiv schützen und den reibungslosen Betrieb ihrer kritischen IT-Anwendungen sicherstellen.