AKAMAI Positionspapier

Wehrhafte Demokratie im Zusammenhang mit Cyberattacken

04.September.2024

Martin Frankenfeldt / Akamai Deutschland GmbH

Inhaltsverzeichnis

Einleitung

Die wehrhafte Demokratie ist ein zentraler Bestandteil der politischen Kultur in Deutschland. Ihr Grundsatz besteht darin, die Demokratie gegen ihre Feinde zu verteidigen, ohne dabei selbst demokratische Prinzipien zu verletzen. In der digitalen Ära stehen Demokratien jedoch vor neuen Herausforderungen, insbesondere durch Cyberattacken. Diese Angriffe können staatliche Institutionen, kritische Infrastrukturen und die freie Meinungsäußerung bedrohen. Es ist daher notwendig, die Prinzipien der wehrhaften Demokratie auf den digitalen Raum zu erweitern und anzupassen.

Bedrohungsszenario

Cyberangriffe nehmen an Umfang und Komplexität zu und richten sich gegen demokratische Institutionen, Unternehmen und Bürger gleichermaßen. Die Bedrohungen reichen von Datendiebstahl und Sabotage über die Manipulation von Wahlen bis hin zur gezielten Verbreitung von Desinformation. Solche Angriffe können nicht nur wirtschaftliche Schäden verursachen, sondern auch das Vertrauen in demokratische Prozesse und Institutionen untergraben.

Zielsetzung

Ziel dieses Positionspapiers ist es, Strategien und Maßnahmen aufzuzeigen, mit denen die wehrhafte Demokratie auf Cyberattacken reagieren kann, um die Integrität und Stabilität der Demokratie in Deutschland zu gewährleisten.

Akamai hat es sich zur Aufgabe gemacht, dieses Ziel zu unterstützen und die technischen Möglichkeiten zur Verfügung zu stellen, um die demokratische Willensbildung zu schützen.

Analyse

1. Gefährdung der staatlichen Souveränität: Cyberattacken auf staatliche Institutionen, wie Ministerien, Parlamente oder Wahlsysteme, können die Funktionsfähigkeit des Staates gefährden. Diese Angriffe zielen darauf ab, das Vertrauen der Bürger in ihre Regierung zu unterminieren und die demokratische Willensbildung zu beeinflussen.

2. Angriffe auf kritische Infrastrukturen: Der Schutz kritischer Infrastrukturen, wie Stromnetze, Wasserversorgung oder Kommunikationsnetze, ist essenziell für das Überleben einer modernen Gesellschaft. Cyberattacken auf diese Systeme können zu erheblichen gesellschaftlichen Störungen und einem Vertrauensverlust in die Handlungsfähigkeit des Staates führen.

3. Manipulation und Desinformation: Die Verbreitung von Fake News und die gezielte Manipulation der öffentlichen Meinung durch soziale Medien können das demokratische Gefüge destabilisieren. Solche Angriffe zielen darauf ab, soziale Spannungen zu verschärfen und Misstrauen gegenüber demokratischen Institutionen zu säen.

Handlungsempfehlungen

1. Stärkung der Cybersicherheitsstrategie: Die Bundesregierung muss eine umfassende Cybersicherheitsstrategie entwickeln, die sowohl präventive als auch reaktive Maßnahmen umfasst. Dazu gehören die Einrichtung spezialisierter Einheiten zur Abwehr von Cyberangriffen, die regelmäßige Überprüfung und Verbesserung der Sicherheitsstandards sowie die Zusammenarbeit mit internationalen Partnern.

2. Bildung und Sensibilisierung: Die Bürger müssen über die Gefahren von Cyberattacken und Desinformation aufgeklärt werden. Bildungsprogramme sollten darauf abzielen, digitale Kompetenz und kritisches Denken zu fördern, um die Bevölkerung widerstandsfähiger gegen Manipulationsversuche zu machen.

3. Rechtliche Rahmenbedingungen: Es ist notwendig, die rechtlichen Rahmenbedingungen für den Schutz der Demokratie im digitalen Raum zu stärken. Dazu gehört die Anpassung bestehender Gesetze sowie die Einführung neuer Regelungen, die gezielte Desinformationskampagnen sowie Cyberangriffe auf staatliche Einrichtungen und kritische Infrastrukturen unter Strafe stellen.

4. Internationale Kooperation: Cyberbedrohungen machen nicht an nationalen Grenzen halt. Deshalb ist eine enge Zusammenarbeit mit internationalen Partnern unabdingbar. Diese umfasst den Austausch von Informationen, die gemeinsame Entwicklung von Abwehrstrategien sowie die koordinierte Reaktion auf Cyberangriffe.

5. Technologische Innovationen: Der Staat sollte die Forschung und Entwicklung im Bereich der Cybersicherheit aktiv fördern. Dies beinhaltet die Unterstützung von Innovationen in der Verschlüsselungstechnologie, der Künstlichen Intelligenz zur Bedrohungserkennung und der Entwicklung robuster, sicherer Infrastrukturen.

Technische Darstellung

Die technischen Lösungen von Akamai für den Schutz vor Cyberattacken basieren auf einer Kombination fortschrittlicher Technologien und einem globalen Netzwerk von Verteidigungsinfrastrukturen. Die Schlüsselelemente der technischen Lösung umfassen unter anderem:

1. DDoS-Erkennung

- Akamai nutzt eine Kombination aus Echtzeitüberwachung und maschinellem Lernen, um DDoS-Angriffe frühzeitig zu erkennen.
- Durch die 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 hochmoderne Filtermechanismen, um schädlichen Datenverkehr von legitimen Anfragen zu trennen.
- Durch die Anwendung von Heuristiken, Whitelists, Blacklists und andere 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. Die im Folgenden aufgeführten Schlüsselprodukte bieten einen umfassenden Schutzmechanismus gegen DDoS-Angriffe. Sie gewährleisten die Verfügbarkeit, Integrität und Sicherheit der Infrastruktur der deutschen Verwaltung.

- "App and API Protection”

  Dieser robuste Web Application Firewall (WAF) Dienst schützt vor DDoS-Angriffen und anderen webbasierten Bedrohungen. Er erkennt und blockiert schädlichen Datenverkehr und lässt nur legitime Anfragen auf die Anwendungen und Websites der deutschen Verwaltung zu. So schützt der Dienst deren kritische IT-Anwendungen.

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

- "Cloud Security Solutions"
  Akamai bietet eine Suite von Cloud-Sicherheitslösungen an, die den Schutz vor DDoS-Angriffen verbessern. Diese 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. Das ist wichtig, um versteckten schädlichen Datenverkehr zu erkennen und zu blockieren, der sich hinter verschlüsselten Verbindungen verbirgt.

Akamai entwickelt diese Produkte kontinuierlich weiter und passt sie an die sich verändernden Bedrohungslandschaften an.

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 einhalten zu können. Entsprechende Informationen sind in dem Privacy Trust Center von Akamai, https://www.akamai.com/legal/compliance/privacy-trust-center, abrufbar.

Schlussfolgerung

Die wehrhafte Demokratie muss sich den Herausforderungen des digitalen Zeitalters anpassen. Cyberangriffe stellen eine ernsthafte Bedrohung für die Stabilität und Integrität der demokratischen Ordnung dar. Es ist daher von entscheidender Bedeutung, dass der Schutz der Demokratie auch im digitalen Raum gewährleistet wird. Durch eine Kombination aus technischer Innovation, rechtlicher Anpassung, internationaler Zusammenarbeit und der Sensibilisierung der Bevölkerung kann Deutschland seine Demokratie auch gegen digitale Bedrohungen erfolgreich verteidigen.