Akamai

WHITEPAPER

Zero Trust Maturity mit Akamai

Unterstützung der bereichsübergreifenden Funktionen der CISA für Bundesbehörden und -ämter

Einführung

Zero-Trust-Sicherheit hat sich zum Maßstab für den Schutz vertraulicher Regierungsdaten, kritischer Infrastruktur und nationaler Sicherheitssysteme entwickelt. Bundesbehörden und -ämter können sich zur Abwehr moderner Bedrohungen nicht mehr auf herkömmliche perimeterbasierte Sicherheitsmodelle verlassen. Cyberangriffe werden immer raffinierter und Cyberkriminelle wenden immer ausgefeiltere Methoden an – Diebstahl von Anmeldedaten, Ransomware und Insiderangriffe. Demzufolge vertrauen immer mehr Bundesbehörden für ihre Sicherheit auf ein Zero-Trust-Framework. Die Umstellung auf ein solches Framework verläuft jedoch bislang bruchstückhaft, und es muss mehr getan werden, um die staatlichen Systeme zu sichern.

Das Zero Trust Maturity Model der Cybersecurity and Infrastructure Security Agency (CISA) kann Bundesbehörden und -ämter bei der Implementierung von Sicherheitsprinzipien unterstützen, die implizites Vertrauen eliminieren und strenge Verifizierungsmechanismen durchsetzen. Das Modell basiert auf fünf Grundpfeilern: Identität, Geräte, Netzwerke, Anwendungen und Workloads sowie Daten. Darüber hinaus sorgen drei bereichsübergreifende Funktionen – Transparenz und Analyse, Automatisierung und Orchestrierung sowie Governance – für einen ganzheitlichen und einheitlichen Ansatz für Cybersicherheit.

Um diese Ziele zu erreichen, muss Mikrosegmentierung als Kernprinzip der Zero-Trust-Sicherheit betrachtet werden. Sie dient als grundlegende Komponente für den Schutz des internen (d. h. East-West) Netzwerks. Durch Segmentierung von Workloads und Einschränkung lateraler Netzwerkbewegungen können Bundesbehörden potenzielle Sicherheitsverletzungen eindämmen und Zero-Trust-Richtlinien durchsetzen. Darüber hinaus sollten umfassende API-Sicherheitslösungen (Application Programming Interface, Anwendungsschnittstelle) implementiert werden, um die externe Kommunikation (d. h. North-South) zu schützen und sicherzustellen, dass nur autorisierte Stellen auf behördliche Anwendungen zugreifen.

In diesem Whitepaper werden die wichtigsten Schritte zum Erreichen von Zero Trust Maturity erläutert. Es wird verdeutlicht, wie Bundesbehörden und -ämter dank der hochentwickelten Sicherheitslösungen von Akamai – darunter Akamai Guardicore Segmentation, Akamai API Security und Akamai Enterprise Application Access – die Richtlinien der CISA erfüllen und ihre Cybersicherheit stärken.

Umstieg von perimeterbasierter Sicherheit auf Zero Trust

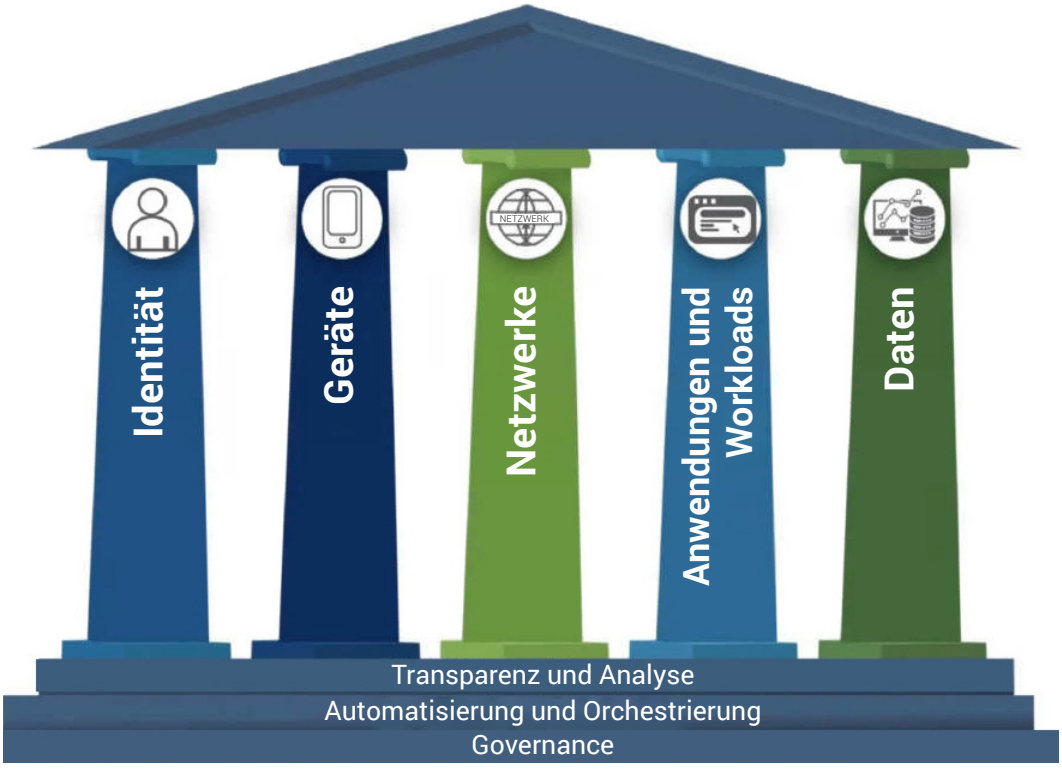
Der herkömmliche Ansatz für Cybersicherheit stützte sich auf perimeterbasierte Abwehrmechanismen. Dabei wurde davon ausgegangen, dass allem innerhalb des Netzwerks vertraut werden kann. Angesichts moderner Cyberbedrohungen hat dieses Modell jedoch wiederholt versagt. Angreifer nutzen schwache Anmeldedaten und falsch konfigurierte Sicherheitseinstellungen aus. Sie arbeiten mit Techniken der lateralen Netzwerkbewegung, um herkömmliche Abwehrmaßnahmen zu umgehen und Zugriff auf vertrauliche Informationen zu erlangen.

Zero Trust eliminiert implizites Vertrauen und erfordert stattdessen eine fortlaufende Überprüfung von Nutzern, Geräten, Anwendungen und Netzwerktraffic. Jede Zugriffsanforderung wird auf der Grundlage von Risikobewertungen in Echtzeit authentifiziert, autorisiert und kontinuierlich überwacht. Durch diesen Ansatz wird die Angriffsfläche erheblich reduziert und unbefugter Zugriff wird verhindert, selbst wenn ein Angreifer in einen Teil des Netzwerks eindringt.

Zero Trust Maturity Model der CISA

Das Zero Trust Maturity Model der CISA bietet für Bundesbehörden und -ämter eine Roadmap zur schrittweisen Stärkung ihres Sicherheitsframeworks (Abbildung). Das Modell basiert auf fünf Grundpfeilern:

- **Identität:** Durchsetzung strenger Authentifizierungs-, Autorisierungs- und Zugriffskontrollen, um sicherzustellen, dass nur legitime Nutzer auf sensible Ressourcen zugreifen dürfen
- **Geräte:** Überwachung, Sicherung und Validierung von Endgeräten, um sicherzustellen, dass diese vor dem Zugriff auf Behördennetze die Sicherheitsrichtlinien erfüllen
- **Netzwerke:** Implementierung von Mikrosegmentierung und erweiterten Zugriffssteuerungsrichtlinien, um unbefugte laterale Netzwerkbewegungen zu verhindern
- **Anwendungen und Workloads:** Schutz von Anwendungen und Workloads durch strenge Richtlinien für identitätsbasierten Zugriff, Laufzeitsicherheit und API-Sicherheitskontrollen
- **Daten:** Sicherstellen, dass vertrauliche Regierungsdaten verschlüsselt, überwacht und vor unbefugtem Zugriff und Extraktion geschützt bleiben



Säulen des Zero Trust Maturity Model der CISA (Quelle: CISA)

Zusätzlich zu diesen Säulen integriert das Modell drei wichtige bereichsübergreifende Funktionen, die für alle Zero-Trust-Komponenten gelten:

- **Transparenz und Analyse:** Kontinuierliche Überwachung, Protokollierung und Erkennung von Anomalien, um Bedrohungen in Echtzeit zu finden und abzuwehren
- **Automatisierung und Orchestrierung:** KI-gestützte Sicherheitsautomatisierung zur Durchsetzung von Richtlinien, Reaktion auf Bedrohungen und Optimierung der Zugriffskontrolle
- **Governance:** Zentralisierte Durchsetzung von Richtlinien, um die Einhaltung von Bundesvorschriften wie dem Federal Information Security Modernization Act (FISMA) und der Special Publication 800-207 des National Institute of Standards and Technology (NIST) sicherzustellen

Bedeutung von Mikrosegmentierung und API-Sicherheit

In herkömmlichen Netzwerksicherheitsmodellen werden Netzwerke in der Regel mithilfe netzwerkbasierter Firewalls in große Segmente unterteilt. Dieser Ansatz bietet zwar ein gewisses Maß an Sicherheit, es fehlt ihm jedoch die Genauigkeit, die für den umfassenden Schutz moderner, verteilter Umgebungen erforderlich ist. In Behörden führt die netzwerkbasierte Segmentierung in der Regel zu einer Überprovisionierung, d. h. Nutzer und Anwendungen haben Zugriff auf mehr Ressourcen, als sie eigentlich benötigen. Dadurch entstehen unbeabsichtigte Möglichkeiten für laterale Netzwerkbewegungen. Wenn Angreifer in einen Teil des Netzwerks eindringen, können sie auch in sensiblere Bereiche gelangen, ohne auf nennenswerten Widerstand zu stoßen.

Das Konzept der Mikrosegmentierung trägt dieser Herausforderung durch engmaschige Kontrolle des East-West-Traffic im Netzwerk Rechnung. In einer mikrosegmentierten Umgebung ist jede Anwendung, jeder Workload oder Service von anderen isoliert, und der Zugriff wird auf Grundlage bestimmter Richtlinien eingeschränkt. Dadurch wird sichergestellt, dass Nutzer, Geräte und Anwendungen nur mit den Ressourcen kommunizieren können, für die sie explizit eine Zugriffsberechtigung besitzen. Durch Implementierung identitätsbasierter, anwendungsorientierter Segmentierung begrenzt die Mikrosegmentierung den potenziellen Schaden durch Cyberangriffe, reduziert die Angriffsfläche und setzt das Zero-Trust-Prinzip durch.

Für den North-South-Netzwerktraffic verlassen sich behördliche Netzwerke zunehmend auf APIs, um die Kommunikation zwischen Systemen zu erleichtern. Daher hat der Schutz von API-Endpunkten höchste Priorität. API-Angriffe – einschließlich Injection-Angriffen, Credential Stuffing und nicht autorisiertem Datenzugriff – haben in den letzten Jahren stark zugenommen. Bundesbehörden und -ämter benötigen umfassende API-Sicherheitslösungen, die vollständigen Schutz während des gesamten Lebenszyklus von APIs bieten und es dem Sicherheitspersonal ermöglichen, den API-Traffic in Echtzeit zu erkennen, zu überwachen und zu sichern. Besonders wichtig ist die API-Erkennung. Es ist nicht ungewöhnlich, dass APIs vorhanden sind, von denen niemand weiß.

Zero-Trust-Lösungen von Akamai auf einen Blick

Identität

Akamai MFA ist eine schlüssellose FIDO2-Identitätslösung, die Mitarbeiterkonten vor Phishing und anderen MITM-Angriffen (Machine in the Middle) schützt. Dadurch wird sichergestellt, dass nur Mitarbeiter auf ihre eigenen Konten zugreifen können, die durch eine starke, identitätsbasierte Nutzerauthentifizierung überprüft wurden. Alle anderen Zugriffsversuche werden verweigert und die Übernahme von Mitarbeiterkonten wird verhindert.

Geräte

Akamai Guardicore Segmentation ist eine branchenführende Mikrosegmentierungslösung, die die East-West-Verbreitung von Ransomware und anderer Malware eindämmt. Durch kontinuierliche Überwachung und Durchsetzung von Richtlinien auf Geräten kann Akamai Guardicore Segmentation Gerätekonfigurationen, Softwareinstallationen und potenzielle Schwachstellen überprüfen und so sicherstellen, dass nur richtlinienkonforme Geräte auf das Netzwerk zugreifen können. Darüber hinaus unterstützt die Lösung einen agentenlosen Ansatz zur Sicherung von IoT-Geräten.

Akamai Enterprise Application Access ist eine umfassende Zero-Trust-Network-Access-Lösung, die sicherstellt, dass nur authentifizierte Nutzer und Geräte auf Anwendungen zugreifen können. Durch Überprüfung der Identität und des Sicherheitsstatus von Geräten ergänzt Enterprise Application Access die Funktionen von Akamai Guardicore Segmentation. Wenn ein Gerät nicht konform ist oder ein Sicherheitsrisiko darstellt, kann Enterprise Application Access den Zugriff auf sensible Anwendungen einschränken.

Netzwerke

Akamai API Security bietet staatlichen Sicherheitsexperten durch kontinuierliche Erkennung und Echtzeitanalyse des North-South-Traffics einen umfassenden Einblick in die gesamte API-Umgebung. Die Lösung entdeckt unbekannte APIs, erkennt Schwachstellen und analysiert das API-Verhalten, damit Sicherheitsteams Angriffe erkennen und Risiken in dieser schnell wachsenden Angriffsfläche beheben können.

Akamai App & API Protector vereint Web Application Firewall, Bot-Abwehr, API-Sicherheit und Schutz vor Layer-7-DDoS-Angriffen (Distributed Denial-of-Service) in einer einzigen Lösung. Die Lösung erkennt schnell Schwachstellen und wehrt Bedrohungen im gesamten Netzwerk und allen API-Umgebungen ab.

Akamai Secure Internet Access Enterprise ist ein cloudbasierter sicherer DNS-Service (Domain Name System), der gewährleistet, dass Nutzer und Geräte unabhängig von ihrem Standort sichere Internetverbindungen herstellen können – ohne die Komplexität und den Verwaltungsaufwand, die mit anderen Sicherheitslösungen verbunden sind.

Akamai Guardicore Segmentation bietet präzise Kontrolle über den Netzwerktraffic und stellt sicher, dass im System nur legitimer Traffic zugelassen wird.

Zero-Trust-Lösungen von Akamai auf einen Blick

Anwendungen und Workloads

Akamai Enterprise Application Access bietet Zero-Trust-Zugriff für Mitarbeiter, Drittanbieter, Partner und mobile Nutzer – unabhängig von ihrem Standort.

Akamai Guardicore Segmentation bietet Transparenz und Einblicke in Anwendungen und Workloads.

Daten

Akamai Secure Internet Access Enterprise bietet sicheren Zugriff auf Daten. Dabei helfen Funktionen wie Inhaltsfilterung, erweiterter Schutz vor Bedrohungen und Schutz vor Datenverlust. Die Lösung unterstützt das Datenbestandsmanagement, indem sie unbefugten Zugriff und Datenlecks verhindert.

Akamai Guardicore Segmentation: Der Schlüssel zum Schutz des East-West-Datenflusses

Akamai Guardicore Segmentation ist eine branchenführende Mikrosegmentierungslösung, die Organisationen – insbesondere Bundesbehörden und -ämter – bei der Implementierung präziser Sicherheitskontrollen in On-Premises- und Cloud-Umgebungen unterstützt.

Präzise Segmentierung von Workloads und Anwendungen

Im Gegensatz zur herkömmlichen Segmentierung, bei der der Zugriff auf Netzwerkebene kontrolliert wird, wendet Akamai Guardicore Segmentation Sicherheitsrichtlinien auf Anwendungs- und Workload-Ebene an. Dadurch wird sichergestellt, dass der Zugang streng eingeschränkt ist. So lässt sich beispielsweise festlegen, dass eine Personalanwendung nur mit der dafür vorgesehenen Personaldatenbank kommunizieren darf. Das hindert Angreifer daran, sich lateral im Netzwerk zu bewegen, wenn ein Verstoß auftritt.

Identitätsbasierte Mikrosegmentierung

Akamai Guardicore Segmentation setzt Segmentierung auf Basis der Nutzer- und Geräteidentität statt nur auf Grundlage von IP-Adressen durch. Auf diese Weise wird sichergestellt, dass der Zugriff dynamisch gewährt wird, basierend auf Rolle, Vertrauensstufe und Echtzeitüberprüfung. Beispiel: Für Auftragnehmer und Drittanbieter kann der Zugriff auf die Systeme beschränkt werden, die sie benötigen, was das Risiko des unbefugten Zugriffs verringert.

Dynamische Durchsetzung von Richtlinien

Akamai Guardicore Segmentation passt Sicherheitsrichtlinien kontinuierlich auf Grundlage von Echtzeitfaktoren an. Dazu gehören Nutzerverhalten, Gerätezustand und Netzwerkaktivität. Wenn verdächtige Aktivitäten erkannt werden, z. B. eine ungewöhnliche Menge an Datenübertragungen, kann Akamai Guardicore Segmentation den Zugriff automatisch einschränken, den Traffic blockieren oder Sicherheitsteams benachrichtigen. Mit diesem proaktiven Ansatz wird gewährleistet, dass Sicherheitsrichtlinien immer weiterentwickelt werden und auch neue Bedrohungen abgewehrt werden können.

Durch Integration der Mikrosegmentierung von Akamai Guardicore Segmentation gelingt es Unternehmen, ihre Zero-Trust-Architektur zu stärken, Risiken zu minimieren und strenge Zugriffskontrollen in ihren Netzwerken aufrechtzuerhalten.

FALLSTUDIE

Akamai Guardicore Segmentation in Behörden

Eine Bundesbehörde implementierte kürzlich die Mikrosegmentierungslösung von Akamai, um ihre internen Systeme vor Angriffen durch laterale Netzwerkbewegungen zu schützen. Vor der Einführung von Akamai Guardicore Segmentation verließ sich die Behörde auf die herkömmliche netzwerkbasierte Segmentierung, deren Genauigkeit begrenzt war und die umfassenden Zugriff auf verschiedene Netzwerksegmente ermöglichte. Daraus ergab sich ein erhebliches Risiko lateraler Netzwerkbewegungen für den Fall, dass ein Teil des Netzwerks kompromittiert wurde.

Mit Akamai Guardicore Segmentation profitierte die Behörde von folgenden Vorteilen:

- Implementierung einer präzisen Segmentierung: Durch die Segmentierung von Workloads auf Anwendungsebene verringerte die Behörde das Risiko von lateralen Netzwerkbewegungen und stellte sicher, dass jede Anwendung nur mit den von ihr benötigten Ressourcen kommunizieren konnte.
- Mehr Transparenz: Dank der Visualisierungstools der Lösung gewann die Behörde einen umfassenden Einblick in den internen Traffic. Sicherheitsteams konnten so potenzielle Bedrohungen in Echtzeit erkennen und abwehren.
- Verbesserte Sicherheit: Durch die Integration von Akamai Guardicore Segmentation in die bestehenden Identitätsmanagement- und Zugriffskontrollsysteme konnte die Behörde Zero-Trust-Prinzipien im gesamten Netzwerk durchsetzen und sicherstellen, dass der Zugriff kontinuierlich überwacht und auf der Grundlage von Risikobewertungen in Echtzeit dynamisch angepasst wurde.

Dieses Beispiel zeigt, wie gut Akamai Guardicore Segmentation die Netzwerksicherheit verbessert, das Risiko von lateralen Netzwerkbewegungen reduziert und Berechtigungen jederzeit auf das erforderliche Minimum beschränkt.

API-Sicherheit: Schutz des North-South-Traffics

Akamai bietet verschiedene Lösungen zur Gewährleistung der API-Sicherheit. Die API-Sicherheitsplattform von Akamai gewährleistet einen umfassenden Einblick in API-Interaktionen, erkennt automatisch Bedrohungen im North-South-Traffic in Echtzeit und wehrt sie ab. Mit leistungsfähigen Verhaltensanalysen können Bundesbehörden und -ämter:

- **Shadow-APIs erkennen**, die von Angreifern ausgenutzt werden könnten
- **API-Trafficmuster überwachen**, um Versuche unbefugten Zugriffs zu erkennen
- **API-Ratenbegrenzung implementieren**, um Missbrauch und Denial-of-Service-Angriffe zu verhindern
- **Vergessene, vernachlässigte oder unbekannte APIs identifizieren**, um potenzielle Angriffspfade aufzudecken
- **Alle APIs inventarisieren**, unabhängig von Konfiguration oder Typ, einschließlich RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC und gRPC

Akamai Secure Internet Access Enterprise ist eine cloudbasierte DNS-Firewall, mit der Sicherheitsteams gewährleisten, dass alle Nutzer und Geräte – innerhalb und außerhalb des Netzwerks – sicher mit dem Internet verbunden werden können. Es blockiert proaktiv bösartige DNS-Anfragen, einschließlich Malware, Ransomware, Phishing und DNS-Datenextraktion mit niedrigem Durchsatz. Secure Internet Access Enterprise reduziert die Komplexität der Sicherheit, da keine Appliances bereitgestellt, verwaltet und aktualisiert werden müssen. Die Lösung ist einfach und intuitiv zu bedienen.

Akamai App & API Protector erkennt und wehrt API-Bedrohungen für Anwendungen und APIs ab, die über die Akamai Cloud ausgeführt werden, und kann Traffic, der von Akamai API Security erkannte potenzielle Bedrohungen enthält, grundsätzlich blockieren. Bei gemeinsamer Bereitstellung bieten die API-Schutzfunktionen von Akamai umfassend und kontinuierlich Einblick in APIs und ermöglichen es dem Sicherheitspersonal, API-Sicherheitsprobleme in der gesamten Anwendungsumgebung zu entdecken, zu prüfen, zu erkennen und zu beheben.

Bereichsübergreifende Funktionen mit Zero Trust

Eine der größten Herausforderungen einer Zero-Trust-Architektur ist das Risiko, Technologiesilos zu schaffen. Silos arbeiten oft unabhängig voneinander, was zur Fragmentierung von Sicherheitskontrollen, Richtliniendurchsetzung und Bedrohungserkennung führt. Daher ist die Integration über alle Sicherheitsebenen hinweg von größter Bedeutung.

Für Bundesbehörden und -ämter, die hochsensible Daten und komplexe Infrastrukturen verwalten, kann dieser fragmentierte Ansatz erhebliche Sicherheitsrisiken mit sich bringen. Angreifer können die mangelnde Transparenz zwischen Silos (oder Säulen) oder die uneinheitliche Durchsetzung von Richtlinien über verschiedene Systeme hinweg ausnutzen. Um diese Risiken zu mindern, müssen Bundesbehörden ein einheitliches, säulenübergreifendes Sicherheitsmodell einführen, das Transparenz, Governance und Automatisierung über alle Säulen hinweg integriert, eine konsistente Durchsetzung von Richtlinien gewährleistet und Lücken schließt, die von Angreifern ausgenutzt werden können.

Zur Schaffung eines einheitlichen Sicherheitsmodells muss der Schwerpunkt bei der säulenübergreifenden Integration auf den drei bereichsübergreifenden Bereichen des Zero Trust Maturity Model der CISA liegen: Transparenz und Analyse, Automatisierung und Orchestrierung und Governance. Diese Elemente sind unerlässlich für eine Zero-Trust-Architektur, in der Zugriff und Berechtigungen dynamisch über alle Säulen hinweg auf der Grundlage von Risikobewertungen in Echtzeit angepasst werden.

Transparenz und Analyse

Transparenz ist entscheidend für die Erkennung von Bedrohungen, das Verständnis des Nutzerverhaltens und die Durchsetzung dynamischer Sicherheitsrichtlinien über alle Säulen hinweg. Ohne umfassende Einblicke in die Interaktion von Identitäten, Geräten, Anwendungen und Daten tappen Sicherheitsteams im Dunkeln und können anomales Verhalten oder unbefugte Zugriffsversuche nur schwer erkennen. Lösungen von Akamai gewährleisten umfassende säulenübergreifende Transparenz.

- Akamai Guardicore Segmentation überwacht den Netzwerktraffic zwischen segmentierten Workloads, bietet einen Überblick über den East-West-Traffic und erkennt alle Versuche lateraler Bewegungen innerhalb des Netzwerks.
- Enterprise Application Access bietet Einblicke in Muster des Zugriffs auf Anwendungen, verfolgt die Interaktion von Nutzern mit sensiblen Anwendungen und stellt sicher, dass der Zugriff auf Basis von Kontextdaten dynamisch angepasst wird.

Durch Integration dieser Funktionen können Bundesbehörden Daten über alle Säulen hinweg korrelieren und so eine einheitliche Ansicht von Sicherheitsereignissen gewinnen. Wenn ein Nutzer Zugriff auf eine Anwendung anfordert, können die Lösungen von Akamai nicht nur die Identität des Nutzers, sondern auch die Sicherheit des Geräts, das verwendete Netzwerk und das Echtzeitverhalten der Anwendung überprüfen. Sicherheitsteams können so potenzielle Bedrohungen schneller erkennen, das Risiko der Berechtigungseskalation minimieren und sicherstellen, dass Berechtigungen basierend auf Risikobewertungen in Echtzeit dynamisch angepasst werden.

Automatisierung und Orchestrierung

Das Reagieren auf Vorfälle und die Durchsetzung von Richtlinien in mehreren Systemen können ein langsamer, manueller Prozess sein. Bei Zero Trust müssen Sicherheitsrichtlinien dynamisch über alle Säulen hinweg durchgesetzt werden, was ein hohes Maß an Automatisierung und Orchestrierung erfordert. Dadurch wird gewährleistet, dass Berechtigungen bei Änderung von Risikostufen sofort an das erforderliche Minimum angepasst werden. So lässt sich die Wahrscheinlichkeit menschlicher Fehler oder verzögerter Reaktionen verringern. Die automatisierten Workflows der Lösungen von Akamai umfassen Identitäts-, Netzwerk- und Anwendungssicherheit.

- Akamai Guardicore Segmentation bietet automatisierte Mikrosegmentierung. Die Richtlinien zur Netzwerksegmentierung werden dynamisch angepasst, basierend auf Echtzeit-Trafficmustern und erkannten Anomalien. So wird sichergestellt, dass verdächtige Aktivitäten im Netzwerk schnell isoliert und laterale Netzwerkbewegungen verhindert werden.
- Enterprise Application Access automatisiert den Prozess der Sicherung des Anwendungszugriffs und gewährleistet, dass Nutzer nur über einen sicheren Proxy auf Anwendungen zugreifen können. Darüber hinaus werden Berechtigungen kontinuierlich auf der Grundlage sich ändernder Risikofaktoren aktualisiert.

Durch Automatisierung dieser Prozesse können Bundesbehörden und -ämter sicherstellen, dass Sicherheitsrichtlinien konsistent und schnell durchgesetzt werden. Damit bleibt Angreifern weniger Zeit, und das Risiko von Sicherheitsverstößen wird reduziert.

Governance

Governance als Grundlage jeder Sicherheitsstrategie gewährleistet, dass Richtlinien konsequent durchgesetzt und Compliance-Anforderungen erfüllt werden. In einem säulenübergreifenden Modell muss Governance sicherstellen, dass alle Sicherheitskontrollen mit den Prinzipien von Zero Trust im Einklang stehen. Mit den Lösungen von Akamai können Behörden Governance-Richtlinien implementieren, die alle Säulen umfassen.

- Identity Governance: Sicherstellen, dass identitätsbasierte Zugriffskontrollen einheitlich für alle Geräte, Anwendungen und Netzwerke durchgesetzt werden und dass Zugriffsberechtigungen regelmäßig überprüft und aktualisiert werden, basierend auf Risikobewertungen in Echtzeit
- Netzwerk-Governance: Dank der Durchsetzung von Richtlinien für die Netzwerksegmentierung und die Überwachung des Traffics in verschiedenen Umgebungen, einschließlich On-Premise-, Cloud- und Hybrid-Infrastrukturen, können Behörden mit Akamai Guardicore Segmentation Richtlinien für die Netzwerksegmentierung definieren und sicherstellen, dass diese Richtlinien in der gesamten Infrastruktur einheitlich angewendet werden.
- Data Governance: Schutz vertraulicher Daten durch Einschränkung des Zugriffs nach dem Prinzip der geringstmöglichen Berechtigungen sowie kontinuierliche Überwachung aller Datenübertragungen auf unbefugten Zugriff oder verdächtige Aktivitäten

Die Technologien von Akamai arbeiten nahtlos zusammen und bieten Bundesbehörden eine vollständig integrierte, säulenübergreifende Sicherheitsarchitektur, die Zero Trust unterstützt.

FALLSTUDIE

Säulenübergreifende Integration in einer Bundesbehörde

Fragmentierte Sicherheitsrichtlinien auf Identitäts-, Netzwerk- und Anwendungsebene stellten eine große Bundesbehörde vor erhebliche Herausforderungen.
Für die Verwaltung von Identitätsüberprüfung, Anwendungszugriff und Netzwerksegmentierung kamen verschiedene Systeme zum Einsatz. Das führte zu einer inkonsistenten Durchsetzung von Sicherheitsrichtlinien und zu Lücken in der Transparenz.

Durch Einführung der integrierten Lösungen von Akamai konnte die Behörde:

- **Identitäts- und Anwendungssicherheit vereinheitlichen:** Die ICAM-Lösung (Identity, Credential, and Access Management) von Akamai, Enterprise Application Access, wurde integriert, um sicherzustellen, dass der Anwendungszugriff stets auf Basis von Identitätsdaten in Echtzeit authentifiziert wird. So war es der Behörde möglich, Anwendungsberechtigungen basierend auf dem Nutzerverhalten und dem Gerätezustand dynamisch anzupassen.
- **Dynamische Netzwerksegmentierung durchsetzen:** Akamai Guardicore Segmentation wurde implementiert, um den Netzwerktraffic auf Basis von Identität und Anwendungszugriff zu segmentieren. Laterale Netzwerkbewegungen zwischen sensiblen Systemen wurden damit unterbunden. Außerdem wurde so sichergestellt, dass Berechtigungen auf der Grundlage von Risikobewertungen in Echtzeit kontinuierlich aktualisiert werden.
- **Transparenz und Automatisierung verbessern:** Die Behörde nutzte die integrierten Analyse- und Automatisierungstools von Akamai, um einen umfassenden Einblick in den Sicherheitsstatus zu erhalten und die Durchsetzung von Richtlinien über alle Säulen hinweg zu automatisieren.

Infolgedessen gelang es ihr, die Angriffsfläche zu reduzieren, die Reaktionszeit bei Vorfällen zu verbessern und die umfassende Einhaltung der staatlichen Sicherheitsvorschriften zu gewährleisten. Dieser Fall zeigt, wie eine fragmentierte Sicherheitsarchitektur dank säulenübergreifender Integration in ein einheitliches, dynamisches Sicherheitsmodell umgewandelt werden kann, das Zero Trust unterstützt.

Fazit

Zero-Trust-Sicherheit ist nicht mehr nur eine Option. Sie ist notwendig, um Bundesbehörden vor komplexen Cyberbedrohungen zu schützen. Durch Implementierung von Mikrosegmentierung, API-Sicherheit und starken Identitätskontrollen gelingt es Bundesbehörden und -ämtern, Risiken drastisch zu reduzieren und gleichzeitig die Einhaltung der staatlichen Vorschriften zur Cybersicherheit zu gewährleisten.

Akamai bietet eine umfassende Palette von Zero-Trust-Lösungen, darunter Akamai Guardicore Segmentation, Akamai API Security und Akamai Secure Internet Access Enterprise. Diese Lösungen ermöglichen Behörden die Etablierung einer proaktiven, anpassungsfähigen Sicherheitsstrategie. Durch Nutzung des Know-hows von Akamai können Bundesbehörden die Implementierung von Zero Trust in kürzerer Zeit erreichen und langfristige Sicherheit gewährleisten.

Jetzt ist es für Bundesbehörden an der Zeit zu handeln. Durch Integration der Sicherheitslösungen von Akamai erlangen Behörden Zero-Trust-Reife, mindern Cyberrisiken und schützen die wichtigsten digitalen Ressourcen des Landes.

Kontaktieren Sie Akamai noch heute, um mehr über unsere umfassenden Sicherheitslösungen zu erfahren.