CLOUDFLARE

WHITEPAPER

Sicherheitsanforderungen im Bankensektor: Schutz vor Cyberangriffen und Einhaltung regulatorischer Vorgaben

Sicherheitsanforderungen im Bankensektor: Schutz vor Cyberangriffen und Einhaltung regulatorischer Vorgaben

Banken müssen digitalisieren, um die Innovationen bieten zu können, die der Markt inzwischen fordert. Nur so gelingt es ihnen, wettbewerbsfähig zu bleiben und ihre Betriebskosten zu senken. Doch durch die Digitalisierung können sich Banken Cyberrisiken aussetzen, die Antworten erfordern. Neben externen Cyberattacken wie DDoS, Phishing und Hacking müssen sie sich auch vor Social Engineering bei den Beschäftigten und Datenabfluss von internen Systemen schützen. Hinzu kommen strenge Regularien im EU-Raum wie der Digital Operational Resilience Act DORA und die Vorgaben der BaFin in Deutschland. Cloudflare kann Banken dabei helfen, die regulatorischen Anforderungen zu erfüllen und größeren Cyberschutz aufzubauen.

Die digitale Transformation ist für Banken keine Option mehr, sondern eine geschäftliche Notwendigkeit. Ohne Digitalisierung können sie die Kundenerwartungen nicht mehr erfüllen, weil es ihnen an technologischen Innovationen mangelt.
2024 wurde der Hebel im Banking endgültig umgelegt und von offline auf online geschaltet, erklärt der Digitalverband Bitkom. Erstmals bilden diejenigen, die ausschließlich Online-Banking nutzen und nie eine Filiale aufsuchen, mit 42 Prozent die größte Gruppe innerhalb der Bankkunden (2023: 38 Prozent) in Deutschland, so eine Bitkom-Umfrage[1]. Knapp dahinter folgen mit 40 Prozent (2023: 43 Prozent) diejenigen, die überwiegend Online-Banking verwenden, aber nur ab und zu eine Filiale aufsuchen und persönlichen Kontakt mit Angestellten haben. Es gibt einen klaren Trend hin zum ausschließlichen Online-Banking. Digitale Angebote gewinnen für Banken immer weiter an Bedeutung.

Bei der Entscheidung für eine Bank spielen für Kunden digitale Angebote eine wichtigere Rolle als etwa die Marke oder das Filialnetz. So finden 75 Prozent der Bankkunden in Deutschland eine benutzerfreundliche App wichtig, 67 Prozent achten auf eine breite Angebotspalette beim Online-Banking und 60 Prozent darauf, ob Mobile-Payment-Anwendungen nutzbar sind. Die hohe Bedeutung digitaler Dienste für Bankkunden bestätigt auch eine Umfrage des Bankenverbandes[2]. Demnach wird Online- bzw. Mobile-Banking in Deutschland immer beliebter und hat sich als bevorzugter Zugangsweg zur Bank durchgesetzt. Die Digitalisierung bringt aber auch Cyberrisiken mit sich, gegen die sich Finanzinstitute wappnen müssen, warnen Beratungshäuser wie McKinsey[3].

Mit der Digitalisierung verbundene Cyberrisiken

Cyberattacken oder IT-Pannen bedrohen aus Sicht der Finanzaufsicht BaFin den Finanzsektor erheblich. Dabei müssen diese Störungen nicht einmal bei den Banken selbst auftreten. Auch Sicherheitslücken bei von ihnen beauftragten Dienstleistern können das ganze System beeinträchtigen, so der BaFin-Bericht „Risiken im Fokus der BaFin 2024“[4]. So warnt der Bankenverband vor Cyberattacken auf Bankkunden[5] (etwa Phishing-Mails[6]), die die Kunden auf gefälschte Online-Banking-Seiten locken sollen, um dort die Zugangsdaten abzugreifen.

Aber auch die Beschäftigten einer Bank stehen im Fokus der Kriminellen. Die Bankangestellten sollen ebenfalls mit Social-Engineering-Methoden getäuscht werden, damit sie ungewollt Zugangsdaten und andere vertrauliche Informationen preisgeben, die weitere Cyberangriffe erleichtern.

DDoS-Attacken legen Online-Banking-Seiten lahm

Zu den häufigsten Cyberattacken auf Banken gehören insbesondere DDoS-Attacken (Distributed-Denial-of-Service-Angriffe), wie eine Auswertung von IT-Vorfällen durch die BaFin[7] zeigt. Die Angreifer versuchen, die Webserver zu überlasten, die Online-Banking-Angebote betreiben. Cloudflare beobachtete[8] im ersten Quartal 2024 41 Milliarden HTTP-DDoS-Angriffsversuche, die auf die Banken-, Finanzdienstleistungs- und Versicherungsbranche abzielten. Ein Wachstum von 57 Prozent im Vergleich zum ersten Quartal im Jahr 2023.

Hat die DDoS-Attacke Erfolg, funktioniert das Online-Banking für die Kunden eine gewisse Zeit nicht mehr, wodurch die Sicherstellung der Stabilität und Kontinuität der Finanzdienstleistungen beeinträchtigt ist. Folglich können erfolgreiche DDoS-Angriffe auf Banken großen Schaden anrichten. So erklärt das BSI (Bundesamt für Sicherheit in der Informationstechnik) in dem aktuellen Bericht zur Lage der IT-Sicherheit[9], dass zum einen finanzielle Schäden für Dienstleister oder Online-Shops entstehen, wenn diese nicht erreichbar sind. Zum anderen können gerade bei Banken Imageschäden und gegebenenfalls Unsicherheit in der Bevölkerung folgen.

Interne Fehler können zu Datenabfluss und -verlust führen

Zusätzlich können fehlerhafte Konfigurationen und unzureichende Nutzerschulungen dazu führen, dass Beschäftigte einer Bank durch Fehler bei der Übertragung oder Sicherung von Daten zu Datenpannen und IT-Sicherheitsvorfällen beitragen. Fehlerhafte Datensicherung und Datenübertragungen werden häufig durch die noch unzureichenden Sicherheitsvorkehrungen zu spät oder gar nicht erkannt und nicht verhindert. Es kann zum ungewollten Datenabfluss an Dritte und zum Verlust kritischer Daten kommen.

Mobiles Arbeiten und die unkontrollierte Cloud- und KI-Nutzung verschärfen die Risikolage

Das verstärkte dezentrale und mobile Arbeiten hat auch in der Finanzbranche Einzug gehalten. Dabei kommen teilweise auch private Endgeräte (BYOD) der Beschäftigten zum Einsatz, deren Sicherheitsstatus unklar ist. Für die Verbindung zwischen dem Homeoffice und den zentralen Banksystemen setzen viele Banken auf das klassische VPN (Virtual Private Network).

VPNs aber gewähren Nutzern und ihren womöglich unsicheren Geräten nach der erfolgreichen Anmeldung umfassenden Zugang zu Anwendungen und Daten, ohne vorherrschende Risiken und den aktuell tatsächlich vorhandenen Bedarf an Berechtigungen zu berücksichtigen[10]. Können Cyberkriminelle VPN-Zugänge übernehmen, erhalten sie Zugang zu internen Banksystemen. Nicht zuletzt könnten auch Innentäter unter den Beschäftigten die umfassenden Zugangsmöglichkeiten über VPN zu bösartigen Zwecken ausnutzen.

Außerdem setzen Beschäftigte der Finanzinstitute zunehmend auf Cloud-Dienste (zum Beispiel für Filesharing) und Lösungen auf Basis von Machine Learning (ML) und künstlicher Intelligenz (KI), darunter zum Beispiel Chatbots. Dabei ist es wichtig, dass die Beschäftigten nur freigegebene Dienste und Lösungen nutzen, sonst droht hier eine riskante Schatten-IT, deren Sicherheitsstatus der IT-Abteilung nicht bekannt ist.

Diesen Schutz benötigen Online-Banking-Seiten und Banking-Applikationen

Die Cyberbedrohungslage für Finanzinstitute und ihre Kunden ist vielfältig. Um zu vermeiden, eine komplexe Sicherheitsstrategie mit zahlreichen separaten Security-Werkzeugen implementieren und betreiben zu müssen empfiehlt sich ein cloudbasierter Plattformansatz[11] mit den erforderlichen Sicherheitsfunktionen:

- **Schutz vor gefälschten Banking-Seiten** (Fake- und Phishing-Sites) durch eine Lösung, die DNSSEC bereitstellt, um zu verhindern, dass Kriminelle die Kunden von der Bank-Website umleiten, indem sie die DNS-Infrastruktur kompromittieren.

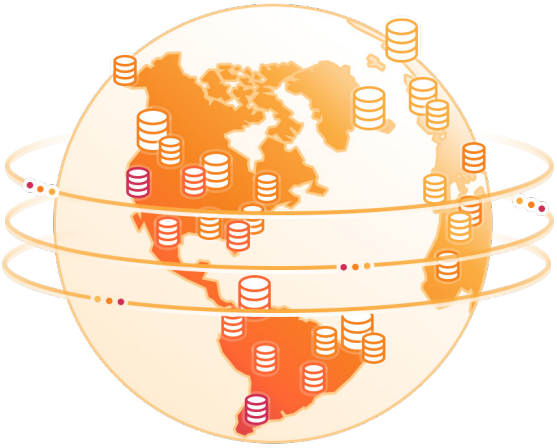
- **Schutz vor bösartigem Datenverkehr** über einen Web-Application-Firewall-Dienst (WAF), um verdächtigen Datenverkehr auf Anwendungsebene zu identifizieren und blockieren.

- **Schutz vor Credential-Stuffing-Angriffen,** bei denen vermehrt automatisiert arbeitende Bots zum Einsatz kommen, indem Bot-Aktivitätsmuster erkannt und Bots, die auf die Banking-Anwendungen zugreifen wollen, blockiert werden.
- **Schutz vor DDoS-Attacken,** die zu Ausfällen im Online-Banking führen können und sich negativ auf die Kundenzufriedenheit und den geschäftlichen Erfolg auswirken[12].
- **Schutz vor unsicheren Remote-Verbindungen** von Beschäftigten im Homeoffice auf zentrale Banking-Systeme.
- **Schutz vor den Risiken durch die Nutzung von privaten Geräten** durch Beschäftigte.
- **Schutz vor den Risiken durch die Nutzung von unkontrollierten Cloud- und KI-Diensten.**

Banken müssen sich öffnen und gleichzeitig abschirmen

Nicht nur die Kommunikationsverbindungen mit Kunden und Beschäftigten einer Bank benötigen Schutz, sondern auch die Schnittstellen (APIs) zu anderen Anbietern und Apps.

Open Banking[13] lautet die Forderung an die Finanzbranche. Diese steht für ein „offenes Bankwesen“, also den Zugang zu personenbezogenen Daten und auch Produktdaten über Unternehmensgrenzen hinweg, und zwar mit Zustimmung des Kunden. So müssen Banken zum Beispiel eine offen dokumentierte Schnittstelle im Internet bereitstellen, die es Zahlungsdrittdienstleistern erlaubt, im Kundenauftrag auf Kundenkonten zuzugreifen (Kontoschnittstelle für Zahlungsdrittdienstleister). Auch diese Verbindungen und Schnittstellen benötigen einen erhöhten Schutz gegen Attacken.



Der Bericht zum Stand der Anwendungssicherheit im Jahr 2024 von Cloudflare[14] zeigt insbesondere:

Die Zahl und der Umfang von DDoS-Angriffen nehmen weiter zu: DDoS-Attacken sind nach wie vor der am häufigsten gegen Webanwendungen und APIs eingesetzte Angriffsvektor. Sie verantworten 37,1 Prozent des gesamten Anwendungstraffics.

Der Wettlauf zwischen Verteidigern und Angreifern beschleunigt sich: Cloudflare sieht, dass neue Zero-Day-Schwachstellen schneller ausgenutzt wurden als je zuvor. In einem Fall lagen zwischen der Proof-of-Concept-Veröffentlichung und dem Missbrauch gerade mal 22 Minuten.

Nicht neutralisierte Schadbots können schwere Störungen verursachen: Bots sind für fast ein Drittel (31,2 Prozent) des gesamten Traffics verantwortlich. Die Mehrheit (93 Prozent) wurde nicht überprüft und gilt als potenziell bösartig.

Die von Firmen zum API-Schutz eingesetzten Strategien sind veraltet: Herkömmliche Web-Application-Firewall-Regeln wenden ein negatives Sicherheitsmodell an, das davon ausgeht, dass der überwiegende Teil des Datenverkehrs im Web gutartig ist. Sie kommen am häufigsten zum Schutz vor API-Traffic zum Einsatz. Deutlich seltener finden dagegen die bewährteren und anerkannteren Verfahren mit positivem Sicherheitsmodell Verwendung.

Banken müssen neue regulatorische Anforderungen umsetzen

Banken unterliegen einer besonders komplexen und strengen Regulierung, wie der Bankenverband[15] erklärt. Die digitale Transformation erfordert weitere Regulierungen und erweitert so die notwendigen Schritte für die Compliance im Finanzsektor.

Mit DORA[16] wurde eine spezifische EU-Verordnung für den Finanzsektor geschaffen, die darauf abzielt, die digitale operative Resilienz zu fördern.

Die Verordnung ist am 16. Januar 2023 in Kraft getreten und findet nun nach einer zweijährigen Übergangszeit seit dem 17. Januar 2025 Anwendung. DORA gilt für verschiedene Arten von Finanzunternehmen sowie für externe Informations- und Kommunikationstechnologie-Dienstleister (IKT) im Finanzsektor. Ziel ist es, die IT-Sicherheit von Finanzinstituten wie Banken, Versicherungsunternehmen und Wertpapierfirmen zu stärken und dafür zu sorgen, dass der Finanzsektor in Europa im Falle einer schweren Betriebsstörung widerstandsfähig bleibt.

BaFin stellt Leitfaden für DORA-Umsetzung zur Verfügung

Die BaFin hat einen Leitfaden zur Umsetzung der DORA-Anforderungen[17] veröffentlicht. Dieses aufsichtsrechtliche Merkblatt unterstützt bei der Umsetzung der darin enthaltenen Anforderungen an das IKT-Risikomanagement sowie das IKT-Drittparteien-Risikomanagement.

Darüber hinaus enthält die Mitteilung konkrete Hilfestellungen für beaufsichtigte Unternehmen, wobei auch Datensicherheit und Datenschutz sowie Hinweise zum Ort der Leistungserbringung im Fokus stehen. So sind Regelungen zu vereinbaren, die sicherstellen, dass sowohl die datenschutzrechtlichen Bestimmungen als auch die aufsichtsrechtlichen Anforderungen an die Informationssicherheit eingehalten werden.

Sicherheit bei der Auslagerung in die Cloud gewährleisten

Finanzunternehmen nutzen zunehmend Cloud-Dienste, wobei die Compliance-Anforderungen weiterhin gewährleistet sein müssen. Wie jede Auslagerung von Dienstleistungen muss auch die Nutzung von Cloud-Diensten der BaFin angezeigt werden[18].

Die BaFin beobachtet die zunehmenden Auslagerungen und Verflechtungen im Finanzsektor sehr genau, da von Ausfällen zentraler IT-Dienstleister erhebliche Risiken für den gesamten Finanzmarkt ausgehen können. Durch die Meldepflicht kann die BaFin eine Datenbank führen und so Konzentrationsrisiken und Abhängigkeiten von einzelnen Dienstleistern erkennen. Im Fall von Sicherheits- oder Cybervorfällen bei Dienstleistern gelingt es so, potenziell betroffene Unternehmen schnell zu identifizieren und zu warnen.

Zu den wesentlichen DORA-Anforderungen gehören:

- **IKT-Risikomanagement**
  (Kapitel II, Artikel 5 bis 16)
- **Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle**
  (Kapitel III, Artikel 17 bis 23)
- **Testen der digitalen operationalen Resilienz einschließlich Threat-led Penetration Testing (TLPT)**
  (Kapitel IV, Artikel 24 bis 27)
- **Management des IKT-Drittparteienrisikos**
  (Kapitel V, Abschnitt I, Artikel 28 bis 30)
- **Überwachungsrahmen für kritische IKT-Drittdienstleister**
  (Kapitel V, Abschnitt II, Artikel 31 bis 44) und Notfallübungen
  (Kapitel VI, Artikel 44 und Artikel Kapitel VII, Artikel 49)

Prüfungen der Betriebsstabilität im Finanzsektor stehen bevor

Der Bericht der europäischen Zentralbank (EZB)[19] macht deutlich: Die Aufsicht wird die Digitalisierungsstrategien der Banken und deren Widerstandsfähigkeit gegenüber Cyberangriffen auch künftig überprüfen. Diese Bemühungen sollen dazu beitragen, dass die Banken stark bleiben und den Weg in eine digitale Zukunft einschlagen.

Die EZB-Bankenaufsicht erklärt entsprechend in den Aufsichtsprioritäten[20] für die Jahre 2024 bis 2026:

- „Die digitale Transformation ist für viele Banken im Ringen um Wettbewerbsfähigkeit zu einem Schwerpunkt geworden. Diese Banken brauchen daher angemessene Sicherheitsvorkehrungen, um die Risiken zu begrenzen, die mit neuen Geschäftspraktiken und -technologien möglicherweise einhergehen. Prüfungen der Bankenaufsicht haben offenbart, dass einige Banken bei der digitalen Transformation bereits gute Fortschritte erzielt haben. Andere haben nicht die erforderlichen Ressourcen eingesetzt, um ihre Ziele zu erreichen."

- „Zunehmende Cyberbedrohungen, die durch die aktuellen geopolitischen Spannungen verstärkt werden, und die zunehmende Abhängigkeit von externen Dienstleistern verdeutlichen außerdem, dass Banken auch bei schwerwiegenden operativen Störungen widerstandsfähig bleiben und die Kontinuität ihrer kritischen Dienstleistungen gewährleisten müssen."

- „Vor diesem Hintergrund und neben den aufsichtlichen Aktivitäten, die im Rahmen dieser Prioritäten eingeleitet werden, werden die Banken in den kommenden Monaten aufgefordert nachzuweisen, dass sie für solche negativen Ereignisse gewappnet sind und sich davon erholen können."

Es besteht Handlungsbedarf bei der Cybersicherheit vieler Finanzinstitute

Eine Umfrage von Cloudflare[21] ergab, dass die Befragten aus dem Finanzdienstleistungssektor in Europa und dem Nahen Osten die eingeschränkte Kontrolle über die IT-Lieferkette (39 %), die Anfälligkeit von in der Public Cloud angesiedelten Anwendungen und Daten (38 %) sowie die übermäßige Abhängigkeit von VPN beim Anwendungsschutz (36 %) als die drei Hauptschwachstellen ihrer Cybersicherheitsarchitektur ansehen.

Um von der digitalen Transformation im Finanzsektor zu profitieren, die Kundenerwartungen zu erfüllen, Innovationen umzusetzen und Compliance-Vorgaben zu gewährleisten, empfiehlt sich ein umfassender Plattformansatz für die Cybersicherheit, wie Cloudflare ihn anbietet.

Anforderungen an Cybersicherheit und Compliance im Banking umsetzen

Zero Trust, DDoS-Mitigation und API-Schutz

Mit fortgeschrittenen Sicherheitsfunktionen auf einer einzigen zentralen Plattform bietet Cloudflare[22] Finanzunternehmen ein sicheres globales Cloud-Netzwerk. Dieses hilft ihnen dabei, ihre digitale Transformation zu beschleunigen, ihre Betriebsleistung zu steigern und gleichzeitig die Anforderungen aus den Regulierungen zu erfüllen:

- **Zero-Trust-Sicherheitsarchitektur:** Diese stellt Cloudflare bereit, weshalb bei den Betriebsabläufen kein implizites Vertrauen erforderlich ist. Jeder Zugriff wird risikobasiert überprüft.
- **API-Sicherheit:** Da Banken für ihre digitalen Dienste eine Anwendungs-Programmierschnittstelle benötigen, bieten die API-Sicherheitstools von Cloudflare automatischen Schutz.
- **Sichere und gesetzeskonforme Datenverwaltung:** Cloudflare hilft Firmen bei der Einhaltung strenger gesetzlicher Vorgaben und bei der Bereitstellung einer transparenten Berichterstattung.
- **Datenschutz und Compliance:** Cloudflares Lösungen stehen im Einklang mit einschlägigen Gesetzen und Vorschriften.
- **Sichere und flexible Lösungen für mobiles Arbeiten:** Die Zero-Trust- und Secure-Gateway-Lösungen von Cloudflare gewährleisten einen sicheren Zugriff von jedem Standort aus.

Lösungen von Cloudflare zur Umsetzung von DORA-Anforderungen

Bewältigung von Sicherheitsvorfällen
Cloudflare bietet proaktive Überwachung und Alarmierung bei Sicherheitsvorfällen sowie Berichte über Sicherheitsereignisse mit datengesteuerten Empfehlungen zu Regeln und Schwellenwerten.

Aufrechterhaltung des Betriebs
Cloudflares umfangreiche Funktionen zum Schutz vor DDoS-Angriffen helfen Organisationen, eine der häufigsten Ursachen für Ausfallzeiten zu vermeiden.

Sicherheit der Lieferkette
Die Cloudflare-Lösung hilft dabei, die Sicherheit von Lieferketten zu erhöhen, indem sie potenzielle Schwachstellen in Anwendungen von Drittanbietern identifiziert, Websites vor Bedrohungen durch Inhalte von Drittanbietern schützt und den Zugriff auf Ressourcen und die Verfügbarkeit von Daten kontrolliert.

Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netzwerken und Informationssystemen
Cloudflare bietet mehrere Möglichkeiten, um Netzwerke und Informationssysteme während ihres gesamten Lebenszyklus zu schützen. So können Organisationen beispielsweise den Internet-Traffic untersuchen, um Phishing, Ransomware und andere Internetrisiken zu verhindern. Sie können Zero-Trust-Richtlinien zur strengen Kontrolle des Zugangs zu Firmennetzwerken und Informationssystemen implementieren. Und sie können die Konnektivität und das Routing sichern und gleichzeitig die Richtlinien der Netzwerk-Firewall durchsetzen.

Bewertung des Risikomanagements
Mit Cloudflare gelingt es, IT-Ressourcen zu inventarisieren, potenzielle Sicherheitsprobleme zu identifizieren und Bedrohungen schnell zu untersuchen und abzuwehren. Außerdem besteht die Möglichkeit, die von Angestellten eingesetzten SaaS-Anwendungen zu katalogisieren und diese Anwendungen auf Risiken zu untersuchen.

Cyberhygiene
Cloudflare hilft dabei, Cyberhygiene-Praktiken zu unterstützen, um vor Bedrohungen zu schützen. So können Firmen zum Beispiel Phishing-Angriffe präventiv erkennen und stoppen. Auch der Schutz lokaler Geräte vor Malware gelingt, indem sie Browsercode im globalen Netzwerk von Cloudflare ausführen.

Kryptografie und Verschlüsselung
Cloudflare integriert modernste Verschlüsselung in alle Produkte und unterstützt bei der Verwaltung der Verschlüsselung. Cloudflare bietet zum Beispiel SSL/TLS-Schutz und eine erweiterte Zertifikatsverwaltung. Darüber hinaus können Organisationen Keyless-SSL-Dienste einsetzen, um ihre privaten Schlüssel zu speichern und zu

verwalten. Sie können zudem die Geo-Key-Verwaltung nutzen, um zu kontrollieren, wo die privaten Schlüssel gespeichert sind. Dabei unterstützt Cloudflare bereits Post-Quantum-Kryptografie.

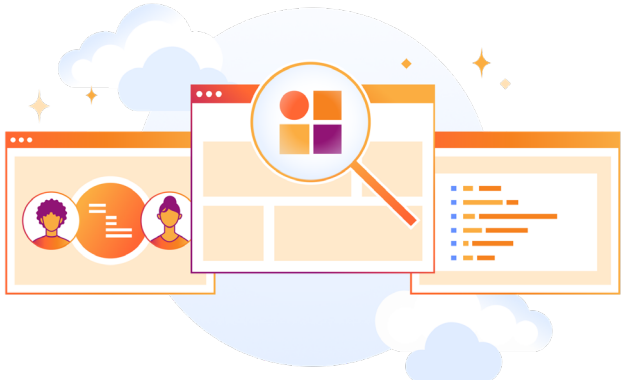
Zugriffskontrolle und Management von Anlagen
Cloudflare hilft bei der Erfüllung der strengen Anforderungen der DORA-Zugriffskontrolle. Die Funktionen der rollenbasierten Zugriffskontrolle (RBAC) legen fest, was Benutzer mit ihren Konten machen und sehen können. Darüber hinaus scannen DLP-Dienste (Data Loss Prevention) den Webtraffic und SaaS-Anwendungen auf sensible Daten. Um die Anforderungen bei der Verwaltung von Anlagen zu erfüllen, verwenden Organisationen Cloudflare-Dienste, um die Eigenschaften bestimmter Endpunkte zu verfolgen und anzuzeigen.

MFA (Mehr-Faktor-Authentifizierung)
Cloudflare unterstützt zudem die MFA-Anforderungen von DORA. Organisationen können die MFA-Durchsetzung und die Sitzungsverwaltung so konfigurieren, dass – je nach Identität des Benutzers, Standort des Geräts und anderen Kriterien – unterschiedliche Verhaltensweisen möglich sind.

Möglichkeit der Datenlokalisierung

Die Cloudflare Data Localization Suite[23] verfolgt bei der Datenlokalisierung einen granularen Ansatz. Unternehmen aus dem Finanzsektor können mit ihrer Hilfe die Festlegung einer Region bestimmen und damit eine Eingrenzung der geografischen Datenverarbeitung:

- Rechenzentren innerhalb der bevorzugten Region entschlüsseln TLS und wenden Dienste wie WAF (Web Application Firewall) an.
- Keyless SSL und Geo Key Manager speichern private SSL-Schlüssel in einer benutzerdefinierten Region.
- Die Customer Metadata Boundary stellt sicher, dass Protokolle die ausgewählte Region nicht verlassen.



Cloudflare kommt häufig im Finanzsektor zum Einsatz

„Cloudflare bietet äußerst wirksame Kontrollmöglichkeiten zur Angriffsabwehr, und zwar in der Cloud. Das war für uns ausgesprochen attraktiv. Weil sich die IT-Sicherheitsabteilung nicht um die Pflege der Infrastruktur kümmern muss, kann sie sich auf bedeutungsvollere Aufgaben konzentrieren."

Bob Varnadoe, **CISO von NCR**[24]

„Wir sind davon überzeugt, dass wir mit Cloudflare nicht nur unsere Kosten senken können, sondern dass das System auch viele Funktionen bietet und sehr leistungsstark ist. Darüber hinaus ist Cloudflare für seine Websicherheit und Mechanismen zur Abwehr von DDoS-Angriffen bekannt und einer der besten Dienste der Branche."

Rei Kakinuma, **Assistant Vice President der Abteilung Digital Solutions Development bei JCB Co., Ltd**[25]

„Die Cloud-Migration und die globale Expansion zwangen uns dazu, unsere Technologie neu zu gestalten und unsere Sicherheitsvorkehrungen zu verstärken. Wir wollten eine cloudnative Sicherheitslösung wie Cloudflare einsetzen, die uns in Zukunft auf globaler Ebene unterstützen kann."

João Pedro Gonçalves, **Global Chief Information Security Officer bei EQT**[26]

„Cloudflare und sein RBI-Service haben es uns ermöglicht, schlank zu bleiben und unser Budget niedrig zu halten. Wir müssen keine Experten einstellen, die sich mit Sicherheitsproblemen befassen oder Zeit damit verbringen, Computer zu installieren oder zu reparieren."

Grant Langhus, **IT-Manager bei Luana**[27]

Über Cloudflare

Cloudflare, Inc. (NYSE: NET) ist der führende Anbieter im Bereich Connectivity Cloud mit der Mission, das Internet besser zu machen. Als Unternehmen versetzt Cloudflare Organisationen in die Lage, ihre Mitarbeitenden, Anwendungen und Netzwerke überall schneller und sicherer zu machen und gleichzeitig Komplexität und Kosten zu reduzieren. Die Connectivity Cloud von Cloudflare bietet die umfassendste konsolidierte Plattform für cloudnative Produkte und Entwicklertools am Markt. Mit dieser Lösung kann sich jedes Unternehmen die für die Arbeit, Produktentwicklung und schnellere Geschäftserfolge erforderliche Kontrolle verschaffen.

Aufbauend auf einem der größten und am besten vernetzten Netzwerke der Welt blockiert Cloudflare für seine Kunden täglich Milliarden von Online-Bedrohungen. Millionen von Organisationen vertrauen auf Cloudflare – von den größten Marken über Unternehmer und kleine Unternehmen bis hin zu gemeinnützigen Einrichtungen, Hilfsorganisationen und Behörden auf der ganzen Welt.

Weitere Informationen und Kontakt:

Kontaktadresse:

Cloudflare Germany GmbH
Rosental 7, 80331 München

Kontakt:

Telefon: +49 (89) 26207202
E-Mail: enterprise@cloudflare.com
https://www.cloudflare.com/de-de