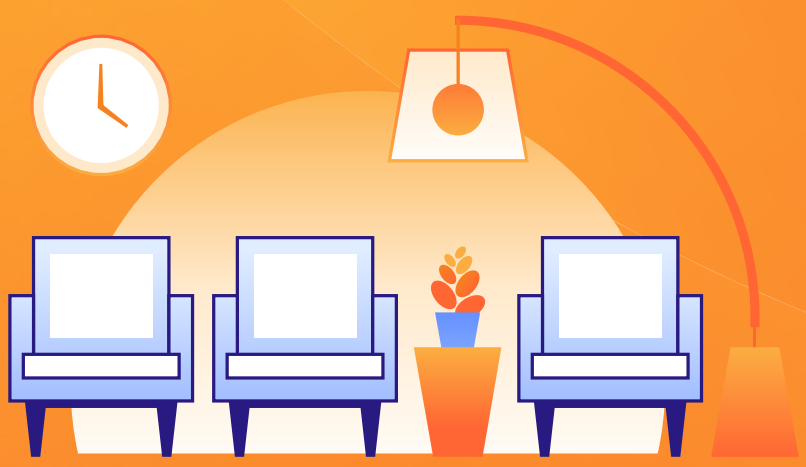
CLOUDFLARE

WHITEPAPER

Cybersicherheit im öffentlichen Sektor – cloudbasierter Schutz für Behörden



Cybersicherheit im öffentlichen Sektor – cloudbasierter Schutz für Behörden

Das lange Warten auf den harten Stühlen der Ämter soll bald weitgehend passé sein, so ist es zumindest die Absicht der Bundesregierung und der Wille der Bürgerinnen und Bürger. Die öffentliche Verwaltung soll effizienter, schneller und transparenter werden. Das erfordert die Bereitstellung eines modernen Onlineangebots und den Aufbau einer leistungsstarken IT-Infrastruktur. Der Königsweg zu diesem Ziel führt über das Internet in die Cloud, doch das ermöglicht Cyberangriffe. Die Informationssicherheit stellt für Behörden und Kommunen eine Herausforderung dar. Diese lässt sich jedoch durch interne Maßnahmen und mithilfe von Sicherheitssystemen externer Anbieter wie Cloudflare gut meistern. Das globale Content Delivery Network (CDN) mit umfangreichen Cybersicherheit-Services des Unternehmens bildet einen starken Schutzschild, an dem auch schwerste Attacken aus dem World Wide Web abprallen.

Die meisten Behördengänge lassen sich problemlos auch online erledigen, davon waren 70 Prozent der Befragten in einer Studie des IT-Branchenverbands Bitkom überzeugt. Der Gesetzgeber treibt die von Gesellschaft und Wirtschaft dringend geforderte Digitalisierung der öffentlichen Verwaltung seit einigen Jahren voran. So verpflichtete das Onlinezugangsgesetz (OZG) Bund, Länder und Kommunen, bis Ende 2022 ihre Verwaltungsleistungen über Verwaltungsportale digital anzubieten und diese zu einem Portalverbund zu verbinden. Den Rahmen für den weiteren Ausbau soll das OZG-Änderungsgesetz (OZGÄndG) abstecken.

Das OZG leitet einen weitgehenden Modernisierungsprozess der öffentlichen Hand ein. Geplant ist eine Ende-zu-Ende-Digitalisierung der Servicenetze für Kommunen und Länder, die teils bis hin zur Bundesebene miteinander verbunden sind. All dies erfordert eine leistungsfähige IT-Infrastruktur, die zudem Schutz vor immer mehr und zunehmend potenten Cyberattacken benötigt. Eine anspruchsvolle Aufgabe, für die jedoch bewährte Maßnahmen und Sicherheitslösungen zur Verfügung stehen.

Datenschutz und Informationssicherheit

Die öffentliche Verwaltung muss neben dem Ausbau ihrer IT-Infrastruktur zwei Konzepte beachten. Zum einen ist sie dem Schutz der teilweise hochsensiblen personenbezogenen Daten verpflichtet, wie es die Europäische Datenschutz-Grundverordnung (DSGVO) vorschreibt. Zum anderen gerät die Informationssicherheit immer mehr in den Fokus, je weiter sich die IT-Infrastruktur nach außen öffnet – etwa an den Schnittstellen mit den Bürgerinnen und Bürgern, die über Webseiten und Portale Onlineservices in Anspruch nehmen. Auch die externe Kommunikation via E-Mail, Remote-Arbeitsplätze der Mitarbeitenden, die zunehmende Vernetzung von Infrastrukturen und Verwaltungsprozessen und Cloud-Lösungen, die vermehrt zum Einsatz kommen, spielen hier zentrale Rollen.

Eine unzureichende Informationssicherheit kann zu erheblichen Schäden führen, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) in drei Kategorien unterteilt:

- **Verlust der Verfügbarkeit:** Grundlegende Informationen sind nicht oder nur eingeschränkt zugänglich. Dies kann zum Beispiel bedeuten, dass Fachaufgaben einer Institution beeinträchtigt oder nicht ausgeführt werden können.
- **Verlust der Vertraulichkeit von Informationen:** Personenbezogene oder vertrauliche Daten werden ungewollt veröffentlicht.
- **Verlust der Integrität (Korrektheit) von Informationen:** Daten werden gefälscht oder verfälscht, verlieren ihre Authentizität (Echtheit und Überprüfbarkeit) und werden zum Beispiel einer falschen Person zugeordnet (gefälschte digitale Identität).

Hinzu kommen rechtliche Unsicherheiten in Bezug auf den Datenschutz sowie eingeschränkte Informationssicherheit als zwei kritische Aspekte von kommerzieller Standardsoftware. Weil ihr Quellcode nicht einsehbar ist, lässt sich nicht nachvollziehen, welche Metadaten gesammelt werden und ob zum Beispiel eine Speicherung von personenbezogenen Daten auf Servern im außereuropäischen Ausland erfolgt. Um die Abhängigkeit von proprietärer Software aufzulösen, entwickelt das Zentrum für Digitale Souveränität der öffentlichen Verwaltung die Deutsche Verwaltungscloud-Strategie (DVS), die Open-Source-Plattform Open CoDE sowie den souveränen Open-Source-Arbeitsplatz.

Vorgaben für die Informationssicherheit

Methoden, Anleitungen, Werkzeuge und Empfehlungen zur Steigerung der Informationssicherheit bietet unter anderem der IT-Grundschutz des BSI. Bei diesem ganzheitlichen Sicherheitsansatz für Behörden, Institutionen und Unternehmen kommen neben der Technik und Infrastruktur auch organisatorische und personelle Themen zum Tragen. Der IT-Grundschutz bildet die bewährte Vorlage für ein Informationssicherheits-Managementsystem (ISMS) sowie die diesbezügliche ISO-27001-Zertifizierung. Hierbei gilt es, zwischen verschiedenen ISO-27001-Zertifikaten zu unterscheiden. So ermöglicht der ISO-Standard 27001 („Information Technology – Security Techniques – Information Security Management Systems – Requirements“) eine Zertifizierung des Informationssicherheits-Managements. Das ISO-27001-Zertifikat auf der Basis von IT-Grundschutz dokumentiert, dass für den betrachteten Informationsverbund alle relevanten Sicherheitsanforderungen gemäß IT-Grundschutz realisiert wurden. Voraussetzung für die Vergabe eines ISO-27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO-27001-IT-Grundschutz-Auditor.

Betreiber kritischer Infrastrukturen sind gemäß dem IT-Sicherheitsgesetz 2.0 dazu verpflichtet, durch organisatorische und technische Vorkehrungen Störungen ihrer IT-Infrastruktur zu vermeiden. Als effektive Maßnahme fordert das Gesetz auch explizit Systeme zur Angriffserkennung (SzA) von Cyberattacken, zu denen das BSI eine Orientierungshilfe verfasst hat. Voraussichtlich Ende 2024 wird das IT-Sicherheitsgesetz durch das Gesetz zur Umsetzung der überarbeiteten EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2UmsuCG) verschärft werden, das einen größeren Adressatenkreis sowie mehr Pflichten vorsieht. Diese müssen neben den Vorgaben der DSGVO in der Regel auch besondere Sicherheitsanforderungen befolgen, wenn sie Cloud-Dienste nutzen. Darunter können zum Beispiel die Mindestanforderungen an sicheres Cloud Computing fallen, die im Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) stehen. Künftig sollen zumindest auch die Einrichtungen der Bundes- und Landesverwaltungen gesetzlichen Verpflichtungen in puncto IT-Sicherheit unterliegen.

Wirksame Maßnahmen für eine sichere IT-Infrastruktur

Neben diesen umfassenden Vorgaben, Verfahren und Gesetzen haben sich für privatwirtschaftliche und öffentliche Organisationen unter anderem folgende Vorgehensweisen zur Festigung der Informationssicherheit bewährt:

- Informationssicherheit ist Chefsache und liegt in der Verantwortung des Topmanagements.
- Für die Informationssicherheit werden genügend personelle und finanzielle Ressourcen bereitgestellt. Als vernünftige finanzielle Ausstattung gelten rund 15 bis 20 Prozent der gesamten IT-Ausgaben.
- Spezialisierte externe Unternehmen führen Sicherheitstest durch.
- Sicherheitsrichtlinien und -verfahren werden erarbeitet, implementiert und für verbindlich erklärt. Dazu gehört unter anderem, Daten regelmäßig zu sichern und aktuelle Back-ups zu erstellen, Regeln für sichere Passwörter einzuführen sowie für die jeweiligen Maßnahmen Verantwortliche zu bestimmen.
- Anwendungen sowie die Software sämtlicher Geräte mit eigenen Betriebssystemen werden stets sofort nach dem Erscheinen von Updates aktualisiert, sodass Patches umgehend Sicherheitslücken schließen.
- Für potenzielle IT-Sicherheitsvorfälle muss ein Notfallplan existieren, der regelmäßige Überprüfungen und Überarbeitungen erfährt.
- Weil am Ende immer Menschen an den Geräten sitzen, die Fehler machen, aber auch Gefahren entdecken können: Alle Angestellten müssen für das Thema IT-Sicherheit sensibilisiert und darin geschult werden.

Ausmaß und Folgen von Cyberkriminalität

Cyberkriminalität ist nicht zu unterschätzen. Das zeigen die Zahlen des Bundeskriminalamts im Bundeslagebild 2022, Befragungen, die Sicherheitskooperation Cybercrime des Branchenverbands Bitkom sowie das Archiv von erfassten Cyberangriffen auf Kommunen und kommunale Einrichtungen der Heinrich-Böll-Stiftung:

- Von 2016 bis 2023 steigerte sich die Zahl der Cyberangriffe auf Kommunen und kommunale Einrichtungen kontinuierlich. Die Attacken wurden dabei stetig professioneller und gefährlicher. Laut dem Bericht zur Lage der IT-Sicherheit in Deutschland 2023 des BSI war die Bedrohung im Cyberraum nie zuvor so hoch.

- 2022 registrierte die Polizei 136.865 Cybercrimefälle. Hierzu zählen alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden.

- Die durch Cyberkriminalität (Diebstahl sensibler Unternehmensdaten, Spionage, Sabotage) entstandenen Schäden beliefen sich 2022 auf 202,7 Milliarden Euro, damit lagen sie rund doppelt so hoch wie noch 2019. Allein durch Cyberattacken, die nur einen Teil der Cyberkriminalität darstellen, entstanden der deutschen Wirtschaft 2023 rund 148 Milliarden Euro Schaden.

- 63 Prozent der 2022 befragten Unternehmen erwarteten einen Cyberangriff in den kommenden zwölf Monaten, davon sahen sich nur 43 Prozent für eine solche Attacke gut genug gerüstet.

- Die primäre Bedrohung für Unternehmen und öffentliche Einrichtungen stellte Ransomware dar. Phishing war hingegen der Haupteintrittsvektor für Schadsoftware, und DDoS-Angriffe (Distributed Denial of Service) liefen erkennbar effizienter als in den Vorjahren ab.

Stolpersteine auf dem Weg zur Informationssicherheit

Um Informationssicherheit zu erreichen und anschließend zu gewährleisten, müssen Behörden, Kommunen und öffentliche Einrichtungen so professionell vorgehen wie ihre potenziellen Angreifer. Orientierung und Empfehlungen für die Umsetzung bieten unter anderem das Konzept „Weg in die Basis-Absicherung“ (WiBA) und das IT-Grundschutz-Kompendium, die beide das BSI entwickelt hat.

Häufig mangelt es Behörden, Kommunen und öffentlichen Einrichtungen jedoch an ausgebildetem Fachpersonal, das die Informationssicherheit umfassend gewährleisten kann. Probleme verursacht zudem vielerorts eine fragmentierte IT-Infrastruktur: Diese Vielfalt an unterschiedlichster, teilweise veralteter Hard- und Software weist Sicherheitslücken auf. In Kombination mit Vor-Ort-, hybridem und Remote-Betrieb lässt sie sich nur schwer ausreichend schützen. In dieser Lage lohnt es sich für Kommunen sowie andere öffentliche Einrichtungen, sich an spezialisierte externe Anbieter zu wenden.

Das CDN von Cloudflare

Als eines der größten Netzwerke der Welt erstreckt sich das CDN (Content Delivery Network) von Cloudflare über 320 Städte in mehr als 120 Ländern, über 57 Millionen HTTP-Anfragen pro Sekunde und bedient jeden Tag Millionen von Internet-Seiten. Um Engpässe zu verhindern, leitet ein Algorithmus den Datenverkehr intelligent über die schnellsten und zuverlässigsten Netzwerkpfade. Zudem sorgt das geobasierte Routing dafür, dass Inhalte von den geografisch nächstgelegenen Servern bereitgestellt werden.

Zur Verbesserung von Geschwindigkeit und Konnektivität sitzen die Server an den Austauschpunkten zwischen verschiedenen Netzwerken. An diesen Internet-Knoten (Internet Exchange Points, IXPs) verbinden sich die Netzwerke verschiedener Internet-Provider. Mit direkten Verbindungen zu nahezu jedem Service- und Cloud-Provider erreicht das Cloudflare-Netzwerk 95 Prozent aller Menschen mit Internet-Anschluss weltweit innerhalb von circa 50 Millisekunden. Anwender in Deutschland haben unter anderem Zugriff auf sechs lokale Rechenzentren in Hamburg, Berlin, Düsseldorf, Frankfurt, Stuttgart und München. Insgesamt ist Cloudflare mit rund 13.000 Netzwerken von Service-Providern, Cloud-Anbietern und großen Unternehmen verbunden.

Durch das Zwischenspeichern von Inhalten auf Edge-Servern ermöglicht Cloudflare eine beschleunigte Auslieferung und reduzierte Latenzzeiten. Für die Verbesserung der Leistung sorgen darüber hinaus verschiedene Optimierungswerkzeuge und -dienste, zum Beispiel für die Bildanpassung und -optimierung sowie für die Minimierung von HTML-, CSS- und JavaScript-Dateien.

Zertifizierungen und externe Validierungen von Cloudflare

Cloudflare hält eine Reihe von externen Zertifizierungen und Validierungen auf der Grundlage internationaler Standards in Bezug auf den Datenschutz sowie die Informationssicherheit:

- Die Lösungen von Cloudflare erfüllen die Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO). Cloudflare stellt für Datentransfers in die USA einen gleichwertigen Schutz persönlicher Daten gemäß DSGVO sicher, sowohl durch seine Standardvertragsklauseln mit ergänzenden Maßnahmen, als auch durch seine Zertifizierung für das EU-U.S.-Data-Privacy-Framework.

- Zu den weiteren Zertifizierungen zählen ISO/IEC 27001:2023 und ISO/IEC 27701:2019 zur Umsetzung von Informationsmanagementsystemen sowie ISO/IEC 27018:2019 zum Schutz von personenbezogenen Daten, deren Verarbeitung in einer öffentlichen Cloud erfolgt.

- Cloudflare erfüllt zudem die C5-Kriterien. Beim Kriterienkatalog Cloud Computing (Cloud Computing Compliance Criteria Catalogue) handelt es sich um einen vom BSI erstellten Prüfungsstandard. Er gewährleistet, dass Anbieter von Cloud-Diensten eine Reihe von Kriterien für die Informationssicherheit einhalten.

- Cloudflare-Dienste entsprechen zudem dem EU Cloud Code of Conduct (EU Cloud CoC). Damit verpflichtet sich Cloudflare, Datenschutzrichtlinien und Sicherheitsmaßnahmen zu implementieren, die mit der DSGVO übereinstimmen.

- Cloudflare ist laut BSI qualifizierter DDoS-Mitigation-Dienstleister.

Ein sicheres Netzwerk als Schutzschirm

Eine mögliche Antwort auf diese schwierige Situation besteht darin, ein sicheres Internet zu schaffen, das Cyberangriffe zuverlässig abwehrt. Cloudflare ermöglicht dies mit seinem vorkonfigurierten Content Delivery Network (CDN). Dieses globale Netzwerk spannt einen Schutzschirm über die Webseiten und Portale seiner Anwender, den Schadsoftware, Multi-Channel-Phishing, Kill Chain oder HTTP/2 Rapid Reset (einer der schwersten DDoS-Angriffe aller Zeiten) nicht durchdringen können. Cloudflare blockt täglich 209 Milliarden Cyberattacken weltweit.

Um diesen hohen Sicherheitsstandard zu erreichen, analysiert Cloudflare in seinem CDN regelmäßig den weltweiten Datenverkehr im Internet. Zudem scannt der nach Google größte Webcrawler der Welt mithilfe von künstlicher Intelligenz wöchentlich das gesamte World Wide Web unter anderem nach Mustern auf Landingpages. Auf diese Weise kann Cloudflare Gefahren mit einem Vorlauf von mehreren Wochen prognostizieren und potenzielle Angriffe schon frühzeitig abwehren.

Das kommunale Schutzmodell von Cloudflare

Mit dem kommunalen Schutzmodell bietet Cloudflare ein modular konfigurierbares Paket für den öffentlichen Sektor. Es beinhaltet eine Vielzahl von Dienstleistungen zum Schutz von Webseiten, Applikationen und Netzwerken. Hierzu gehören unter anderem die Anbindung an das CDN, der Schutz vor DDoS-Angriffen, die cloudbasierte Web Application Firewall (WAF), Datenlokalisierung in Deutschland und der EU, Zertifikatsverwaltungen, Integritäts-Checks und Sicherheitslösungen wie Zero Trust. Das Zero-Trust-Modell beinhaltet eine strikte Identitätsprüfung für alle Personen und Geräte, die auf Ressourcen in einem privaten Netzwerk zugreifen möchten, egal, ob sie sich innerhalb oder außerhalb des Netzwerkperimeters befinden. Hinzu kommt Unterstützung bei Implementierung, Onboarding und Konfigurationsmanagement.

Um die Sicherheit ihrer Onlinedienste und Website zu steigern, entschied sich zum Beispiel die Stadt Bocholt für den DDoS-Schutz ihrer Netzwerk-Präfixe von Layer 3 bis Layer 7, für die Web Application Firewall mit Machine Learning sowie die Data Localization Suite (DLS). Dadurch erfolgt die Bearbeitung von Kundenanfragen wahlweise nur in Deutschland – ein enormer Vorteil, wenn es darum geht, gesetzliche Anforderungen zur Datenlokalisierung zu erfüllen.

Die Stadtwerke Aalen lösten dagegen die Performance-Probleme ihrer VPN-Lösung, die erheblichen Support-Aufwand benötigte, mit einer deutlich leistungsstärkeren und leichteren VPN-Lösung auf Basis des Wireguard-Protokolls und entschieden sich für Cloudflare One Zero Trust. Zu den wichtigsten Komponenten zählen dabei eine VPN-Lösung mit WARP-Benutzerclients, Cloud Access zur Absicherung des Zugriffs auf interne Applikationen, Cloud Gateway zur Absicherung der Internet-Nutzung sowie Remote Browser Isolation zum Schutz vor Phishing-Attacken.

Für die Informationssicherheit sind externe Dienstleister eine gute Lösung

Die Digitalisierung der Verwaltung schreitet voran – und im Rahmen dieser Entwicklung bildet die Informationssicherheit einen Schwerpunkt. Die Vorgaben und Regelungen zu diesem komplexen Thema übersteigen jedoch häufig vor allem die personellen Ressourcen der betroffenen Stellen, denen für diese Aufgaben oft die geeigneten Fachleute fehlen. Für öffentliche Stellen besteht jedoch die Möglichkeit, ihre Informationssicherheit durch externe Dienstleister zu gewährleisten. Hierfür bietet Cloudflare mit seinem Content Delivery Network effektiven Schutz vor Cyberangriffen. Mit dem kommunalen Schutzmodell des Anbieters können sich öffentliche Einrichtungen genau das Sicherheitspaket schnüren, das für ihre Situation erforderlich und am besten geeignet ist.

Weitere Informationen und Kontakt:

Über Cloudflare

Cloudflare, Inc. (NYSE: NET) ist der führende Anbieter im Bereich der Connectivity Cloud. 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. Aufbauend auf einem der größten und am besten vernetzten Netzwerke der Welt blockiert Cloudflare für seine Kunden täglich Milliarden von Online-Bedrohungen.

Kontaktadresse:

Cloudflare Germany GmbH
Rosental 7, 80331 München

Kontakt:

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