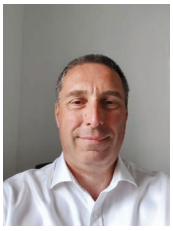
Vollständige Datenkontrolle mit On-Premise MFA

Worauf Unternehmen und Organisationen achten müssen, die keine Cloud-basierte Authentifizierung verwenden können.

© imago-images.de @Panthermedia

Laut Bericht des BSI zur Lage der IT-Sicherheit in Deutschland 2022 erreichte die Gefährdungslage durch Malware einen neuen Höchststand. Besonders besorgniserregend seien dabei die Art und Weise der Angriffe auf Unternehmen, staatliche Institutionen und Privatpersonen. Denn diese basieren auf intelligenten Algorithmen unter Einsatz modernster Technologien. Im aktuellen Berichtszeitraum (Juni 2021 bis Mai 2022) werden identitätsbasierte Bedrohungen als eine der Hauptquellen für Angriffe auf die Unternehmens-IT identifiziert. „Die professionelle Authentifizierung von Anwendern ist daher das A und O einer unternehmensweiten Sicherheitsstrategie. Eine bessere Identitätserkennung sowie optimierte Strategien zur Bedrohungsabwehr schützen die Unternehmens-IT, deren Applikationen und sensiblen Daten und sorgen so für eine erhöhte Identitätssicherheit“, so Robert Korherr, Geschäftsführer der ProSoft GmbH. Zur Minimierung der Angriffsfläche empfiehlt das BSI, nicht nur die Anzahl der von außen zugänglichen Systeme zu reduzieren, sondern auch deren Nutzung durch Unbefugte zu erschweren, beispielsweise durch die Nutzung eines VPN-Netzwerks oder den Einsatz einer Multi-Faktor-Authentifizierung (MFA).



© SecurEnvoy

Autor:
Chris Martin
Head of Solution Architecture
SecurEnvoy
https://securenvoy.com/de/

Multi-Faktor-Authentifizierungslösung

Vielen Unternehmen ist die aktuelle Bedrohungslage durch Cyberangriffe durchaus bewusst, sie möchten daher gerne auf eine Multi-Faktor-Authentifizierungslösung setzen, um die firmeninternen Mitarbeiterkonten zu schützen. Doch meist sind auf der Suche nach der geeigneten Lösung einige Hürden zu nehmen. Beispielsweise werden Unternehmen oft mit Cloud-basierten Lösungen konfrontiert, die sie nicht einsetzen können, da sie darauf angewiesen sind, Anwendungen und Datenspeicherungen On-Premise zu halten. Für Organisationen im Regierungssektor bedarf es beispielsweise einer strengen Datenkontrolle. Energie- oder Versorgungsunternehmen können nicht einmal eine Stunde Ausfallzeit tolerieren und für Unternehmen, die ein schrittweises Vorgehen für die Cloud-Migration verfolgen, ist On-Premise entweder die einzige Option oder Teil eines hybriden On-Premise/Cloud-Ansatzes.

On-Premise als Lösung

Mit „On-Premise“ sind insbesondere Anwendungen gemeint, die innerhalb der physischen Grenzen eines Unternehmens und somit in einem Rechenzentrum auf einem Server oder in einer privaten Cloud untergebracht sind, und nicht remote auf Servern oder in der öffentlichen Cloud gehostet werden.

On-Premise ist für viele Unternehmen und Organisationen nach wie vor alternativlos. Während die Cloud für viele Unternehmen die naheliegende Wahl sein mag, um die Kosten für die Verwaltung von Anwendungen zu senken, gibt es einige Gründe, warum sich andere gegen die öffentliche Cloud entscheiden.

Datensicherheit

Bei der Verlagerung von Daten in die Cloud ist der Anwender auf die Sicherheits- und Zugriffskontrollen des Cloud-Anbieters angewiesen. Das bedeutet auch, dass Organisationen, die sensible personenbezogene Daten wie Gesundheitsinformationen oder andere streng vertrauliche Informationen schützen müssen, unter Umständen strengere Kontrollen benötigen.

Datenhoheit

Aufgrund unterschiedlicher Datenschutzgesetze in verschiedenen Ländern müssen einige Organisationen gegebenenfalls bestimmte Daten On-Premise speichern, um sicherzustellen, dass sie das Land nicht verlassen. Wenn die Zero-

© bigstockphoto.com @Dzmitry Dzemidovich

© *bigstockphoto.com @Jakub Jirsak*

Trust-Richtlinie im Unternehmen die Übertragung von Daten ins Ausland nicht zulässt, muss man sich vor Cloud-Anwendungen in Acht nehmen, da die Backups in Rechenzentren anderer Länder durchgeführt werden.

Ausfallsicherheit

Keine Cloud bietet eine 100%ige Verfügbarkeit was insbesondere für Unternehmen und Organisationen aus dem KRITIS-Umfeld problematisch ist, denn selbst ein Ausfall von nur einer Stunde kann ernste Auswirkungen haben. Angesichts der zunehmenden Sicherheitsverletzungen bei Cloud-basierten Lösungen stellt sich die Frage, ob die Cloud sicher genug für die eigenen Daten ist.

Für Regierungsinstitutionen mit sensiblen Daten, die nicht kompromittiert werden dürfen, für Versicherungs- und Gesundheitsorganisationen, die große Mengen sensibler Daten verarbeiten, für Verkehrsnetzwerke und nationale Infrastrukturen, die sicherstellen müssen, dass die Dienste weiterlaufen, oder für Organisationen, die keinerlei Sicherheitsrisiken eingehen dürfen, ist On-Premise die sicherste Option für alle Aspekte, einschließlich der Authentifizierung.

Hybride Architektur

Vielleicht möchten manche Unternehmen aber auch weiterhin eine Mischung aus On-Premise und Cloud-basierten Anwendungen nutzen und im Rahmen einer hybriden Architektur in die Cloud wechseln. Der Bedarf an On-Premise MFA ist nach wie vor vorhanden, ebenso wie die Notwendigkeit, dieselben Funktionalitäten für die Cloud-Lösung bereitzustellen.

Wann ist eine MFA-Lösung wirklich On-Premise?

Die Herausforderung, mit der sich zahlreiche Unternehmen konfrontiert sehen, besteht darin, dass viele der heute verfügbaren MFA-Lösungen Cloud-basierte Software-as-a-Service-Lösungen sind – und den damit verbundenen Sicherheits- und Datenkontrollrisiken unterliegen. Wenn Anbieter sowohl On-Premise- als auch Cloud-Lösungen anbieten, kann der Nachteil darin bestehen, dass es sich um zwei separate Quellcode-Grundlagen handelt; häufig an einer Einschränkung der Funktionen erkennbar, da diese bei genauerer Betrachtung von On-Premise und Cloud nicht übereinstimmen. Andere Anbieter verfügen zwar über On-Premise-Lösungen, verlagern ihren Quellcode jedoch in die Cloud.

Was die Authentifizierung betrifft, so benötigen einige Methoden eine Internetverbindung, um eine Anfrage an ein Mobiltelefon zu senden, z. B. SMS oder Push-OTP. Falls Unternehmen also eine vollständige On-Premise Lösung benötigen, sollte eine OTP-App auf dem Mobiltelefon oder ein Hardware-Token verwendet werden.

Bei der Registrierung neuer Benutzer in einer streng gesicherten Umgebung ist es zudem ratsam, dies intern im lokalen Netzwerk vorzunehmen und nicht über das Internet, wo das Risiko von Sicherheitslücken besteht.

Schlüsselfragen

Worauf Unternehmen und Organisationen bei On-Premise MFA achten sollten: Es gibt einige Schlüsselfragen, die bei der Suche nach einer On-Premise MFA-Lösung berücksichtigt werden sollten, um herauszufinden, ob die Lösung wirklich geeignet ist und die erforderliche Funktionalität und Zukunftssicherheit bietet:

- Bietet der MFA-Anbieter wirklich On-Premise MFA an? Kann die Lösung auch verschiedene Authentifizierungsmethoden wie Hardware-Token oder eine OTP-App auf dem Mobiltelefon unterstützen, um eine Verbindung mit dem Internet zu vermeiden?
- Falls Unternehmen bereits On-Premise MFA verwenden, können sie einfach in die Cloud wechseln und die gleichen MFA-Funktionen in einer Hybrid-Umgebung nutzen?
- Ist die MFA-Lösung in der Lage, sich an die unterschiedlichen On-Premise und Cloud-Anforderungen in verschiedenen Ländern anzupassen? Ist die MFA-Lösung in der Lage die jeweiligen Datenschutzbestimmungen oder Sicherheitsanforderungen zu erfüllen?
- Wenn Sicherheit von besonderem Interesse ist, können Mitarbeiter und Verwaltungspersonal On-Premise registriert werden, um das Risiko von Sicherheitslücken durch webbasierte Anmeldungen zu reduzieren?

Eine Weiterentwicklung der MFA

Um sicherzustellen, dass Unternehmen in der Lage sind, alle Sicherheitsanforderungen und die unterschiedlichen Bedürfnisse aller Organisationsbereiche und Nutzer zu erfüllen, ist mehr als eine klassische MFA notwendig. Bei der „modernen Authentifizierung“ wird die Authentifizierung anhand von Merkmalen wie Standort, Netzwerk, Tageszeit und Browser verifiziert, um beispielsweise festzustellen, ob ein Benutzer Zugang haben sollte – unabhängig davon, ob sich der Benutzer über eine der verschiedenen Authentifizierungsmethoden und Geräte, die ihm zur Verfügung stehen, korrekt verifiziert hat. Moderne Authentifizierung erlaubt es, die am besten geeignete Technologie für verschiedene Anwendungsfälle und Sicherheitsstufen in der Organisation zu wählen. Zusätzlich bietet sie Gewissheit, dass alle Daten On-Premise (oder in der Cloud) sicher sind.

Wer schreibt:

SecurEnvoy ist seit über zwei Jahrzehnten führend im Bereich der MFA-Innovationen. Die Authentifizierungslösungen befinden sich weltweit erfolgreich im Einsatz, vom Regierungssektor, über das Gesundheits- und Finanzwesen, bis hin zur Fertigungsindustrie und verschiedenen Hilfsorganisationen. ◄

© *bigstockphoto.com @Pikovit*