De-Globalisierung - welche Softwareservices Unternehmen wählen sollten

Die Diskussion um De-Globalisierung hat in letzter Zeit erheblich an Bedeutung gewonnen. Einst war die Globalisierung der Schlüssel zum Erfolg, heute sehen sich Unternehmen und Regierungen mit einer Reihe von Herausforderungen konfrontiert, die von Protektionismus, eingeschränkter Lieferfähigkeit bis zu Sicherheitsrisiken reichen. Diese Entwicklungen haben auch Auswirkungen auf die Auswahl von Softwareservices und Identity & Access Management Systemen (IAM). Im Besonderen, weil darüber Mitarbeiter-, Partner- als auch Kundenidentitäten und deren Zugriffe verwaltet werden und somit ein kritischer Aspekt der IT-Sicherheit und Compliance in Unternehmen, sowie der Grundstein von (digitalen) Geschäftsmodellen liegt – ohne Login geht nämlich fast nichts mehr. In diesem Artikel werfen wir einen Blick auf die möglichen Implikationen der De-Globalisierung für IAM-Strategien.

Lokale Vorschriften und Datenschutz

Mit der De-Globalisierung steigt der Druck auf Unternehmen, sich an lokale Gesetze und Vorschriften zu halten, insbesondere in Bezug auf den Datenschutz. Beispielsweise hat die Europäische Union mit der Datenschutz-Grundverordnung (DSGVO) strikte Regeln für den Umgang mit personenbezogenen Daten eingeführt. Ähnliche Gesetze existieren in anderen Regionen, wie der California Consumer Privacy Act (CCPA) in den USA oder der Personal Information Protection Law (PIPL) in China. Hinzukommen internationale Konflikte, Wirtschafts- und Handelskriege, sowie (nicht tarifäre) Handelshemmnisse, die einen unsicheren Rechtsrahmen schaffen und zu Einschränkungen führen. Auf diese Weise hat die De-Globalisierung massive Auswirkungen auf das Identity & Access Management und den Umgang mit Nutzerdaten, sowohl für Kunden-, Partner- als auch Mitarbeiteridentitäten.

Während in der Vergangenheit ein IAM-System ggf. im eigenen Rechenzentrum installiert und betrieben wurde, sind die meisten IAM-Services, die technologisch gut sind, in der Cloud zu finden. Durch die oben skizzierten Situationen könnte es bei der Nutzung von diesen Services zu Einschränkungen kommen, denen man vielleicht am besten aus dem Weg geht, in dem man Softwareservices aus dem gleichen Rechtsraum (Europa) verwendet.

Schutz der Unternehmens-Assets

Ein sehr unangenehmer Nebeneffekt sind Hackerangriffe, die sowohl von nicht staatlichen als auch zunehmend von staatlichen Organisationen auf Unternehmen durchgeführt werden, zum Teil, um daraus Geld zu erpressen und zum Teil auch aus den gewonnenen Informationen eigenen Nutzen zu ziehen.

Tatsächlich ist die „Primärsicherheit“, bei der Nutzer im Unternehmen, als Authentifizierungsverfahren lediglich die Benutzerkennung und ein Passwort verwenden - und dies meist noch von suboptimalen Systemen implementiert ist - weit weg von sicher und daher einer der Haupteinfallstore für Hacker. Dies ist sicherlich ein wichtiger Grund, warum es auch zur De-Globalisierung kommt und warum Cyber-Versicherungen eine sichere Verwaltung von Benutzeridentitäten und in jedem Fall eine Multifaktorauthentifizierung (MFA) fordern (Bild 1).

Schutz für Maschinen

Jedoch auch für Maschinen und Geräte, die immer mehr vernetzt sind, sowie deren Managementsysteme bieten moderne Identity und Access Management Systeme, wie cidaas, Schutz. Die Geräteautorisierung folgt im Grunde dem Ansatz, dass ein Gerät eine andere Ressource nur erreichen kann, wenn es sich autorisieren kann und andersrum ein Gerät eine analoge Autorisierung bereitstellt, welche sicherstellt, dass auf das Gerät nicht unbefugt zugegriffen wird (Bild 2).

Auswahlkriterien für einen IAM-Softwareservice

95 % der Innovationen im Bereich Identity & Access Management kommen mittlerweile aus dem Kunden-, Konsumentenumfeld und weniger

Bild 1: Die wichtigsten MFA-Verfahren auf einen Blick, © widas

Autor:
Sadrick Widmann
CEO
cidaas by Widas ID GmbH
https://www.widas.de/

aus dem Unternehmensinternen Umfeld. Das trifft selbstverständlich auch auf die Vernetzung in der Industrie zu, wo Services angeboten werden, die das IoT wahr werden lassen.

Dies vorausgeschickt, sind folgende IAM-Auswahlkriterien wichtig:

1. **Zukunftssicherheit:** Aufbau des IAM-Softwareservice auf modernen Technologien.
2. **Standards, Zukunftssicherheit, Funktionalität, Sicherheit:** Unterstützung von zeitgemäßen IAM-Standards, wie OIDC, OAuth2, Device Autorisation, SAML2 zur Benutzerautorisierung, Device Autorisierung und für die Absicherung von Web-APIs.
3. **Sicherheit:** Bereitstellung von mehreren Authentifizierungsverfahren, die auf Inhärenz und Besitz basieren und auch Wissen.
4. **Sicherheit:** Integrierte Betrugserkennung zur Blockierung von verdächtigen Zugriffen
5. **Sicherheit:** Multifaktor Authentifizierungsmöglichkeiten basierend auf der Kritikalität des Zugriffs und der Erkennung von Risiken.
6. **Funktionsumfang, Benutzerkomfort:** Verfügbarkeit eines Einwilligungsmanagements, welches ermöglicht Benutzereinwilligungen bei Registrierung, Login oder aktionsbasiert einzuholen.
7. **Sicherheit, Device Autorisierung, Funktionsumfang:** Verfügbarkeit eines Device-Managements.
8. **Sicherheit, Verlässlichkeit, Vertrauen:** IAM-Anbieter, die sich im gleichen Rechtsraum wie ihr Unternehmen befinden.
9. **Sicherheit, Verlässlichkeit:** Betrieb des IAM-Services, welches in einer DSGVO-konformen Umgebung erfolgt (zwischenzeitlich gibt es einige Cloud Anbieter).
10. **Verlässlichkeit, Verfügbarkeit:** Der IAM-Service bietet eine exzellente Verfügbarkeit ohne geplante Unterbrechungen.
11. **Vertrauen, Zukunftssicherheit, Zusammenarbeit:** Der IAM-Anbieter ist innovativ und arbeitet mit den neuesten technologischen Standards
12. **Servicequalität, Zusammenarbeit, Verlässlichkeit:** Der IAM-Anbieter bietet einen Migrations-Support und Beratung.

Die Kompatibilität, nicht als Auswahlkriterium nominiert, da bei der Auswahl eines IAM-Services die Kompatibilität ein sehr weites Feld ist, nachdem es viele in die Jahre gekommene Mechanismen gibt, wie Microsofts AD, andere LDAP-Server oder Kerberos, die im Grunde wenig sicher und End-of-life sind. Daher sollte vielmehr der Migrationspfad im Vordergrund stehen. Das kann zwar bedeuten, dass man eine Kompatibilität schaffen muss, dies sollte aber im Wesentlichen dazu führen, dass man eine IAM-Konsolidierung in seiner IAM-Strategie erreicht (Bild 3).

Fazit

Die De-Globalisierung macht uns gegenbenenfalls feinfühliger bei der Auswahl von Services und Partnern. Für die geschäftliche Kontinuität sind viele Faktoren zu beachten, die Auswahl der Softwareservices und dessen reibungslosen Betrieb kommt spätestens seit IoT und der

Bild 2: Möglichkeiten der Device Autorisierung in der Industrie, © widas und © Benjamin & Blue Planet Studio & natanaelginting – stock.adobe.com

Digitalisierung eine große Bedeutung zu, weil Industrie-Unternehmen immer mehr verknüpft sind, mit ihren Kunden. Andersrum sind die Maschinen, die ein Unternehmen einsetzt, verknüpft mit den Lieferanten.

Dieser Beitrag soll zu einem Perspektivwechsel anregen, um die IAM-Strategie zukunftssicher anzugehen und aufzuzeigen, dass IAM-Services der modernen Art, wie cidaas, viele Aufgaben bereits lösen, die ggf. aktuell noch mit unterschiedlichen Techniken und Konzepten mühsam angegangen werden.

Wer schreibt:

Sadrick Widmann ist Chief Executive Officer von cidaas, dem ersten in Deutschland entwickelten und gehosteten (Customer) Identity & Access Management. Er kennt und versteht die Anforderungen, die mit einer digitalisierten Welt einhergehen und hilft Kunden beim Aufbau identitätsbasierter Geschäftsmodelle.

Die Widas Unternehmensgruppe bietet seit 1997 “Software made in Germany” an und ist stolz mit cidaas eine umfassende Identity Plattform entwickelt zu haben, die in Deutschland entwickelt und gehostet wird. ◄

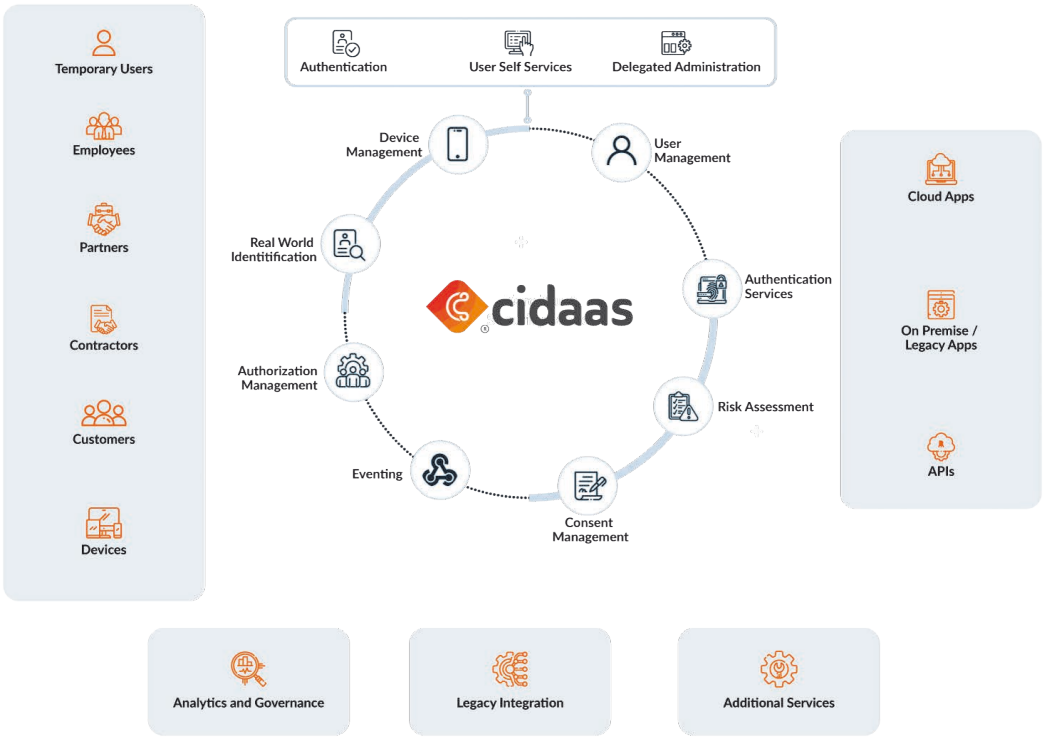

Bild 3: Feature Matrix eines Identity & Access Managements, © widas