DTS

DTS

Identity as a Service (IDaaS)

Identity as a Service (IDaaS)

Digitale Identitäten und Berechtigungen spielen in der IT eine wichtige Rolle. Ein Identity & Access Management (IAM) soll diese Identitäten zuweisen und sämtliche Zugriffsberechtigungen abbilden. Ohne IAM sind Einfallstore für kompromittierte Logins und Zugänge, Ransomware, Phishing, Malware u.v.m. geöffnet. Das Ziel: Daten sichern und Compliance-Richtlinien erfüllen.

Als Cyber-Security-Softwarehersteller wollen wir zum einen Cyberkriminelle und unautorisierte Nutzer am Zugriff auf Apps und Daten hindern. Darum haben wir eine Plattform entwickelt, welche die Benutzeridentifizierung entkoppelt und verwaltet. Das Ergebnis ist ein einziges, sicheres Tor für User, Apps und die Cloud – für ganze Unternehmen, deren Kunden und Anbindungen. Zum anderen liefern wir Ihnen die Antwort auf diese Fragen:

Sie wollen sich mit Multi Factor Authentication & Access Management besser schützen?

Sie wollen Wildwuchs bei Anwendungen, Rechten & Freigaben sowie dem Zugangsmanagement vermeiden?

Sie wollen die EU-DSGVO einhalten & dies auch vorweisen?

Sie wollen Daten nicht in die USA & das Ausland auslagern?

Sie wollen dynamisch wachsen & die Features sollen passend mitwachsen?

Unsere Antwort: „Cyber Security made by DTS" mit dem DTS Identity as a Service (IDaaS). Wir ermöglichen ein zentrales, Mittelstand-freundliches IAM nach höchsten Maßstäben. Die selbst entwickelte, intuitive Plattform gewährleistet sichere Authentifizierung, Zugriffskontrolle und Profilmanagement – automatisch, skalierbar und sicher aus der deutschen, zertifizierten DTS Cloud bereitgestellt!

- IAM & CIAM auf einer zentralen Plattform
- Aus eigenen, zertifizierten & EU-DSGVO konformen Rechenzentren bereitgestellte SaaS
- Multi Factor Authentication, Zugriffsverwaltung & Profilmanagement
- Zentrales, intuitives Dashboard für gesamtes Management & Anwendungen
- Access Gateway für Identity-Standards SAML & OIDC
- SSO für lokale oder Cloud Apps
- Self-Service, inkl. CI-Customizing
- Cyber-Security-Fokus

Das IDaaS folgt dem Prinzip einer Multi Factor Authentication, bei der sich ein User per Single Sign-On (SSO) bei allen verbundenen, lokalen oder Cloud Apps einmalig anmeldet. Sämtliche Anwendungen mit OIDC- oder SAML-Standard können gebündelt werden. Die freigegebenen Apps sind nach der einmaligen Anmeldung auf einem Dashboard sichtbar und können von dort zentral angesteuert werden – alles auf einen Blick. Eine eigene Datenbank verwaltet sämtliche Userdaten und Passwörter. Zudem können per AD/LDAP-Anbindung bestehende Verzeichnisdienste oder Systeme zur Authentifizierung, Verwaltung von Gruppen und Speicherung von Attributen genutzt werden.

Mittels Role-based Access Control (RBAC) können verschiedene Rollen erstellt werden. Sobald einem User eine Rolle zugeteilt wird, erhält er die vordefinierten Berechtigungen und Zugänge in den Anwendungen. Eine App erfährt automatisch, welche Rolle der User hat und kann dementsprechend Ressourcen anzeigen bzw. freigeben. Auf diese Weise bleibt Ihrer IT die separate Verteilung von Freigaben erspart, ein schnelles Onboarding ist möglich und es grenzt möglichen Wildwuchs von Berechtigungen ein. Das IDaaS leistet ebenso Machine-to-Machine (M2M) API Authorization. Dabei authentifiziert sich eine Anwendung mit dem IDaaS, welches diese Information validiert und einen Access Token zurückgibt. Die Anwendung kann den Access Token anschließend verwenden, um Ressourcen dieser API abzufragen – voll automatisch.

Die Verwaltung des DTS IDaaS ist auf eine intuitive User Experience ausgerichtet. Jeder User kann auf der Self-Service-Oberfläche, je nach Rechtevergabe, eigenständig Daten und Einstellungen bearbeiten. Das betrifft neben der Zugangsverwaltung auch die Sprache, Verifizierungsoptionen oder das CI-Customizing. Im Dashboard sind für Admins alle Aktivitäten innerhalb der Plattform sichtbar, also u. a. die Anzahl der Logins, die Anzahl der User, angebundene Organisationen, verbundene Apps und APIs. Im Management können dann neue Organisationen angelegt, User eingeladen, Berechtigungen und Rollen verteilt, Apps und APIs angebunden sowie Logs eingesehen werden.

Unser Fokus liegt auf moderner Cyber Security. Aus diesem Grund werden Passwörter bei externen Systemen bereits im Browser verschlüsselt und nie durch das IDaaS eingesehen. Auch der Schutz vor Brute-Force-Angriffen ist gewährleistet. Das IDaaS gleicht die häufigsten Passwörter mit der Auswahl des Users ab und bittet notfalls darum, ein anderes zu verwenden. Sollten Login-Daten genutzt werden, die kompromittiert sind, zeigt die Breached Password Detection dies an, mit der Aufforderung das Passwort zu ändern. Neben dem Passwort kann ein weiterer Faktor konfiguriert werden, z. B. Nachrichten per SMS oder E-Mail. Das Log Reporting, also das Nachvollziehen aller Aktivitäten, vervollständigt das hohe Sicherheitslevel.

Das Spektrum an Unternehmen ist groß, bei denen die AD-Verwaltung und das Berechtigungsmanagement nicht einheitlich erfolgen. Gleichzeitig existieren meist verschiedenste Apps oder Micro Services, auf die mehrere Personenkreise zugreifen können. „as a Service" bedeutet, dass wir das IDaaS aus unserer DTS Cloud zur Verfügung stellen, inkl. Support, damit Sie es in einer dedizierten, automatisierten Umgebung nutzen können. Auf diese Weise ermöglichen wir allen Unternehmen eine zentrale Plattform.

Use Cases, von denen Sie ganz besonders profitieren:

- **Dynamische Einsetzbarkeit als IAM & CIAM,** egal ob für B2E, B2B oder B2C
- **Erfüllung von Compliance-Anforderungen,** z. B. in Bezug auf die EU-DSGVO, welche die Minimierung der Zugriffsrechte sowie Nachweise des Compliance und Einwilligungsmanagements für Kundendaten einfordert
- **Transparenz & Kontrolle** durch die Übersicht zu allen eingebundenen Apps und verbundenen Usern
- **Durchsetzung von Policies,** z. B. bei internen Richtlinien zur Nutzung von Homeoffice
- **Effiziente, standortübergreifende On- & Offboardings** für zielgerichtete, automatisierte Berechtigungsstrukturen
- **Standardisierte Passwort-Politik & -Verwaltung**
- **Sichere Einbindung von Kunden & Partnern,** z. B. falls externen Benutzern der Zugang auf das Firmennetzwerk gezielt und kontrolliert gewährt werden muss
- **Einheitliches Kundenprofil** für „one face to the customer", inkl. eigener CI
- **Übersicht der Kundenaktivitäten** auf dem übersichtlichen Dashboard
- **Unterstützung der Eigenentwicklungen** bzgl. Authentifizierung und Autorisierung von Benutzern, um unsichere Produkte zu vermeiden und ohne Daten ins Ausland zu verlagern

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de