

Digitale Souveränität durch Identity- und Access-Management

Warum IAM auch für KMUs unverzichtbar ist



Alle Bilder © Widas Group

„Die Digitale Souveränität in Europa ist eine Priorität“ – mit diesem Bekenntnis hat Bundeskanzler Friedrich Merz jüngst ein klares Signal gesetzt.

Doch wie wird dieses Ziel Realität? Der Bundesverband IT-Mittelstand (BITMi) bringt es auf den Punkt: Ohne den innovativen IT-Mittelstand lässt sich Digitale Souveränität nicht erreichen. Damit politische Ambitionen zu gelebter Praxis werden, braucht es Technologien, die Sicherheit, Transparenz und Selbstbestimmung in den Mittelpunkt stellen. Eine Schlüsselrolle dabei spielt Identity & Access Management (IAM).



Autor:
Stefan Lutz
PreSales Consultant
Widas Group | cidaas | cnips
Strategischer IT Berater mit Fokus auf
IAM & IT-Security
www.cidaas.com
www.cnips.io

IAM als Enabler für Digitale Souveränität

Unternehmen jeder Größe stehen heute vor der Herausforderung, digitale Identitäten sicher zu verwalten und Zugriffe effektiv zu steuern. Steigende Cyberangriffe, zunehmende Regulierung und die Erwartung nutzerfreundlicher digitaler Services machen IAM zu einem zentralen Erfolgsfaktor.

Ein modernes IAM-System:

- schützt vor Cyberbedrohungen wie Ransomware und Phishing,
- sorgt für die Einhaltung von DSGVO, NIS2 und branchenspezifischen Vorgaben,
- ermöglicht sichere und komfortable digitale Geschäftsmodelle durch Single Sign-On, Multi-Faktor-Authentifizierung und Self-Service.

Dabei ist IAM weit mehr als ein Login-Dienst: Es verwaltet Identitäten über den gesamten Lebenszyklus, stellt Sicherheit wie Komfort sicher und legt die Basis für Zero-Trust-Strategien. Nach dem Prinzip „never trust, always verify“ wird jeder Zugriff konsequent überprüft – auch innerhalb des eigenen Netzwerks.

IAM als Schlüssel für KMU

Gerade kleine und mittelständische Unternehmen stehen vor einem Dilemma: Einerseits

geraten sie immer stärker ins Visier von Cyberangriffen, andererseits verfügen sie nicht über die Sicherheitsressourcen großer Konzerne.

Hier eröffnet sich eine Chance: Mit einem modernen IAM-System können KMU ihre Sicherheit, Compliance und Effizienz auf ein neues Niveau heben – ohne unverhältnismäßigen Aufwand.

Vorteile

Die Vorteile liegen auf der Hand:

- **Sicherheit:** Klare Rollen- und Rechte Modelle sowie Multi-Faktor-Authentifizierung erschweren unautorisierte Zugriffe.
- **Compliance:** IAM unterstützt Nachweise über Zugriffsrechte und Datenverarbeitung – essenziell für DSGVO, NIS2 und branchenspezifische Vorgaben.
- **Effizienz:** Automatisierte Prozesse wie Self-Service-Registrierung, Passwort-Reset oder rollenbasierte Zuweisungen entlasten die IT und senken Kosten.
- **Skalierbarkeit:** Neue Mitarbeitende, Partner oder Anwendungen lassen sich problemlos integrieren – ohne Insellösungen.
- **Vertrauen:** Kunden und Geschäftspartner erwarten sichere digitale Services. Ein IAM stärkt die Glaubwürdigkeit und Wettbewerbsfähigkeit.

Gerade für KMU ist die Cloud-Fähigkeit entscheidend: Sie reduziert den Betriebsaufwand, macht Lösungen schneller verfügbar und minimiert Investitionen in Hardware. Damit wird IAM auch für Unternehmen mit begrenzten Ressourcen praktikabel.

Auswahlkriterien für Entscheidungsträger

Die Auswahl einer IAM-Lösung ist komplex. Das Angebot reicht von internationalen Konzernen bis zu europäischen Spezialisten. Im Kontext digitaler Souveränität kann es sinnvoll sein, europäische Anbieter zu bevorzugen, die Datenschutz, Compliance und offene Standards in den Mittelpunkt stellen. Entscheidend ist, dass die Lösung zu den eigenen Geschäftsprozessen, Sicherheitsanforderungen und strategischen Zielen passt.



erhalten Unternehmen eine souveräne Basis für sichere Identitäten und effiziente Prozesse.

Handlungsempfehlungen für den Einstieg

Damit IAM zum Erfolg wird, sollten Entscheidungsträger:

1. **Strategisch denken:** IAM ist kein reines IT-Projekt, sondern betrifft Geschäftsmodelle, Kundenerlebnisse und Compliance.
2. **Pilotprojekte starten:** Erste Anwendungsfälle (z. B. Mitarbeiter-SSO) liefern schnelle Erfolge.
3. **Stakeholder einbinden:** Zusammenarbeit zwischen IT, Fachbereichen und Management ist entscheidend.
4. **Zero Trust umsetzen:** IAM als Fundament nutzen, um das „never trust, always verify“-Prinzip in der Praxis zu verankern.
5. **Regelmäßig prüfen:** Audits und kontinuierliche Anpassung sichern nachhaltigen Erfolg

Fazit

IAM als Fundament für Souveränität: Die politische Debatte um Digitale Souveränität ist wichtig – aber ohne praktische Umsetzung in den Unternehmen bleibt sie abstrakt. IAM macht Souveränität greifbar: Es gibt Organisationen jeder Größe die Kontrolle über Daten, Zugriffe und Identitäten zurück.

Für KMU bedeutet das: mehr Sicherheit, mehr Effizienz, mehr Wettbewerbsfähigkeit.

Für Europa bedeutet das: weniger Abhängigkeit, mehr Resilienz.

Ein modernes IAM für KMU muss heute mehr leisten als Benutzerzugänge zu verwalten. Es muss Sicherheit, Effizienz, Datenschutz und Benutzerfreundlichkeit vereinen – und dabei flexibel und skalierbar sein.

Digitale Souveränität wird zum Wettbewerbsfaktor: Wer Identitätsdaten in Europa hält, auf Standards wie OpenID Connect und OAuth setzt und auf Anbieter im europäischen Rechtsraum vertraut, behält langfristig die Kontrolle.

Wer auf IAM setzt, stärkt nicht nur seine Cyber-Resilienz, sondern auch die Digitale Souveränität Europas. ◀

Ein modernes IAM muss heute mehr können

Wichtige Kriterien sind:

1. **Klarheit über Anforderungen:** Welche Nutzergruppen und Use Cases sind entscheidend? Unternehmen sollten vorab analysieren, welche Nutzergruppen (Mitarbeiter, Kunden, Partner) eingebunden werden und welche Use Cases besonders wichtig sind. So lässt sich ein IAM-System gezielt auf die relevanten Geschäftsprozesse zuschneiden.
2. **Benutzerfreundlichkeit:** Sicherheit und Komfort müssen Hand in Hand gehen. Ein IAM-System sollte Sicherheit und Komfort verbinden. Features wie Self-Service-Registrierung, Passwort-Reset oder Social Login erhöhen die Akzeptanz. Komplexe Anmeldeprozesse hingegen führen zu Frustration und Workarounds.
3. **Flexibilität und Skalierbarkeit:** Die Lösung sollte mit dem Unternehmen wachsen. Gerade in wachsenden Organisationen muss IAM dynamisch auf neue Anforderungen reagieren können – sei es durch Integration neuer Anwendungen oder die Unterstützung zusätzlicher Authentifizierungsverfahren.
4. **Integration:** Offene Standards (OAuth 2.0, OpenID Connect) erleichtern den Anschluss an bestehende IT-Landschaften.

5. **Ob On-Premise-Systeme, Cloud-Services oder hybride Szenarien:** IAM muss reibungslos in vorhandene Infrastrukturen integriert werden. Offene Standards wie OAuth 2.0 oder OpenID Connect erleichtern dies. Moderne Anbieter setzen hier auf offene Schnittstellen und modulare Architekturen.

6. **Compliance und Auditfähigkeit:** DSGVO, ISO 27001, NIS2 müssen unterstützt werden. Ein gutes IAM-System sollte alle regulatorischen Anforderungen unterstützen und Nachvollziehbarkeit durch Protokollierung sowie Reporting sicherstellen.

7. **Kosten und Aufwand:** Neben Lizenzgebühren zählen auch Implementierungsaufwand, Schulungen und der laufende Betrieb. Ein Kosten-Nutzen-Abgleich ist daher unverzichtbar.

Analysten wie Gartner empfehlen, IAM nicht nur als technische Lösung, sondern als integralen Bestandteil der Unternehmensstrategie zu sehen.

Beispiele wie cidaas, eine Cloud-native IAM-Plattform aus Deutschland, zeigen, dass leistungsfähige Alternativen nicht aus Übersee stammen müssen. In Kombination mit cnips, einer Orchestrierungs- und Workflow-Plattform,

Handlungsempfehlungen für den Einstieg



Handlungsempfehlungen für den Einstieg in ein IAM-Projekt