THEMENBLATT **Digitale Identitäten**

Identity- und Access-Management

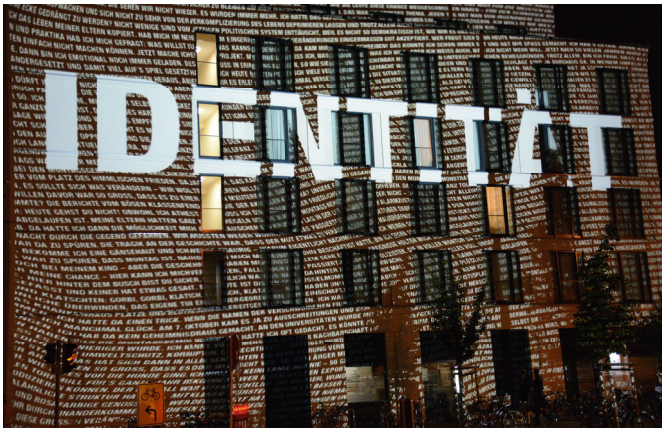
- ✓ Maßnahmen zur Einhaltung des Datenschutzes nach DSGVO
- ✓ Automatisierung sicherheitsrelevanter Vorgaben
- ✓ Anwendung starker digitaler Identitäten
- ✓ Transparenz über Authentifizierungen und Nutzerrechte

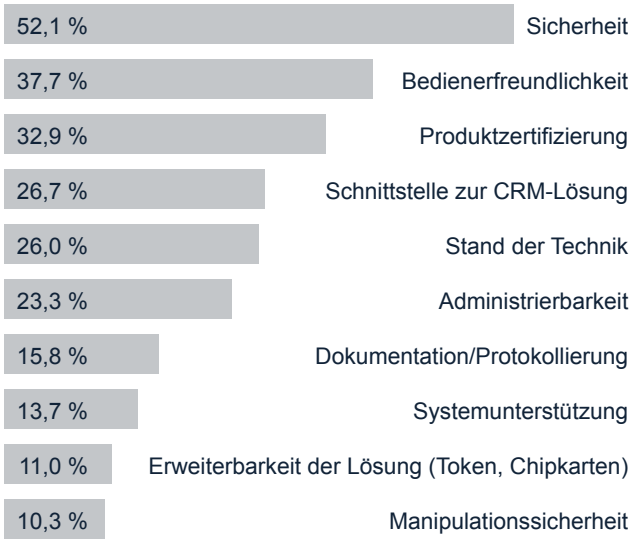
Die Herausforderung

Betrachtet man die Vielzahl der Cyber-Attacken etwas genauer stellt man fest, dass die meisten dieser Bedrohungen mit dem Missbrauch elektronischer Identitäten verknüpft sind. Entsprechende Studien und Untersuchungen weisen sogar eine Zunahme dieses Risikos aus. Zusätzlich verstärken gesetzliche Rahmenbedingungen wie die DSGVO und die wachsende Vernetzung von Maschinen, Sensoren, KI-Lösungen und Applikationen den Anspruch an die Sicherheit elektronischer Identitäten. Letztendlich bestimmen die Zuverlässigkeit und Vertrauenswürdigkeit digitaler Identitäten den Erfolg und die Akzeptanz vollständig digitaler Abläufe. Dies gilt nicht nur für den internen, sondern vor allem auch für den externen Datenaustausch. Bei der Bewältigung dieser Herausforderungen kommt einem zuverlässigen Identity- und Access-Management (IAM) eine zentrale Bedeutung zu.

IAM - Transparenz und Compliance

Identity- und Access-Management ist der zusammenfassende Begriff für alle Prozesse innerhalb und gegebenenfalls außerhalb einer Organisation, die sich mit der Verwaltung und Pflege von Benutzerkonten und Ressourcen im Netzwerk befassen, einschließlich der Berechtigungsverwaltung für Benutzer auf Anwendungen und Systeme. Primär geht es um sinnvolle Verknüpfung von Identitäten mit den entsprechenden Zugriffsberechtigungen.





Auswahlkriterien einer Authentifizierungslösung zur Absicherung digitaler Geschäftsprozesse
(IDG-Studie Identity- und Access-Management 2017)

Ein Unternehmen mit mehreren hundert oder gar tausenden Mitarbeitern und/oder Kunden muss eine Unmenge personenbezogener Daten erheben und absolut sicher verwalten. Diese Daten dienen einerseits der sicheren Authentifizierung von Personen, andererseits werden jeder dieser Personen innerhalb komplexer Regelwerke individuelle Rechte und Rollen zugewiesen.
Hinsichtlich der strengen Anforderungen und der verbindlichen gesetzlichen Regelungen ist die Einhaltung von Compliance priorisiert. Im Rahmen von IAM bedeutet Compliance explizit die Berücksichtigung aller Regularien im Bereich von Benutzern und deren IT-Zugriffrechten. Die Einhaltung der Compliance kann durch regelmäßige Audits überprüft werden. Dabei werden die Ist-Zustände in den Systemen und Datenbanken mit dem durch die gesetzlichen Vorgaben und eigenen Regularien definierten Soll Zustand verglichen. Entspricht der Ist-Zustand dem Soll, ist die Compliance erfüllt.

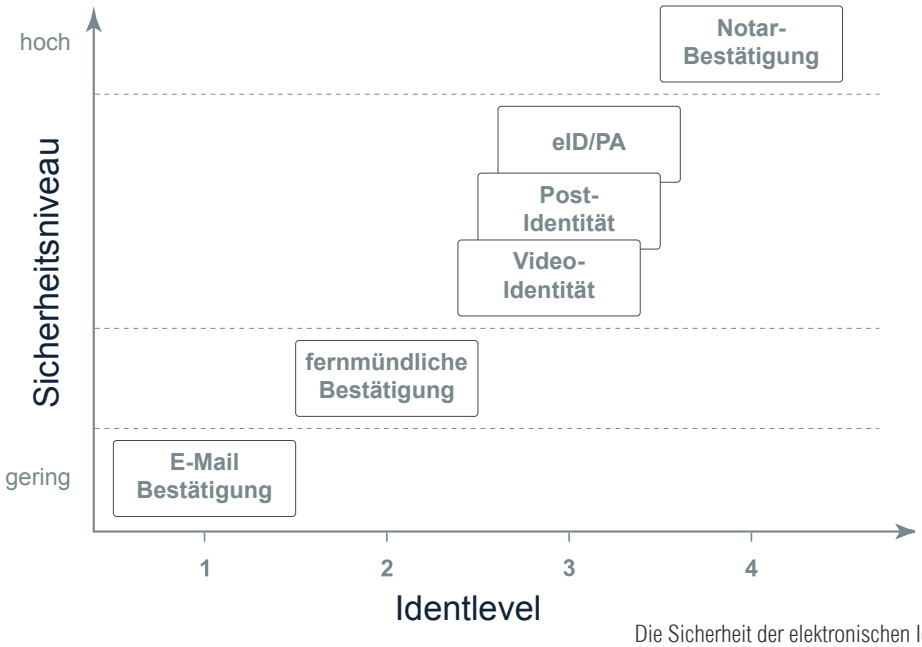
THEMENBLATT **Digitale Identitäten**

Identity- und Access-Management

IAM – Die Praxis

Immer häufiger nutzen Unternehmen und Behörden ein zentrales IAM, in welchem neben eigenen Mitarbeitern auch Lieferanten, externe Dienstleister und Kunden geführt werden. Die Anzahl der Geschäftsmodelle und -prozesse, die direkt über das Internet bzw. die Cloud abgewickelt werden, nimmt stetig zu.

Analog gilt dies auch in der Außenbeziehung bei wachsender Öffnung von Abläufen. Hier bedarf es Festlegungen, welche elektronischen Identitäten an welcher Stelle akzeptiert werden. Aber auch diese Rollen unterliegen Änderungen und bedürfen einer ständigen Pflege.



Die Sicherheit der elektronischen Identität wird durch die Art und Weise der Identitätsbestätigung bestimmt.

Daher müssen die IAM-Systeme jetzt auch verstärkt diese externen Partner und Kunden integrieren. Diese Dienstleister und Konsumenten sollten sich registrieren können. Sie benötigen Zugriff auf Systeme sowie Benutzerkonten und deren Zugriffsrechte sind zu verwalten.

Damit ist das Thema IAM kein reines IT-Thema mehr, sondern orientiert sich bei wachsender Öffnung auch an den Kundenbedürfnissen. In Sachen Identitäts-Management heißt das: Verfahren für Single-Sign-On oder Multi-Faktor-Authentifizierung müssen einfach sein! Erfahrungsgemäß steigt die Gefahr des Scheiterns von IAM-Projekten, wenn man separate Hardware benötigt. Deshalb kommen in Zukunft bei der Authentisierung sicherlich auch verstärkt biometrische Verfahren zum Einsatz.

Bei der Auswahl eines IAM-Tools müssen diese Perspektiven und die Möglichkeit der Skalierung gegeben sein, denn je größer die Firma, desto mehr Bereiche sind betroffen. Ein modularer Aufbau des IAM-Tools ist also angeraten. Im Idealfall lassen sich aus der Rolle des einzelnen Mitarbeiters alle Zugriffsrechte eindeutig ableiten.

So sind z. B. Geldinstitute gemäß der neuen EU-Zahlungsdienstrichtlinie PSD II gezwungen, sich zu öffnen. In anderen Branchen geht es für viele Unternehmen jetzt darum, Internet of Things (IoT) und Automation umzusetzen. Bei Verwaltungen stehen vollständig digitale Bürgerservices oben auf der Agenda.

Kontakt

procilon GROUP
Leipziger Straße 110
04425 Taucha

+49 342 98 48 78-31
anfrage@procilon.de
www.procilon.de