Identity Governance and Administration

Modernisieren mit Identity Security

Digitale Identitäten werden immer zentraler. Bei der Implementierung gibt es Herausforderungen. SECURIX gewährt Einblick in die Praxis und zeigt auf, wie Projekterfolg nachhaltig sichergestellt wird.

→ VON GABRIEL WEPFER

DER AUTOR

Gabriel Wepfer
ist Head of Sales bei SECURIX.
→ www.securix.swiss

Die Pandemiejahre 2020 und 2021 haben die «Cloud first»-Strategie wieder in den Fokus vieler Unternehmen gerückt. Kein CTO oder CISO kam und kommt an diesem Thema vorbei, dies konstatiert der Marktforscher Gartner regelmässig. Unternehmen wollen durch Nutzung der Cloud effizienter werden, die Customer Experience verbessern und sensible Daten besser schützen. Digitale Identitäten und deren Zugriffsberechtigungen erhalten dadurch einen zentralen Stellenwert. Die wichtigsten Herausforderungen beim Etablieren digitaler Identitäten und sicherer Prozesse in Zusammenhang mit Zugriffsberechtigungen zeigen wir Ihnen hier auf.

IAM-DISZIPLINEN DIFFERENZIEREN

Viele Marketingunterlagen sprechen heute immer noch allgemein von IAM, was die Unterscheidung der einzelnen Disziplinen erschwert. Innerhalb des IAM haben sich die Begriffe IGA, CIAM und PAM etabliert:

- Identity Governance and Administration (IGA): Verwaltung von Identitäten, Accounts und Zugriffsberechtigungen von internen und externen Mitarbeitenden sowie Service Accounts.
- Customer Identity And Access Management (CIAM)/ Third Party Access Management: Verwaltung von Kundenkonten, Lieferanten- und Partnerportalen im Kontext von Registrierung, Login und Stammdatenmanagement.
- Privileged Access Management (PAM): Verwaltung von internen und externen Accounts mit privilegierten Zugriffen, wie z. B. Systemadministratoren.

Im Folgenden fokussieren wir uns auf die Disziplin der Identity Governance and Administration (IGA). Damit die Unterscheidung von Anfang an gelingt, ist es empfehlenswert, bereits in frühen Phasen auf spezialisiertes Wissen zurückzugreifen, sei dies durch Weiterbildung und/oder unabhängige Beratung.

IAM ALS ORGANISATIONSPROJEKT

Projekte rund um digitale Identitäten und Zugriffsberechtigungen haben starken Organisations- und Prozesscharakter. Es ist daher essenziell, dass das Projekt vom Management gestützt und gefördert wird und darüber hinaus eine breite Akzeptanz und aktive Partizipation der betroffenen Stakeholder erfährt. Nebst Technik und Informationssicherheit sollten deshalb das HR und der Service Desk von Anfang an ins Projekt involviert werden. Nur so gelingt es, bestehende Businessprozesse zu hinterfragen und gegebenenfalls zu modernisieren.

STANDARDS NUTZEN

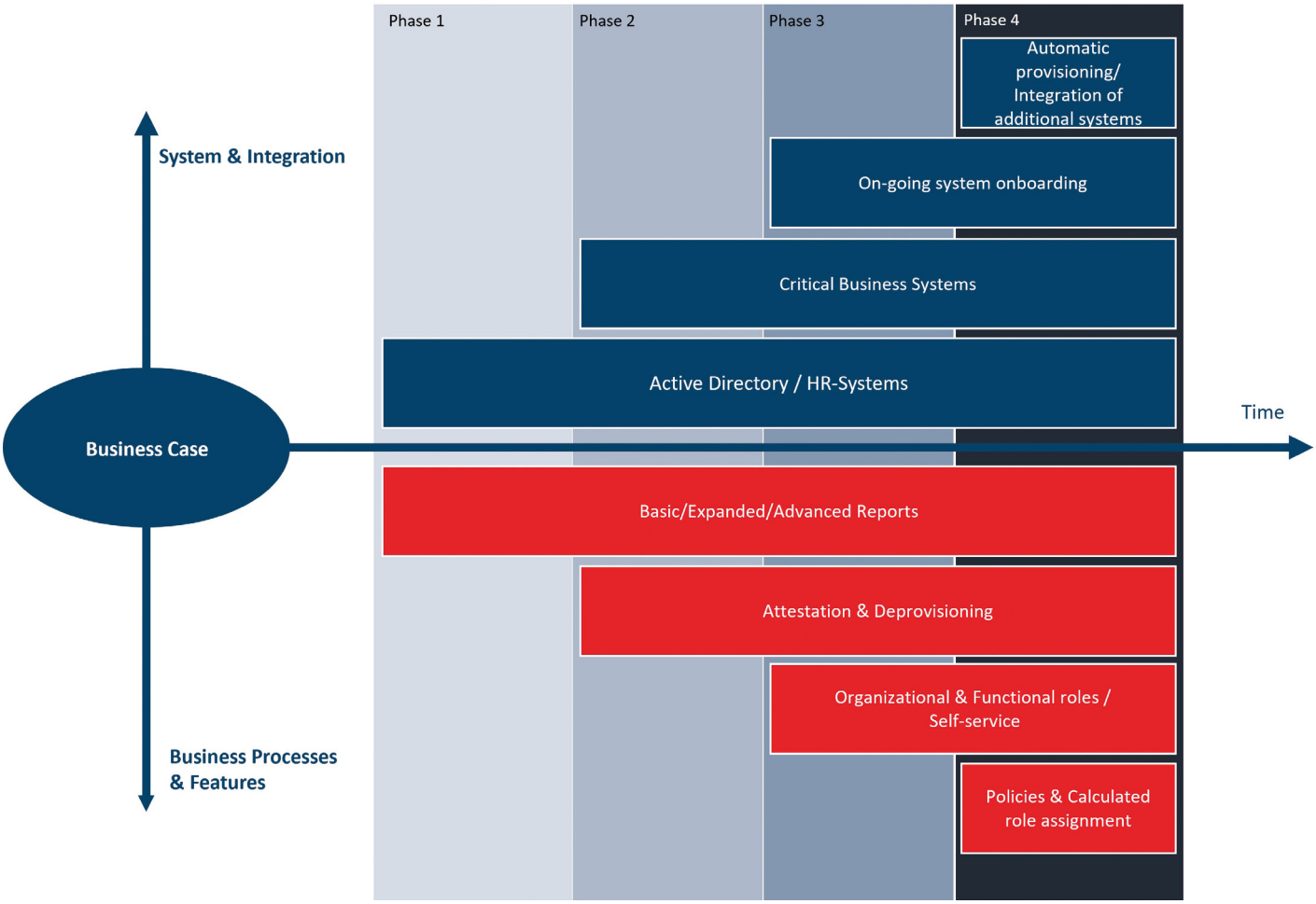
Gängige IGA-Lösungen bieten oft die Möglichkeit, individuelle Anforderungen sehr detailliert nach Kundenwunsch umzusetzen. Hinsichtlich Kosten-Nutzen-Verhältnis ist dieses Vorgehen jedoch bedenklich und wird von Experten nicht empfohlen. Beraterinnen und Berater legen heute den Fokus viel mehr darauf, die bestehenden Businessprozesse gemeinsam mit den Stakeholdern zu analysieren – immer mit dem Ziel, die eingesetzte IGA-Technologie zu konfigurieren, anstatt mit Entwicklungsaufwand zu customizen. Standardisierung anstatt Individualisierung ist hier das Motto.

So gelingt es, cloudbasierte SaaS-Lösungen nachhaltig und vollumfänglich einzusetzen, um sich damit vor riskanten Upgradeprojekten und aufwändigen Zusatzentwicklungen zu schützen und IT-Budgets zu schonen.

TECHNOLOGIE ALS BUSINESSMEHRWERT

Ein zentraler Erfolgsfaktor in der Identity Security ist es, die Anforderungen aus dem Business und der Technik zu verstehen und einen Konsens mit der Technologie zu finden. Das Sprichwort «a fool with a tool is still a fool» trifft es sehr gut. Auch die ausgefeilteste Technologie kann Unternehmen weder sicherer noch effizienter machen, wenn

Bild: Securix Implementation Framework



IGA-Projektphasen staffeln, um damit schnelleren Projekterfolg zu erzielen

diese nicht im Detail verstanden worden ist und auf die konkreten Anforderungen gemappt werden kann.

Es ist empfehlenswert, auch innerhalb von bereits laufenden Projekten Proof of Concepts mit einem definierten Prozess durchzuführen, um die Machbarkeit und den Nutzen vorab zu prüfen.

DATENQUALITÄT KRITISCH

IGA-Lösungen unterstützen den gesamten Lebenszyklus (Eintritt, Übertritt, Austritt) von Identitäten und beinhalten meist hoch entwickelte Mechanismen zur automatischen Rechtevergabe. Mittels Policies respektive Regeln wird definiert, aufgrund welcher Kriterien automatisch bestimmte Rechte in ein Zielsystem (zum Beispiel Active Directory) provisioniert werden sollen. Beispielsweise können aufgrund der Zugehörigkeit des Mitarbeiters zu einer Organisationseinheit bestimmte organisationsabhängige Rechte automatisch vergeben werden.

Ziel einer IGA-Lösung ist die zentrale Verwaltung von Identitäten und deren Rechte, die Sicherstellung der Compliance und die Schaffung von mehr Sicherheit im Kontext von Identitäten und Zugriffsberechtigungen. Ein weiteres wichtiges Ziel ist die Erhöhung der Effizienz bei der Vergabe von Berechtigungen, diese kann nur über entsprechende Automatismen erreicht werden.

Die Datenqualität in IGA-Lösungen ist daher von zentraler Bedeutung. Wenn man von ihren Vorteilen profitieren will, müssen Daten im Quellsystem gepflegt werden. Nur dann funktioniert der installierte Automatismus.

PHASENWEISE EINFÜHRUNG

Wer bereits IGA-Lösungen konzipiert und eingeführt hat, weiss, dass ein solches Projekt, ganz unabhängig von der gewählten Technologie, sehr schnell an Komplexität zunimmt. Diese Komplexität ist ein wichtiger Grund, weshalb IGA-Projekte oftmals nicht als Success Story, sondern viel häufiger als never-ending Story bekannt werden. Es ist daher unabdingbar, den Weg der kleinen Schritte zu wählen und IAM phasenweise zu implementieren und weiterzuentwickeln. Agile Projektmethoden unterstützen die Beteiligten dabei, die Durchlaufzeiten bei der Umsetzung von Lieferobjekten zu verkürzen, somit schneller Resultate zu erzeugen und den Erfüllungsgrad kontinuierlich zu bewerten.

Damit dies möglich wird, muss im Vornhinein im gesamten Projektumfeld ein Framework verstanden und etabliert werden. In der Abbildung oben ist ein grafisches Beispiel zu sehen, wie wir das bei unseren Kunden einsetzen.

FAZIT

Identity Security ist kein einmaliges Projekt mit definiertem Anfang und Ende, sondern eine fortlaufende Aufgabe für das gesamte Unternehmen. Dabei müssen verschiedene Geschäftsbereiche eng zusammenarbeiten, was klare Verantwortlichkeiten erfordert. Auch ist eine strukturierte und schrittweise Umsetzung nach Prioritäten wichtig. Das ermöglicht die sukzessive Anpassung von Richtlinien und Abläufen sowie einen systematischen Erfahrungs- und Lernprozess. ←