IAM Managed Services von iC Consult

Wie Unternehmen auf vielfältige Weise von IAM als Managed Services profitieren

Der traditionelle Perimeter löst sich seit Jahren zunehmend auf, und so rücken die Security-Architekten der Unternehmen verstärkt starke Identitäten und klare Zugriffsregelungen als erste Verteidigungslinie in den Fokus: Ein robustes Identity & Access Management (IAM) ist heute eine tragende Säule moderner Netzwerk- und Cybersecurity-Konzepte, nicht zuletzt, weil viele innovative Ansätze wie Zero Trust und Secure Access Service Edge (SASE) – die Analysten und Hersteller übereinstimmend als zukunftsweisende Modelle für ganzheitliche Netzwerk- und Security-Architekturen sehen – ebenfalls einen klaren Fokus auf IAM setzen. Mit Blick auf die enge Verzahnung und die hohe Integrationstiefe des Identity-Managements mit den übrigen Komponenten der Unternehmens-IT entwickelt sich die Verwaltung der Identitäten für viele IT-Teams immer mehr zur Herausforderung. Das Outsourcing von IAM an spezialisierte Managed Service Provider und Systemintegratoren wird zur attraktiven Alternative, die neben der Entlastung eigener Teams eine Reihe weiterer wertvoller Vorteile bietet.

Das vorliegende Whitepaper geht zunächst auf die wichtigsten Treiber und die aktuellen Challenges im Bereich Identity & Access Management ein. Anschließend zeigen wir auf, wie sich diese zum Teil enormen Herausforderungen mit Unterstützung eines spezialisierten Dienstleisters meistern lassen. Managed Services sichern neben signifikanten Einsparpotenzialen auch nachhaltige Entlastung für das Team – und schaffen so wertvolle finanzielle und zeitliche Freiräume für eigene Innovationsprojekte. Bei der Wahl eines Managed Service Providers oder eines Systemintegrators gilt es jedoch, eine Reihe wichtiger Aspekte zu beachten, um die Weichen für ein nachhaltiges und zeitgemäßes Management der Identitäten zu stellen.

Managed Services liefern signifikante Einsparpotenziale und können Teams nachhaltig entlasten.

1. Einführung: Die Driver im Bereich Identity & Access Management

Der Markt für das Identity & Access Management wächst rasant – und wird nach einhelliger Meinung der Analysten auch in den kommenden Jahren signifikant zulegen. Dies liegt vorrangig an folgenden wichtigen Treibern:

Security ist zweifellos der wichtigste Treiber, der viele Unternehmen dazu bewegt, ihr IAM kritisch auf den Prüfstand zu stellen: In Zeiten weitverzweigter Netzwerke mit einer Vielzahl dezentraler Endpunkte werden Identitäten immer mehr zum neuen Perimeter – und damit zum zentralen Kontrollpunkt für die Zugriffe auf alle digitalen Assets.

Diese Schlüsselrolle liefert auch das Fundament für moderne Security- und Netzwerk-Konzepte wie Zero Trust und SASE, die branchenweit als IT-Infrastrukturmodelle der Zukunft gelten. Auf den Punkt gebracht: Das IAM stellt sicher, dass stets nur die richtigen Identitäten mit minimalem Zugriffsprivileg auf die tatsächlich benötigten Ressourcen zugreifen können – und reduziert damit maximal die Angriffsfläche.

Intern klar definierte Vorgaben und Richtlinien für Berechtigungen vermeiden Konflikte und Rückfragen durch Mitarbeitende.

Dies erfordert allerdings eine Vergabe granularer Zugriffsrechte, die für viele SOCs (Security Operation Centers) unter unternehmenspolitischen Gesichtspunkten alles andere als einfach ist: Wenn jedem Mitarbeitenden nur die geringsten Rechte eingeräumt werden, sind Konflikte und Rückfragen vorprogrammiert. Dementsprechend wichtig ist es, intern klare Vorgaben und Richtlinien für die Berechtigungen zu definieren und diese natürlich mit der Vielzahl externer Anforderungen und Gesetze (z.B. GLBA, PSD2) sowie den branchenspezifischen Vorgaben in Einklang zu bringen. Der zweite große Treiber im Bereich IAM ist daher die **Compliance.** Moderne IAM-Plattformen sind bei der Sicherstellung und Dokumentation der Einhaltung regulatorischer Vorgaben eine wertvolle Hilfe – vorausgesetzt, es wurden systematische Prozesse für die Umsetzung etabliert. Mit den richtigen Tools und Prozessen lassen sich interne oder externe Policies zudem gut automatisieren, um den IT-Verwaltungsaufwand zu minimieren.

Automatisierung spielt in Zeiten der dynamischen Digitalisierung, der immer komplexeren Systeme und der notorisch unterbesetzten IT-Abteilungen generell eine entscheidende Rolle. Auch, da die Anzahl und die Arten von Identitäten tendenziell immer weiter zunehmen: Neben klassischen Mitarbeiteraccounts managt ein modernes IAM heute auch die Identitäten von Kunden, Partnern und Lieferanten – und im Zuge der IoT-Migration und vernetzter Geräte dürfte diese Zahl auch in den kommenden Jahren weiter rasant ansteigen. Diese Identitäten können Unternehmen ohne einen hohen Automatisierungsgrad manuell kaum mehr wirtschaftlich verwalten.

Zwei weitere, eng mit der Automatisierung verwandte IAM-Treiber sind **Agilität und Servicebereitstellung.** Unternehmen sollten sich heute darauf konzentrieren, ihre individuellen Stärken auszuspielen und ihre konkreten USPs weiterzuentwickeln – und nicht wertvolle Ressourcen darauf verwenden, die Zugriffsrechte von Kunden oder Mitarbeitenden zu steuern. Agile On- und Offboarding-Prozesse und Provisionierungen bieten auch handfeste wirtschaftliche Vorteile: Wenn die Mitarbeitenden nicht warten müssen, bis sie notwendige Zugangsrechte erhalten, können sie Kunden schneller und besser bedienen – und wenn sie sich beispielsweise dank Single-Sign-On nicht bei jeder Anwendung neu anmelden müssen, können sie ihre Arbeit schneller erledigen.

Der letzte Treiber ist **passwortlose Authentifizierung:** Das Passwort als Authentifizierungsfaktor genügt den heutigen Security-Anforderungen schlichtweg nicht mehr. Immer höhere Rechenleistung, auch mit Blick auf die enormen Fortschritte im Quantencomputing, führt dazu, dass Angreifer auch lange Passwörter in immer kürzerer Zeit entschlüsseln können. Dies gilt umso mehr, da Passwörter oft vergessen, nicht regelmäßig gewechselt, nicht sicher genug aufbewahrt und nicht für eine agile Servicebereitstellung optimiert werden. Das klassische Passwort wird also immer mehr zum Risikofaktor, und verursacht zudem hohe Kosten im Management und im Support. Passwortlose Multi-Faktor-Authentifizierungsverfahren mit starken biometrischen Komponenten – wie sie von vielen IAM-Plattformen unterstützt werden – sind heute der State-of-the-Art.

2. Herausforderungen für Unternehmen

Betrachtet man neben den Treibern auch die Pain Points, vor denen Unternehmen beim Management der digitalen Identitäten und Zugriffsrechte stehen, zeichnen sich hier ebenfalls einige übergreifende Trends ab:

Steigende Sicherheitsanforderungen:
IT-Security ist heute nicht nur ein entscheidender Wettbewerbsfaktor, sondern auch eine tragende Säule jedes Business Continuity Konzepts – immerhin nimmt die Zahl und Wucht der Cyber-Attacken kontinuierlich zu. Die Krisen der vergangenen Jahre haben das ihre dazu beigetragen, die Lage zu verschärfen: Zunächst zwang die Corona-Pandemie Unternehmen weltweit dazu, Beschäftigte ins Homeoffice zu schicken. Unternehmensnetzwerke mussten also rasch geöffnet und dezentralisiert werden, um den neuen Anforderungen Rechnung zu tragen. Unmittelbar im Anschluss lies der Ukraine-Krieg die Zahl der Cyber-Vorfälle durch staatlich motivierte Akteure explodieren. Die zunehmende ideologische Spaltung zwischen autokratischen und demokratischen Staaten wird auch künftig zu einer konstanten Zunahme der Angriffe führen – und das Risiko für Unternehmen weiter steigern. Hinzu kommt: Nachdem sich Identitäten mehr und mehr zum neuen Perimeter der Unternehmen entwickeln, stehen sie auch zunehmend im Visier der Angreifer, etwa wenn Hacker versuchen, Angestellte durch Social Engineering zum Einlass ins Netzwerk zu bewegen.

Steigender Umfang der IAM-Projekte:
IAM ist somit in vielen Unternehmen heute die wichtige erste Verteidigungslinie vor Bedrohungen aller Art, und fällt daher auf den ersten Blick typischerweise in den Verantwortungsbereich des IT-Security-Teams. Bei der Umsetzung der Projekte zeigt sich aber schnell, dass das Management der Identitäten auf unterschiedlichste weitere Bereiche und Stakeholder des Unternehmens ausstrahlt, und als zentrale Schnittstelle nahezu alle Systeme, Technologien, Endpunkte und Authentifikatoren zusammenführen muss. Das Thema IAM spielt beispielsweise also auch im Bereich Human Resources eine wichtige Rolle, wo es gilt, ausscheidende Mitarbeiter aus den Systemen zu entfernen und neue Mitarbeiter einzupflegen – ein Vorgang, der eng mit der Vergabe (oder, oft noch wichtiger, der Aufhebung!) von Rollen und Berechtigungen einher geht. Nur so lässt sich sicherstellen, dass neue Mitarbeiter vom ersten Tag an auf benötigte Systeme und Anwendungen zugreifen können, und ausgeschiedene Mitarbeiter ebenso zeitnah ihren Zugang verlieren. Somit muss die Personalabteilung eng mit den Bereichen IT, Security, Compliance und Governance zusammenarbeiten, um die Rollenvergabe mit allen internen und externen Anforderungen in Einklang zu bringen. Ein zweites Beispiel für die hohe Integrationstiefe einer IAM-Lösung ist die Anwendungsentwicklung, deren Aufgabe es ist, alle Systeme und Anwendungen über komfortable und sichere Konnektoren mit IAM-Systemen zu verbinden. Auch hier entwickeln sich im Projektverlauf erfahrungsgemäß hochkomplexe Abhängigkeiten, die sich mit jeder beteiligten Business Unit und jedem involvierten Stakeholder vervielfachen.

IAM muss als zentrale Schnittstelle nahezu alle Systeme, Technologien, Endpunkte und Authentifikatoren eines Unternehmens zusammenführen.

Bildlich gesprochen, wird das Identity & Access Management schnell zu einem Eisberg: Zehn Prozent des Projekts befinden sich weithin sichtbar über dem Wasser: die Login-Interfaces, die Benutzernamen und die Authentifizierungsmethoden, mit denen jeder Nutzer zu tun hat. Doch der überwiegende Teil der Lösung, die restlichen 90 Prozent, schwimmt unter der Oberfläche und ist auf den ersten Blick nicht zu sehen.

Verwaltungs- und Personalaufwand:
Das schnelle – mitunter sogar exponentielle – Wachstum der IAM-Lösung führt dazu, dass die Gesamtkomplexität des Identitäts- und Zugriffsmanagements immer weiter zunimmt. Die hohe Integrationstiefe des Identity & Access Managements hält Unternehmen jedoch oft davon ab, grundlegende Änderungen oder Modernisierungen vorzunehmen, um den Verwaltungsaufwand zum Beispiel mittels Automatisierung zu verringern. Stattdessen wird den IT-Abteilungen immer mehr abverlangt.

Nicht selten führt dies zu einer Überforderung der IT-Teams. Doch in der aktuellen Arbeitsmarktlage ist es schwer, fachkundige IT-Kräfte zu finden. Noch schwieriger wird es für Unternehmen, die nicht nur Personal für die IAM-Verwaltung suchen, sondern die eigene IAM-Architektur grundlegend modernisieren möchten. Dies gilt umso mehr, da es sich bei der Einführung eines neuen IAM-Programms um ein klassisches Einmal-Projekt handelt – in der Regel also inhouse keinerlei Erfahrungen bestehen, auf die man aufsetzen könnte, und wo es noch schwerer ist, zusätzliche Experten zum Team hinzuzuziehen. Ein weiterer Faktor ist der heterogene Personalaufwand über den fortlaufenden Prozessverlauf: Am Anfang stehen die Entwicklung und Implementierung der IAM-Lösung. Dies ist ein enorm arbeitsaufwändiger Schritt, der viel Ressourcen und Personal bindet. Doch steht das Gerüst erst einmal, und sind die wiederkehrenden Verwaltungsprozesse zu einem hohen Grad automatisiert, ist der Personalaufwand wesentlich geringer. Dieses Personalungleichgewicht zwischen der Entwicklungs- und Implementierungsphase zum Regelbetrieb erzeugt eine Unwucht, derer sich das Unternehmen bewusst sein muss.

Fehlende Marktkenntnis:
Das geringe Angebot an qualifizierten IAM-Fachkräften ist nur ein Teil des Problems. Verschärfend kommt hinzu, dass die vorhandenen Inhouse-Teams häufig nur am Rande mit dem aktuellen IAM-Angebot vertraut sind. Doch genau hier braucht es tiefes Expertenwissen: Auf dem Markt tummeln sich unzählige Anbieter mit zum Teil ganzheitlichen Lösungsansätzen oder speziellen Insellösungen. Bei der Wahl des richtigen Anbieters gilt es, die Spezifikationen der unterschiedlichen Produkte neutral mit der eigenen Lösungslandschaft und dem angestrebten Soll-Zustand abzugleichen – und auf Basis vieler objektiver Kriterien eine fundierte Entscheidung zu treffen. Dies ist nur für die wenigsten und am besten ausgestatteten internen Abteilungen machbar. An dieser Stelle zeichnet sich bereits deutlich ab, dass das Hinzuziehen eines externen Spezialisten enormen Mehrwert bietet.

Unternehmen sind mit zahlreichen Herausforderungen rund um IAM konfrontiert – einen externen Spezialisten hinzuzuziehen kann enormen Mehrwert bieten.

3. Vorteile von Managed Services

Die steigenden Herausforderungen bei der Implementierung und Verwaltung moderner IAM-Lösungen veranlassen viele Unternehmen dazu, in diesem Bereich auf externe Dienstleister zu setzen. Spezialisierte Systemintegratoren und Managed Service Providern erschließen das volle Potenzial moderner IAM-Technologien – und tragen nachhaltig zur Robustheit und zur Usability des Identity & Access Managements bei.

Herstellerneutrales Knowhow
Externe, unabhängige IAM-Dienstleister verfügen über kundige Experten, eine breite Marktkenntnis und umfassendes Knowhow in allen Bereichen der Identitäts- und Zugriffsverwaltung. Als Spezialisten sind sie mit den Lösungen der führenden Hersteller bestens vertraut, kennen die individuellen Vorteile der Produkte und können die Kompatibilität mit Bestandssystemen optimal einschätzen. Aufsetzend auf etablierten Best-Practices

und Integrationen helfen sie dabei, eine nahtlose Integration im Zeit- und Kostenrahmen sicherzustellen. Und: Ihre umfangreiche Projekterfahrung und die eingespielten Prozesse verkürzen die Zeit zum Go-Live und minimieren den späteren Verwaltungsaufwand.

Standardisierte Vorgänge und kurze Reaktionszeit
Nach oft Hunderten erfolgreicher Projekte verfügen IAM-Dienstleister über ein standardisiertes Vorgehen und etablierte Prozesse, die sich in der Praxis in verschiedensten Szenarien bewährt haben. Von der Planung und Moderation betrieblicher Prozesse über die Implementierung einer neuen IAM-Lösung und die Modernisierung des Funktionsumfangs bis zur Integration neuer Anwendungen spart dies enorme Ressourcen.

Die standardisierten Abläufe garantieren zudem kurze Reaktionszeiten – und helfen so, ungeplante Ausfälle proaktiv zu verhindern oder zumindest wesentlich schneller zu beheben, bevor hohe finanziellen Schäden oder teure Compliance-Verstöße entstehen. Ob 8/5 oder 24/7 – vertraglich festgelegte, maßgeschneiderte Service- und Support-Modelle garantieren schnelle Unterstützung durch den Managed Service Provider. Dank robuster Patch- und Updateprozesse sind die Systeme zudem jederzeit auf dem neuesten Stand und bieten maximale Sicherheit und Verfügbarkeit.

Schlüsselfertige Integrationen
Nirgends wird der hohe Komplexitätsgrad einer unternehmensweiten IAM-Lösung so deutlich, wie bei der Arbeit mit großen, global agierenden Konzernen: Diese Organisationen haben häufig Tausende von Anwendungen im Einsatz, die es alle nahtlos in das IAM zu integrieren gilt. Dabei kann je nach Größe des Teams schon eine einzige neue Integration mehrere Tage in Anspruch nehmen. Ein Dienstleister mit einem breiten Arsenal schlüsselfertiger Integrationen kann den Zeit-, Personal- und Kosten-Aufwand signifikant verringern – und die Time-to-Market spürbar verkürzen.

OpEx statt CapEx
Hinzu kommen handfeste wirtschaftliche Argumente: Wer sich für das Outsourcing seines Identitätsmanagements entscheidet, überführt hohe Einmal-Investments in überschaubare monatliche Betriebsausgaben. Das schont das Eigenkapital, schafft Freiräume für weitere Investitionen, senkt die TCO und stellt die Weichen für einen raschen Return-on-Investment.

4. Professionelle Systemintegration und Managed Services

Bei der Auswahl eines Systemintegrators und Managed Service Providers für ihr IAM-Projekt sollten Unternehmen folgende Aspekte berücksichtigen:

Unabhängige Beratung, agile IAM-Entwicklung sowie flexible Ansätze sollten bei der Auswahl eines Managed Service Providers berücksichtigt werden.

Unabhängige Beratung
Die Auswahl einer IAM-Lösung (ob komplett oder in Teilbereichen) erfolgt meist nicht ganz unvoreingenommen, sondern hängt unter anderem vom vorhandenen Tech-Stack und von den guten wie schlechten Erfahrungen mit einzelnen Herstellern ab, die interne Teams oder Verantwortliche gemacht haben. Infolgedessen fällt die Wahl leider nicht immer auf das optimale Produkt. Spezialisierte Dienstleister wie iC Consult gehen Ihr Projekt unbelastet und herstellerunabhängig an und können in der Regel besser einschätzen, welche Produkte das gewünschte Ergebnis für den jeweiligen Use Case erbringen werden.

→ Achten Sie bei der Wahl des Dienstleisters auf ein breites Partnerportfolio mit den führenden Herstellern und machen Sie sich mit den Referenzen vertraut.

Agile IAM-Entwicklung
Viele MSP-Ansätze fokussieren vorrangig auf die betriebliche und damit weniger auf die funktionale Seite einer IAM-Lösung. Technologische Optimierungen kommen dabei oft zu kurz, was dazu führt, dass der IAM-Service über kurz oder lang nicht mehr optimal in die moderne IT-Landschaft passt. Unternehmen sollten daher darauf achten, dass der MSP-Vertrag auch zeitnahe, funktionale Optimierungen vorsieht, um neue Angebote der SaaS-Anbieter in die Organisation einbringen zu können. Je agiler ein MSP ist, desto besser kann er die Lücke zwischen dem klassischen Managed Services und dem, was Unternehmen in Zeiten immer kürzerer Entwicklungszyklen tatsächlich brauchen, überbrücken, um einen handfesten Mehrwert zu bieten.

→ Achten Sie neben der traditionellen Verwaltung Ihrer IAM-Lösung auf die agile und zeitgemäße Weiterentwicklung der Systeme.

Flexible Ansätze
Ihr Identity & Access Management wird sich kontinuierlich an neue Anforderungen anpassen müssen – und sollte Ihrem internen Team auch die Möglichkeit bieten, schnell auf die Wünsche der Anwender zu reagieren. Unternehmen sollten daher bei der Wahl eines Systemintegrators oder Managed Service Providers auf flexible Deployment-Methoden achten, um sich ein hohes Maß an Flexibilität und Skalierbarkeit zu bewahren und die Wettbewerbsfähigkeit zu sichern. Self-Services, Accelerators und Factory Patterns unterstützen schnelle Änderungen am IAM-Ökosystem und können entscheidend sein.

→ Achten Sie auf fortschrittliche Methoden wie Self-Services, Accelerators und Factory Patterns und bewahren Sie sich die notwendige Flexibilität für Ihre Lösung.

5. IAM Managed Services von iC Consult

Als weltweit größter herstellerunabhängiger IAM-Systemintegrator verfügen wir über hunderte renommierte Spezialisten, die sowohl den IAM-Markt als auch die einzelnen Lösungen der Best-of-Breed-Hersteller bis ins Detail kennen. Als herstellerunabhängiges Beratungs- und Integrationsunternehmen gehen wir Ihre Projekte also kundenorientiert, nachhaltig und ohne Scheuklappen an – und finden garantiert die perfekte IAM-Lösung für Ihr Unternehmen.

Die Vorteile der IAM Managed Services von iC Consult auf einem Blick:

- Renommierte IAM-Experten an Ihrer Seite – von der Planung bis zur Einführung Ihres gewünschten IDaaS-Produkts
- Dedizierter Service Delivery Manager für eine nachhaltige Service-Erbringung
- Nahtlose Integration von Best-Of-Breed-Komponenten
- Proaktive und zeitnahe Einbindung technologischer Innovationen
- 24/7 Support und Operations, produktseitig sowie bei allen Deployment-Fragen
- Monatlich planbare Kosten statt hohe Einmalinvestitionen
- Höchste Sicherheit und Service-Qualität
- Auch für international tätige Unternehmen mit anspruchsvollen, komplexen Use Cases
- Weltweit verfügbar, inklusive China
- Agile und automatisierte Lösungen – durch den Einsatz von DevOps, Infrastructure as Code & Configuration as Code
- Lückenloses Reporting und durchgängige Compliance
- Flexibilität und Skalierbarkeit

Wenn Sie mehr über unsere IAM Managed Services erfahren möchten, stehen Ihnen auf www.ic-consult.com umfangreiche Informationen zur Verfügung.

Das sind wir

iC Consult ist der führende unabhängige Berater, Systemintegrator und Managed Services Anbieter für Identity & Access Management (IAM) mit mehr als 800 Mitarbeitenden weltweit.

Mit unserer Hingabe zu Exzellenz und Innovation und den besten Technologien im IAM-Umfeld bieten wir unseren Kunden erstklassige Cyber Security Lösungen. Unser Service-Portfolio umfasst Managed Services für IAM einschließlich Beratung, Architektur, Implementierung, Integration, Support und Betrieb.

iC Consult hat seinen Hauptsitz in München und Niederlassungen in Deutschland, der Schweiz, Österreich, Frankreich, Belgien, Spanien, Bulgarien, Großbritannien, den USA, Kanada, Indien und China. Die größten Marken der Welt vertrauen auf unsere Expertise, um ihre wertvollsten Güter zu schützen und zu verwalten: Ihre Identitäten.