Cybersicherheit: Mit strategischer Weitsicht die Zukunft gestalten

Waldemar Reimche, Patrick Piotrowski und Anke Schäfer

Die NIS2-Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau in der EU markiert einen Wendepunkt in der Security Awareness tausender europäischer Unternehmen. Erstmals wird Cybersicherheit als eine ganzheitliche Gemeinschaftsaufgabe verstanden, die eines intensiven Austauschs und koordinierten Handelns bedarf. Der Normadressatenkreis geht dabei weit über die klassischen KRITIS-Betreiber hinaus und umfasst nunmehr geschätzt 25.000 bis 30.000 „wichtige“ und „besonders wichtige Einrichtungen“ aller Branchen und Größenordnungen. Das NIS2-Umsetzungsgesetz überführt diese Vorgaben in deutsches Recht. Mit dessen Inkrafttreten am 17. Oktober 2024 wächst der Handlungsbedarf zur Entwicklung eines umfassenden Cybersicherheitskonzeptes, das die technologischen Weichen für die Zukunft stellt.

Strategiewechsel als Chance zur erfolgreichen Neuaufstellung

Die letzten Monate haben es gezeigt: Die Umsetzung der NIS2-Richtlinie sensibilisiert nicht nur für blinde Flecken in der eigenen Sicherheitsstrategie, sie ist auch ein Game Changer und Katalysator für technologische Innovationen. Für viele der NIS2 unterliegenden Unternehmen geht die Notwendigkeit zur Implementierung höherer Sicherheitsstandards zudem mit einer noch grundlegenderen Frage einher: Wie können wir uns nach der Abkündigung von SAP IDM leistungsstark aufstellen? Jahrelang galt SAP IDM als zentrale Plattform und Rückgrat für die Verwaltung digitaler Identitäten – ein unverzichtbares Werkzeug, um komplexe Prozesse erfolgreich zu orchestrieren. Mit der Entscheidung, die Wartung für das eigene Identity Management einzustellen, eröffnet der Marktführer ungewollt seinen Kunden auch die Chance zu einem erfolgreichen eigenen Strategiewechsel.

Gerade im Bereich der Cybersicherheit ist die digitale Revolution rasant vorangeschritten. Gewachsene Geschäftsanforderungen und technische Neuerungen beflügeln einander und stellen Unternehmen zunehmend vor die Herausforderung, ihre IT-Systeme immer wieder neu zu überdenken und anzupassen. So kam SAP IDM in den letzten Jahren z. B. in puncto Cloud-Services, automatisierte Compliance-Überwachung und anpassungsfähige Benutzerverwaltungssysteme an seine Grenzen.

Wir sind an der Schwelle einer neuen Ära, die geprägt ist von digitaler Effizienz, höheren Sicherheitsstandards und einer ganzheitlichen Definition von Compliance. Es empfiehlt sich daher, die eigene Aufbau- und Ablauforganisation zu optimieren, Prozesse zu verschlanken und mit einer sauberen Datenbasis in das neue IT-System durchzustarten. Die gewählte Identitätsmanagement-Lösung sollte dabei flexibel genug sein, um mit den sich stetig verändernden gesetzlichen Vorgaben Schritt zu halten. Zugleich ist frühzeitig die Frage zu klären, welches Softwarebereitstellungsmodell (hybrid oder aus der Cloud) für die nächsten Jahre das richtige ist.

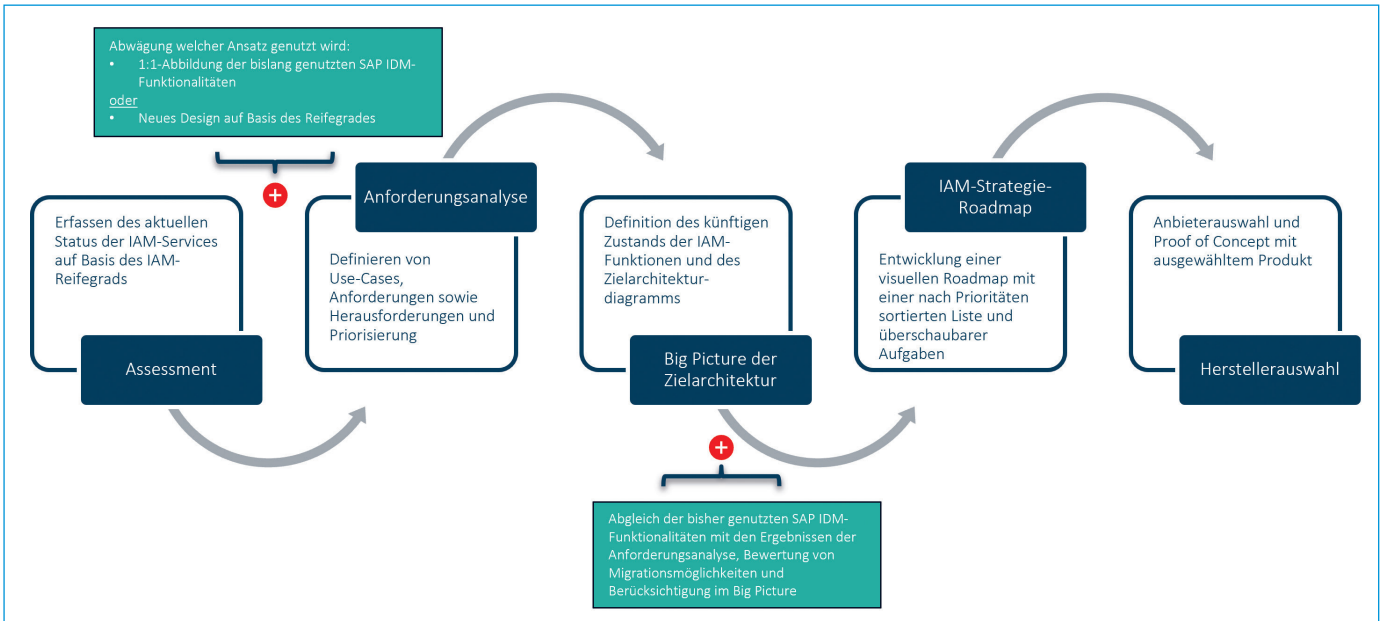

Abb. 1 **IAM-Strategie-Roadmap: Meilensteine einer strategischen Neuausrichtung**

Quelle: eigene Darstellung

Moderne SOCs – Effizienz und Sicherheit im Fokus

Angesichts der zunehmenden Komplexität von Cyberangriffen wird die kontinuierliche Überwachung von Unternehmenssystemen immer entscheidender. Um diesen Herausforderungen zu begegnen, setzen Unternehmen zunehmend auf Security Operations Center (SOCs). Diese stellen zumeist rund um die Uhr eine zentrale Anlaufstelle für die Überwachung, Analyse und Abwehr von Cyber-Bedrohungen dar. SOCs sind nicht nur Wächter, die auf Bedrohungen reagieren. Sie sind proaktive spezialisierte Einheiten, die kontinuierlich die Sicherheitslage analysieren, Schwachstellen identifizieren und präventive Maßnahmen entwickeln. Das ist unerlässlich, um mit den sich rasch verändernden Bedrohungsszenarien Schritt zu halten.

IAM und PAM (Privileged Access Management) sind in diesem Zusammenhang nicht nur Werkzeuge zur Verwaltung von Zugriffsrechten. Sie stellen auch die erste Verteidigungslinie gegen eine Vielzahl interner und externer Bedrohungen dar. Durch die effektive Verwaltung und Überwachung von Zugriffsrechten tragen sie dazu bei, Sicherheitsrisiken zu minimieren, die von privilegierten Benutzerkonten und potenziellen Insidern ausgehen. Ihre Bedeutung wird durch die Notwendigkeit, Compliance-Anforderungen zu erfüllen und Audit-Trails für forensische Untersuchungen bereitzustellen, weiter erhöht.

IAM und PAM sind tragende Säulen innerhalb der SOCs, deren Rolle bei der Gewährleistung von Sicherheit, Compliance und effektiver Risikominderung in der modernen Cyber-Sicherheitslandschaft nicht hoch genug eingeschätzt werden kann. Ihre Integration sowie die Wahl zwischen einem nationalen 24/7-Service oder einem Follow-the-Sun-Modell sind mehr als nur taktische Entscheidungen. Sie sind strategische Notwendigkeiten, die das Fundament der Sicherheitsarchitektur eines jeden Unternehmens stärken.

Entwicklung einer individuell passenden Roadmap

Die Umsetzung der NIS2-Richtlinie bedarf strategischer Weitsicht. Zur Auswahl einer passenden, zukunftsstarken IAM-Lösung sind daher eine detaillierte Marktanalyse und eine klare Vision für die Integration in die bestehende IT-Infrastruktur unerlässlich. Eine sorgfältig geplante Migration minimiert technische Schwierigkeiten und ermöglicht auch weiterhin einen reibungslosen Geschäftsbetrieb. Für eine bereichsübergreifende Akzeptanz kommt es nicht zuletzt auch auf eine frühzeitige vertrauensvolle Einbindung aller Mitarbeiter an.

Damit die Einführung der neuen IAM-Lösung ein voller Erfolg wird, müssen nicht nur die Leistungsmerkmale der IT sorgfältig ausgewählt werden, sondern auch die zugrundeliegenden Prozesse genau beleuchtet und optimiert werden. Die Fähigkeit, neue Technologien und Prozesse effizient zu integrieren, ist ein klarer Game Changer und schafft eine solide Basis für Innovation und Wachstum.

Abb. 1 beschreibt die Meilensteine einer strategischen Neuausrichtung – von einem umfassenden Assessment und der Entwicklung eines Big Pictures der Zielarchitektur bis hin zur IAM-Strategie-Roadmap und Herstellerauswahl. Darauf aufbauend startet die eigentliche Migration, bei der im Rahmen des bewährten Vorgehensmodells das Organizational Change Management eine zentrale Rolle einnimmt. Es bindet alle Stakeholder von Anfang an partnerschaftlich durch Schulungen und eine regelmäßige, wertschätzende Kommunikation ein und soll sie für das neue IAM-System begeistern. Unternehmen sind gut beraten, sich hierbei frühzeitig branchenerfahrene Partner ins Boot zu holen – für die aktuellen Herausforderungen und zukünftige Wachstumschancen.

Investition in Sicherheit und Zukunftsfähigkeit

In der DACH-Region, in der Datenschutz und Compliance eine besonders wichtige Rolle spielen, bietet der Betrieb eines nationalen 24/7 SOC klare Vorteile (siehe Textkasten). Die Möglichkeit, schnell und in Übereinstimmung mit lokalen Gesetzen und Standards reagieren zu können, ohne sich den zeitlichen und logistischen Herausforderungen eines Follow-the-Sun-Modells stellen zu müssen, ist für viele Unternehmen ein entscheidender Faktor.

Ein effektives SOC ist eine Investition in die Sicherheit, Effizienz und Zukunftsfähigkeit jedes Unternehmens. Es schützt nicht nur vor aktuellen Bedrohungen, sondern passt sich auch zukünftigen Herausforderungen an, um das Unternehmen widerstandsfähig gegen die Unwägbarkeiten einer digital vernetzten Welt zu machen.

W. Reimche, Geschäftsführer, P. Piotrowski, Senior Business Consultant IAM und Sales Representative, OEDIV SecuSys GmbH, Rostock; Dr. A. Schäfer, Dr. Schäfer PR- und Strategieberatung, Rostock
www.secusys.de