Individuelle IAM-Assessments für Cybersicherheit und -resilienz

Waldemar Reimche, Patrick Piotrowski und Anke Schäfer

Bislang wirkte sich die KRITIS-Gesetzgebung vor allem auf größere Institutionen aus. Die am 16. Januar 2023 in Kraft getretene NIS-2-Richtlinie der EU markiert einen neuen Meilenstein, die Themen Cybersicherheit und -resilienz auf eine breitere Basis zu stellen. Den Mitgliedstaaten bleibt bis 17. Oktober 2024 nur noch gut ein Jahr, die deutlich erweiterten Anforderungen und Sanktionsmöglichkeiten in nationales Recht umzusetzen. Mit dem im Mai 2023 vorgelegten Referentenentwurf zum NIS2UmsuCG hat das Bundesinnenministerium hier bereits erste Leitplanken gesetzt.

Durch die neue Richtlinie steigt nicht nur die Zahl der betroffenen Unternehmen massiv an. Es gibt auch einen höheren Durchsetzungsdruck – mit einer verschärften persönlichen Geschäftsführerhaftung, neuen Tatbeständen und gestiegenen Bußgeldern. Während beispielsweise bislang in der Energiebranche der Anwendungsbereich der NIS auf Unternehmen beschränkt war, die Energie im Strom- und Gassektor erzeugen, liefern oder regulieren, ist zu erwarten, dass nunmehr die gesamte Liefer- und Wertschöpfungskette – von der Herstellung der Windturbinen bis hin zum Betrieb der Ladestationen für Elektrofahrzeuge – erfasst wird.

Es ist also an der Zeit, proaktiv die eigene Betroffenheit herauszufinden, Umsetzungslücken zu identifizieren, geeignete Maßnahmen zu entwickeln sowie starke Cybersicherheits- und Überwachungsmechanismen zu entwickeln und zu implementieren.

IAM als eine der tragenden Säulen des IT-Sicherheitskonzeptes

Eine zentrale Rolle nimmt das Thema Identity & Access Management (IAM) ein – also eine zentrale Identitäts-, Rollen- und Zugriffsverwaltung über sämtliche Systeme und Anwendungen einer Organisation hinweg. Grundsätzlich wird dabei jede in die internen Strukturen eingebundene Person mit einer individuellen digitalen Identität verknüpft, aus der nachvollzogen werden kann, wer (auch über unterschiedliche Accounts) wann auf welche Daten, Ordner und Systeme Zugriff hat. Angesichts immer neuer Höchststände an Cyberangriffen und immer strikterer regulatorischer Anforderungen wie der NIS-2-Richtlinie oder des IT-Sicherheitsgesetzes 2.0 sollte ein effektives IAM als eine der tragenden Säulen des IT-Sicherheitskonzeptes verstanden werden.

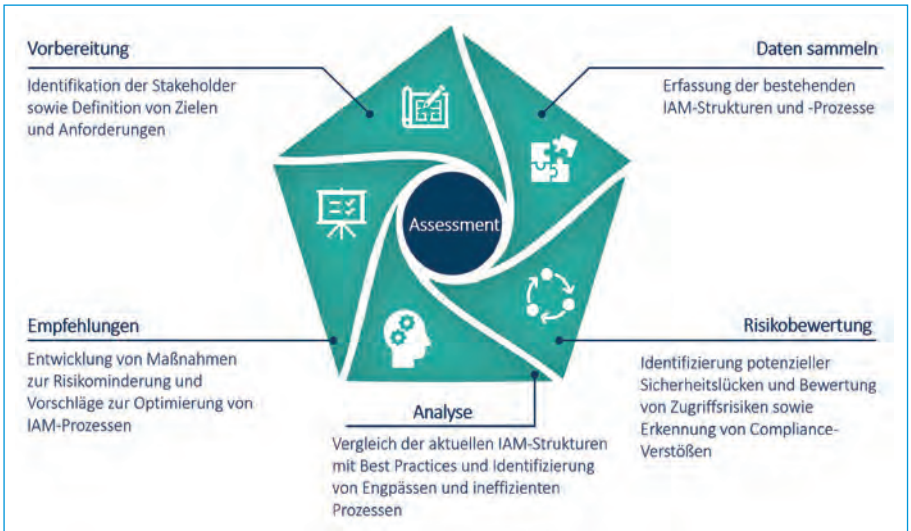

Abb. **Vorgehensmodell individueller IAM-Assessments**

Bild OEDIV SecuSys

Im Rahmen eines IAM-Assessments erstellen die Branchenexperten der OEDIV SecuSys GmbH eine ehrliche, den Kundenbedürfnissen entsprechende Bestandsaufnahme, geben konkrete Handlungsempfehlungen und entwickeln gemeinsam mit ihren Kunden ein ganzheitliches Zielbild für ein rechtskonformes und sicheres Benutzer- und Berechtigungsmanagement. Konzipiert wurde das Vorgehensmodell von Patrick Piotrowski, der aus seiner mehrjährigen Praxis in der Beratung von Unternehmen in regulierten Bereichen um die Bedeutung einer rollen- und regelbasierten Daten-Compliance weiß.

Cybersicherheit als ein kontinuierlicher interner Verbesserungsprozess

Fakt ist: Cybersicherheit ist kein statischer Zustand, sondern ein kontinuierlicher Verbesserungs- und Selbstoptimierungsprozess, der vom obersten Management getragen und vorangetrieben werden muss. Dabei gibt es nicht die eine hocheffektive IAM-Software. Stattdessen ist IAM eine vielschichtige Sicherheitsdisziplin.

Welche Tools bestmöglich den individuellen Anforderungen gerecht werden, lässt sich im Rahmen eines umfassenden 360-Grad-IAM-Assessments herausfinden. Die folgenden drei Bereiche spielen dabei eine zentrale Rolle:

- *Die Identity Governance & Administration (IGA)* beschäftigt sich hauptsächlich mit der Verwaltung und Überwachung von Identitäten innerhalb einer Organisation. Sie wird meist aus einem Personalverwaltungssystem mit Stammdaten gespeist und provisioniert gekoppelte Systeme. Grundlage ist ein Business-Rollenmodell. Hinzu kommen weitere Self-Servi-

ces, u. a. für Compliance-Praktiken wie den Kennwort-Reset, die Rezertifizierung von Rollen oder das Monitoring der Umsetzung der Segregation of Duties. Durch die organisatorische Funktionstrennung werden auch mögliche Interessenkollisionen vermieden.

- *Das Privileged Access Management (PAM)* verwaltet privilegierte Zugänge, z. B. administrative Konten mit hohen Berechtigungen. Die Credentials – also die Berechtigungsnachweise – dieser Konten werden gehärtet, die Zugriffsrechte der administrativen Konten streng reguliert, die Sessions geloggt und Bedrohungsanalysen gefahren.
- *Das klassische Access Management System (AMS)* – also die Zugriffsverwaltung – besteht im Kern meist aus einem Identity Provider (IdP), der Identitäts- und Authentifizierungsinformationen an andere IdP oder Anwendungen weitergibt und damit u. a. einen Single Sign-On (SSO) – also eine Einmalanmeldung – ermöglicht. Für die Nutzer bedeutet das, dass sie sich mit einem einzigen Zugang an verschiedensten Anwendungen anmelden können. Den IT-Verantwortlichen wird die Verwaltung der Anwendungen durch diese Zentralisierung erleichtert.

Das IAM-Assessment in der Praxis

Vor dem Hintergrund neuer regulatorischer Game Changer wie der NIS-2-Richtlinie ist ein IAM-Assessment eine unverzichtbare Positionsbestimmung und Zielorientierung. Im Rahmen eines IAM-Assessments werden zunächst die IAM-Anforderungen und -Risiken der Organisation identifiziert und bewertet. Auf Basis ihres umfangreichen Lösungsportfolios geben die Branchenexperten der OEDIV SecuSys GmbH eine objektive Empfehlung zu passenden Tools. Im Vordergrund steht dabei die Frage, welche IAM-Praktiken die Organisation nach Best Practices implementieren sollte. Hier werden selbstverständlich auch geeignete IAM-Lösungen aus dem breit gefächerten Partnernetzwerk berücksichtigt. Teile des IAM-Assessments sind in die Basis-Check-Software Ailaa der OEDIV integriert.

Die enge, vertrauensvolle Einbindung der Kundenunternehmen sollte in einem IAM-Assessment stets im Mittelpunkt stehen. In der Phase des Initial Consultings werden daher Anforderungen an die Compliance, die Komplexität der Organisation und weitere Faktoren grob abgesteckt, um den individu-ellen Herausforderungen im anschließenden vertiefenden IAM-Assessment bestmöglich gerecht zu werden.

W. Reimche, Geschäftsführer, P. Piotrowski, Sales Manager, OEDIV SecuSys GmbH; Dr. A. Schäfer, Dr. Schäfer PR- und Strategieberatung, Rostock
www.secusys.de
www.ailaa.de