Aktuelle Herausforderungen beim Identity & Access Management in der Finanz- und Versicherungsbranche

Dr. Oliver Dörr, Senior Consultant, iC Consult

1. Einleitung

In der digitalisierten Business-Welt von heute ist ein robustes Management der Identitäten und Zugriffe über alle Branchen hinweg von zentraler Bedeutung. Nirgends ist es aber wichtiger als in der Finanz- und Versicherungsbranche: Nicht nur, weil die Kunden von ihren Banken und Finanzdienstleistern heute ganz selbstverständlich erwarten, dass alle Services auch online mit höchstem Bedienkomfort und lückenloser Sicherheit bereitstehen – sondern auch, weil der Umgang mit den Mitarbeiter- und Kundenidentitäten strengsten regulatorischen Auflagen unterliegt.

Eine Schlüsselrolle kommt in diesem Zusammenhang den Rundschreiben 10/2017 (Fassung vom 16.8.2021) und 10/2018 (Fassung vom 3.3.2022) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zu: Diese definieren sehr konkrete „Bankaufsichtliche und Versicherungsaufsichtliche Anforderungen an die IT" (BAIT/VAIT) – und setzen dabei insbesondere auch wichtige Leitplanken für das Management der Identitäten, Zugriffsrechte und Berechtigungen in der Branche.

Bei unseren Projekten im Finanz- und Versicherungswesen stoßen wir immer wieder auf die gleichen Probleme, die häufig auch von Auditoren bemängelt werden.

Auch wenn die Rundschreiben und ihre Inhalte schon seit vielen Jahren bekannt sind, tun sich viele Einrichtungen mit der Umsetzung der Anforderungen immer noch schwer – gerade, was die in Kapitel 6 spezifizierten Vorgaben an das Identitäts- und Rechtemanagement betrifft.

Zusätzlich verschärft wird die Situation, da in vielen Einrichtungen unter dem Druck der Pandemie in den letzten beiden Jahren immer wieder Maßnahmen eingeleitet wurden, die den heutigen strengen Standards nicht durchgehend gerecht werden – etwa mit Blick auf den quasi über Nacht absolvierten Wechsel ins Home-Office, die überhastete Migration in die Cloud oder die unter Hochdruck erfolgte Einführung von Microsoft 365, um in der Krise handlungsfähig zu bleiben.

Die Folge: Banken und Versicherer stehen im Bereich IAM heute vor einer Reihe komplexer Herausforderungen – und nicht jedes Institut verfügt über die personellen Spielräume und das interne Knowhow, um diese ohne externe Unterstützung zu modernisieren.

Als IAM-Spezialist mit tiefer Branchenexpertise in der Finanzwirtschaft sind wir dennoch überzeugt, dass wir gemeinsam jede dieser Herausforderungen meistern können.

Das vorliegende Whitepaper ist unser erster Schritt in diese Richtung: Es fasst für Sie die wichtigsten Anforderungen an das IAM in der Finanz- und Versicherungsbranche kompakt zusammen – und gib Ihnen konkrete Handlungsempfehlungen für die Umsetzung der BAIT- und VAIT-Vorgaben.

Wir hoffen, Sie finden es hilfreich – und stehen Ihnen gerne für alle Fragen zur Verfügung.

2. Die BaFin Rundschreiben 10/2017 und 10/2018

Im Oktober 2017 definierte die BaFin im wichtigen Rundschreiben 10/2017 („Bankaufsichtliche Anforderungen an die IT") verbindliche Anweisungen für die sichere Ausgestaltung der IT-Systeme und Prozesse sowie für die IT-Governance in Bankunternehmen. Ein Jahr später folgte mit dem Rundschreiben 10/2018 („Versicherungsaufsichtliche Anforderungen an die IT") eine zweite, inhaltlich identische, aber präziser formulierte Ausarbeitung für Versicherungsunternehmen.

Seither wurden die Vorschriften mehrfach aktualisiert, etwa mit Blick auf die KRITIS-Gesetzgebung, doch sie gelten nach wie vor als verbindlicher Leitfaden für das Management der IT-Ressourcen und das IT-Risikomanagement in der Branche.

Die Praxis aber zeigt: Viele Einrichtungen tun sich mit der Umsetzung der Rundschreiben nach wie vor schwer. Dabei sind es immer wieder die gleichen Punkte, die von Auditoren moniert werden – auch im Bereich des Identity & Access Managements. Vier Abschnitte sind dabei von besonderer Bedeutung, und sollen im Folgenden ausführlich besprochen werden:

- BAIT/VAIT 6.2 – Berechtigungskonzepte
- BAIT/VAIT 6.2 – Funktionstrennung
- BAIT/VAIT 6.3 – Handelnde Personen
- BAIT/VAIT 6.7 – Protokollierung

Auf den folgenden Seiten bieten wir Ihnen jeweils einen kurzen Überblick über die aktuellen Herausforderungen in diesen Bereichen – und geben Ihnen dann konkrete Handlungsempfehlungen für die Umsetzung an die Hand.

Berechtigungskonzepte legen den Umfang und die Nutzungsbedingungen der Berechtigungen fest.

2.1 BAIT/VAIT 6.2 – Berechtigungskonzepte

Zitat BAIT/VAIT 6.2: *„Berechtigungskonzepte legen den Umfang und die Nutzungsbedingungen der Berechtigungen für die IT-Systeme (Zugang zu IT-Systemen sowie Zugriff auf Daten) sowie die Zutrittsrechte zu Räumen konsistent zum ermittelten Schutzbedarf sowie vollständig und nachvollziehbar ableitbar für alle bereitgestellten Berechtigungen fest."*

Experten fordern schon seit einiger Zeit klare Berechtigungskonzepte für alle IT-Systeme, und auch die Prüfer rücken diesen Bereich bei ihren Audits verstärkt in den Fokus. Dabei zeigen Gespräche mit Auditoren immer wieder, dass diese hier erheblichen Handlungsbedarf sehen.

Eine inhaltliche Ausrichtung der Berechtigungskonzepte liefern:

Bankaufsichtliche Anforderungen an die IT (BAIT)

Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

Mindestanforderungen an das Risikomanagement (MARisk)

2.1.1 Inhalt

Bei der Entwicklung von Berechtigungskonzepten sollten die Inhalte stets zentral vorgeben werden. Einen robusten Leitfaden für die inhaltliche Ausrichtung liefern dabei BAIT, VAIT, MARisk und natürlich eventuell vorhandene hausinterne Vorgaben. Zu beachten ist, dass die Berechtigungen stets abhängig zum Schutzbedarf vergeben werden müssen, sodass die Wirtschaftlichkeit bei Systemen mit niedrigerem Schutzbedarf eine stärkere Rolle spielen darf. Auch die Bündelung der Berechtigungen durch Rollen wird seitens der Prüfer derzeit akzeptiert. Allerdings stehen die Wirtschaftsprüfer dem Verzicht auf ein rollenbasiertes Modell skeptisch gegenüber – schon mit Blick auf die schiere Masse an Berechtigungen. IAM-Systeme können bei der Dokumentation helfen und diese auch automatisch übernehmen.

Beispiel: Inhalt eines Berechtigungskonzepts

Die individuellen Anforderungen jedes Unternehmens hängen von einer Vielzahl von Faktoren ab – etwa dem Schutzbedarf, den internen Strukturen und den gesetzlichen Vorgaben. Die folgende Übersicht zeigt wie sich ein exemplarisches Berechtigungskonzept zusammensetzen kann:

- **Authentifizierung und Autorisierung**
  Die Authentifizierung ist der erste Schritt in jedem Berechtigungskonzept. Sie dient dazu, zu überprüfen, ob die Benutzer auch wirklich die sind, als die sie sich ausgeben. Moderne Authentifizierungslösungen nutzen dabei eine Vielzahl verschiedener Faktoren. Der nach wie vor häufigste ist das Passwort in Kombination mit einem Benutzernamen. Je nach Sicherheitsstandards kann aber auch eine Zwei- oder Mehr-Faktor-Authentisierung, die Abfrage von biometrischen Daten oder die Verwendung von Einmal-PINs vorgegeben werden. Die anschließende Autorisierung – die meist automatisch das IAM übernimmt – regelt, welchen Benutzern welche Zugriffsrechte auf welche Funktionen und Ressourcen gewährt werden.

- **Philosophie**
  Diese definiert den Umgang des IT-Systems/des Unternehmens mit den Berechtigungsobjekten, sprich: welche Mittel zum Einsatz kommen und wie hoch der Schutzbedarf der Objekte ist. Dabei wird die Philosophie in vielen Bereichen von externen Faktoren geprägt. So gelten im Banken- und Versicherungswesens strenge gesetzliche Auflagen, die vorschreiben, was Berechtigungssysteme erfüllen müssen, um den Schutz von Daten zu gewährleisten.

- **Liste aller Berechtigungsobjekte**
  Moderne IAM-Lösungen sind in der Lage, diese Liste automatisch zu erstellen und zu verwalten. Um Verwirrungen und Probleme zu vermeiden, sollten jedem Objekt einzigartige Merkmale zugewiesen werden. Darüber hinaus gilt es für jedes Objekt zu definieren, wer darauf zugreifen darf und wer nicht – und besonders kritische oder privilegierte Berechtigungsobjekte eindeutig zu kennzeichnen.

- **Berechtigungen im System**
  Um die Weichen für eine umfassende Automatisierung zu stellen und sensible Daten zuverlässig zu schützen, sollten Benutzer in unterschiedliche Kategorien eingeteilt werden. Ein möglicher Ansatz:
  - Der Großteil der Mitarbeiter fällt in die Kategorie der **Natürlichen Benutzer**. Sie haben Zugriff auf Berechtigungsobjekte, die sie für ihre tägliche Arbeit brauchen.
  - **Technische Nutzer** erhalten zusätzlich Zugriff auf Server und Datenbaken mit weitreichenden Rechten. Diese sind bereits im System hinterlegt und können je nach Bedarf aktiviert werden.

- **Privilegierte Nutzer** – etwa die IT-Verantwortlichen des Unternehmens – erhalten besonders weitreichende Privilegien und können tiefgreifende Änderungen im System vornehmen.
- Eine wichtige vierte Kategorie sind die **Notfallbenutzer**. Diese sind in der Regel eng in das Notfallkonzept eingebunden und kommen lediglich bei der Behebung von Systemausfällen zum Einsatz.

Selbstverständlich kann jedes Unternehmen darüber hinaus noch zahlreiche weitere Kategorien definieren. Wichtig ist, dass sie alle dokumentiert werden – und dass die Verantwortlichen schlüssig herleiten können, dass alle Berechtigungen auf diese Weise erfasst wurden.

2.1.2 Prozesse

Zitat BAIT/VAIT 6.2: *„Berechtigungskonzepte sind regelmäßig und anlassbezogen zu überprüfen und ggf. zu aktualisieren."*

Um die Einhaltung der Richtlinie zu dokumentieren, sollten alle Konzepte jährlich re-zertifiziert werden. Die entsprechenden Prozesse lassen sich dabei erfahrungsgemäß mithilfe der IAM-Lösung einfach und schnell implementieren.

Die Rezertifizierung des Berechtigungskonzepts umfasst dabei mehrere Phasen:

- Zu Beginn werden die Privilegien zusammengestellt und auf Änderungen überprüft – etwa Rechteänderungen bei Mitarbeitern, neu erstellte Berechtigungsprofile oder inaktive Profile von ehemaligen Angestellten.
- Danach erfolgt die Archivierung der aktualisierten Liste. Das ursprüngliche Berechtigungskonzept wird dearchiviert und gelöscht.
- Im letzten Schritt erfolgt die Rezertifizierung des neuen, überarbeiteten und aktualisierten Berechtigungskonzept, die bei gegebenem Anlass über Arbeitsanweisungen und/oder SfO geregelt werden kann.

Um eine einheitliche Qualität sicherzustellen, sollten die Abläufe zudem eng in die Qualitätssicherung eingebunden werden.

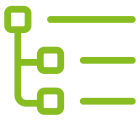
Wer kümmert sich darum?

Wer sollte die Berechtigungskonzepte am besten erstellen und rezertifizieren? Erfahrungsgemäß empfiehlt es sich, Mitarbeiter zu beauftragen, die das IT-System fachlich und technisch am besten verstehen – auch wenn diese in der Regel Anleitungen, Schulungen und einen Ansprechpartner bei Fragen brauchen werden. Hier ist es oft hilfreich, die interne Qualitätssicherung zu Rate zu ziehen – aber auch externe Experten können eine kompetente Anlaufstelle sein.

2.2 BAIT/VAIT 6.2 – Funktionstrennung

Zitat BAIT/VAIT 6.2: *„Berechtigungskonzepte haben die Vergabe von Berechtigungen nachdem Sparsamkeitsgrundsatz („Need-to-know" und „Least-Privilege" Prinzipien) sicherzustellen, die Funktionstrennung auch berechtigungskonzeptübergreifend zu wahren und Interessenskonflikte zu vermeiden."*

Das Zitat könnte nicht deutlicher sein: Eine durchgängige Funktionstrennung für alle IT-Assets ist Pflicht. Doch gerade mit dieser Forderung tun sich viele Unternehmen schwer: Immer wieder wird bei Audits eine nicht-bankfachliche Funktionstrennung gerügt, und auch in der Versicherungsbranche steigt die Zahl der Monierungen. Und auch während der Bestellung von Rechten wird immer öfter eine Prüfung angemahnt.



Die Umsetzung der Funktionstrennung soll durch die Einführung von Kategorien vereinfacht werden.

2.2.1 Einführung von Kategorien zur Funktionstrennung

Ein möglicher Ansatz zur einfachen Umsetzung der Funktionstrennung ist die Unterscheidung nach Kategorien – etwa in bankfachliche SoD-Kategorien wie Markt, Marktfolge, Rechnungswesen, Revision usw. sowie in nicht bankfachliche Kategorien wie die Administration, die Entwicklung und die Benutzerverwaltung. Beide Modelle können dann je nach individuellen Vorgaben nacheinander betrachtet oder zusammengeführt werden. Auf diese Weise lassen sich Konflikte in der Regel einer der beiden Kategorien zuordnen – und die konkreten Berechtigungen durch die Fachbereiche der entsprechenden Kategorie festlegen.

Dieses Verfahren bietet eine Reihe von Vorteilen:

- Konflikte lassen sich einfach definieren.
- Die Implementierung der Kategorien ist überaus performant.
- Fachbereiche können Berechtigungen einfach den erstellten Kategorien zuordnen.

Der einzige Nachteil dieses Ansatzes liegt darin, dass die Einführung von Funktionstrennungskategorien eventuell von bereits etablierten Systemen abweicht. Wie relevant dies ist, gilt es im Einzelfall abzuwägen.

2.2.2 Prüfung von Konflikten bei der Funktionstrennung

Im IAM lassen sich zwei unterschiedliche Ansätze zur Prüfung von Funktionstrennungskonflikten implementieren:

- **Prüfung bei Bestellung der Berechtigung**
  Die Verantwortlichen überprüfen während der Auswahl der Rechte oder im Rahmen des Bestellprozesse, ob die neuen Berechtigungen einen Konflikt mit alten auslösen.

- **Prüfung des Komplettsystems**
  Hier handelt es sich um eine nachträgliche und regelmäßige Prüfung des kompletten Systems, ob Funktionstrennungskonflikte bestehen.

Auch wenn die Prüfung bei Bestellung aufgrund ihrer Unmittelbarkeit immer beliebter wird, zeigt die Erfahrung, dass beide Verfahren benötigt werden und kombiniert werden sollten: Immerhin vergeht zwischen Bestellung und Zuweisung stets eine gewisse Zeit, in der sich das Gesamtsystem ändern kann, und so kann lediglich die Prüfung im Nachhinein den belastbaren Nachweis erbringen, dass keine Konflikte vorliegen.

2.2.3 Mitigation von Risiken

Von Mitigation spricht man, wenn Risiken weiterhin bestehen und vom Unternehmen akzeptiert werden. Ob Prüfer eine Mitigation hinnehmen, ist stets ungewiss – dieses Mittel sollte also nur sporadisch zum Einsatz kommen.

Mitunter ist die Mitigation aber die einzige Option – etwa, weil sich Risiken eines Geschäftsbetriebes nicht gänzlich ausräumen lassen. In diesem Fall muss das Risikomanagement die verbleibenden Risiken beurteilen und einordnen. Daraus lassen sich Maßnahmen ableiten, um die Risiken weiter zu minimieren oder sogar komplett auszuräumen.

Bleibt auch nach Umsetzung der Maßnahmen ein Restrisiko, gilt es, die Mitigation zu dokumentieren. Dabei wird jede Änderung eingetragen, und es erfolgt auch hier eine regelmäßige Prüfung, Archivierung, Dearchivierung und Löschung. Darüber hinaus sollte das Risikomanagement die bestehenden Risiken turnusmäßig neu bewerten.

Durch eine Dokumentation der Mitigation werden Restrisiken minimiert oder sogar komplett ausgeräumt.

Beispiel: Inhalt der Dokumentation der Risikomitigation

Folgende Inhalte sind für eine lückenlose Dokumentation der Mitigation wichtig:

- **Welche Berechtigungen liegen hier im Konflikt?**
  Spezifizieren Sie genau, welche Berechtigungen im Konflikt liegen und welche IT-Assets betroffen sind.
- **Welche Informationseigentümer sind daran beteiligt?**
  Stellen Sie fest welche verantwortlichen Mitarbeiter für die Informationsverarbeitung im Konflikt stehen – auch mit Blick auf die Rolle in Ihrem Unternehmen.
- **Wer hat mit welcher Begründung zugestimmt?**
  Begründen Sie plausibel, warum Sie das Risiko akzeptieren und nicht vollständig beheben können.
- **Wie lange ist die Mitigation gültig?**
  Da es unklar ist, was seitens des Auditors akzeptiert wird, empfiehlt es sich, die Mitigation auf ein Jahr zu beschränken. Gegebenenfalls können Sie sie nach Ablauf weiter verlängern.
- **Welche Person hat die Mitigation geprüft, bevor sie eingerichtet wurde?**
  Halten Sie genau fest welcher verantwortliche Mitarbeiter wann und wo die Mitigation überprüft hat. In Anbetracht der oft unzulänglichen Prüfungsverfahren muss die Mitigation sehr sorgfältig validiert werden.
- **Für welche Personen soll die Mitigation akzeptiert werden?**
  In der Praxis ist es mit Blick auf das Risikomanagement niemals sinnvoll, ein Risiko für alle Personen zu akzeptieren. Stattdessen gilt es klar zu definieren, für wen und in welchem Kontext das Unternehmen das Risiko zu tragen bereit ist.

2.3 BAIT/VAIT 6.3 – Handelnde Personen

Jede Berechtigung, jeder technische Account und jeder Schnittstellenbenutzer liegt in der Verantwortung eines delegierten Mitarbeiters.

Zitat BAIT/VAIT 6.3 *„Zugriffe und Zugänge müssen jederzeit zweifelsfrei einer handelnden bzw. verantwortlichen Person (möglichst automatisiert) zuzuordnen sein. Beispielsweise müssen automatisierte Aktivitäten verantwortlichen Personen zuordenbar sein. Abweichungen in begründeten Ausnahmefällen und die hieraus resultierenden Risiken sind zu bewerten, zu dokumentieren und anschließend von der fachlich verantwortlichen Stelle zu genehmigen.“*

Letztlich fordern BAIT und VAIT damit, dass jede Berechtigung, jeder technische Account und jeder Schnittstellenbenutzer in der Verantwortung eines delegierten Mitarbeiters liegen müssen. Diese Forderung wird später in BAIT/VAIT 6.7 noch einmal verschärft.

2.3.1 Dokumentation der Zuordnung

Um die Zuordnung der handelnden Personen lückenlos zu dokumentieren, hat sich ebenfalls der Einsatz einer IAM-Lösung bewährt. Wir empfehlen dafür die Einführung von technischen Identitäten, die jeweils von einer natürlichen Person (z. B. Abteilungsleiter oder Produktverantwortlicher) verantwortet werden. Auf diese Weise können Gruppen von Mitarbeitern mit dieser Identität arbeiten und diese beispielsweise nutzen, um technische Benutzerkonten und Berechtigungen zu beantragen.

Im Zuge der Einführung technischer Identitäten sollte darüber hinaus ein Datenabgleich erfolgen. Dabei identifizierte Benutzerkonten werden möglichst automatisch einer technischen Identität zugeordnet und nachbeantragt. Ist eine Zuordnung nicht möglich, muss das Benutzerkonto in einen Klärungsprozess überführt oder gelöscht werden. Schon aus Eigeninteresse sollte auch hier eine zyklische Rezertifizierung aller Benutzerkonten erfolgen, um sicherzustellen, dass die Verantwortlichkeiten aktuell bleiben.

2.3.2 Zuordnung abseits des IAM

Abseits der IAM-Lösung muss die Dokumentation der Zuordnung in den jeweiligen Berechtigungskonzepten stattfinden. Auch hier ist die zyklische Aktualisierung der technischen Benutzerkonten und ihrer Berechtigungen von entscheidender Bedeutung. Zusätzlich kann eine anlassbezogene Aktualisierung erforderlich sein, wenn umfangreiche Änderungen an einem IT-Asset vorgenommen werden. In der Summe bedeutet dies gerade bei größeren Systemen einen regelmäßigen und nicht unerheblichen manuellen Aufwand, der durch die Integration eines entsprechend implementierten IAM-Systems weitgehend entfällt.

2.4 BAIT/VAIT 6.7 – Protokollierung

Zitat BAIT/VAIT 6.7: *„Das Institut hat nach Maßgabe des Schutzbedarfs und der Soll-Anforderungen Prozesse zur Protokollierung und Überwachung einzurichten, die überprüfbar machen, dass die Berechtigungen nur wie vorgesehen eingesetzt werden. Aufgrund der damit verbundenen weitreichenden Eingriffsmöglichkeiten hat das Institut insbesondere für die Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten angemessene Prozesse zur Protokollierung und Überwachung einzurichten. Die übergeordnete Verantwortung für die Prozesse zur Protokollierung und*

Regelmäßige Prüfungen gewährleisten, dass privilegierte Zugriffe auf Systeme mit besonders hohem Schutzbedarf immer protokolliert werden.

Überwachung von Berechtigungen wird einer Stelle zugeordnet, die unabhängig vom berechtigten Benutzer oder dessen Organisationseinheit ist. Zu privilegierten Zutrittsrechten zählen in der Regel die Rechte zum Zutritt zu Rechenzentren, Technikräumen sowie sonstigen sensiblen Bereichen.“

Auditoren und Wirtschaftsprüfer leiten aus diesem Abschnitt häufig die Forderung nach einem modernen PAM-System (Privileged Access Management-System) ab. Auf diese Weise soll gewährleistet werden, dass bei Systemen mit besonders hohem Schutzbedarf sämtliche privilegierte Zugriffe jederzeit protokolliert werden und nachvollziehbar sind. Dabei müssen Banken und Versicherungsunternehmen damit rechnen, dass diese Aufzeichnungen schon jetzt im Rahmen von Prüfungen regelmäßig kontrolliert werden.

2.4.1 Privilegierte Zugriffe – Einordnung der Situation

BAIT/VAIT 6.7 kann durchaus als Erweiterung von 6.3 interpretiert werden: Abschnitt 6.3 fordert, dass klar festzulegen ist, wer für eine Berechtigung verantwortlich zeichnet. Abschnitt 6.7 ergänzt, dass nachvollziehbar sein muss, wie die Berechtigung genutzt wird.

Wie genau privilegierte Rechte definiert sind, wird im Rahmen von BAIT/VAIT allerdings nur im letzten Satz angedeutet („Zu privilegierten Zutrittsrechten zählen in der Regel die Rechte zum Zutritt zu Rechenzentren, Technikräumen sowie sonstigen sensiblen Bereichen.“). Dies hat den Vorteil, dass jede Einrichtung selbst eine – plausibel begründbare – Definition von Privilegien vornehmen kann. Die Unschärfe birgt allerdings auch das Risiko, dass der Begriff im Lauf der Jahre durch die BaFin und/oder Wirtschaftsprüfer nachjustiert werden könnte. Verantwortliche sollten dies nicht außer Acht lassen, und auf eventuelle Anpassungen vorbereitet sein.

2.4.2 Ansätze zur Definition von privilegierten Rechten

Software-Hersteller legen den Fokus bei der Definition des Begriffs „privilegiert“ oft auf die Aufrechterhaltung der Geschäftstätigkeit und die Vertraulichkeit sensibler Daten: Alle Berechtigungen, die zu einer Gefährdung dieser Bereiche führen können, gelten als privilegiert.

Eine andere Möglichkeit ist die prozesstechnische Definition: Dabei werden alle Berechtigungen als privilegiert gewertet, die vorher festgelegte und definierte Prozesse im Unternehmen unterlaufen können.

Wirtschaftsprüfer wiederum konzentrieren sich bei der Definition im Rahmen von Audits derzeit noch auf hohe Berechtigungen bei der Administration der IT. Es ist aber nicht auszuschließen, dass schon bald auch fachliche Berechtigungen einen ähnlich hohen Stellenwert erhalten werden. Dies sollten Sie bei Implementierungen schon jetzt berücksichtigen, um künftige Projekte nicht unnötig zu erschweren.

2.4.3 Implementierung privilegierter Zugriffe im IAM

Moderne IAM- und dedizierte PAM-Lösungen können Sie bei der Verwaltung und beim Schutz privilegierter Benutzerkonten erheblich entlasten: Gemäß BAIT/VAIT 6.7 gilt jedes Benutzerkonto, das über eine oder mehrere privilegierte Berechtigungen verfügt, als privilegiert – ebenso wie alle administrativen Accounts. Diese Klassifizierung in

Ihrem IAM vorzunehmen und die Liste der privilegierten Benutzerkonten zu pflegen, ist ein wichtiger erster Schritt.

Ein Schlüsselbegriff in der Forderung der BaFin ist dabei das Wort „angemessen“: Nutzen Sie es, um die Auswahl der als privilegiert eingestuften IT-Assets unter fachlichen und/oder sicherheitsrelevanten Kriterien kritisch zu filtern – und beispielsweise auf rechnungsrelevante IT-Assets oder IT-Assets mit hohem Schutzbedarf zu beschränken. So lassen sich die Kosten für die Umsetzung spürbar reduzieren.

Ein PAM-System trägt maßgeblich zur IT-Security bei.

2.4.4 Implementierung im PAM-System

Die Protokollierung der Einhaltung von BAIT/VAIT 6.7 kann über ein PAM-System erfolgen, das dann die geforderten Protokolle liefert und maßgeblich zur IT-Security beiträgt. Besonders bewährt hat es sich dabei, Zugriffe auf privilegierte Benutzerkonten durchgehend mit starker Mehrfaktor-Authentifizierung zu schützen.

Mit Blick auf ein effizientes Access Management kann es sinnvoll sein, für privilegierte und nicht privilegierte Zugriffe unterschiedliche Benutzerkonten zu verwenden. Auf diese Art können Kollegen bei ihrer täglichen Arbeit vorrangig das bequeme, nicht privilegierte Benutzerkonto nutzen – und nur dann auf das etwas aufwändigere, privilegierte Konto wechseln, wenn sie die Privilegien tatsächlich benötigen. Dies verringert nachhaltig die Menge der generierten Protokolle und macht es damit auch wesentlich einfacher, privilegierte Aktionen zu auditieren oder – im Falle des Falles – den Missbrauch nachzuvollziehen.

In der Summe bietet also bereits ein grundlegendes PAM-System mit wenigen Protokollen eine Vielzahl von Vorzügen: Ihre Kollegen müssen ihre etablierten Arbeitsprozesse kaum ändern und werden doch ganz automatisch wesentlich bewusster mit den privilegierten Berechtigungen umgehen. Optional besteht zudem die Möglichkeit, die Nutzung der Privilegien an weitere Bedingungen (etwa wie das Vorhandensein eines Problem-Tickets) zu knüpfen.

2.4.5 Weitere Vorzüge einer PAM-Lösung

Die Einführung einer dedizierten PAM-Lösung eröffnet Ihnen mit Blick auf die Sicherheit und Compliance Ihrer Identitäten und Zugriffe viele weiterer Optionen:

- Die Integration mit einem SIEM-System (Security Information and Event Management-System) ermöglicht es Ihnen, Angriffe auf Ihre Systeme proaktiv zu entdecken, da viele Attacken vom üblichen Zugriffsmuster abweichen.
- Durch die Verwendung der API der PAM-Lösung lässt sich das Hinterlegen von Passwörtern in Automationslösungen nachhaltig reduzieren, was die Angriffsfläche weiter minimiert.
- Bei eventuellen Angriffen über das PAM-System lässt sich anhand der entsprechenden Protokolle exakt nachvollziehen, wie die Angreifer vorgegangen sind.
- Das PAM ist in der Lage, Passwörter für privilegierte Benutzerkonten zu generieren, zu verwalten und regelmäßig zu aktualisieren. So müssen sich die Mitarbeiter auch keine Passwörter mehr merken.
- Und schließlich: Audits der PAM-Prozesse können künftig vollständig auf der Basis der Protokolle der PAM-Lösung erfolgen.

3. BAIT/VAIT und Microsoft 365

Unter dem Druck der Pandemie haben in den beiden vergangenen Jahren zahlreiche Einrichtungen in der Finanz- und Versicherungsbranche Microsoft 365 eingeführt, um handlungs- und entscheidungsfähig zu bleiben – und ihre Mitarbeiter auch abseits der Offices produktiv einsetzen zu können. Mit Blick auf das Management der Identitäten und Zugriffsrechte im Allgemeinen – und die konkreten Anforderungen von BAIT/VAIT im Besonderen – präsentiert MS 365 aber eine Reihe neuer Herausforderungen.

Cloud-basierte Lösungen verändern die IT-Systeme von Banken und Versicherungen und stellen sie vor neue Herausforderungen.

Management von Berechtigungen durch Azure AD
Microsoft 365 verwaltet die Berechtigungen der Anwender über Azure AD – und denkt das Thema als Cloud-basierte Lösung ganz neu: Azure AD arbeitet mit einer Vielzahl von Berechtigungsobjekten (Identitäten/Accounts, Rollen, Gruppen, Service Principals etc.) und überlässt dem Anwender die Entscheidung, wer welchen Zugriff auf welche Daten erhält. Das übergeordnete Unternehmen kann lediglich globale Richtlinien vorgeben.

Auch wenn es viele pragmatische Gründe für diesen Ansatz gibt: Die Anforderungen der BAIT/VAIT lassen sich auf diese Weise in vielerlei Hinsicht nicht abbilden. Banken und Versicherungen kommen also nicht umhin, die entsprechenden Risiken bei der Einführung zu dokumentieren und explizit zu akzeptieren.

Wie lässt sich damit umgehen?
Für den Umgang mit dieser Herausforderung empfehlen wir folgende Best Practices:

- Das Management der meisten Berechtigungsobjekte in Azure sollte über Ihr IAM erfolgen.
- Nicht verwaltete Objekte wie Service Principals können über Eigenimplementierungen integriert werden.
- Passen Sie die Berechtigungsprozesse soweit möglich an die von Microsoft definierten Standards an.
- Implementieren Sie sinnvolle risikominimierende Maßnahmen.
- Erstellen Sie klare Arbeitsanweisungen für alle Mitarbeiter und überwachen Sie die Einhaltung mithilfe begleitender Audit-Maßnahmen.
- Dokumentieren Sie die Risiken, und bearbeiten Sie sie kontinuierlich im Rahmen der Risiko-Management-Prozesse weiter.

4. Fazit

Die Jahre der Pandemie haben die IT-Systeme der Banken und Versicherungen nachhaltig verändert – auch und vor allem mit Blick auf das Management der Identitäten und Zugriffsrechte, das bei Auditierungen unterschiedlichster Institute immer wieder bemängelt wird.

Die Weichen für robuste, BAIT- und VAIT-konforme Abläufe zu stellen, ist in den zunehmend Cloud-basierten, von Microsoft 365 dominierten Anwendungslandschaften von heute alles andere als einfach. Die Themen Identity & Access Management und

Privileged Access Management werden die Unternehmen noch lange beschäftigen – zumal der regulatorische Druck wächst, und die Branchenstandards kontinuierlich an neue Vorgaben angepasst werden.

Mit zeitgemäßen IAM- und PAM-Lösungen lassen sich heutige und künftige Anforderungen aber zuverlässig abbilden. Angesichts der hohen Komplexität und Integrationstiefe der entsprechenden Projekte sind die Unternehmen aber gut beraten, frühzeitig erfahrene Consultants und Integratoren hinzuzuziehen.

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.