_betasystems

Der zukunftssichere Mainframe

Berechtigungsmanagement im digitalen Zeitalter

Wie Unternehmen den wachsenden Anforderungen im digitalen Zeitalter begegnen und die Administration der Mainframe-Zugriffsrechte sicher und effizient gestalten können.

www.betasystems-dci.de

Der Zukunftssichere Mainframe

Unternehmen mit Mainframe-Systemen stehen derzeit vor großen Herausforderungen. Ihre Spezialisten für die Großrechner gehen allmählich in Rente, und es rücken nur wenige nach, um diese zu ersetzen. Dabei bleiben Mainframes auch in Zukunft unverzichtbar und müssen sogar wachsenden Anforderungen gerecht werden. Die Digitalisierung, immer neue gesetzliche Vorgaben sowie organisatorische Veränderungen verlangen von den Mainframe-Systemen, dass sie sich schnell an veränderte Bedingungen anpassen. Die Unternehmen sind hier gefordert, entsprechende Strategien zu entwickeln. Dabei geht es auch darum, wie sie das Zugangsmanagement mit RACF einfacher und sicherer gestalten können.

Dieses Whitepaper wendet sich an Leiter von Rechenzentren, in denen RACF-Systeme im Einsatz sind. Sie erfahren hier, welche Herausforderungen bei der RACF-Administration im Alltag zu bewältigen sind und wo mögliche Sicherheitsrisiken liegen. Das Whitepaper zeigt ihnen, wo sie anssetzen können, um das Berechtigungsmanagement zu optimieren und die Sicherheit im Unternehmen zu erhöhen. Dabei stehen Lösungen im Mittelpunkt, mit denen sich RACF-Berechtigungen auch ohne Spezialwissen effizient verwalten lassen. Mit ihnen bleiben Unternehmen handlungsfähig, um auch künftig auf veränderte Rahmenbedingungen schnell reagieren zu können.

Mainframes bleiben zentraler Bestandteil der IT

Keiner anderen Plattform wurde häufiger das Ende vorausgesagt als dem Mainframe. Doch selbst nach über 50 Jahren hat er noch immer seinen festen Platz in der IT-Infrastruktur zahlreicher großer Unternehmen. Dies gilt nicht nur für Finanzdienstleister wie Banken und Versicherungen, sondern auch für Einzelhändler, Automobilhersteller und andere Industrieunternehmen. Der Grund für die unverändert hohe Bedeutung des Mainframes sind seine unerreicht hohe Ausfallsicherheit und Performance. Auf keinem anderen System können so viele Benutzer gleichzeitig arbeiten und so viele Anwendungen parallel laufen. Banken wickeln darüber zuverlässig eine hohe Anzahl an Finanztransaktionen ab. Vor dem Hintergrund der steigenden Anzahl regulatorischer Vorgaben und Prüfungen durch Aufsichtsbehörden schätzen sie dabei vor allem die hohe Sicherheit der Plattform.

Fehlendes Mainframe-Know-how ist einer der Hauptgründe für Überlegungen, den Mainframe abzulösen.

Trotz der Vorteile denken IT-Verantwortliche darüber nach, ihren Mainframe durch eine moderne IT-Landschaft abzulösen. Ein häufig genannter Grund ist die Annahme, dass Mainframes in Zeiten von Mobile- und Cloud-Konzepten nicht mehr dem Stand der Technik entsprechen würden. Auch die hohen Kosten für Lizenzen und Hardware, die Abhängigkeit vom Hersteller IBM sowie fehlendes Mainframe-Know-how infolge von Fachkräftemangel werden als Argumente für eine Ablösung genannt. Dabei ist das fehlende bzw. verloren gegangene Know-how oft ein hausgemachtes Problem: Die Unternehmen haben es versäumt, rechtzeitig Nachwuchskräfte für Mainframes auszubilden. Doch nun gehen die Experten, die die Mainframes betreiben, nach und nach in Rente. Gleichzeitig aber sind immer mehr Aufgaben im Mainframe zu erledigen. Dieses Dilemma – weniger qualifizierte Mitarbeiter, mehr Aufgaben – zwingt die Unternehmen zum Handeln. Sie müssen eine Lösung finden, mit der sich ein zuverlässiger Mainframe-Betrieb weniger spezialisierten Fachkräften weiter aufrechterhalten lässt.

Ihre hohe Rechenleistung macht Mainframes auch in Zeiten von Mobile und Cloud Computing unverzichtbar.

Denn den Mainframe komplett abzulösen, scheint für die meisten Unternehmen heute kein Thema mehr zu sein: 89 Prozent der Mainframe-Nutzer gehen laut einer aktuellen Umfrage davon aus, dass Mainframes auch in Zukunft eine unverzichtbare Plattform sein werden.[1] Grund ist die überlegene Rechenleistung, mit der sich große Datenmengen leicht verarbeiten und analysieren lassen. Und das ist in Zeiten der Digitalisierung ein schlagendes Argument. Denn das Datenvolumen steigt stetig: Bereits 2015 führten Nutzer von Mobilgeräten im Schnitt 37 Transaktionen pro Tag durch[2], 91 Prozent ihrer Apps interagierten dabei mit einem Mainframe.[3] Bei so gut wie jeder Kreditkartenzahlung, jedem Versandauftrag und jeder Flugticket-Reservierung kommt es zu einer oder mehreren Interaktionen mit einem Mainframe. Dafür braucht es verlässliche Systeme. Eine digitale Welt ohne Mainframe-Services ist daher kaum vorstellbar.

> *"Mainframes play a key role in digital business as many digital applications are based on mobile or handheld device access to data stored on the mainframe. This is driving growth in mainframe transactions and data volumes."*
>
> *Tim Grieser, IDC Analyst*

---

1 BMC Mainframe Research Report 2016. In: manage it, Dez. 2016. http://ap-verlag.de/der-mainframe-ist-auch-im-zeitalter-des-digitalen-wandels-unverzichtbar/28923/

2 IBM Digital Analytics Benchmark 2015. In: Forbes.com, Jan. 2015. https://www.forbes.com/sites/ibm/2015/01/14/the-digital-economy-is-the-new-app-economy/#74ed07743ec4

3 BMC Mainframe Research Report 2016. In: manage it, Dez. 2016. http://ap-verlag.de/der-mainframe-ist-auch-im-zeitalter-des-digitalen-wandels-unverzichtbar/28923/

Berechtigungsmanagement mit RACF: Herausforderungen & Risiken

Administration von RACF im Alltag

In rund 80 Prozent aller globalen z/OS-Installationen kommt RACF (Ressource Access Control Facility) zum Einsatz. Dabei handelt es sich um ein Sicherheitssystem von IBM für die Verwaltung der Berechtigungen im Mainframe-Umfeld. Das Produkt ist bereits seit mehr als 40 Jahren am Markt und wird heute unter dem Namen *SecureWay Security Server* vertrieben. RACF sorgt dafür, dass nur diejenigen Nutzer Zugriff auf eine angefragte Ressource erhalten, die dazu autorisiert sind. Versucht ein nicht autorisierter Benutzer auf eine geschützte Ressource – das können Daten, Applikationen oder Hardware sein – zuzugreifen, so erfasst und meldet das System diesen Zugriffsversuch.

RACF erfüllt damit folgende Grundfunktionen:

- Identifikation und Verifikation von Benutzern mittels Benutzerschlüssel und Passwortprüfung (Authentifizierung)
- Schutz von Ressourcen durch Verwaltung von Zugriffsrechten (Autorisierung)
- Logging der Zugriffe auf geschützte Ressourcen (Auditing).

Aus diesen Funktionen leiten sich für die IT-Abteilung verschiedene Tätigkeiten ab: Sie muss zum einen die Berechtigungsstrukturen pflegen und zum anderen die Zugriffe auf geschützte Ressourcen kontinuierlich überwachen und für interne oder externe Audits dokumentieren.

Pflege der Berechtigungsstrukturen

Die Pflege der Berechtigungsstrukturen mit RACF erfordert Spezialwissen.

Zentrale Aufgabe der IT-Abteilung ist es, dafür zu sorgen, dass jeder Nutzer genau die Berechtigungen erhält, die er benötigt. Dafür muss sie unter anderem neue Benutzer anlegen, Kennworte zurücksetzen oder Benutzern weitere Rechte zuordnen – relativ einfache Administrationsaufgaben, die sich allerdings mit RACF oft als sehr aufwändig gestalten. Dafür gibt es zwei Gründe: Zum einen sind die Berechtigungsstrukturen bei Unternehmen mit vielen Mitarbeitern und einer hohe Zahl an eingesetzten Anwendungen meist sehr komplex. Zum anderen ist die Bedienung von RACF nicht gerade userfreundlich: Das IBM-System bietet von Haus aus keine grafische Benutzeroberfläche. Für Änderungen an der RACF-Datenbank müssen komplizierte RACF-Befehle eingegeben werden. Dabei sind oft viele Einzelaktionen nötig. Das erfordert Spezialwissen.

Bei Massenupdates nach Restrukturierungen oder bei RZ-Migrationen ist der Aufwand besonders hoch.

Vor besonders großen Herausforderungen stehen IT-Administratoren immer dann, wenn umfangreiche Änderungen nötig sind. Das ist zum Beispiel dann der Fall, wenn Rechensysteme zusammengelegt werden oder das Rechenzentrum an einen Dienstleister ausgelagert wird und in diesem Zusammenhang die Berechtigungsstrukturen migriert werden müssen. Ein anderes Beispiel sind Restrukturierungen im Unternehmen, bei denen eine Vielzahl an Mitarbeitern neue Berechtigungen erhalten. Solche Massenupdates gestalten sich in Mainframe-Systemen aufgrund der komplexen Berechtigungsstrukturen und der manuellen Befehle als

extrem aufwändig und fehleranfällig. Eine automatisierte Verarbeitung wäre hier eine enorme Arbeitserleichterung für die IT-Abteilung.

Monitoring

Die Bedrohungen durch Datenmissbrauch und –diebstahl machen ein verlässliches Echtzeit-Monitoring unverzichtbar.

Neben der Pflege der Berechtigungsstrukturen gehört auch das Monitoring zu den Kernaufgaben der RACF-Administratoren. Sie müssen die Nutzerzugriffe auf die Ressourcen kontinuierlich und idealerweise in Echtzeit überwachen, damit auf Sicherheitsverstöße umgehend reagiert werden kann. Denn die Bedrohungen durch Datenmissbrauch und -diebstahl wachsen kontinuierlich: Mehr als die Hälfte aller Unternehmen in Deutschland (53 Prozent) ist in den vergangenen zwei Jahren Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Dadurch ist ein Schaden von rund 55 Milliarden Euro entstanden[4]. Im Finanzsektor waren in einem Zeitraum von 12 Monaten sogar 93 Prozent aller Institute betroffen.

Die Sicherheitsbedrohungen wachsen:

- 53 % aller Unternehmen sind in den letzten 2 Jahren Opfer von Spionage oder Datendiebstahl geworden.
- Bis zu 60 % aller Cyberattacken gehen auf Identitätsmissbrauch zurück.
- Attacken durch Mitarbeiter verursachen größere Schäden (fast 200 % je Schadensfall) als externe Angriffe.
- 80 % der Datendiebstähle erfolgten innerhalb eines Tages, aber nur 12 % wurden am gleichen Tag entdeckt.

Täter sind in den meisten Fällen häufig aktuelle oder ehemalige Mitarbeiter des Unternehmens (62 Prozent)[5]. Diese Angriffe verursachen zudem wesentlich größere Schäden als externe Attacken. Ein zuverlässiges Monitoring, das sicherheitsrelevante Events erfasst und eskaliert, ist daher für alle Unternehmen unverzichtbar. RACF allein bietet diese Möglichkeit nicht.

[4] Bitkom Research: Wirtschaftsschutz in der digitalen Welt. Juli, 2017. https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html

[5] Ebd.

Abb.: Bei Datendiebstahl, Spionage oder Sabotage sind meist die eigenen Mitarbeiter involviert. Für Unternehmen ist daher ein Echtzeit-Monitoring der Zugriffe unverzichtbar, um solche Fälle schnell zu erkennen.

Reporting

Zum Nachweis der Compliance müssen Reportings manuell aufbereitet werden.

Eine immer größere Rolle im Alltag der RACF-Administratoren nimmt das Reporting ein. Denn Unternehmen müssen regelmäßig Sicherheits-Audits durchführen, um die Compliance mit gesetzlichen Vorschriften nachzuweisen. Besonders für Banken und Versicherungsdienstleister gelten hohe Anforderungen. Viele Unternehmen führen bereits im Vorfeld der verpflichtenden Zertifizierungen interne Audits durch, um eventuelle Schwachstellen aufzudecken und rechtzeitig Maßnahmen zur Erhöhung der Sicherheit ergreifen zu können. Unabhängig davon, ob es sich um ein vorbereitendes Audit oder eine externe Prüfung handelt:

Das erforderliche Reporting gestaltet sich im z/OS-Umfeld aufgrund des hohen Datenvolumens und der meist komplizierten RACF-, SMF- und Betriebssystemeinstellungen als sehr aufwändig. Durch den Einsatz plattformübergreifender Reporting-Tools kann der Aufwand nach Erfahrungen von Beta Systems um 50-80 Prozent reduziert werden.

Risiken für die Unternehmenssicherheit

Fehlendes RACF-Know-how kann zu eklatanten Sicherheitsrisiken führen.

Grundsätzlich sind Mainframes zuverlässiger und leistungsfähiger als viele Serversysteme. Doch beim Berechtigungsmanagement kann es zu eklatanten Sicherheitsrisiken kommen, wenn fehlendes Know-how mit der komplizierten Bedienung von RACF zusammenkommt. Die wichtigsten Risiken werden im Folgenden kurz dargestellt.

1. Mangelnde Transparenz bei komplexen Berechtigungsstrukturen

Die Gruppen- und Profilhierarchien in RACF sind sehr komplex. Dies resultiert häufig aus der Verschmelzung verschiedener Datenbanken. Die ineinander verschachtelten Zugriffsberechtigungen transparent darzustellen ist äußerst schwierig, so dass Sicherheitsverstöße bei unqualifizierter Nutzung manchmal unentdeckt bleiben.

2. Bedienfehler durch mangelndes Know-how

Berechtigungen können bei RACF nur von Spezialisten geändert werden, die die nötigen Befehle und Einzelaktionen beherrschen. Ist dieses Know-how im Unternehmen nicht vorhanden, kann es passieren, dass zum Beispiel Zugriffsrechte falsch definiert werden und geschützte Applikationen von nicht autorisierten Personen(gruppen) editiert werden können.

Ein weiteres Sicherheitsrisiko entsteht, wenn es versäumt wird, das Kommando zum Herunterfahren von RACF zu schützen und jeder Mitarbeiter dies einfach deaktivieren kann. Damit solche Bedienfehler vermieden und Schwachstellen schnell aufgedeckt werden können, ist tiefes und langjähriges Fachwissen erforderlich. Doch RACF-Experten werden immer seltener. Die Spezialisten gehen in Rente, und junge, Windows- und Mac-gewöhnte Administratoren rücken nach, die den Mainframe-Computer ohne RACF-Know-how bedienen müssen. Das macht es

schwierig, die Sicherheitsstufe aufrechtzuerhalten, um geschäftskritische Ressourcen zuverlässig zu schützen.

3. Keine einfachen Backup-Möglichkeiten

Kommt es bei Änderungen an der RACF-Datenbank zu Fehlern, beispielsweise durch falsche RACF-Kommandos, so bietet das IBM-System kaum Möglichkeiten, diese schnell zu bereinigen.

4. Wissensverlust bei selbstgeschriebenen Lösungen

Aufgrund der wenig komfortablen Bedienung von RACF haben viele Unternehmen selbst Interfaces geschrieben, die es ihnen ermöglichen, Berechtigungen in RACF einfacher zu verwalten. Bei diesen selbstgeschriebenen Lösungen gibt es jedoch ein Problem: Verlässt der Mitarbeiter, der sie entwickelt hat, das Unternehmen, dann geht auch das Know-how verloren, um diese Lösungen weiter pflegen und an RACF-Erweiterungen oder neue Sicherheitsbedrohungen anpassen zu können.

5. Fehlende Kontinuität von Administrationssoftware

Nicht nur mit eigenen Lösungen versuchen Unternehmen das RACF-System besser handhabbar zu machen. Im Markt gibt es mittlerweile eine Reihe von Standardlösungen, die bei der Administration unterstützen. Nicht selten kommt es allerdings vor, dass Anbieter nach einigen Jahren ihre Software abkündigen und keinen Support mehr bieten. Das bedeutet für die Unternehmen ein signifikantes Sicherheitsrisiko, da durch die fehlende Administration ihre Lösung den aktuellen Bedrohungen nicht mehr gerecht werden kann.

Wachsende Anforderungen durch die Digitalisierung

Sowohl die Anzahl als auch die Art der Zugriffe auf Mainframe-Systeme verändern sich.

In Zeiten von Cloud Services und Mobile Computing steigen die Anforderungen an Identitäts- und Zugangsmanagement-Lösungen. Immer mehr Applikationen greifen auf die datenführenden Mainframe-Systeme zu. Und auch die Anzahl der Interaktionen mit dem Mainframe steigt rasant. Die IT-Abteilung ist hier gefordert, den Benutzern einen unkomplizierten und reibungslosen Zugriff auf die Vielzahl an Ressourcen zu ermöglichen. Gleichzeitig muss sie sicherstellen, dass kritische Daten und Infrastrukturen zuverlässig geschützt sind und dazu beispielsweise moderne Sicherheitskonzepte wie Zertifikate auf dem Großrechner integrieren. Um diese Aufgaben zu bewältigen braucht es spezielle Systeme. Selbstgeschriebene RACF-Interfaces sind den Anforderungen in der Regel nicht gewachsen. Die meisten Unternehmen sind sich dessen auch bewusst: In einer aktuellen Studie von Kuppinger Cole Ltd.[6] gaben 87 Prozent der Befragten an, dass eine ausgereifte IAM-Lösung eine wichtige Voraussetzung für eine erfolgreiche digitale Transformation sei.

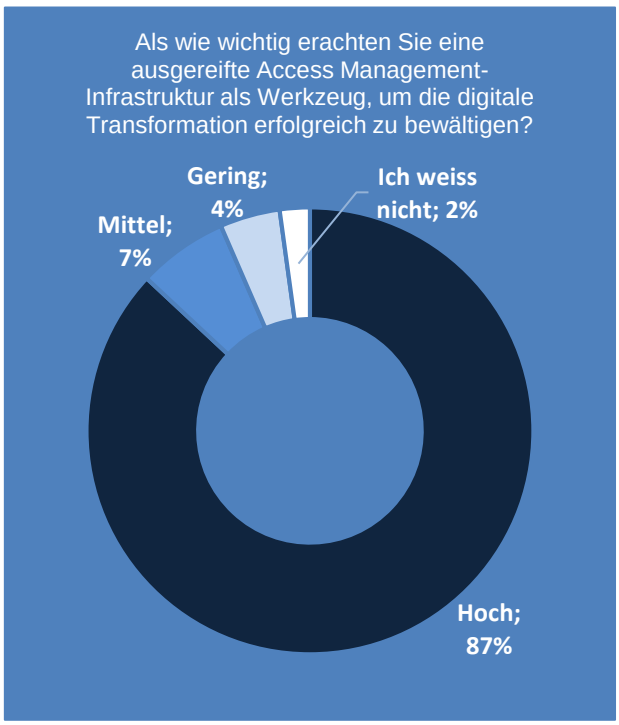

Abb. Die Notwendigkeit einer ausgereiften Identity & Access Management-Infrastruktur zur erfolgreichen Bewältigung der digitalen Transformation.

Immer mehr Änderungen sind in immer kürzeren Abständen auf einer eigentlich starren Umgebung durchzuführen.

Mehr Schnittstellen, mehr User, mehr Daten – die Mainframe-Systeme müssen sich diesen wachsenden Anforderungen anpassen. Und das in einer immer höheren Geschwindigkeit. Denn durch die digitale Transformation ändert sich auch die Erwartungshaltung. Und zwar nicht nur die der Kunden, für die es heute selbstverständlich ist, von überall schnell auf alle Anwendungen zuzugreifen, sondern auch die des Managements: Großrechner sollen sich heute genauso schnell anpassen können wie neue Applikationen bereitgestellt werden. Doch Großrechner sind eine sehr kontrollierte und stabile Umgebung. Für das IT-Team ist es daher eine echte Herausforderung, in immer kürzeren Abständen immer mehr Änderungen auf dem System durchzuführen. Sie sind gebunden mit Altapplikationen, die sie nicht verändern können, müssen aber Daten und Anwendungen schnellstmöglich nutzbar machen.

> *"Mehr Schnittstellen, mehr User, mehr Daten – die Mainframe-Systeme müssen sich diesen wachsenden Anforderungen anpassen. Und das in einer immer höheren Geschwindigkeit."*

[6] Kuppinger Cole / CXP Group: Identity and Access Management in the Digital Age, 2017.

Compliance mit gesetzlichen Vorschriften

Unternehmen müssen Compliance mit einer Vielzahl an Regularien sicherstellen.

Unternehmen müssen heute eine Vielzahl an gesetzlichen Bestimmungen erfüllen. Dies gilt besonders für stark regulierte Branchen wie den Finanzsektor. Für die Unternehmen ist mit den Compliance-Anforderungen in der Regel ein hoher zeitlicher und finanzieller Aufwand verbunden. Und es kommen immer neue Regelungen hinzu, wie aktuell zum Beispiel die Europäische Datenschutzgrundverordnung. Sie alle möglichst effizient umzusetzen, ist die zentrale Herausforderung, denen die Unternehmen heute gegenüberstehen. Im Folgenden werden drei der wichtigsten Vorschriften mit ihren Auswirkungen auf das Berechtigungsmanagement skizziert.

1. DSGVO für EU-weit einheitlichen Datenschutz

Eine der bedeutendsten Veränderungen im Datenschutzbereich der letzten 20 Jahre ist die Europäische Datenschutzgrundverordnung (DSGVO, englisch: General Data Protection Regulation, GDPR). Ihr Ziel ist es, den Datenschutz EU-weit einheitlich zu regeln. Dazu definiert sie Mindeststandards für den Umgang, die Sicherung und die Weitergabe von personenbezogenen Daten. Halten Unternehmen die DSGVO-Vorschriften nicht ein, drohen hohe Bußgelder. Gemäß einer von Bitkom veröffentlichten Umfrage[7] war die Reform aber im Juni 2017 noch für jedes fünfte Unternehmen kein Thema. Und 42 Prozent der Unternehmen beschäftigen sich zwar mit der DSGVO, haben aber noch keine Maßnahmen begonnen.

Die DSGVO schreibt Unternehmen unter anderem vor, dass alle Instanzen von Kundendaten nachverfolgbar sein müssen, dass sie die Zustimmung der Betroffenen zur Nutzung ihrer Daten einholen sowie die eingesetzten Maßnahmen zur Verwaltung dieses Prozesses für Auditoren dokumentieren müssen[8]. Dies ist gleich aus mehreren Gründen schwierig: Erstens steigt die Menge der gesammelten Daten rasant an, so dass deren Management immer aufwändiger wird. Zweitens erhöhen Trends wie agile Development und DevOps die Veränderungsgeschwindigkeit. Und drittens sind durch digitale Technologien und die Auslagerung von Prozessen an Dienstleister die IT-Strukturen immer komplexer geworden, so dass es schwierig ist, den Überblick über die im Unternehmen verarbeiteten personenbezogenen Daten zu behalten. Viele Unternehmen wollen daher im Zuge der DSGVO-Umsetzung in Information Governance Lösungen investieren. Auch der Bedarf nach Identity and Access Management (IAM) wächst, um das erforderliche Datenschutzniveau in allen Unternehmensbereichen sicherstellen zu können.

2. PCI-DSS regelt Umgang mit Karten- und Transaktionsdaten

Für Unternehmen, die Kreditkartentransaktionen tätigen, gilt darüber hinaus der Payment Card Industry Data Security Standard, kurz PCI-DSS. Dieser definiert Sicherheitsanforderungen, die Unternehmen in Bezug auf die Verarbeitung, Speicherung und Übertragung von Karten- und Transaktionsdaten erfüllen müssen.[9]

---

[7] Bitkom Research, Umfrage Juni 2017: https://www.bitkom.org/Presse/Presseinformation/Jedes-fuenfte-IT-Unternehmen-ignoriert-bislang-Datenschutzgrundverordnung.html

[8] Antworten auf die wichtigsten Fragen zur EU-Datenschutz-Grundverordnung sowie Leitfäden zur datenschutzkonformen Datenverarbeitung bietet Bitkom unter: https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/Inhaltsseite-2.html

[9] Das PCI Security Standards Council bietet das komplette Regelwerk zum Download unter: https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss.

Dazu gehören ein striktes Passwortmanagement sowie die automatischen Generierung von „Audit-Trails“, mit denen der Zugriff auf Systemkomponenten einzelnen Usern zugeordnet werden kann. Außerdem müssen Protokolle und Systemereignisse kontinuierlich auf Unregelmäßigkeiten oder verdächtige Aktivitäten überprüft werden. Die PCI-Konformität muss regelmäßig durch eine Zertifizierung nachgewiesen werden, die eine Selbstbewertung ebenso wie externe Schwachstellen-Scans durch einen Approved Scanning Vendor (ASV) umfassen.

3. MaRisk definiert strenge Zugriffsrechte

Unternehmen aus dem Finanzsektor müssen zusätzlich die Bestimmungen der MaRisk beachten. In dem Regelwerk hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) strikte Vorgaben für die Vergabe und Kontrolle von Zugriffsrechten definiert – für die Prozesse ebenso wie für die damit verbundener Aufgaben, Verantwortlichkeiten und Kontrollen. Deren Einhaltung wird im Rahmen der Jahresabschlussprüfung geprüft und ist auch häufig Gegenstand von Sonderprüfungen. Im Bereich „kritischer Berechtigungen“ sind sogar mindestens halbjährliche Überprüfungen vorgeschrieben. Die MaRisk verweisen auf die Einhaltung des IT-Grundschutzkatalogs des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[10] und des Standards ISO/IEC 2700X.

Unternehmen sind nicht ausreichend vorbereitet

Selbstentwickelte Lösungen sind in den Unternehmen sehr verbreitet, werden aber den neuen Anforderungen nicht gerecht.

Wie die oben genannte Studie von Kuppinger Cole zeigt, hat ein Großteil der Unternehmen zwar erkannt, dass sie zur Bewältigung der aktuellen Herausforderungen auf ausgereifte Lösungen im Bereich Identity und Access Management setzen müssen. Doch bei vielen hapert es noch an der Umsetzung: Über 70 Prozent der Unternehmen setzen für das IAM derzeit noch auf einem Mix aus Standardsoftware und selbstentwickelten Lösungen[11]. Das ist riskant, denn Eigenentwicklungen stoßen oft an ihre Grenzen, wenn neue Anforderungen hinzukommen. So sind die Systeme beispielsweise in den meisten Unternehmen nicht in der Lage, Cloud-basierte Umgebungen zu unterstützen. Nur 19 Prozent geben an, mit ihrem IAM-System sowohl die Zugriffsrechte für Cloud Service als auch für Applikationen auf den eigenen Servern steuern zu können. Angesichts der Tatsache, dass aber fast jedes Unternehmen Cloud Services nutzt, besteht hier dringender Handlungsbedarf.

Ähnliches gilt in Bezug auf die Europäische Datenschutz-Grundverordnung: Während mehr als 70 Prozent damit rechnen, dass die neue Verordnung Auswirkungen auf ihr Unternehmen haben wird, fühlt sich nur die Hälfte darauf vorbereitet.[12] 52 Prozent gehen sogar davon aus, dass sie die Anforderungen nicht rechtzeitig bis Mai 2018 erfüllen können – auch wenn sie das Thema mittlerweile ganz oben auf ihrer Agenda gesetzt haben.

---

[10] Das BSI definiert in M4.211 des IT-Grundschutzkatalogs konkrete Regeln zum Einsatz von RACF: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04211.html

[11] Kuppinger Cole / CXP Group: Identity and Access Management in the Digital Age, 2017, S. 14.

[12] Ebd., S. 22.

Die Digitalisierung und der Zwang zur Compliance erhöhen somit den Druck auf die IT-Verantwortlichen, ihr Berechtigungsmanagement zu modernisieren und auf ausgereifte Standardlösungen zu setzen. Doch sie sollten es dabei nicht nur als Pflicht verstehen, sondern auch als Chance: Denn eine Modernisierung trägt auch dazu bei die Produktivität des eigenen Teams zu steigern und Sicherheitsrisiken besser abzuwehren.

Abb. Die meisten Organisationen gehen davon aus, dass sich die EU-DSGVO in hohem Maße auf ihre Geschäftsprozesse auswirken wird.

Wege zur Optimierung des Berechtigungsmanagements

Um das Berechtigungsmanagement in Mainframe-Systemen zu vereinfachen und gleichzeitig sicherer zu gestalten, können IT-Leiter an unterschiedlichen Stellen ansetzen. Diese Maßnahmen sollten jedoch nicht isoliert betrachtet werden. Vielmehr kommt es in der Praxis auf eine sinnvolle Kombination an.

1. Bereinigen Sie Ihre Berechtigungsstrukturen regelmäßig.

Aufgrund der komplizierten Bedienung von RACF und des fehlenden Know-hows kommt es häufig vor, dass IT-Mitarbeiter sich nicht trauen, Berechtigungen zu löschen oder neu zu strukturieren. So werden die Berechtigungsstrukturen mit der Zeit immer komplexer und undurchsichtiger. Lassen Sie Ihr System daher regelmäßig von einem Experten überprüfen und bereinigen. Entsprechende Dienstleistungen bieten zahlreiche Unternehmen, u.a. auch Beta Systems, an.

2. Setzen Sie Monitoring-Tools ein, um Strukturen transparent zu machen.

Mit Software, die überwacht, welche Berechtigungen noch aktiv genutzt werden, lässt sich schnell erkennen, was deaktiviert und im nächsten Schritt gelöscht werden kann. Mit solchen Monitoring-Lösungen sind zwar Investitionen verbunden, diese zahlen sich aber durch die Zeitersparnis bei der Fehlersuche und vor allem durch die größere Systemsicherheit schnell wieder aus.

3. Bauen Sie intern Know-how für das Berechtigungsmanagement auf.

Aufgrund des Fachkräftemangels denken einige Unternehmen darüber nach, das Berechtigungsmanagement an einen externen Dienstleister auszulagern. Doch diese Lösung befreit nicht davon, sich mit dem Thema zu beschäftigen. Denn ein Dienstleister kann nur mit einem bereinigten System arbeiten, so dass diese Aufgabe in jedem Fall vorab zu erledigen ist. Außerdem ist er aufgrund fehlender Kenntnis der internen Strukturen auf eine enge Zusammenarbeit angewiesen. Zu bedenken ist auch, dass es sogar das Sicherheitsrisiko erhöhen kann, wenn ein sensibles Thema wie die Kontrolle über den Schutz der eigenen Ressourcen an Externe übertragen wird. Machen Sie sich bewusst, dass die Verantwortung für das Berechtigungsmanagement in jedem Fall im Unternehmen liegt. Definieren Sie hierfür klare Verantwortlichkeiten und bauen Sie Know-how auf.

4. Ersetzen Sie selbstgeschriebene Interfaces durch eine Standardlösung.

Lösungen für die RACF-Administration müssen sich jederzeit an veränderte Bedingungen anpassen lassen. Das ist bei selbstgeschriebenen Interfaces oft schwierig, wenn die Programmierer nicht mehr im Unternehmen sind. Um dem Know-how-Verlust entgegenzuwirken, empfiehlt sich der Einsatz von Standardlösungen. Wichtig dabei ist, zu prüfen, dass der Anbieter die Software langfristig warten und weiterentwickeln kann.

Argumente für eine Standardlösung:

- Schnelligkeit und Sicherheit bei der Modifikation der Mainframe-Applikationslogik
- Zeitersparnis und Kostenreduktion bei der Benutzerverwaltung
- Erhöhung des Sicherheits- und Compliance-Levels
- Transparenz in der Governance
- Agile Reaktion auf Änderungen in der Organisation und Anforderungen der Kunden
- Abschwächung des drohenden Verlusts von Mainframe-Fähigkeiten

5. Führen Sie regelmäßig RACF-Audits durch.

RACF muss permanent überprüft werden, um Schwachstellen aufzudecken: Ist das System noch in der Lage, Risiken im IT-Betrieb rechtzeitig zu erkennen? Gibt es Implementierungsfehler, die die Sicherheit gefährden? Um alle möglichen Fehlerquellen abzudecken, empfiehlt sich die Nutzung eines Prüfleitfadens, der sich am IT-Grundschutzkatalog des BSI[13] orientiert. Darin sind Vorgehen und Inhalte eines RACF-Audits detailliert beschrieben. Grundsätzlich sollten im Rahmen des Audits immer zwei Bereiche geprüft werden: die Konfiguration der RACF Sicherheitseinstellungen sowie die aufgezeichneten Events, die auf mögliche Angriffe deuten können.

Um die Auditierung zu vereinfachen bietet sich der Einsatz spezieller Software-Lösungen an. Diese können den Auditierungsprozess deutlich verkürzen und damit die Kosten um bis zu 50 Prozent senken. Doch die Unternehmen sollten bedenken, dass es mit der Installation einer solchen Zusatzsoftware allein nicht getan ist. Die Beurteilung der aufgedeckten Schwachstellen muss durch Menschen erfolgen, weshalb grundsätzlich eine Kombination von Tools und Beratung sinnvoll und empfehlenswert ist.[14]

[13] Informationen zu den IT-Grundschutzkatalogen des BSI: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[14] Weitere Tipps zur Durchführung von RACF-Audits bietet Beta Systems in einem Blogbeitrag: http://blog.betasystems-dci.de/racf-audit-minimiert-risiken-bei-mainframe-kunden/

Effiziente und sichere RACF-Administration mit Beta 88

Als Antwort auf die wachsenden Anforderungen bei der Verwaltung der Zugriffsrechte hat Beta Systems die Software-Suite Beta 88 entwickelt. Damit können auch Personen ohne Spezialwissen den z/OS Security Server RACF sicher verwalten und Audit-Berichte erstellen. Denn die Lösung zeichnet sich durch ein im Vergleich zu anderen Administrationslösungen besonders einfaches Handling aus.

Standardaufgaben wie das Zurücksetzen von Passwörtern lassen sich an Helpdesk-Mitarbeiter übertragen, was für die zentrale IT-Administration eine große Entlastung bedeutet. Als Überwachungstool benachrichtigt Beta 88 zudem in Echtzeit über das Auftreten kritischer RACF-Ereignisse, beispielsweise wenn auf sensible Daten zugegriffen oder User-Attribute geändert werden. Diese Funktionen sowie die Möglichkeiten, Versionen vorzuhalten und Backups zu erstellen, erhöhen die Systemsicherheit ganz wesentlich.

Die Module von Beta Systems z/OS Access Rights Management Suite für RACF, kurz Beta 88, entsprechen den typischen Tätigkeitsfeldern der RACF-Administration und lassen sich einzeln sowie in Kombination einsetzen.

Beta 88 Administrator

- ✓ Effizientes und sicheres RACF Berechtigungsmanagement
- ✓ Automatische Generierung von RACF-Befehlen
- ✓ Zusammenführen mehrerer RACF-Datenbanken
- ✓ Pflege der RACF-Profile

Beta 88 Auditor

- ✓ Sicherheitslücken im RACF-System aufdecken und Compliance Vorgaben erfüllen
- ✓ Berichte über Berechtigungen und Rollenvergabe erstellen
- ✓ Audits mit der anwenderfreundlichen Windows-Oberfläche

Beta 88 Web Helpdesk

- ✓ Standard-Aufgaben können über eine moderne Web-Administrations-Oberfläche von Helpdesk-Mitarbeitern erledigt werden
- ✓ Änderungen nach Freigabe für RACF-Berechtigungen und Profile

Beta 89 Monitor

- ✓ Automatische Benachrichtigungen beim Auftreten von sicherheitsrelevanten RACF-Ereignissen
- ✓ Generieren von einfachen Audit-Reports für bestimmte Ereignisse

Beta 88 Report Generator

- ✓ Umfassende und vollständige Informationen zu RACF-Daten nach Bedarf
- ✓ Flexible und leicht zu erweiternde Reports

Beta 88 Resource Drill-Down Facility

- ✓ RACF-Daten im familiären Windows-Look & Feel
- ✓ Transparenz der RACF-Daten für Auditoren, auch ohne Mainframe-Know-how
- ✓ Mehrsprachige Oberfläche

Fazit: Mainframe-Security der nächsten Generation

Unternehmen stehen bei der Verwaltung ihrer sichersten Plattform vor großen Herausforderungen: immer größere Datenmengen, das Verschwinden traditioneller Netzwerkgrenzen, die Verpflichtung zur Überwachung der Zugriffskontrolle, ein Mangel an qualifiziertem Personal, – all das kann hohe Kosten und schwerwiegende Sicherheitsprobleme nach sich ziehen. Unternehmen sind hier auf eine Lösung angewiesen, mit der das Berechtigungsmanagement in Mainframe-Systemen sowohl sicherer als auch effizienter wird.

Schwerpunkte sind dabei vor allem eine einfach zu handhabende Benutzerverwaltung, das Monitoring von sicherheitsrelevanten RACF-Ereignissen in Echtzeit sowie das Automatisieren von Reporting- und Prüfaufgaben. Damit ist es auch Personen ohne Spezialwissen möglich, den z/OS Security Server RACF sicher zu verwalten und Audit-Berichte schnell und zuverlässig zu erstellen. Die IT-Administration wird so deutlich entlastet, Kosten werden gesenkt und die Sicherheit im Unternehmen wesentlich erhöht.

Über Beta Systems DCI Software AG

Beta Systems entwickelt seit über 30 Jahren hochwertige Infrastruktur-Softwareprodukte für die sichere und effiziente Verarbeitung großer Datenmengen zur bestmöglichen Erfüllung aller rechtlichen und geschäftlichen Anforderungen. Die Multiplattform-Softwarelösungen für z/OS-, Unix-, Linux- und Windows-Umgebungen automatisieren, dokumentieren und analysieren geschäftstragende IT-Abläufe in Rechenzentren von Großunternehmen, IT-Dienstleistern, öffentlichen Einrichtungen und mittelständischen Betrieben. Das Data-Center-Intelligence-Portfolio von Beta Systems fokussiert auf die Bereiche Output-Management & Archivierung, Log/ Security Information Management und Workload Automation.

Beta Systems DCI Software AG
Alt-Moabit 90 d
10559 Berlin

Tel. +49 (0) 30 726 118-0
Fax: +49 (0) 30 726 118-800
info@betasystems.com

www.betasystems-dci.de