Bild: © Fotolia.com/sellingpix

Besondere Herausforderung für Finanzinstitute: EU-DS-GVO und BAIT

Wer darf was? – Zugriffsrechte sicher verwalten

Die Europäische Datenschutz-Grundverordnung (EU-DS-GVO) regelt ab dem 25. Mai 2018 den Schutz personenbezogener Daten. In vielen Unternehmen überwiegt die Unsicherheit, und IT-Verantwortliche wissen oft noch nicht genau, was zu tun ist. Dabei gibt es Software-Tools, die die Umsetzung stark vereinfachen können. Für die sichere Verwaltung der Zugriffsrechte erfüllt eine EU-DS-GVO-konforme Access-Governance-Lösung die Anforderung. Zudem entlastet das System die IT-Abteilung und spart Kosten.

Nach dem Stichtag müssen Unternehmen personenbezogene Daten gegen Verlust und unbeabsichtigte Änderungen sichern.[1] Zu diesem Zweck schreibt der Gesetzgeber mit der DS-GVO unter anderem die regelmäßige „Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“[2] vor. Dies gilt auch für die Mitarbeiterzugriffsberechtigungen für Daten in Unternehmen.

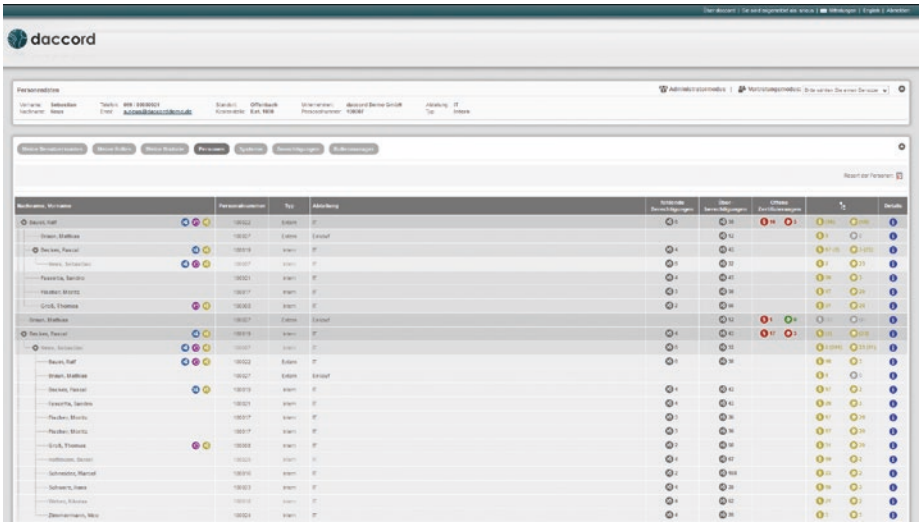
Hinzu kommen weitere technische und organisatorische Schutzmaßnahmen. Die DS-GVO verpflichtet Unternehmen außerdem dazu, Verletzungen des Datenschutzes innerhalb von 72 Stunden einer Aufsichtsbehörde zu melden.[3] Bei besonders schweren Fällen müssen sie zusätzlich die betroffene Person benachrichtigen. Bei Datenschutzverletzungen dürfen Unternehmensverantwortliche also keine Zeit verlieren. Das betroffene Unternehmen muss schnell nachweisen können, dass alle vorgeschriebenen Maßnahmen zum Schutz der Daten erfüllt wurden. Bei Nichteinhaltung der Anforderungen drohen hohe Strafen. Die Regelung sieht Bußgelder vor von bis zu 20 Millionen Euro beziehungsweise vier Prozent des Jahresumsatzes.

Doch insbesondere bei Unternehmen mit komplexen IT-Landschaften fehlt es den Administratoren an den passenden Lösungen. Bei der Kontrolle von Zugriffsberechtigungen zum Beispiel brauchen sie praktikable Lösungen zur übersichtlichen Darstellung der Rechtestrukturen. Diese Darstellung hilft, Verstöße aufgrund von fehlerhaften Berechtigungen zu vermeiden. Kommt es dennoch zu einem Verstoß, wird die Ursache schnell erkannt. Zusätzlich liefert die Lösung wichtige Informationen für die Meldung an die Aufsichtsbehörden und eine Schließung der Lücke.

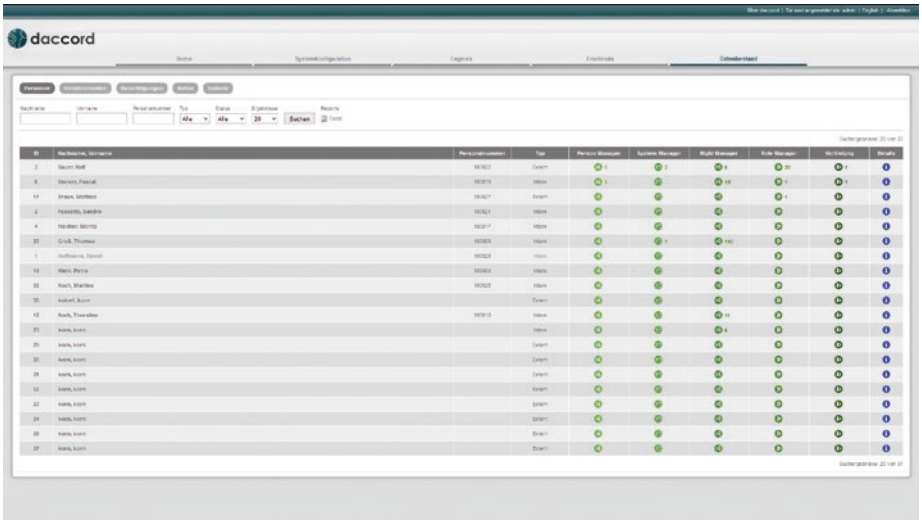
Nicht nur in großen Unternehmen ist die transparente und aktuelle Darstellung der Mitarbeiterberechtigungen eine Herausforderung: Zahlreiche Mitarbeiter mit ständig wechselnden Zuständigkeiten nutzen tagtäglich viele verschiedene Systeme. Ändern sich die Zuständigkeiten innerhalb der Belegschaft, müssen auch die Berechtigungen wieder neu zugeordnet werden, das heißt alte Berechtigungen werden entfernt und neue hinzugefügt. Immer wieder kommt es so zur Ansammlung von fehlerhaften Berechtigungen, die in der komplexen IT-Landschaft schnell übersehen werden. Diese Unregelmäßigkeiten in der Berechtigungsvergabe können jedoch schwerwiegende Folgen für das Unternehmen haben. Sie gefährden die firmeninterne IT-Sicherheit und können zu den erwähnten Bußgeldern führen.

Sicherheitslücke: fehlerhafte Berechtigung

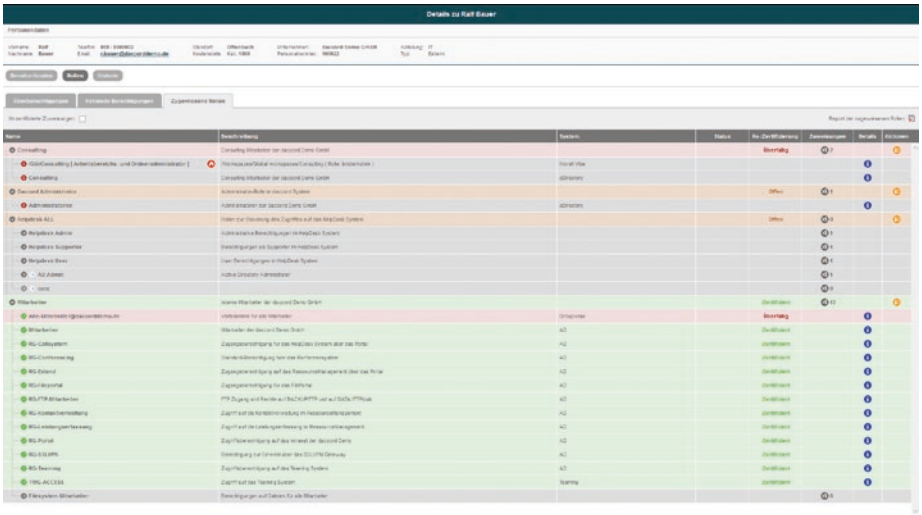
Finanzinstitute wie Banken stellen hier einen Sonderfall dar. Sie tragen die Verantwortung für tausende personenbezogene Datensätze sowie hochsensible Informati-



Rollen-Rezertifizierung (Quelle: G+H Systems)



Überarbeitung der Person-Manager-Sicht im User-Frontend (Quelle: G+H Systems)



Überarbeitung der Personenzuordnung im Admin Frontend (Quelle: G+H Systems)

onen. Dazu zählen neben Kundeninformationen – wie Name und Anschrift – auch bedeutsame Kontodetails. Auch deshalb geraten Banken häufig ins Visier von Hackern, die für diese Informationen auf dem Schwarzmarkt horrende Summen erhalten. Ein weiterer Grund ist noch naheliegender: Die Gruppe MoneyTaker erbeutete in den Jahren 2016 und 2017 bei mehreren Cyberattacken auf zwanzig Banken über zehn Millionen US-Dollar. Dazu infiltrierten sie die Systeme der Banken und verschafften sich nach und nach höhere Rechte. Diese nutzten sie, um zum Beispiel Geldkarten zu bestellen, deren Limit zu entfernen und anschließend damit Geld abzuheben.[4] Nicht selten werden derartige Cyberangriffe auch durch Insider, also eigene Mitarbeiter einer Organisation, durchgeführt oder vorbereitet beziehungsweise unterstützt. Durch fehlerhafte, unkontrollierte Berechtigungen entstehen also schnell erhebliche Schäden. Das Risiko solcher Angriffe kann mit einer Access Governance-Software minimiert werden. Sie überprüft kontinuierlich die Berechtigungsstruktur, erkennt Fehler frühzeitig und macht den Verantwortlichen auf Abweichungen aufmerksam.

Komplexe Rechtestrukturen von Banken

Die Rechtestrukturen von Banken und anderen Finanzdienstleistern sind gesetzlich stark reglementiert und äußerst komplex. Diese Komplexität erschwert die Verwaltung der Berechtigungsvergabe zusätzlich und erleichtert so Angriffe wie die von MoneyTaker. Häufig wird versucht, die Zugriffsberechtigungen manuell zu kontrollieren. Dafür müssen Einstellungen in vielen verschiedenen Systemen umständlich und zeitaufwendig ausgelesen, analysiert, abgeglichen und aktualisiert werden. Zudem fehlt es meist an einer übersichtlichen Darstellung der Berechtigungen, die deren Verwaltung und Kontrolle für die Personal- und Systemverantwortlichen deutlich vereinfachen würde. Dieser Überblick ist aber unerlässlich, um Vorgaben, wie die der Bundesanstalt für Finanzdienstleistungsaufsicht, zu erfüllen. Weitere Auflagen kommen von den „Bankaufsichtlichen Anforderungen an die IT" (BAIT), die unter anderem auch

den Umgang mit Benutzerberechtigungen regeln. Sie schreiben ein angemessenes internes Kontrollsystem vor, das Transparenz über den gesamten IT-Bereich bringt. Die BAIT verlangen, die Vorgaben eines Berechtigungskonzepts mit Genehmigungs- und Kontrollprozessen einzuhalten.[5] Eine Access-Governance-Lösung erfüllt diese Auflagen automatisiert. Sie unterstützt also bei der Erfüllung der verschiedenen rechtlichen Anforderungen (BAIT, MaRisk, DS-GVO etc.) und steigert gleichzeitig die interne IT-Sicherheit.

Wirtschaftlichkeit: Mitarbeiterzugriffsrechte effizient verwalten

Die manuelle Kontrolle von Zugriffsrechten ist – neben dem erhöhten Fehlerrisiko – kosten-, zeit- und personalintensiv. Um die IT-Verantwortlichen zu entlasten, kann ebenfalls eine Access-Governance-Lösung eingesetzt werden. Diese liest die bestehenden Rechtestrukturen eines Unternehmens aus und stellt sie dem definierten Soll-Konzept gegenüber. Darüber hinaus können Verantwortliche anhand eines Rollenmodells schnell und einfach überprüfen, welcher Mitarbeiter auf welche Daten zugreifen kann und ob er diese Berechtigung auch tatsächlich haben soll. Stellt die Software bei einer automatischen Routineprüfung fest, dass Soll- und Ist-Zustand voneinander abweichen, wird der für die Berechtigungen verantwortliche Mitarbeiter alarmiert. Risikobehaftete Überberechtigungen oder nicht eingehaltene Funktionstrennungen (Segregation of Duties) können schnell erkannt und beseitigt werden. So entlastet die Software IT-Verantwortliche, in dem sie die Rechtestrukturen eines Unternehmens kontinuierlich überprüft. Sie erfasst die Zugriffsrechte sämtlicher IT-Systeme und unterstützt eine fehlerfreie Berechtigungsvergabe.

Access-Governance-Lösung: Worauf achten?

Aber woran erkannt man eine gute Access-Governance-Lösung? Erfahrungen aus dem Beratungsalltag legen nahe, dass sie mindestens die folgenden fünf Punkte erfüllen sollte:

1. Sie erfasst, strukturiert und kontrolliert vollständig und kontinuierlich alle Informationen über Mitarbeiterzugriffsrechte aus sämtlichen Anwendungen der firmeninternen IT-Landschaft.
2. Die Software unterstützt neben den herkömmlichen Anwendungen auch weniger verbreitete und selbst entwickelte Systeme. Dabei ist es unerheblich, ob es sich um lokale oder um cloudbasierte Systeme handelt.
3. Zur Abstraktion der Berechtigungen ist die Bildung eines Rollenmodells zu empfehlen. Das erleichtert die Verwaltung von Berechtigungen in Gruppen und beugt so Fehlern vor.
4. Um die Rechteverwaltung weiter zu vereinfachen, verfügt die Software über die Möglichkeit eines Soll-Ist-Abgleichs. Damit können Verantwortliche Abweichungen in der Berechtigungsvergabe auf einen Blick feststellen. Eine automatische Benachrichtigungsfunktion bei Fehlern erleichtert die Kontrolle in komplexen Systemlandschaften zusätzlich.
5. Die Darstellung der Berechtigungen ist übersichtlich und lässt sich für verschiedene Nutzergruppen individuell anpassen. So erhöht eine Access-Governance-Lösung die Transparenz und vereinfacht notwendige Rezertifizierungsprozesse.

Fazit: keine Angst vor dem Datenschutz

Viele Unternehmen sehen in der Datenschutz-Grundverordnung in erster Linie eine aufwendige Neuerung. Zusätzlicher Druck durch drohende hohe Strafen verstärkt eine eher negative Wahrnehmung. Dennoch bietet die DS-GVO aber auch eine Chance: Der Datenschutz wird auf ein höheres Niveau gehoben. Davon profitieren alle: die Eigentümer der Daten ebenso wie die Organisationen, deren interne IT durch die Umsetzung besser geschützt ist. Viele der DS-GVO-Anforderungen lassen sich durch den Einsatz einer geeigneten Software schnell und einfach umsetzen. Eine Access-Governance-Lösung entlastet die Verantwortlichen, indem sie für den Schutz der Unternehmensinformationen sorgt. Das spart Kosten, und die IT-Mitarbeiter können sich anderen, ebenfalls wichtigen Aufgaben widmen. Access Governance bringt Kontrolle und Transparenz über sämtliche IT-Berechtigungen aller Anwendungen eines Unternehmens. Dadurch wird die Gefahr eines unberechtigten Zugriffs auf sensible Daten und Informationen deutlich minimiert. Eine Access-Governance-Lösung spart also Zeit und Kosten. Gleichzeitig sorgt sie für eine höhere IT-Sicherheit und unterstützt bei der Umsetzung gesetzlicher Vorgaben. ■

Quellenangaben:

[1] *Art. 5 Abs. 1 DS-GVO; https://dsgvo-gesetz.de/art-5-dsgvo/*

[2] *Art. 32 Abs. 1 DS-GVO; https://dsgvo-gesetz.de/art-32-dsgvo/*

[3] *Art. 33 Abs. 1 DS-GVO; https://dsgvo-gesetz.de/art-33-dsgvo/*

[4] *https://www.heise.de/newsticker/meldung/Hackergruppe-MoneyTaker-erbeutet-10-Millionen-US-Dollar-von-ueber-zwanzig-Banken-3916118.html*

[5] *https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=6*

JÜRGEN BÄHR,
Geschäftsführer bei G+H Systems