

# TRANSPARENZ AUF

## ACCESS GOVERNANCE – DATENSCHUTZ UND BERECHTIGUNGEN.

**?** **it security:** Herr Gertler, Sie und Herr Bähr blicken zusammen auf mehr als 30 Jahre Erfahrung im Bereich Identity & Access Management zurück. Sie haben mit daccord vor 8 Jahren eine eigene Access Governance-Software auf den Markt gebracht. Was war der Auslöser für diese Entwicklung?

**Thomas Gertler:** Wir haben in unseren Kundengesprächen immer wieder festgestellt, dass es vielen IT-Verantwortlichen nicht möglich war, schnell und einfach einen Überblick über die Zugriffsberechtigungen im Unternehmen zu erhalten. Bis dahin war es ein kosten- und zeitintensiver Vorgang manuell – oftmals in Excelsheets – alle Informationen zu erfassen. Zudem schlichen sich auch häufig Fehler ein. Gerade in Hinblick auf gesetzliche Vorgaben, wie ganz aktuell die DSGVO, gewinnen automatisierte Lösungen, die auf Knopfdruck alle notwendigen Informationen zur Verfügung stellen und kontinuierlich bereithalten, immer mehr an Bedeutung. Damit wir diese Transparenz auch möglichst lückenlos über alle Systeme in der IT-Landschaft im Unternehmen gewährleisten können, war es uns von Anfang an besonders wichtig, herstellerunabhängig zu sein.

**?** **it security:** Die DSGVO war in den vergangenen Wochen allgegenwärtig. Haben Sie den Eindruck, dass die Unternehmen fit sind in Sachen Datenschutz?

**Jürgen Bähr:** In unserem Geschäftsalltag erleben wir durchaus, dass viele Unternehmen sich der Gefahren durch Datenmissbrauch und Datenabfluss sowie deren Folgen bewusst sind. Vertrauliche Unternehmensinformationen, Kundendaten und Zugriffsberechtigungen werden aber dennoch oftmals nicht ausreichend geschützt. Das geschieht aus meiner Sicht nicht aus Unkenntnis, sondern liegt gerade im Mittelstand daran, dass zu wenig Zeit und Ressourcen für das Thema Sicherheit zur Verfügung stehen. Das kann für einen IT-Verantwortlichen im Arbeitsalltag zu einer unmöglichen Mission

werden. Hier sind einfache und schnelle Lösungen ein echter Mehrwert. Denn spätestens seit dem Stichtag der DSGVO müssen Unternehmen für den Schutz aller personenbezogenen Daten sorgen. Die Konsequenzen bei Nichteinhaltung der gesetzlichen

einsatzbereit sind und sofort Entlastung bieten sowie Unsicherheiten beseitigen.

**?** **it security:** Wo sehen Sie die größten Schwierigkeiten für Unternehmen in Hinblick auf die Mitarbeiterberechtigungen?

”

OFTMALS FEHLT ES IN DER KOMPLEXEN IT-LANDSCHAFT BEI DER MITARBEITERERFASSUNG AN EINER ÜBERSICHTLICHEN DARSTELLUNG DER RECHTESTRUKTUREN.

Thomas Gertler,  
Geschäftsführer  
G+H Systems GmbH  
[www.guh-systems.de](http://www.guh-systems.de)



Vorgaben sind abgesehen vom Imageschaden auch finanziell schmerzhaft.

**?** **it security:** Die Datenschutzgrundverordnung stellt viele Unternehmen vor eine große Herausforderung. Wie nehmen Sie die Herangehensweise der IT-Verantwortlichen in Bezug auf die DSGVO wahr?

**Jürgen Bähr:** Wir stellen immer wieder fest, dass in vielen Unternehmen die Unsicherheit überwiegt. Anstehende Prüfungen und die möglichen hohen Strafen, die bei Verstößen drohen, erhöhen zusätzlich den Druck auf die Unternehmen. Sie erleben die DSGVO tendenziell eher als Belastung und haben das Gefühl, dass ihnen die Zeit wegrennt. Umso wichtiger ist es für uns, Unternehmen in dieser Phase sinnvolle, einfache Lösungen an die Hand zu geben. Tools, die schnell

**Thomas Gertler:** Oftmals fehlt es in der komplexen IT-Landschaft bei der Mitarbeitererfassung an einer übersichtlichen Darstellung der Rechtestrukturen. Ein Mitarbeiter wechselt die Abteilung, ein neuer kommt – die Zuständigkeiten im Unternehmen können sich schnell ändern. Neue Zuständigkeiten beinhalten in der Regel auch neue Berechtigungen und dabei ist fast noch wichtiger, alte Berechtigungen wieder zu entziehen. Zusätzlich erschwert die gewachsene Struktur aus verschiedenen Systemen und Anwendungen die Kontrolle dieser Zugriffsrechte. Für IT-Verantwortliche und Fachabteilungen ist es eine Herausforderung, hier den Überblick zu bewahren. Die Rechtestrukturen transparent zu halten, kann viel Zeit in Anspruch nehmen und kostenintensiv sein. Immer wieder kommt es zu fehlerhaften Berechtigungen, die in der

# KNOPFDRUCK



”

FÜR UNS IST ES WICHTIG UNTERNEHMEN SINNVOLLE, EINFACHE LÖSUNGEN AN DIE HAND ZU GEBEN. TOOLS, DIE SCHNELL EINSATZBEREIT SIND UND SOFORT ENTLASTUNG BIETEN.

Jürgen Bähr,  
Geschäftsführer  
G+H Systems GmbH  
www.guh-systems.de

voll, aber zum Einstieg nicht zwingend notwendig: Mit daccord kann der Anwender zum Beispiel individuelle Rollenmodelle anlegen. So lassen sich Soll-Berechtigungen für bestimmte Abteilungen oder Positionen klar definieren. Auf Knopfdruck zeigt die Software Vergleiche zwischen dem Soll- und dem Ist-Zustand. Über- oder Unterberechtigungen der Mitarbeiter werden so schnell aufgedeckt, und Löschungen können über die Anwendung direkt initiiert werden. Bestenfalls erfolgt die Kommunikation mit einem IAM-System, das den Workflow automatisiert. In einem ersten Schritt kann es aber auch einfach eine Mail an den Verantwortlichen oder Ähnliches sein. Da sind wir mit daccord ganz flexibel – je nachdem, wie die IT im Unternehmen organisiert ist.

**?** **it security:** Wer gehört zur Zielgruppe Ihrer Access Governance-Lösung? Großunternehmen oder auch der Mittelstand?

komplexen IT-Landschaft schnell übersehen werden. Das kann die IT-Sicherheit eines Unternehmens erheblich gefährden.

**?** **it security:** Wie können Unternehmen die Kontrolle der Zugriffsrechte im Sinne der DSGVO reibungslos umsetzen?

**Thomas Gertler:** Es gibt Software-Tools, die bei der Umsetzung der Datenschutzgrundverordnung unterstützen und den Prozess dadurch wesentlich vereinfachen. Das Gleiche kann eine Access Governance-Software wie daccord für die Verwaltung der internen Rechtestrukturen leisten. Für ein effektives Management der Zugriffsrechte erfüllt eine DSGVO-konforme Access Governance-Lösung sämtliche Anforderungen. Die Software schafft Transparenz über die Rechtestrukturen im Unternehmen und verringert so den Verwaltungsaufwand in der IT-Abteilung.

**Jürgen Bähr:** Die Verantwortlichen sollten darauf achten, dass die Access Governance-Software sämtliche Zugriffsrechte der eingesetzten Cloud- und On-Premise-Anwendungen einliest und diese übersichtlich in personalisierten Web-Frontends darstellt. So lassen sich alle relevanten Informatio-

nen zu den Mitarbeiterberechtigungen auf einen Blick einsehen und überprüfen. Das spart neben Zeit auch Kosten. Die interne IT-Abteilung wird deutlich entlastet und kann die Verantwortung über die Kontrolle von Zugriffsrechten erstmalig an Fachabteilungen übergeben. Mit einer zusätzlichen Alarmierungsfunktion bei Abweichungen in der Berechtigungsvergabe ist man auf der sicheren Seite. Denn so ist eine unmittelbare Reaktion möglich, um eventuelle Unstimmigkeiten schnell zu beheben und Risiken zu minimieren.

**?** **it security:** Wie sehen Sie Access Governance-Lösungen im Vergleich zu IAM-Systemen?

**Thomas Gertler:** Auch wenn beim Kunden bereits ein IAM-System besteht, ist eine Access Governance-Software wie daccord sinnvoll, um zu kontrollieren, welche Daten tatsächlich im Zielsystem ankommen. Aufgrund unserer langjährigen Erfahrung im IAM-Bereich unterstützen wir viele Unternehmen bei der Implementierung ihres IAM-Systems. Hier stellen wir immer wieder fest, wie wichtig und hilfreich es ist, eine Access Governance-Software zusätzlich im Einsatz zu haben. Ein IAM-System ist sinn-

**Jürgen Bähr:** Da sprechen Sie einen wichtigen Punkt an. daccord ist derzeit sowohl bei Großunternehmen als auch im Mittelstand erfolgreich im Einsatz. Ob Banken, Krankenhäuser, Behörden oder kleine und mittelständische Betriebe – eine Access Governance-Software eignet sich für Unternehmen jeder Größe. Denn entscheidend ist nicht die Unternehmensgröße, sondern die Wichtigkeit der zu kontrollierenden Daten. Aufgrund des transparenten Lizenzmodells sowie einer kostengünstigen, individuell ausgearbeiteten Schnellanalyse im Vorfeld, ist unsere Lösung für jedes Unternehmen interessant, das bei der Kontrolle von Zugriffsberechtigungen Zeit- und Kostenersparnisse sucht sowie den gesetzlichen Anforderungen effektiv begegnen möchte.

**!** **it security:** Herr Gertler, Herr Bähr, wir danken für das Gespräch.

”  
THANK  
YOU