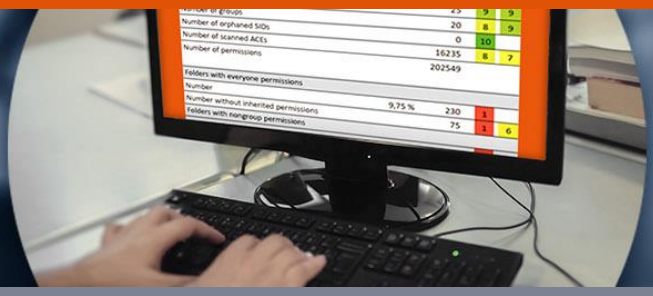
betasystems

GARANCY DATA ACCESS GOVERNANCE

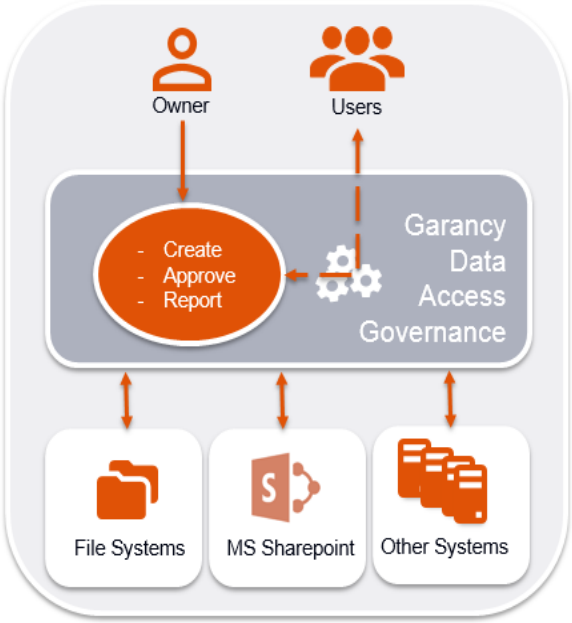


Sichere Steuerung des Zugriffs auf unstrukturiert abgelegte Daten

- *Wer vergibt bei Ihnen die Zugriffsrechte auf sensitive unstrukturierte Daten?*
- *Wissen Sie, wer der ‚Verantwortliche' für diese Daten ist?*
- *Wissen Sie, ob Ihre Zugriffssteuerung die Compliance-Anforderungen erfüllt?*

Erhöhte Sicherheit und verbesserte Genauigkeit

Die Menge an unstrukturierten Daten wie beispielsweise Dokumente, Tabellen, Präsentationen oder Emails wächst rasant. Dateisysteme und Berechtigungen werden zunehmend unüberschaubar. Die Informationssicherheit ist bedroht von ungewollten Rechteanhäufungen, mehrfach verwendeten Accounts und nicht entfernten Zugriffsrechten ausgeschiedener Mitarbeiter. Es muss daher klar sein, wer worauf Zugriff hat, wer den Zugang steuert und ob strukturelle Schwächen im Dateisystem ungewollten Datenabfluss begünstigen.



Fachabteilungen vergeben selbst Berechtigungen
Mit GARANCY Data Access Governance (DAG) kommt die Verantwortung für die gespeicherten Informationen zurück in die Fachabteilungen:

- Hier regeln Dateneigentümer ohne direktes Zutun der IT-Administration und in einer für sie verständlichen Form schnell und einfach, wer, wann, wo, welchen Zugriff auf bestimmte Datenressourcen haben soll.
- GARANCY DAG erlaubt die Zugriffsverwaltung unterhalb der Active Directory-Gruppenebene bis hinab auf die Ordner- und Dateiebene wie z.B. auf File Servern, in Microsoft SharePoint oder anderen Dokumenten Management Systemen.
- Integrierte Genehmigungs-Workflows oder Portal-Self-Services binden die jeweiligen Dateneigentümer oder Projektverantwortlichen automatisch in die Vergabeverfahren ein.

GARANCY DAG ermöglicht somit die kontrollierte Selbstverwaltung der Fachabteilungen mit Daten, Ressourcen und Zugriffsrechten in Einklang mit den relevanten Gesetzen und Normen.

Auf Basis einer bewährten Methodik wird ein **Berechtigungs-Audit** durchgeführt. Darauf basierend kann eine **automatisierte Konsolidierung der Dateisysteme** hinsichtlich der Zugriffsverwaltung erfolgen.

Drei-Phasen-Modell:

1. Analyse & Reporting: Berechtigungsaudit

- Berechtigungsanalyse: Automatisierte Identifikation und Analyse von Berechtigungen auf unstrukturiert abgelegte Daten mit Reporting „Wer darf was und wer hat wem welche Rechte erteilt?“
- Sicherheits-Analyse: Auflistung und Ranking der Gefährdungspotentiale unter Risikoaspekten mittels KPI's.
- Ergebnisberichte: Bewertung des Aufwands zur Behebung der Schwachstellen verbunden mit Handlungsempfehlungen.

2. Konsolidierung und Migration der bestehenden Systeme: Clean-Up

- Software Tool-unterstützte Restrukturierung der Ablage- und Berechtigungsstrukturen.
- Daten- und Rechtemigration ohne Beeinträchtigung der Geschäftsprozesse.

3. Data Access Governance: Kontrolle und Steuerung der Zugriffsrechte

- Sichere Verwaltung von Informationen, Berechtigungen und Ressourcen in Systemen mit unstrukturierten Daten.
- Dateneigentümer in den Fachbereichen steuern ihre Zugriffe selbst ohne direktes Zutun der IT.
- Keine Rechtevergabe mehr unter Umgehung der Regelprozesse: Rechtesteuerung über businessorientierte geregelte Antrags- und Genehmigungs-Workflows und Rollen von ihrer Anforderung über die Vergabe bis zu ihrer Validierung und dem sicheren Entzug.
- Integrierte Compliance-Checks: Automatische Einhaltung von unternehmensinternen und gesetzlichen Richtlinien für die Zugriffssteuerung auf kritische Daten (SOX, BDSG, MaRisk, GoBS/GDPdU, KonTraG etc.).
- Soll-Ist-Rechte-Abgleich mit unmittelbarem Aufdecken von riskanten Abweichungen.

Vollständige Integration mit GARANCY IAM

Das Data Access Governance Modul GARANCY DAG lässt sich mit der GARANCY IAM Suite koppeln, von der losen Anbindung bis zur tiefen Integration. Alle Informationen werden dem übergeordneten IAM-System zur Verfügung gestellt.

- Dateneigentümer regeln ohne direktes Zutun der IT und in einer für sie verständlichen Form wer, wann, wo, welchen Zugriff auf bestimmte Informationen haben soll.
- Administratoren, Operatoren oder User bleiben in ihrer gewohnten Umgebung und müssen sich nicht in ein weiteres System einarbeiten.
- Single Point of Administration.
- Aufnahme in bestehende Self-Service-Portale und Integration in bestehendes Reporting.

Kontaktieren Sie uns!

Beta Systems IAM Software AG

Alt-Moabit 90d | 10559 Berlin, Germany
+49 (0) 30 726 118 0
iam@betasystems.de
www.betasystems-iam.com

Partner