betasystems

GARANCY IAM SUITE

Passende Identity & Access Management Lösungen für dynamische Unternehmen!

60% aller Datendiebstähle in Unternehmen

werden durch Insider verursacht.

Diese verursachen einen 200% größeren Schaden

als Attacken von außen!

Laut AT Kearney kamen 30.000.000 Cyber-Angriffe in 2014 von innerhalb der Unternehmen

GARANCY IAM SUITE bildet die erste Verteidigungslinie

Fakten Check:

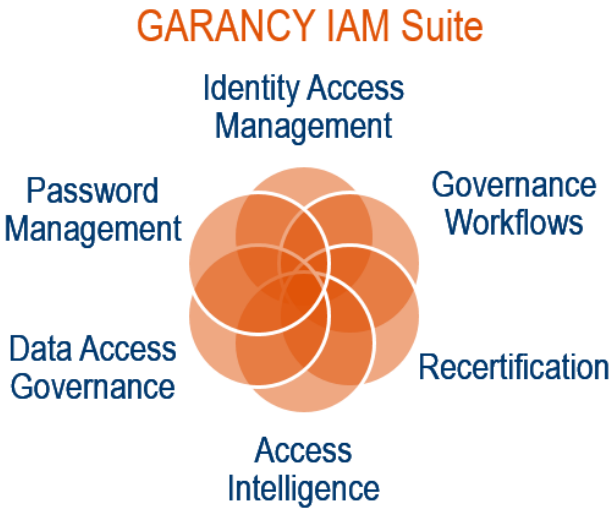
- Die Anzahl von Cyber-Angriffen auf Unternehmen wächst weiter.
- Weltweit >42.800.000 Angriffe registriert pro Jahr / 9 Attacken pro Sekunde.
- 60% der Angriffe werden durch Insider verursacht.
- Insider Attacken führen zu 200% größeren Schaden im Vergleich zu Angriffen von außen.
- Noch immer unterschätzen Unternehmen das potentielle Risiko innerhalb der Organisation.

Die Notwendigkeit einer ordnungsgemäßen Berechtigungsverwaltung und die Beschränkung der Zugriffsrechte auf ein erforderliches Minimum für die jeweilige Rolle werden immer wichtiger. Daher sollte Identity Access Management (IAM) auf der Agenda 2017 eines jeden IT Security Managers stehen.

Mit der GARANCY Identity Access Management Suite von Beta Systems steuern und überwachen Unternehmen den Zugriff auf Daten und Anwendungen gemäß der individuellen organisatorischen Anforderungen und fachlichen Rolle eines jeden Benutzers.

Die Module der GARANCY IAM Suite

Die Module der Beta Systems' IAM Suite bedienen alle Aufgaben von Identity Access Governance und sind sowohl in der Cloud als auch ‚on premise' verfügbar.



IAM – Brücke zwischen Business und Security

Das Provisioning Modul ermöglicht die zentrale Administration und Steuerung aller Berechtigungs-informationen der Anwender (Identitäten, Gruppen, Rollen) in sämtlichen IT-Systemen:

Provisionierung:

- Anbindung und Steuerung von IT-Applikationen durch die größte auf dem Markt verfügbare Auswahl von Out-of-the-Box Konnektoren.
- Flexibler und hochskalierbarer Abgleich des Identity Managements mit den anzubindenden Zielsystemen.
- Bereitstellung, Konsolidierung und Abgleich der Zugriffsrechte.
- Umsetzung von Veränderungen in Echtzeit.

User Management

- Automatischer Datenimport der HR Daten
- Unterstützung des User-Lebenszyklus (Eintritte, Kündigungen und Versetzungen).
- Differenzierung zwischen unterschiedlichen Benutzertypen (z.B. interne und externe Mitarbeiter).

Access Governance

- Role Lifecycle Management mit Rollen Hierarchien.
- Role Mining und automatische Zuordnung zu Rollen je nach identifiziertem Profil des Benutzers.
- Durchsetzung von SoD Regeln (Segregation of Duties).
- Steuerung der Autorisierung basierend auf Rollen und internen IT-Sicherheitsrichtlinien.

Audit und Security

- Festlegung von Audit-Prüfungen für die vergebenen Zugriffsrechte.
- Historisierung der Zugriffsrechte und deren Veränderungen.
- Single Point of Information und Umsetzung der Zugriffsrichtlinien.
- Unabhängige Verwaltung mehrerer Objekte durch eine einzelne IAM Plattform.

Insider Attacken verursachen fast 200% größeren Schaden

Ø je Schadensfall im Vergleich zu Angriffen von außen!

Studie der Carnegie Mellon University

Governance Workflow – Einbindung der Fachabteilungen

Die Verwendung von Governance Workflows innerhalb des IAM Systems ermöglicht es Kunden, ihre Prozesse digital zu gestalten und alle Prozesse, die in Verbindung mit Zugriffsrechten stehen, zu beschleunigen.

Sie binden Fachabteilungen direkt ein und stellen gleichzeitig sicher, dass die IT-Sicherheitsrichtlinien eingehalten werden und die zugewiesenen Berechtigungen rückverfolgbar und auditierbar sind.

Sie übertragen die Verantwortung für die Verwaltung der Zugriffsrechte auf die Fachabteilungen.

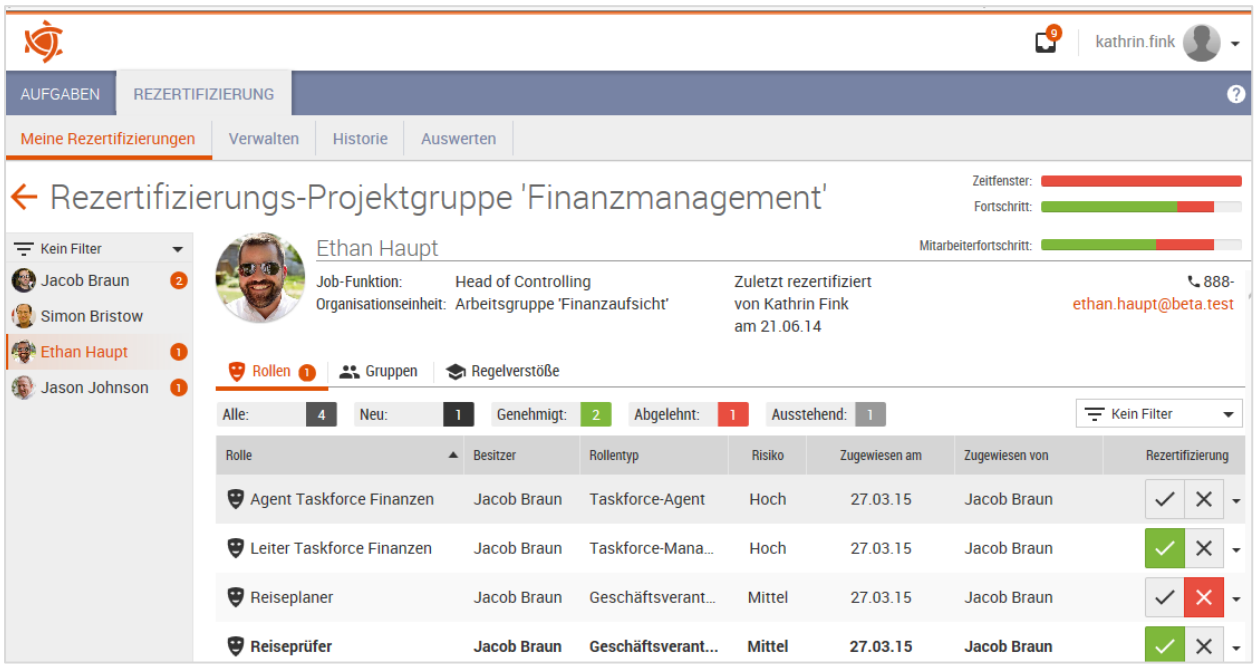
- Verkürzte Bearbeitungszeiten für Zugriffsfreigaben.
- Lückenlose Nachvollziehbarkeit für die Vergabe von Zugangsberechtigungen für IT-Anwendungen.
- Erhöhte Zufriedenheit der Anwender: Sie erhalten unmittelbar die benötigten Zugriffe.
- Einhaltung der Compliance-Vorgaben hinsichtlich regulatorischer Vorschriften, Normen und Standards
- Verringerter Arbeitsumfang für IT-Administratoren aufgrund der Einbindung der Fachabteilungen.
- Verkürzte Durchlaufzeiten aller Antragsprozesse

Rezertifizierung von Zugriffsrechten – Kontrolle ist besser als Vertrauen

Unsere Browser-basierte Portal Lösung für die effiziente Rezertifizierung von Zugriffsrechten ermöglicht es Unternehmen, die Zugriffsrechte interner und externer Benutzer zu überprüfen, erneut zu vergeben oder Zugriffsrechte zu widerrufen.

Dadurch wird die Sicherheit erhöht und die Genauigkeit der Berechtigungsvergabe verbessert.

- Am Risiko orientierte Rezertifizierung und Entzug von Zugriffsrechten.
- Rezertifizierungskampagnen auf Basis von Organisationen, Aufgaben oder Risikobewertungen.
- Substitution / Delegation über Workflows.
- Viele Ansichten: Single User Ansicht, Gruppenübersicht, SoD-Verletzungen, ...
- Fortschritt des Rezertifizierungsprozesses jederzeit einsehbar, inkl. Details wie Fälligkeitstermin, entzogene & rezertifizierte Berechtigungen.
- Schnellrezertifizierung und automatische „Out-of-the-Box“-De-Provisionierung.
- Auditierbare Kampagnen: vollständige Ereignisprotokollierung und Archivierung.
- Optimiert für die Nutzung auf Desktop und das mobile Arbeiten mit Tablet oder Mobilgeräten.



Password Management – Sicher und effizient

Das Password Management dient dem sicheren und einfachen Zugriff von Computern auf verschiedene IT-Plattformen oder Anwendungen in verteilten Systemen. Es vereinfacht die Durchsetzung der IT Sicherheitsrichtlinien, die mit Passwörtern verbunden sind.

Password Reset ermöglicht es den Anwendern, browser-basiert selbst Passwörter zurückzusetzen und zu ändern.

- Deutliche Entlastung des Helpdesks.
- Erhöhte Produktivität der Anwender aufgrund kürzerer Unterbrechungszeiten.

Password Synchronization ermöglicht den Mitarbeitern Zugriff auf verschiedene Plattformen oder Anwendungen mit einem einzigen Passwort. Passwortänderungen werden in allen gekoppelten Systemen und Anwendungen automatisch synchronisiert und sind anwendungs-übergreifend für den Benutzer verfügbar.

Access Intelligence – Reporting & Analytics

Das Access Intelligence-Modul nutzt Business Intelligence, um Zugriffsrechte zu verwalten. Die Lösung bietet Berichte und multidimensionale Analysen für die Prüfung der Berechtigungsstrukturen im Unternehmen und die Identifizierung potentieller Berechtigungsrisiken.

- 360° dynamisches Monitoring: Übersicht über Zugriffsrechte und damit verbundene Risiken.
- Vollständiger Überblick über Security Indikatoren in Form von benutzerfreundlichen Dashboards.
- Business orientierte und einfach zu verwendende Reporting und Audit Werkzeuge: out-of-the-box oder kundenspezifische Analysen.
- Dynamische Historisierung: jede Änderung wird unmittelbar identifiziert und kann nachverfolgt werden.
- Schnelle Korrektur von Autorisierungsfehlern oder Sicherheitslücken.
- Sicherere Zugriffskontrolle und verbesserte Governance auf Faktenbasis.

Data Access Governance – Management unstrukturierter Daten

Die Menge an unstrukturierten Daten wie beispielsweise Dokumente, Tabellen, Präsentationen oder Emails wächst rasant. Sie erfordern ein gut strukturiertes Berechtigungs-management zusätzlich zu den herkömmlichen Identity Access Management Lösungen.

Das Data Access Governance (DAG) Modul bietet ein spezielles Administrations- und Kontrollmodul für den Zugriff auf diese unstrukturierten Daten. Es ist vollständig integriert in die IAM Suite von Beta Systems.

- Dateneigentümer steuern ihre Zugriffe selbst und ohne direktes Zutun der IT.
- Integrierte Compliance Checks unter Einbezug der Dateneigentümer in den Fachabteilungen.
- Automatische Einhaltung von unternehmens-internen und gesetzlichen Richtlinien für die Zugriffssteuerung auf kritische Daten.
- Keine Rechtevergabe mehr unter Umgehung der Regelprozesse: Rechtesteuerung über businessorientierte geregelte Antrags- und Genehmigungs-Workflows.
- Soll-Ist-Rechte-Abgleich: unmittelbares Aufdecken von riskanten Abweichungen.
- Beta Systems' IAM als Single Point of Administration. Auch verfügbar als portalbasierte Stand-Alone Lösung.

_betasystems

Beta Systems IAM Software AG

Josef-Lammerting-Allee 14 | 50933 Köln | Germany
Phone: +49 (0) 221 650 15 155
iam@betasystems.com | www.betasystems-iam.com

Beta Systems Partner: