beta systems

Garancy®

Risikoorientierte Anbindung von Zielsystemen an Garancy

In einer Zeit wachsender Cyberbedrohungen und steigender regulatorischer Anforderungen rücken **Informationssicherheit und Compliance** stärker denn je in den Fokus. Unternehmen stehen vor der Herausforderung, ihre IT-Landschaft wirksam abzusichern – ohne unverhältnismäßig viele Ressourcen in Systeme mit geringem Schutzbedarf zu investieren.

Ein wirkungsvoller **Identity & Access Management (IAM)-Prozess** setzt daher nicht auf die flächendeckende Anbindung aller Systeme, sondern **beginnt gezielt bei den besonders kritischen Zielsystemen** – dort, wo Sicherheitsrisiken und regulatorischer Druck am höchsten sind.

Beta Systems zeigt, wie eine risikoorientierte Anbindung von Zielsystemen an die Garancy Suite gelingt – mit besonderem Fokus auf Schutzbedarfsanalysen und die Priorisierung sicherheitskritischer Systeme.

Empfohlene Schritte zur Umsetzung

Für Unternehmen, die ihre Sicherheitsarchitektur modernisieren und gleichzeitig regulatorische Anforderungen wie DORA, ISO 27001 oder den BSI-Grundschutz erfüllen möchten, ist der risikoorientierte Ansatz ein entscheidender Erfolgsfaktor.

1. **Durchführung** einer Schutzbedarfsanalyse aller relevanten Zielsysteme
2. **Festlegung** einer verbindlichen Anbindungsreihenfolge, die auf dem Schutzbedarf basiert
3. **Umsetzung** der priorisierten Anbindung mit Garancy, inklusive automatisierter Prozesse
4. **Regelmäßige Überprüfung** und Anpassung der Klassifizierungen

Beta Systems IAM Software AG
Ernst-Reuter-Platz 6, 10587 Berlin

Tel. +49 (0) 30 726 118-0
www.betasystems.com, info-iam@betasystems.com

Warum ein risikoorientierter Ansatz?

In vielen klassischen IAM-Projekten erfolgt die Anbindung von Zielsystemen nach organisatorischen oder technischen Kriterien – etwa nach Abteilung, Benutzeranzahl oder verfügbaren Schnittstellen. Diese Herangehensweise birgt Risiken: Besonders kritische Systeme werden häufig erst spät eingebunden und bleiben über längere Zeiträume unzureichend kontrolliert.

Beta Systems verfolgt einen risikoorientierten Ansatz und kehrt die Prioritäten um. Die **Anbindung erfolgt nach Schutzbedarf und Sicherheitsrelevanz**, insbesondere mit Blick auf folgende Schutzziele:

- **Vertraulichkeit**
  Schutz sensibler Informationen vor unbefugtem Zugriff, z. B. personenbezogene Daten oder vertrauliche Geschäftsinterna
- **Integrität**
  Gewährleistung der Unverfälschtheit und Korrektheit von Daten und Systemzuständen, etwa bei Systemen mit geschäftskritischen Konfigurationen oder Produktionsdaten
- **Verfügbarkeit**
  Sicherstellung, dass Systeme und Informationen jederzeit zugänglich und nutzbar sind, wie z. B. operative Kernsysteme in Produktion oder Service
- **Authentizität**
  Echtheitsnachweis von Identitäten, Daten und Kommunikationspartnern – besonders relevant bei Systemen mit Authentifizierungsfunktionen wie Single Sign-On, PKI-Infrastrukturen oder Identity Providern sowie bei sensiblen Anwendungen, bei denen fehlerhafte Identitätszuordnungen fatale Folgen haben können

Zielsysteme mit hohem oder sehr hohem Schutzbedarf, insbesondere im Hinblick auf Vertraulichkeit, Integrität und Authentizität, bergen ein **erhebliches Risiko**, wenn sie nicht frühzeitig in das IAM-System eingebunden und überwacht werden.

Unregelmäßigkeiten oder Missbrauch bleiben ohne zentrale Kontrolle oft unentdeckt – mit potenziellen Folgen für die Sicherheit, Compliance und Betriebsstabilität.

Gerade für **Unternehmen in regulierten Branchen** gilt: Applikationen und Systeme, die gesetzlichen Anforderungen unterliegen, sollten bevorzugt angebunden und dauerhaft überwacht werden.

Beta Systems IAM Software AG
Ernst-Reuter-Platz 6, 10587 Berlin

Tel. +49 (0) 30 726 118-0
www.betasystems.com, info-iam@betasystems.com

Beta Systems – Ihr Partner für schutzbedarfsbasierte Systemanbindung

Beta Systems unterstützt Sie bei der risikoorientierten Anbindung Ihrer Zielsysteme – mit einem strukturierten und bewährten Vorgehen, das Sicherheit, Effizienz und Compliance vereint.

Ihre Vorteile auf einen Blick

Priorisierung nach Schutzbedarf

Zielsysteme werden anhand vordefinierter Schutzbedarfskategorien bewertet und priorisiert. Kritische Systeme, wie z. B. SAP-Produktivumgebungen oder Anwendungen mit personenbezogenen Daten, werden bevorzugt angebunden.

Automatisierung und Governance

Ab der ersten Anbindung greifen automatisierte Abläufe für Benutzerbereitstellung, Rechtevergabe, Rezertifizierung und Deprovisionierung – inklusive Workflows, Genehmigungsstufen und klarer Verantwortlichkeiten.

Revisionssichere Dokumentation

Mit der Garancy Suite lassen sich alle Entscheidungen und Prozesse lückenlos und auditfähig nachverfolgen – ein klarer Vorteil gegenüber Aufsichtsbehörden und im Rahmen externer Prüfungen.

Effizienter Ressourceneinsatz

Anstatt alle Systeme gleichzeitig zu integrieren, werden Projektressourcen gezielt für die Integration jener Zielsysteme eingesetzt, bei denen ein realer Sicherheitsgewinn entsteht.

Fazit: Sicherheit gezielt steuern

Die risikoorientierte Anbindung von Zielsystemen an die **Garancy Suite** stärkt die Informationssicherheit Ihres Unternehmens messbar, optimiert den Ressourceneinsatz und unterstützt die Einhaltung regulatorischer Vorgaben.

Ihr Vorteil: besserer Schutz kritischer Systeme und nachvollziehbare Fortschritte gegenüber internen und externen Stakeholdern.

Sie möchten mehr erfahren?

Unser Experte Steve Ettlich aus dem Bereich Professional Services steht Ihnen gerne für eine unverbindliche Erstberatung zur Verfügung.

steve.ettlich@betasystems.com

+49 30 726118 603