garancy

egerer

WHITEPAPER

Von der Pflicht zur Chance: NIS-2 und der strategische Wert von Identity & Access Management

Inhalt

Zusammenfassung

NIS-2 verändert den Umgang mit Cyberrisiken grundlegend: Organisationen müssen ihre Sicherheitsmaßnahmen nicht mehr nur dokumentieren, sondern nachweislich wirksam umsetzen. Besonders im Identitäts- und Zugriffsmanagement wird dies konkret. Die NIS-2-Richtlinie und ihre Durchführungsverordnung verlangen eindeutige Identifizierbarkeit, ein konsequentes Need-to-Know-Prinzip, vollständige Protokollierung sowie die kontinuierliche Überwachung sämtlicher digitaler Identitäten. Für viele Unternehmen – insbesondere im Mittelstand – bedeutet das eine deutliche Abkehr von manuellen, historisch gewachsenen Verfahren.

Identity & Access Management (IAM) entwickelt sich damit zunehmend vom technischen Randthema zum strategischen Steuerungsinstrument. Eine saubere Governance, klare Prozesse und ein belastbares Rollenmodell bilden die Grundlage, um Risiken beherrschbar zu machen und regulatorische Anforderungen zu erfüllen. Gleichzeitig wird deutlich: Ab einer gewissen Komplexität lassen sich diese Aufgaben ohne Automatisierung kaum noch effizient bewältigen.

Eine moderne IGA-Lösung wie Garancy adressiert genau diese Anforderungen. Sie zentralisiert die Berechtigungsverwaltung, automatisiert den gesamten Identitätslebenszyklus, unterstützt prüfbare Rollenmodelle und liefert die historische Transparenz, die Aufsichtsbehörden im Rahmen von NIS-2 erwarten.

Die eigentliche Konsequenz aus NIS-2 ist damit klar: Ein IAM, das Zugriffe verlässlich steuert, alle Änderungen belegbar dokumentiert und Risiken früh sichtbar macht, wird zur Grundvoraussetzung für einen sicheren und stabilen Unternehmensbetrieb.

> *„Wer in der Vergangenheit bereits seine Hausaufgaben in Bezug auf Informationssicherheit gemacht hat und z. B. ein ISMS auf Basis von ISO 27001 betreibt, hat bereits eine sehr gute Grundlage für die Umsetzung von NIS-2 gelegt.*

David Capriati
Managing Consultant – Business Resilience Consulting
egerer Consulting GmbH

1. NIS-2: Ein EU-weiter Rahmen für die Cyberresilienz

1.1 Die NIS-2-Richtlinie macht Cyber-Risikomanagement zur Pflicht

Die **„EU-Richtlinie zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union – (EU) 2022/2555“**, kurz NIS-2, ist mehr als eine Aktualisierung der Vorgängerrichtlinie. Denn während letzterer nur ein Dasein als Papiertiger beschieden blieb, hat NIS-2 durchaus „Biss“: Mit ihr erfolgt eine fundamentale Verschiebung hin zu einem **EU-weit einheitlichen, verbindlichen und vor allem auch proaktiven Cybersecurity-Risikomanagement.**

NIS-2 verpflichtet Organisationen nicht nur zur bloßen Reaktion auf Sicherheitsvorfälle, sondern zur Gewährleistung umfassender, robuster Informationssicherheit. Auch der Weg dorthin ist vorgeschrieben: Betroffene Einrichtungen müssen die Resilienz sowohl ihrer organisatorischen Abläufe als auch ihres IT-Betriebs signifikant erhöhen.

1.2 Die Kernbereiche von NIS-2

Das Risikomanagement ist der Dreh- und Angelpunkt von NIS-2. Es ist angelehnt an etablierte Normen wie die ISO 31000 (allgemeines Risikomanagement) bzw. das darauf aufbauende, spezifischere Cybersecurity-Risikomanagement der ISO/IEC 27001.

Es zielt ab auf das Identifizieren, Erkennen, Bewerten und Behandeln von Risiken, unter Rückgriff auf standardisierte Methodiken. Und obwohl Begriffe wie Risikowert, Eintrittswahrscheinlichkeit oder Risikoakzeptanzkriterien beim Erstkontakt abschreckend wirken mögen – hier wird das Rad nicht neu erfunden. Falls nicht bereits ohnehin unternehmensweit verankert, stehen die Chancen gut, dass einzelne Organisationseinheiten bereits normgerechtes Risikomanagement praktizieren und sich dadurch an Bestehendes anknüpfen lässt.

NIS-2 geht jedoch noch etwas weiter, wiederum angelehnt an einschlägige Normen der Informationssicherheit. Die Richtlinie umfasst zudem folgende Bereiche:

1. **Governance**
   Hierunter fällt alles rund um die strategische Einbettung und die Organisation der Informationssicherheit im Unternehmen. NIS-2 stellt dabei die Haftung der Geschäftsführung in den Fokus und verlangt die regelmäßige Teilnahme des Managements an Cybersicherheitsschulungen.
   Dies stellt sicher, dass die Risikomanagement-Strategie auf oberster Ebene getragen und mit den notwen-digen Ressourcen ausgestattet wird.
2. **Incident Management**
   Falls präventive Maßnahmen versagen, bedarf es klarer Regeln für den Umgang mit (schweren) Sicherheitsvorfällen. NIS-2 legt dabei nicht nur fest, was überhaupt als solcher gilt, sondern gibt auch Regeln für Pflichtmeldungen an die zuständigen Aufsichtsbehörden vor.
3. **Business Continuity Management**
   Falls präventive Maßnahmen fehlschlagen und trotz aller Bemühungen aus einem Cybervorfall eine Krise erwächst, können vorab definierte Notfallpläne und erweiterte Befugnisse dabei helfen, schneller vom Not- in den Regelbetrieb zurück zu gelangen. Auch hierfür hält NIS-2 passende Anforderungen bereit.
4. **Technisch-organisatorische Maßnahmen**
   Hierunter lässt sich alles fassen, was NIS-2 an spezifischen Cybersecurity-Anforderungen bereithält – von der Awareness-Förderung durch regelmäßige Schulungen für Mitarbeitende über die Sicherheit entlang der Lieferkette bis hin zum Zugriffsmanagement.

1.3 Geltungsbereich: Die NIS-2-Sektoren und der Fokus auf die Digitalwirtschaft

Ein implizites Ziel bei der Ausarbeitung der NIS-2-Richtlinie war auch die Etablierung eines angemessen hohen Cybersicherheitsniveaus „in der Breite" – entsprechend betrifft NIS-2 ein ganzes Spektrum an Wirtschaftsbereichen. Der Geltungsbereich von NIS-2 erstreckt sich über insgesamt 18 Sektoren, und bereits ab 50 Mitarbeitenden oder 10 Mio. Euro Umsatz bzw. Bilanzsumme sind Organisationen aus diesen Sektoren von NIS-2 betroffen. Des Weiteren werden sogenannte wichtige, besonders wichtige und KRITIS-Einrichtungen unterschieden, wobei diese Einordnung wenig Einfluss auf die sich ergebenden Pflichten hat.[1]

Neben den „traditionellen" kritischen Infrastrukturen wie Energieerzeugung, Verkehrs- und Gesundheitswesen rücken neben Unternehmen der industriellen Fertigung nun auch die **„Digitalen Dienste"** in die Reichweite einer EU-weiten Regulierung. Gemäß der NIS-2-Anhänge I und II werden unter anderem benannt:

- **Managed Service Provider** (MSP)
- **Cloud Computing Service Provider** (IaaS, PaaS, SaaS)
- **Anbieter von Rechenzentrumsdiensten**
- **Online-Marktplätze, Suchmaschinen** und **Soziale Netzwerke**

Und für ebenjene Digitalwirtschaft mit ihren hochgradig vernetzten Dienstleistungen hat die EU-Kommission aufgrund der herausragenden gesamtwirtschaftlichen Bedeutung sogar eine ergänzende Gesetzesnorm erlassen.

Denn NIS-2 stellt zwar insgesamt ein recht umfassendes „Set" an Regelungen auf, die alle zusammen auf die Stärkung der Cybersicherheit einzahlen. Die Richtlinie allein bleibt dabei aber oftmals eher unspezifisch und eröffnet damit einen gewissen Gestaltungsspielraum in Bezug auf die konkrete Umsetzung. Dagegen präzisiert die **NIS-2-Durchführungsverordnung (EU) 2024/2690** die allgemeinen Anforderungen der Richtlinie deutlich.

Das bedeutet: Für Unternehmen der Digitalwirtschaft, die von den Anhängen I und II der NIS-2-Richtlinie erfasst werden, gelten nicht mehr die allgemeinen NIS-2-Anforderungen, sondern – soweit gegeben – die spezifischeren Pflichten der NIS-2-Durchführungsverordnung. Diese liefert dann konkrete technische und methodische Maßnahmen (TOMs), die damit auch nicht länger nur „Nice-to-have" sind.

Denn anders als eine EU-Richtlinie wie NIS-2 „allgemein" bzw. (EU) 2022/2555 braucht eine EU-Verordnung wie (EU) 2024/2690 keine nationalen Umsetzungsgesetze, um Rechtsverbindlichkeit zu entfalten. **Die Regelungen der NIS-2-Durchführungsverordnung sind daher schon seit ihrer Verabschiedung 2024 in Kraft.**

2. NIS-2-Pflichten im Bereich des Identitäts- und Zugriffsmanagements

2.1 Die NIS-2-Richtlinie und der „Stand der Technik"

Spätestens im Kontext der NIS-2-Durchführungsverordnung wird deutlich: Für Organisationen, die hiervon betroffen sind, wird es in zahlreichen organisatorischen und technischen Bereichen äußerst konkret. So manches Thema aus dem Bereich der TOMs, das innerhalb der NIS-2-Richtlinie noch im Unverbindlichen verbleiben musste, entfaltet sich mit der Durchführungsverordnung zu einem zentralen Handlungsfeld.

Ausgangspunkt bleibt dabei jedoch zunächst die Richtlinie, die das allgemeine Ziel „mehr digitale Resilienz durch effektives Cybersecurity-Risikomanagement" verfolgt. Dies wird in der Praxis durch zielgerichtete Maßnahmen umgesetzt, durch die erkannte Risiken minimiert werden sollen.

[1] Genaueres zu den NIS-2-Schwellwerten, der damit verbundenen Unterscheidung zwischen wichtigen und besonders wichtigen Einrichtungen, den sich ergebenden Pflichten sowie eine interaktive Betroffenheitsprüfung finden Sie unter: *https://egerer-consulting.de/leistungen/business-resilience/nis-2.*

Da sich die digitale Welt stetig weiterentwickelt (und mit ihr auch die möglichen Risiken bzw. Bedrohungen für die Cybersicherheit), findet sich in der Richtlinie eine sehr einfache Formulierung mit großer Tragweite:

> *„Die […] Maßnahmen müssen unter Berücksichtigung des Stands der Technik […] ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist."*
>
> Richtlinie (EU) 2022/2555, Art. 21 (1) Satz 2

Diese einleitende Formulierung erlaubt es, im Folgenden nur noch die groben Bereiche aufzuzählen, in denen Cybersecurity-Risikomanagement betrieben werden soll. Denn alle letztlich getroffenen Maßnahmen haben dem Stand der Technik zu genügen. Einschließlich derer, die sich in Art. 21 (2) i und j finden: **Konzepte für die Zugriffskontrolle** sowie Lösungen zur **Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung.**

Dies stellt auch mit eine der konkretesten technischen Pflichten der gesamten Richtlinie dar. Die Forderung ist damit zwar hinreichend klar benannt, in Bezug auf ihre Umsetzung ist die NIS-2-Richtlinie jedoch keine große Hilfe. Immerhin findet sich in den vorangestellten Erwägungsgründen (gewissermaßen dem Äquivalent zum „Kleingedruckten" im Rahmen der EU-Legislative) noch folgender Hinweis:

> *„Die wesentlichen und wichtigen Einrichtungen sollten eine breite Palette grundlegender Praktiken der Cyberhygiene anwenden, z. B. Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugriffsmanagement […].*
>
> Richtlinie (EU) 2022/2555, Erwägungsgrund 89

Genau hier setzt auch die NIS-2-Durchführungsverordnung mit ihrem umfassenden Set an Detailregelungen an, um die konkrete Ausgestaltung handhabbarer zu machen. Darin zeigt sich erneut die Orientierung von NIS-2 an etablierten interna-tionalen Normen – die recht allgemein gehaltene ISO/IEC 27001 wird ja auch erst in Verbindung mit den konkreten Controls aus der ISO 27002 wirklich greif- und umsetzbar.

2.2 Identitäts- und Zugriffsmanagement im Licht der NIS-2-Durchführungsverordnung

Ausgehend von der Forderung nach risikomindernden Maßnahmen entsprechend dem Stand der Technik wird die Erwartungshaltung des Gesetzgebers mit der Durchführungsverordnung endlich greifbar: Im umfangreichen Anhang („Technische und methodische Anforderungen gemäß Artikel 2 der vorliegenden Verordnung") finden sich die gesuchten Details unter Punkt 11 **„Zugriffskontrolle (Art. 21 Absatz 2 Buchstaben i und j der Richtlinie (EU) 2022/2555)".**

An erster Stelle steht – für Kenner von ISO 27001 und Co. sicher nicht unerwartet – die Forderung nach einem Konzept, das für die Verankerung des Identitäts- und Zugriffsmanagements (IAM) in der Organisation sorgen soll.

Der Punkt **11.2. Management von Zugangs- und Zugriffsrechten** fährt fort mit der Organisation des IAM auf Basis von „Need-to-Know" und Nutzungsnotwendigkeit. Dabei wird deutlich, dass das reine „Tun" entlang dokumentierter Workflows und Freigabeprozesse allein nicht ausreicht.

Es soll etwa auch sichergestellt werden, dass der Zugang organisationsfremder Personen bzw. Entitäten durch angemessene Einschränkungen in Bezug auf Umfang und Dauer geregelt wird. Das Führen eines Registers der gewährten Zugangs- und Zugriffsrechte sowie das Protokollieren durchgeführter Tätigkeiten wird ebenfalls verlangt (vgl. (EU) 2024/2690, 11.2.2. d, e und f).

Die in der Praxis oftmals „härteren Nüsse" hält jedoch **11.5. Identifizierung** bereit. ISO 27001-zertifizierte Unternehmen mögen vielleicht noch über die Forderung nach individuellen Nutzerkennungen lächeln – die Ablösung der „bequemen" gemeinsam genutzten User-Accounts („Shared User") haben sie längst hinter sich gebracht.

Die Pflicht zur durchgehenden Überwachung, festgehalten in den Punkten c und d, ist jedoch das genaue Gegenteil einer „Einmal-Aktion". Denn hierin steckt letztlich die **Forderung nach lückenloser und durchgehender Überwachung sämtlicher (digitaler) Identitäten der Organisation** (vgl. (EU) 2024/2690, 11.5.2. a-d).

2.3 Synthese: Eine strenge Nachweispflicht

Es lässt sich zusammenfassend festhalten, dass Organisationen der Digitalwirtschaft, die von der NIS-2-Durchführungsverordnung erfasst werden, die folgenden Fragen präzise beantworten müssen:

- → **Wer** hat **wann** auf **welche** Systeme und Daten Zugriff erhalten?
- → **Wer** hat **wann** Zugriffsrechte entzogen bekommen?
- → **Wie** wurde dieser gesamte Lebenszyklus dokumentiert?

Die IAM-bezogenen Pflichten gemäß (EU) 2024/2690 gehen also ein ganzes Stück weit über reine Handlungsanweisungen hinaus. Insbesondere die Forderung nach Überwachung und Protokollierung, die auch in anderen Kontexten immer wieder in NIS-2 auftaucht, lässt sich ohne Rückgriff auf unterstützende Lösungen – und zwar solche auf dem Stand der Technik – nur schwer erfüllen.

Im Überblick:

Verordnung (EU) 2024/2690	Fokus der Anforderung
11.2.2. d (Externe Identitäten)	Berücksichtigung von Dritten (Anbieter, Diensteanbieter) durch Beschränkung in Umfang und Dauer
11.2.2. e und f (Protokollierung)	Führen eines Registers der Rechte und Protokollierung des Managements von Zugangsrechten
11.5.2. a und b (Identifizierung)	Eindeutige Kennungen für Systeme und Nutzer, die mit einer einzigen Person verknüpft sind, als Standard
11.5.2. c und d (Überwachung)	Überwachung von Kennungen und Protokollierung des Managements von Identitäten

3. Die Consulting-Perspektive: Strategische Schritte zur NIS-2-Compliance

Die Umsetzung der NIS-2-Pflichten ist nicht „Sache der IT". In Zusammenhang mit den vorangegangenen Überlegungen sollte vielmehr deutlich geworden sein, dass die Herstellung von NIS-2-Compliance ein strategisches Umsetzungsprojekt darstellt. Es geht insgesamt darum, die Lücken zwischen den gesetzlichen Anforderungen und dem organisationsweiten Status quo zu erkennen und zu schließen.

3.1 Bestandsaufnahme

Der erste Schritt zur NIS-2-Compliance im Bereich des IAM sollte stets eine ehrliche Bestandsaufnahme sein:

1. **Der Governance-Rahmen**
   Existiert eine Policy, in welcher die Grundlagen des IAM entsprechend NIS-2 (von Verantwortlichkeiten und Zuständigkeiten bis hin zu Prinzipien wie „Least Privilege") festgehalten sind?
2. **Die Prozesse**
   Wie sehen die derzeitigen IAM-Workflows aus – wer darf Prozesse zum Erstellen und Löschen von Nutzerkonten oder zur Vergabe von Berechtigungen anstoßen, wer führt aus, wer kontrolliert?
3. **Die technisch-administrative Umsetzung**
   Wie werden Identitäten konkret erstellt, Zugriffsberechtigungen gesetzt und dabei die Dokumentation und das Führen einer „Gesamtübersicht" gewährleistet?

3.2 Governance und Prozesse: Die Grundlagen für eine gesunde „Identity-Landschaft"

Technische Lösungen ohne klare Governance laufen schnell ins Leere – insbesondere im Kontext von NIS-2. Denn letztlich dreht sich alles um das Management von Cybersecurity-Risiken. Die Forderung nach Maßnahmen entsprechend dem Stand der Technik ist schließlich kein Selbstzweck, sondern soll dabei helfen, Risiken für die eigene Informationssicherheit zu reduzieren.

Der erste Schritt sollte also in der Etablierung eines tragfähigen Regelwerks bestehen, etwa in Form von:

- **Rollenkonzepten:** Entwicklung von Rollen, die dem Least-Privilege-Prinzip folgen. Das Ziel ist, Benutzern ausschließlich die Berechtigungen zu geben, die sie für ihre aktuelle Tätigkeit benötigen – nicht mehr und nicht länger.
- **Identity-Lebenszyklus:** Implementierung klarer, automatisierter Workflows. Insbesondere beim Austritt von Mitarbeitenden muss die sofortige und lückenlose Entziehung aller Zugriffsrechte sichergestellt werden, um das Risiko verwaister oder unautorisierter Konten zu eliminieren.
- **Zugriffsrezertifizierung:** Regelmäßige Überprüfung, ob die zugewiesenen Rechte noch notwendig sind. Dies ist ein Schlüssel zur Reduzierung von Überberechtigungen, die im Laufe der Zeit entstehen – den allseits bekannten „Azubi-Effekt" gilt es zu vermeiden.

3.3 Herausforderungen wachsender Organisationen: Skalierung und Audit-Sicherheit

Gerade Unternehmen aus dem gehobenen Mittelstand auf dem Sprung zum Konzern stehen oftmals vor einem Dilemma: Ihre Komplexität ist bereits zu hoch für eine weiterhin manuelle Steuerung, aber die Ressourcen für umfangreiche, monolithische Enterprise Security-Suiten sind begrenzt.

Die oft wahrgenommene Ausgangslage, gemünzt auf den Bereich des Identitäts- und Zugriffsmanagements: Cybersecurity-Grundstrukturen wie Richtlinien und (C)ISO-Rollen sind vorhanden, aber weite Teile der Unternehmens-IT (und damit auch das IAM) sind fragmentiert. Über die Zeit hinweg haben die verschiedenen Organisationseinheiten jeweils eigene Wege gefunden, „die Dinge zu regeln" – und Zugriffsfreigaben laufen über E-Mails, Excel-Listen und/oder dezentrale Tools.

Letztlich sind es aber weiterhin oft manuelle Verfahren, die zur Anwendung kommen. Und die vertragen sich eben kaum mit den Anforderungen, die aus NIS-2 erwachsen:

Problem	NIS-2-Risiko
Keine Skalierung	Hohe Zahlen an Mitarbeitenden und häufige Rollenwechsel führen zu einer unüberschaubaren Rechte-Landschaft und veralteten Berechtigungen.
Fehleranfälligkeit	Manuelle On- und Offboarding-Prozesse sind fehleranfällig; Konten von ehemaligen Mitarbeitenden bleiben aktiv.
Mangelnde Transparenz	Fehlende zentrale Dokumentation macht die Nachweisführung (z. B. nach Punkt 11.2.2. e) unmöglich.
Erhöhte Angriffsfläche	Unentdeckte Überberechtigungen (Access Creep) stellen ideale Einfallstore für laterale Angriffe dar.

4. Zwischenfazit IAM und NIS-2: Ohne Automatisierung wird es schwierig

Es dürfte bis hierhin deutlich geworden sein: Ohne technische Lösungen, die Prozesse automatisieren und dabei auch revisionssicher protokollieren, ist es ab einer gewissen Organisationsgröße kaum mehr möglich, die Anforderungen der NIS-2-Durchführungsverordnung vollumfänglich zu erfüllen. Für den Teilbereich des Identitäts- und Zugriffsmanagements sind technische Lösungen fast schon zwingend erforderlich, um

- → **lückenlose Nachweise** über den gesamten Lebenszyklus von Nutzerkonten hinweg zu erbringen,
- → **die Angriffsfläche** durch strikte Zugriffsprinzipien (Least Privilege) **zu reduzieren** und
- → **Nachweissicherheit** gegenüber Aufsichtsbehörden herzustellen.

Die Etablierung eines Governance-Rahmens und effektiver Prozesse steht auch hier am Anfang. Sobald dies erfolgt ist, kann zielgerichtet eine passgenaue IAM-Lösung ausgewählt und implementiert werden. Diese sorgt dann für eine effiziente, sichere Umsetzung der regulatorischen Pflichten.

Im folgenden Abschnitt zeigen wir, wie eine moderne IAM-Plattform die zuvor beschriebenen Herausforderungen beherrschbar macht. Hier erfahren Sie, wie Sie die NIS-2-Anforderungen mit der richtigen Technologie nicht nur erfüllen, sondern die Cyberresilienz Ihres Unternehmens nachhaltig stärken.

5. Die technische Umsetzung mit Garancy

Der folgende Abschnitt zeigt, wie sich die zuvor erläuterten regulatorischen und organisatorischen Anforderungen mit Garancy praktisch umsetzen lassen. Die Beispiele veranschaulichen, wie eine IGA-Lösung nicht nur Compliance sicherstellt, sondern zugleich viele der in Kapitel 2 und 3 beschriebenen strukturellen Herausforderungen entschärft – etwa fragmentierte Prozesse, fehlende Transparenz oder den steigenden Druck, Berechtigungen auditfähig nachzuweisen.

5.1 Die Rolle von IGA im modernen Identitätsmanagement

Das moderne **Identitätsmanagement (auch IAM genannt) besteht aus den drei sich ergänzenden Segmenten IGA, AM und PAM** mit klar voneinander abgegrenzten Funktionsbereichen.

Access Management (AM) ist in erster Linie für Authentifizierungsverfahren (SSO, MFA) sowie die Durchsetzung von Zugriffsentscheidungen zuständig. Zu diesem Zweck werden Identity Provider (IdP) bereitgestellt, an die sich die Applikationen über Standardprotokolle anbinden können. **Privileged Access Management (PAM)** adressiert die besonderen Risiken privilegierter Administrationskonten. **Identity Governance & Administration (IGA)** konzentriert sich auf die Kontrolle darüber, welche Identität welche Berechtigungen erhält – und aus welchem Grund.

Garancy ist vollständig im IGA-Segment verortet. Sie verwaltet Identitäten, Rollen und Berechtigungen über alle angebundenen Zielsysteme hinweg und sorgt dafür, dass nur geprüfte, nachvollziehbare und genehmigte Zugriffe entstehen. Diese Funktionen bilden eine zentrale Grundlage, um die regulatorisch geforderte eindeutige Identifizierung, die Beschränkung von Zugängen auf das notwendige Maß sowie die vollständige Nachvollziehbarkeit des gesamten Berechtigungslebenszyklus sicherzustellen.

Damit übernimmt Garancy die Aufgabe, jene organisatorischen und technischen Konzepte umzusetzen, die für ein modernes, risikoorientiertes Identitätsmanagement unverzichtbar sind: Transparenz, Berechtigungskontrolle, Automatisierung und Nachweisbarkeit. Die zuvor skizzierten Governance- und Prozessanforderungen werden so nicht nur auf Papier formuliert, sondern technisch abgesichert in den täglichen Betrieb überführt.

5.2 Zentrale Steuerung und Kontrolle von Berechtigungen

Die Fähigkeit, Identitäten und Berechtigungen über Systeme hinweg zentral zu verwalten, ist eine wesentliche Voraussetzung für ein zuverlässiges und gesetzeskonformes Berechtigungsmanagement. Garancy bildet hierfür die zentrale Instanz und konsolidiert sämtliche relevanten Informationen an einer Stelle. Die Kommunikation mit den Zielsystemen erfolgt über geeignete Konnektoren, mit denen sich lesende und schreibende Datenflüsse realisieren lassen.

Bereits bei der Anbindung eines Zielsystems werden über einen **Initial-Load** alle vorhandenen Benutzer (Accounts) und deren Berechtigungen vollständig übernommen, sodass Garancy ein **präzises Abbild der Ist-Situation** besitzt. Dieser Datenbestand wird mittels des **Live-Balancing-Vorgangs** (Reconciliation) regelmäßig mit den realen Daten der angeschlossenen Systeme abgeglichen. So erkennt Garancy mögliche Abweichungen zwischen Soll- und Ist-Bestand und kann diese automatisch und regelbasiert korrigieren.

Mithilfe der **Provisionierung** werden alle von Garancy genehmigten Änderungen unmittelbar und konsistent in den Zielsystemen umgesetzt. Das verhindert, dass veraltete oder manuell erzeugte Berechtigungen bestehen bleiben, die weder kontrolliert noch dokumentiert sind. Auf diese Weise entsteht eine zentral orchestrierte Berechtigungslandschaft, die klar strukturiert, nachvollziehbar und jederzeit vollständig aktualisiert ist. Damit wird genau jene Transparenz und Nachvollziehbarkeit geschaffen, die NIS-2 und die Durchführungsverordnung in Form eines aktuellen Registers aller Zugangs- und Zugriffsrechte (vgl. 11.2.2. e und f) einfordern.

5.3 Rollenmodelle als Grundlage für Need-to-Know

Ein **wirkungsvolles Rollenmodell** ist der entscheidende Hebel, um das **Need-to-Know-Prinzip** dauerhaft einzuhalten. Garancy setzt dieses Prinzip konsequent über Business-Rollen um, die fachliche Tätigkeiten in klar abgegrenzte Berechtigungspakete übersetzen.

Die Rollen abstrahieren die oft sehr technischen Berechtigungen der Zielsysteme und machen sie für Fachbereiche verständlich und steuerbar. Dadurch wird die Zuweisung von Berechtigungen nicht länger durch Einzelentscheidungen auf Basis technischer Details geprägt, sondern durch eine fachlich nachvollziehbare Logik. Jede Rolle steht für ein klar definiertes Aufgabenprofil; eine Person erhält nur jene Rolle, die für ihre aktuelle Tätigkeit erforderlich ist.

Das Rollenmodell selbst wird strukturiert entwickelt. Um eine Grundausstattung sicherzustellen, werden grundlegende Berechtigungen beispielsweise pro Abteilung oder Jobfunktion zu Basisrollen zusammengefasst. Zusätzliche Spezial- oder Sonderaufgaben werden hingegen durch separate Rollen abgebildet. Durch die ergänzende Analyse realer Berechtigungsdaten mittels Role-Mining lassen sich Muster identifizieren, aus denen sich wiederum weitere Rollen oder Optimierungen des bestehenden Modells ableiten lassen.

Das Ergebnis ist ein konsistentes, wartbares Rollenmodell, das nicht nur das Need-to-Know-Prinzip wirksam umsetzt, sondern zugleich die fachliche Verantwortung stärkt und die technische Komplexität auf ein kontrollierbares Maß reduziert.

5.4 Automatisierte Identitäts- und Berechtigungsprozesse

Die sichere Verwaltung von Identitäten erfordert einen **durchgängigen, automatisierten Lebenszyklus,** der alle Phasen vom Eintritt über Versetzung bis zum Austritt abdeckt, aber auch temporäre Abwesenheiten wie z. B. Elternzeit, Sabbatical oder Jahresurlaub berücksichtigt. Garancy stellt hierfür vollständig **automatisierte Prozesse** bereit. In der Regel liefert dazu ein HR-System täglich die erforderlichen Daten zu den internen Mitarbeitenden.

Neue Mitarbeitende werden automatisch erkannt und unmittelbar mit den notwendigen Rollen und Accounts ausgestattet, sodass sie vom ersten Arbeitstag an arbeitsfähig sind. Ändern sich organisatorische Rahmenbedingungen, etwa durch einen Abteilungswechsel oder eine neue Funktion, passt Garancy die zugewiesenen Rollen und Berechtigungen sofort an und entzieht alle nicht mehr benötigten Zugriffe.

Beim Austritt eines Mitarbeitenden werden sämtliche Accounts in allen angebundenen Systemen zuverlässig deaktiviert oder gelöscht. Das verhindert verwaiste Zugänge, die in vielen IT-Landschaften ein relevantes Sicherheitsrisiko darstellen. Die zuvor erläuterte Problematik manueller, fehleranfälliger On- und Offboarding-Prozesse wird dadurch nachhaltig entschärft.

Besonders streng reguliert sind externe Mitarbeitende, deren Berechtigungen oft nur temporär vergeben werden dürfen. Garancy unterstützt **zeitlich definierte Rollen und automatisch auslaufende Berechtigungen**, wodurch die Dauer und der Umfang des Zugriffs präzise gesteuert werden können. Die Informationen über externe Mitarbeitende können über zusätzliche Quellsysteme geliefert oder alternativ über einen Workflow manuell erfasst werden.

In Garancy sind **Personen, Identitäten und Accounts klar voneinander getrennt**. So bleibt jede Zugriffsberechtigung eindeutig einer natürlichen Person zugeordnet. Dies ist eine zwingende Voraussetzung für Transparenz und Nachvollziehbarkeit sowie für Anforderungen hinsichtlich Funktionstrennung (SoD). Gleichzeitig erfüllt diese eindeutige Zuordnung die in Kapitel 2.2 dargestellten Erwartungen der NIS-2-Durchführungsverordnung an Identifizierung und Überwachung von Kennungen (11.5.2. a-d).

5.5 Kontinuierliche Überprüfung von Zugriffsrechten

Die fortlaufende Kontrolle von Berechtigungen ist unverzichtbar, um sicherzustellen, dass die tatsächlichen Rechte einer Person stets mit ihren aktuellen Aufgaben im Unternehmen übereinstimmen. Garancy unterstützt diesen Prozess durch **individuell konfigurierbare Rezertifizierungskampagnen.** Diese können sowohl auf Ebene einzelner Personen als auch auf Ebene der Rollen ansetzen.

Bei der Überprüfung einzelner Personen wird beurteilt, ob die ihnen zugeordneten Rollen weiterhin notwendig sind. Dadurch lassen sich **veraltete oder nicht mehr benötigte Rechte zuverlässig entfernen.** Parallel dazu werden auch die Rollen selbst regelmäßig bewertet. Dabei wird analysiert, ob die enthaltenen Berechtigungen weiterhin den Anforderungen der jeweiligen Aufgabe entsprechen oder ob Bereinigungen notwendig sind.

Durch diese kontinuierliche Überprüfung wird verhindert, dass sich mit der Zeit übermäßige oder unpassende Berechtigungen ansammeln. Das Ziel besteht im Wesentlichen darin, die Angriffsfläche zu verringern, aber auch Insider-Bedrohungen und Datenschutzverstöße zu reduzieren. Gleichzeitig schafft sie **Transparenz für Fachbereiche und Sicherheitsverantwortliche** und bildet einen wichtigen Baustein für einen risikoarmen und kontrollierten Betrieb der gesamten Berechtigungslandschaft. Damit unterstützt IGA genau jene kontinuierlichen, risikomindernden Maßnahmen, die in Punkt 3 gefordert werden und für ein belastbares Sicherheitsniveau unerlässlich sind.

5.6 Vollständige Transparenz durch historische Nachweise

Ein wesentliches Merkmal eines wirkungsvollen IGA-Systems ist die Fähigkeit, alle sicherheitsrelevanten Ereignisse präzise zu erfassen, zu protokollieren und historisch auszuwerten. Garancy sorgt dafür, dass sämtliche **Änderungen an Personen, Rollen, Accounts und Berechtigungen vollständig dokumentiert** werden. Auf diese Weise lassen sich die essenziellen Kernfragen – „Wer hat wann worauf zugegriffen, wer hat Rechte vergeben oder entzogen und wie wurde dies dokumentiert?" – faktenbasiert beantworten.

Die erfassten Logdaten fließen in den Access Intelligence Manager (AIM), der die Daten in einem strukturierten Data-Warehouse speichert und korreliert. So entsteht eine **lückenlose Historie der Berechtigungslandschaft.** Unternehmen können jederzeit nachvollziehen, welche Berechtigungen zu einem bestimmten Zeitpunkt bestanden haben, wer die Änderung durchgeführt hat und wie sich Rollen und Identitäten im Zeitverlauf entwickelt haben.

Diese Transparenz ermöglicht nicht nur eine zuverlässige Erfüllung gesetzlicher Nachweispflichten. Sie bietet auch einen erheblichen Mehrwert im operativen Sicherheitsmanagement, etwa bei der Untersuchung von Vorfällen, bei internen Revisionen oder bei der Vorbereitung externer Audits.

6. Effiziente Implementierung und Unterstützung im Mittelstand

Viele mittelständische Unternehmen sehen sich mit einer zunehmenden regulatorischen und technischen Komplexität konfrontiert, verfügen aber nicht über die Ressourcen für groß angelegte IAM-Programme. Garancy ist daher so konzipiert, dass es **in kurzer Zeit einsatzfähig** ist und gleichzeitig eine robuste Grundlage für weitere Ausbaustufen bietet.

Vordefinierte Governance-Modelle, erprobte Anbindungsmuster für gängige Zielsysteme und klar strukturierte Rollenmodelle verkürzen die Einführungszeit erheblich. Ergänzende Dienstleistungen – etwa Beratung zum Rollendesign, Unterstützung bei der Definition von Verantwortlichkeiten oder Hilfe beim technischen Onboarding komplexer Systeme – erleichtern den Einstieg zusätzlich.

Der Ansatz „Schnell starten, später ausbauen" erlaubt es Unternehmen, innerhalb kurzer Zeit ein funktionierendes und auditfähiges Berechtigungsmanagement aufzubauen, das den regulatorischen Anforderungen entspricht und gleichzeitig eine belastbare Basis für zukünftige Weiterentwicklungen bildet.

7. Fazit

Eine **moderne IGA-Lösung wie Garancy** ist weit mehr als ein technisches Werkzeug. Sie übersetzt die regulatorischen Vorgaben aus NIS-2 in gelebte Praxis und schafft die **Grundlage für ein belastbares, skalierbares und nachweisfähiges Identitäts- und Zugriffsmanagement.** Garancy verbindet zentrale Steuerung, transparente Rollenmodelle, automatisierte Prozesse und kontinuierliche Kontrolle zu einem konsistenten Gesamtbild, das sowohl Sicherheit als auch Effizienz fördert.

Damit wird deutlich: Die zuvor beschriebenen NIS-2-Anforderungen lassen sich nur dann dauerhaft erfüllen, wenn Governance und Technologie ineinandergreifen. Garancy liefert dafür die passende technische Basis und macht NIS-2 nicht nur erfüllbar, sondern auch handhabbar.

Kontaktieren Sie uns, um mehr über unsere Lösung zu erfahren. Garancy lässt sich an Ihre Bedürfnisse anpassen und ist sowohl On-Premise als auch in der Cloud verfügbar.

https://garancy.com/de/

Als spezialisierte Unternehmensberatung u. a. im Bereich Business Resilience kombiniert **egerer Consulting** rechtliches Wissen mit technischer Praxis, um Ihnen eine sichere und wirtschaftlich tragfähige Lösung zur Erfüllung der NIS-2-Vorgaben zu bieten.

https://egerer-consulting.de/leistungen/business-resilience/nis-2