VON PAPIER ZU NACHWEIS

Was deutsche Datenschutz- und Informationssicherheitsbeauftragte MSPs 2026 sagen

Juli 2026

Rund 100 Fachgespräche mit deutschen Datenschutz- und Informationssicherheitsbeauftragten

Eine qualitative Studie im Vorfeld der niederländischen NIS2-Umsetzung (Cyberbeveiligingswet, 15. August 2026)

Auftraggeber

GUARDIAN 360°

Kruisplein 484, 3012 CC Rotterdam – Niederlande

Einleitung

Seit dem 6. Dezember 2025 ist das NIS2-Umsetzungsgesetz in Deutschland ohne Übergangsfrist in Kraft. Für MSPs bedeutet das: Ihre Kunden fragen heute nicht mehr nur „sind wir sicher?“, sondern „können wir das nachweisen?“

Um zu verstehen, wie deutsche Datenschutzbeauftragte (DSB) und Informationssicherheitsbeauftragte (ISB) diese Frage in der Praxis beantworten, hat Guardian360 rund 100 offene, qualitative Fachgespräche über einen konkreten Ansatz geführt: die Verknüpfung technischer Sicherheitsbefunde mit DSGVO-, NIS2- und ISO-27001-Pflichten.

Dies ist ausdrücklich keine repräsentative Benchmark-Erhebung, sondern eine qualitative Sammlung von Fachmeinungen. Die hier genannten Anteile beziehen sich auf die erhaltenen Rückmeldungen und sollten als Tendenz, nicht als statistisch belastbare Kennzahl gelesen werden.

Dieser Bericht fasst zusammen, was wir gelernt haben, und was das für Ihr Kundengespräch bedeutet.

Kernbefund 1: Die Lücke zwischen Dokumentation und Nachweis

Aus den Gesprächen mit DSB und ISB ist deutlich geworden: Die größte Schwachstelle liegt selten in der Technik selbst, sondern darin, dass dokumentierte Kontrollen nach ihrer Einführung kaum noch erneut überprüft werden. Rund jeder zwanzigste Gesprächspartner (ca. 5 %) beschrieb unabhängig dasselbe Muster: eine Maßnahme wird einmal umgesetzt, dokumentiert, und im jährlichen Audit-Rhythmus nicht mehr hinterfragt, bis Verantwortlichkeit „im Sand verläuft“.

> **Zitat aus einem Gespräch**
> *„Gesetze sind risikobasiert, Scanner sind binär.“ So beschrieb es ein IT-Sicherheitsauditor.*

Diese Beobachtung deckt sich mit externen Daten: Eine Studie von Proliance unter 122 Entscheidern im deutschen Mittelstand zeigt, dass Unternehmen ihren eigenen Sicherheitsreifegrad überwiegend als hoch einschätzen, während gleichzeitig eine hohe Zahl schwerwiegender Sicherheitsvorfälle und erhebliche Unsicherheit bezüglich NIS2 bestehen (Quelle: Proliance, „Lage der Informationssicherheit im deutschen Mittelstand 2025“).

> **Was das für Sie als MSP bedeutet**
> *Ihre Kunden glauben oft, gut aufgestellt zu sein, weil eine Maßnahme einmal dokumentiert wurde; der Nachweis der fortlaufenden Wirksamkeit ist ein Gespräch, das die wenigsten von sich aus führen, aber die meisten brauchen.*

Kernbefund 2: NIS2 lässt sich technisch besser abbilden als die DSGVO

Eine der aufschlussreichsten Erkenntnisse betrifft einen Unterschied, den wir in unserem ursprünglichen Ansatz nicht in dieser Deutlichkeit vorausgesetzt hatten: Rund 6 % der Gesprächspartner, überwiegend erfahrene Juristen und Auditoren, wiesen unabhängig voneinander und ungefragt darauf hin, dass sich technische Befunde deutlich direkter auf NIS2-Anforderungen als auf DSGVO-Artikel abbilden lassen. Ein Gesprächspartner formulierte es pointiert: „NIS2-Mapping kann einen Mehrwert bieten, DSGVO-Mapping meines Erachtens nicht."

Der Grund: NIS2-Anforderungen sind großteils technisch und organisatorisch ausgerichtet und daher vergleichsweise gut durch technische Evidenz zu belegen. Die DSGVO hingegen ist bewusst technologieneutral und risikobasiert formuliert. Art. 32 DSGVO verlangt eine Risikoabwägung anhand des Verarbeitungskontexts, der Art der personenbezogenen Daten sowie der Risiken für Betroffene, etwas, das ein Schwachstellenscanner grundsätzlich nicht beurteilen kann. Ein Gesprächspartner wies zusätzlich auf Art. 6 DSGVO hin: Ob eine Verarbeitung überhaupt eine Rechtsgrundlage hat, sieht ein Scanner gar nicht, unabhängig von der Qualität des technischen Mappings.

Deutlich breiter, bei etwa jedem zehnten Gesprächspartner (ca. 10 %), fiel die allgemeinere Warnung: Eine technische Zuordnung soll immer als Indikator und Priorisierungshilfe verstanden werden, nie als automatisierter Compliance-Nachweis. Ein Fund ist keine Verletzung.

Was das für Sie als MSP bedeutet

Wenn Sie Ihren Kunden technische Sicherheitsnachweise anbieten, positionieren Sie diese realistisch: als starken, direkten Beitrag zur NIS2-Nachweisführung; und als wertvollen, aber ergänzenden Baustein für die DSGVO, der die juristische Bewertung durch einen DSB nicht ersetzt. Diese Differenzierung schützt Sie und Ihre Kunden vor einem falschen Sicherheitsgefühl und macht Ihr Angebot glaubwürdiger.

Kernbefund 3: Eigenverantwortung schlägt Kontrollzwang, aber nur mit Namen und Frist

Rund 5 % der Gesprächspartner bestätigten unabhängig voneinander: Maßnahmen, die zur Unternehmensrealität passen, werden freiwillig gelebt. Maßnahmen, die an der Praxis vorbeigehen, versanden fast immer.

Zitat aus einem Gespräch

„risikoadäquat", so beschrieb es ein Gesprächspartner: am konkreten Unternehmensalltag ausgerichtet und nach Risiken gestaffelt

Gleichzeitig braucht es klare Verantwortlichkeit. Ein Auditor mit Datenschutzhintergrund erklärte, warum eine reine Abteilungszuordnung („die IT ist zuständig") in der Praxis nicht ausreicht: Bei einer Rückfrage der Aufsichtsbehörde oder im Streitfall ist „die IT" keine belastbare Antwort. Nötig ist ein Name mit Zeitstempel; und ein Mechanismus, der bei Nichterledigung automatisch eskaliert.

Ein weiterer Gesprächspartner ergänzte eine oft übersehene Facette: Selbst wenn das SOC oder die IT einen Befund korrekt behebt, bleibt dies häufig „im Stillen" innerhalb der IT und erreicht die Unternehmensleitung nicht, obwohl diese das eigentliche Haftungsrisiko trägt.

Interessant: Nicht jede Organisation kämpft mit diesem Problem. Ein einzelner Gesprächspartner, dessen Unternehmen Änderungen konsequent über ein Change- und Ticketsystem abwickelt, berichtete, dass bei jeder Änderung automatisch die gesamte nachfolgende Prozesskette mitgeprüft wird. Das jährliche Audit-Problem entsteht bei ihm strukturell gar nicht erst, ein klarer Einzelbeleg dafür, dass das Problem lösbar ist, wenn Verantwortlichkeit und Auslöser sauber miteinander verzahnt sind.

Was das für Sie als MSP bedeutet

Wenn Sie Sicherheitslösungen bei Kunden einführen, achten Sie auf zwei Dinge: dass Maßnahmen zur tatsächlichen Unternehmensrealität passen (sonst werden sie ignoriert); und dass jede Kontrolle einen benannten, zeitlich nachvollziehbaren Verantwortlichen hat, keine Abteilung, und mit sichtbarem Weg zur Geschäftsleitung.

Warum das besonders für MSPs relevant ist

In den Gesprächen kam wiederholt ein Muster auf, das direkt die Rolle von MSPs betrifft: Bei kleineren Organisationen trägt häufig eine einzige Person die Verantwortung für Datenschutz, Informationssicherheit und NIS2 gleichzeitig. Diese Person hat selten die Zeit oder die Spezialisierung, alle drei Bereiche gleichermaßen tief zu durchdringen.

Das erklärt, warum externe Unterstützung gerade im Mittelstand so gefragt ist. Als Hauptgründe für Rückstand bei der NIS2-Umsetzung nennen Unternehmen laut Marktstudien den Bedarf an spezialisiertem Fachwissen (62 Prozent) und fehlende interne Kapazitäten (39 Prozent) (Quelle: Proliance-Studie 2025). Genau das ist die Lücke, die MSPs schließen können, vorausgesetzt, sie können nicht nur behaupten, sondern auch zeigen, dass Kontrollen wirken.

Ein Blick auf die Niederlande: Was lässt sich lernen?

Während Deutschland seit Dezember 2025 unter dem NIS2-Umsetzungsgesetz steht, wird die NIS2-Richtlinie in den Niederlanden erst zum 15. August 2026 in nationales Recht überführt (Cyberbeveiligingswet). Niederländische Organisationen und MSPs stehen damit vor derselben Herausforderung, aber mit einem zeitlichen Vorsprung, um aus der deutschen Erfahrung zu lernen.

Die zentrale Lehre aus den deutschen Gesprächen: Der Übergang gelingt dort am besten, wo Verantwortlichkeit frühzeitig und namentlich geklärt ist, statt erst kurz vor dem Stichtag pauschal Abteilungen zuzuweisen. Ebenso zeigt sich, dass Organisationen, die Sicherheitsmaßnahmen bereits vor der gesetzlichen Pflicht „risikoadäquat“ statt rein formal aufgesetzt haben, den Übergang spürbar reibungsloser erleben. Niederländische MSPs haben bis August 2026 die Gelegenheit, genau diese zwei Punkte, benannte Verantwortlichkeit und risikoadäquate statt pauschale Maßnahmen, bereits jetzt mit ihren Kunden zu klären, statt unter Zeitdruck zu reagieren.

Praktische Ansatzpunkte für das Kundengespräch

Basierend auf den Rückmeldungen der befragten DSB und ISB empfehlen wir MSPs folgende Gesprächsansätze:

1. Fragen Sie nach dem letzten Nachweis, nicht nur nach der letzten Dokumentation. „Wann wurde zuletzt geprüft, ob diese Maßnahme noch wirkt?“ ist oft eine Frage, die viele Kunden nicht beantworten können, und die zeigt, wo der eigentliche Bedarf liegt.
2. Trennen Sie NIS2- und DSGVO-Kommunikation bewusst. Bieten Sie technische Nachweise selbstbewusst für NIS2 an, aber kommunizieren Sie bei der DSGVO ausdrücklich, dass die rechtliche Endbewertung beim DSB verbleibt. Das schafft Vertrauen statt Skepsis.
3. Benennen Sie immer eine Person, nie eine Abteilung. Wenn Sie Maßnahmenpläne mit Kunden vereinbaren, sorgen Sie dafür, dass jeder Punkt einen namentlichen Verantwortlichen mit Frist hat, und dass compliance-relevante Befunde auch bei der Geschäftsleitung ankommen, nicht nur im SOC oder der IT.
4. Zeigen Sie, was zwischen den Audits passiert. Kunden mit jährlichem Audit-Rhythmus sind anfällig für genau die Lücke, die in unseren Gesprächen am häufigsten genannt wurde. Ein Angebot zur kontinuierlichen, statt nur jährlichen, Überprüfung ist ein klares Differenzierungsmerkmal.

Wie Guardian360 Lighthouse dabei unterstützt

Guardian360 Lighthouse führt technische Scans täglich statt einmalig jährlich durch und verknüpft jeden Befund direkt mit einer klar benannten, zeitlich nachvollziehbaren Empfehlung. Das adressiert unmittelbar die in diesem Bericht beschriebenen Lücken: Es macht den Nachweis der Wirksamkeit fortlaufend statt punktuell verfügbar, unterstützt eine ehrliche Trennung zwischen technischem Indikator und rechtlicher Bewertung, und schafft die Grundlage, damit compliance-relevante Befunde nachvollziehbar bei den richtigen Verantwortlichen ankommen. Befunde sind mit ISO 27001, der DSGVO, dem deutschen NIS2-Umsetzungsgesetz, TISAX und ISO 80001 sowie weiteren Normen verknüpft, wodurch die technische Wirksamkeit ergriffener Maßnahmen nachweisbar wird, statt nur abgehakt zu werden. Guardian360 Lighthouse ist als technische Ergänzung zum Managementsystem eines Kunden konzipiert, nicht als Ersatz dafür.

Über diese Studie

Die in diesem Bericht zusammengefassten Erkenntnisse stammen aus einer qualitativen Gesprächsreihe, die Guardian360 mit deutschen Datenschutzbeauftragten, Informationssicherheitsbeauftragten und Auditoren geführt hat, im Rahmen der Validierung eines Ansatzes, der technische Sicherheitsbefunde mit DSGVO-, NIS2- und ISO-27001-Pflichten verknüpft. Die genannten Anteile beziehen sich auf die erhaltenen Rückmeldungen und sind als qualitative Tendenz, nicht als repräsentative Statistik zu verstehen. Externe Quellenangaben sind entsprechend gekennzeichnet.

Guardian360 ist ein niederländisches Unternehmen mit ISO-27001-Zertifizierung. Über die Plattform Guardian360 Lighthouse unterstützen wir MSPs und IT-Dienstleister europaweit dabei, ihren Kunden eine kontinuierliche Sicherheitsüberwachung anzubieten.

Kennzahl	Wert
Erhaltene inhaltliche Fachgespräche	ca. 100
Zeitraum	Juni bis Juli 2026
Zielgruppe	Datenschutz- und Informationssicherheitsbeauftragte in Deutschland
Methode	Offene, qualitative Fachgespräche (keine repräsentative Erhebung)