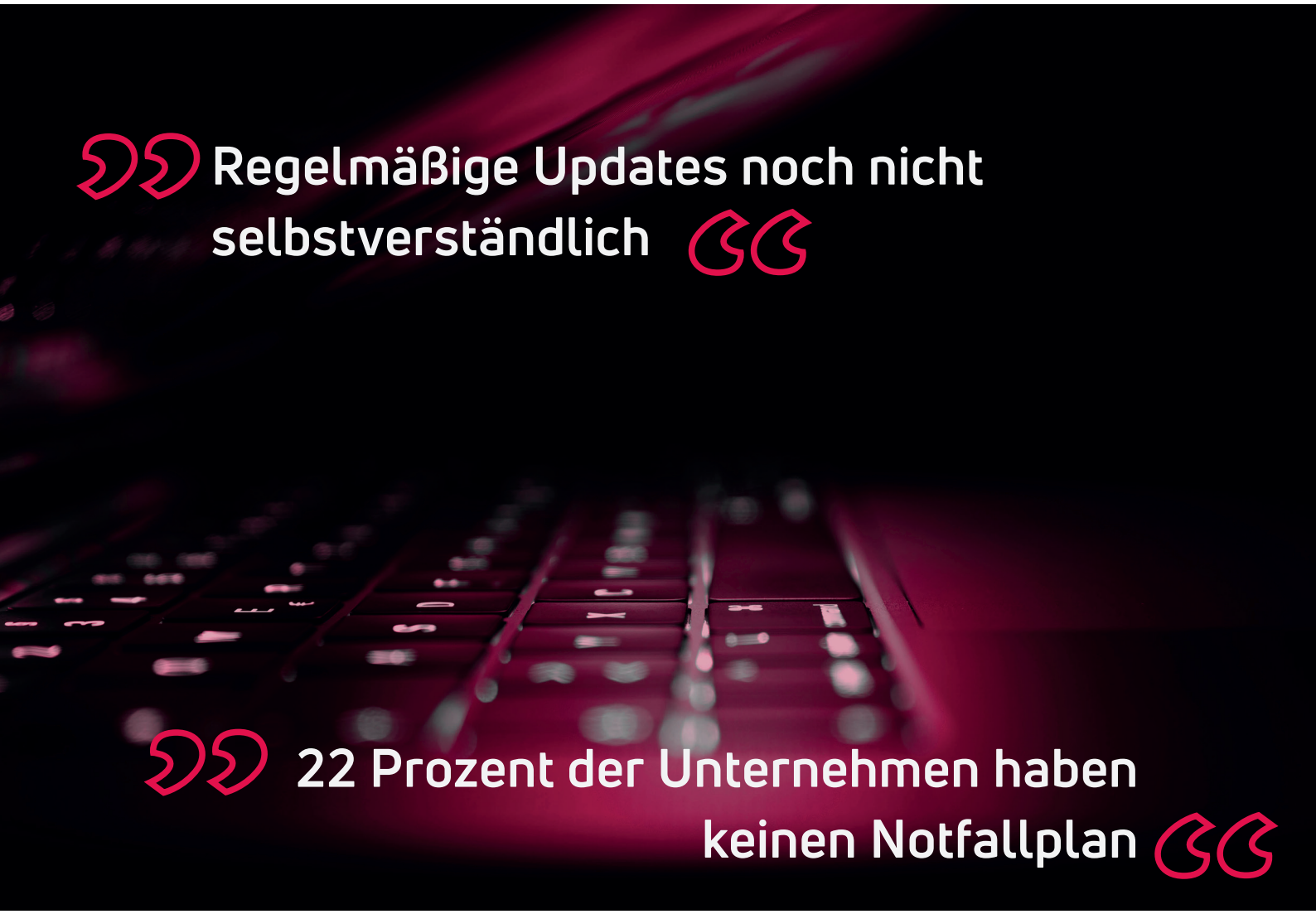
KSV1870

KSÖ

CyberRisk Report

AUSGABE 2025



Aktuelle Ergebnisse
Wie gut sind Österreichs Betriebe auf NIS2 vorbereitet?

Abschlussfazit
Ein Blick in die Zukunft der Cybersicherheit Österreichs.

IMPRESSUM:
Medieninhaber: KSV1870 Nimbusec GmbH, 4020 Linz, Kaisergasse 16b
www.nimbusec.com/www.cyberrisk-rating.at
Herausgeber: Robert Staubmann; Verlagsort: Linz;
Autoren dieser Ausgabe: Robert Staubmann, Alen Kocaj, Sabrina Sablatnigg,
Layout: Sabrina Sablatnigg; Lektorat: Angelika Peinhaupt

Hinweis: Aus Gründen der Lesbarkeit wird darauf verzichtet, geschlechtsspezifische Formulierungen zu verwenden.
Soweit personenbezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf alle Geschlechter.

Vorwort

Die Wirtschaft wird zunehmend digitaler. Damit einhergehend ist in den vergangenen Jahren die Internetkriminalität in Österreich deutlich gestiegen – rund 60.000 derartige Fälle werden aktuell pro Jahr gezählt. Nachrichten über gezielte Cyberattacken auf Unternehmen und Organisationen kommen in den Medien regelmäßig vor. Dennoch überschätzen viele Betriebe ihre IT- und Cybersicherheit und sind mit der Implementierung notwendiger Schutzmaßnahmen überfordert. Das muss sich rasch ändern.

Dass Cyberattacken nicht „nur" ein technisches Risikothema sind, sondern auch die Finanzen eines Unternehmens im Ernstfall massiv belastet werden können, ist bekannt. Spätestens mit Inkrafttreten der EU-NIS2-Richtlinie in Österreich, die für ein höheres Sicherheitsniveau von Netz- und Informationssystemen sorgen soll, kann das Missachten entsprechender IT-Sicherheitsvorkehrungen bereits deutlich früher als im Fall einer Cyberattacke zu empfindlichen finanziellen Einbußen führen. Denn im Zuge der bevorstehenden Richtlinie wird es sowohl für Unternehmen kritischer Sektoren ebenso wie für deren Geschäftspartner de facto nur noch dann möglich sein, Geschäfte abzuschließen, wenn auf beiden Seiten ein entsprechender Nachweis über konkrete Maßnahmen in Bezug auf Cybersicherheit vorgelegt werden kann.

Ricardo-José Vybiral
CEO der KSV1870 Holding AG

Als KSV1870 setzen wir uns für ein hohes Cybersicherheitsniveau ein und fordern, diesem Thema höchste Aufmerksamkeit zu widmen. IT-Sicherheitsvorfälle können jeden Betrieb treffen – den international tätigen Großkonzern ebenso wie den regionalen Installateur. Um das Sicherheitslevel der Betriebe auf ein höheres Niveau zu heben, haben wir gemeinsam mit der KSV1870 Nimbusec GmbH das CyberRisk Rating entwickelt – und unterstützen die Unternehmen dabei, NIS-konform zu agieren.

Die Zeit des Handelns ist gekommen. Verbessern Sie heute Ihr IT-Sicherheitsniveau, um morgen keinen finanziellen Kollaps zu erleiden. Wir helfen Ihnen gerne dabei.

Foto: WILKE | Ricardo-José Vybiral

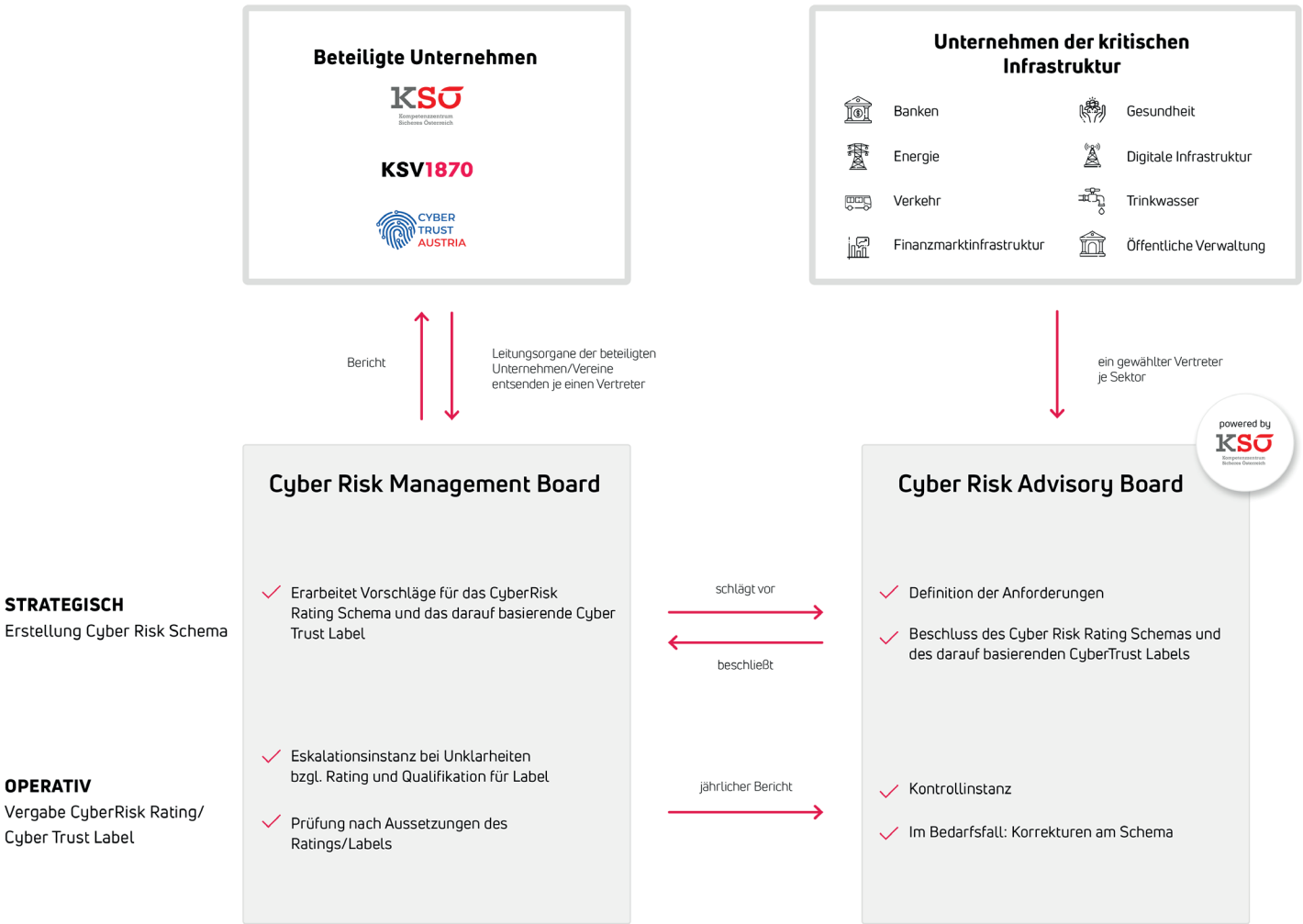
Mit einer soliden Basis beginnt der Erfolg.

Die Basis dieses Reports sowie die damit verbundene Auswertung bilden das KSV1870 CyberRisk Rating sowie das dahinterliegende KSÖ CyberRisk Schema.

Die Kriterien des Cyber-Risk-Schemas wurden von renommierten Cyber-Risk-Managern aus allen Bereichen der kritischen Infrastruktur sowie von Vertretern bedeutender österreichischer Unternehmen festgelegt. Dadurch ist das CyberRisk Rating für alle Branchen und Wirtschaftssektoren relevant. Das Rating basiert auf insgesamt 25 Fragen - 14 Basisfragen müssen für ein B-Rating beantwortet werden, die Beantwortung weiterer elf Fragen ist für ein A-Rating erforderlich.

Das Schema wird kontinuierlich aktualisiert, um auf neue Entwicklungen und Herausforderungen reagieren zu können.

Das Schema und weitere Informationen finden Sie auf **cyberrisk-rating.at**



Wie läuft ein Rating ab?

Das KSV1870 CyberRisk Rating hilft, zentrale Anforderungen des NIS-Gesetzes im Bereich Lieferantenrisiken zu erfüllen und zu bewerten.

Einfach und in drei Schritten umsetzbar.

BEANTWORTUNG

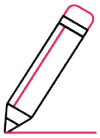
Anforderungen beantworten

Das Assessment besteht aus 25 Fragen, die mit Ja oder Nein zu beantworten sind. Im Falle einer "Ja"-Beantwortung, muss textuell beschrieben werden, wie die jeweilige Maßnahme im Unternehmen umgesetzt wird.

RÜCKFRAGE/ VALIDIERUNG

Rückfrage zu den gegebenen Antworten

Die im Assessment gegebenen Antworten des zu bewertenden Unternehmens werden von qualifizierten Prüfern validiert. Nur schlüssige und fachlich korrekte Antworten werden akzeptiert.



KORREKTUR

Unklare Antworten genauer ausführen

Das zu bewertende Unternehmen hat einmalig die Möglichkeit, für den Prüfer unklare Antworten genauer auszuführen und zu korrigieren.

RE-EVALUIERUNG

Finale Validierung der gegebenen Antworten

Auf Basis der korrigierten Antworten berechnen unsere Prüfer das CyberRisk Rating des jeweiligen Unternehmens.

VERÖFFENTLICHUNG

A- oder B-Rating auswählen

Das zu bewertende Unternehmen hat nun die Möglichkeit, zwischen der Veröffentlichung des A- (Advanced Security) oder B-Ratings (Basic Security) zu wählen.

Welche Vorteile bietet das KSV1870 CyberRisk Rating?

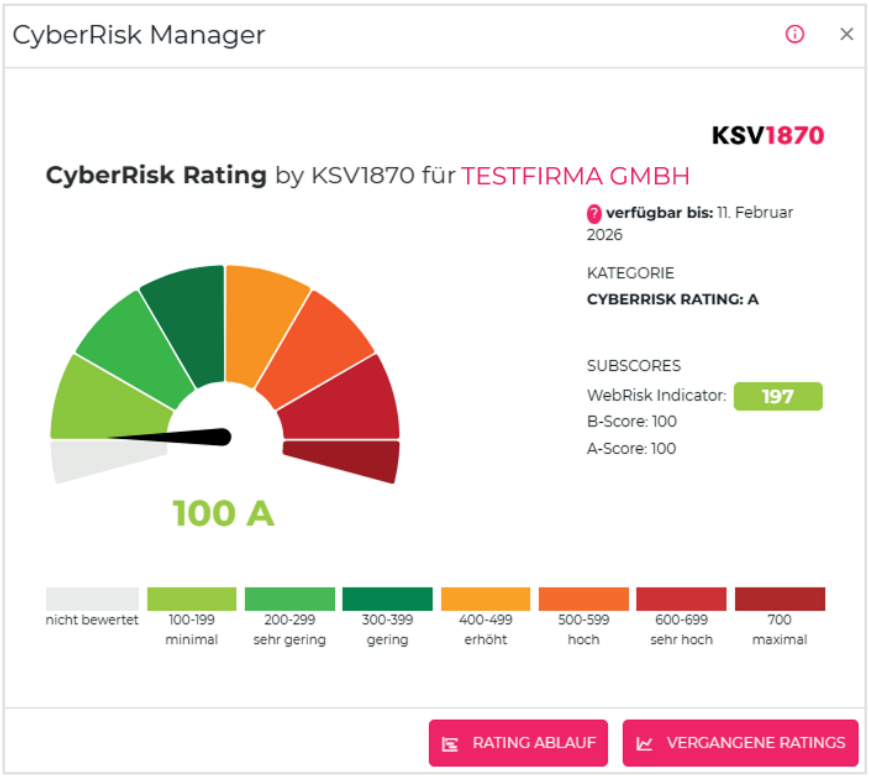
EU-Vorgaben wie NIS, DORA, DSGVO sowie diverse Sicherheitszertifizierungen fordern ein professionelles Cyber-Risikomanagement für Dienstleister, Lieferanten und Dritte.

Das CyberRisk Rating von KSV1870 bietet einen standardisierten Ansatz, um diese Anforderungen zu erfüllen, macht Cyberrisiken in globalen Lieferketten transparent und ermöglicht deren gezielte Reduktion.

Zusätzlich gibt es folgende Vorteile:

- professionell validiert
- kosteneffizient durch standardisierte Prozesse
- weniger Aufwand für Lieferant und Auftraggeber

Beispiel



Das KSV1870 CyberRisk Rating erfüllt laut der österreichischen operativen NIS-Behörde (BMI) die Anforderungen des NIS-Gesetzes für Lieferantenrisiken (§ 11 Abs. 1 Z 2 iVm Anlage 1 NISV) und ist im NIS Fact Sheet unter "Best Practises" gelistet.

KSV1870 CyberRisk Rating
Auswertung

nimbusec
Part of KSV1870

Foto: Freepik

KSV1870 CyberRisk Rating Auswertung

Durch das CyberRisk Rating konnten wichtige Daten von Unternehmen erhoben werden, um einen Überblick über die Cybersicherheit in Österreich zu gewähren. Es wurden Daten von Unternehmen zwischen 2024 und 2025 analysiert, die im Rahmen der Erstellung von CyberRisk Ratings Anwendung fanden.

DATENANALYSE: Alen Kocaj | **TEXT:** Robert Staubmann, Sabrina Sablatnigg, Alen Kocaj

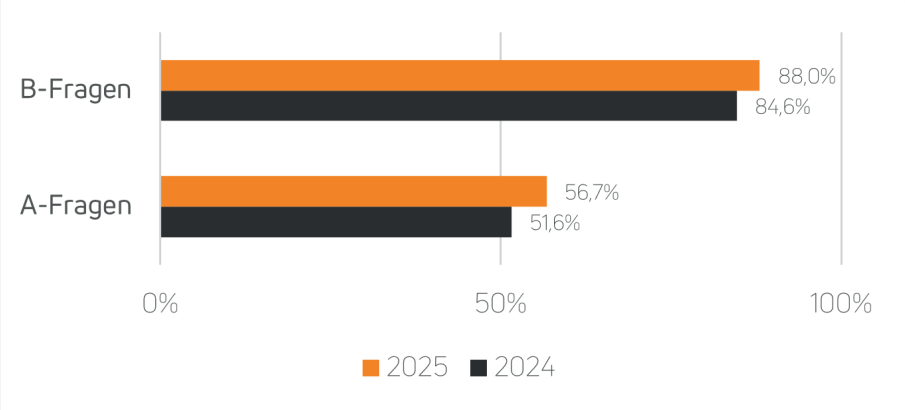
Vorgehensweise

Für die genaue Analyse wurden die gesammelten Ja/Nein-Antworten der A- und B-Fragen inklusive ihrer Validierung von über 500 abgeschlossenen CyberRisk Ratings herangezogen. Sämtliche Ergebnisse und prozentuelle Werte beziehen sich auf dieses Datenset.
Wichtig Die Daten sind Echtdaten. Die Auswertungen bilden reale Ist-Zustände aus Validierungen und Audits ab.

Überblick

Diese Auswertung bildet ein gesamtheitliches Bild über die Jahre bis 2024 und 2025 ab. Wobei die Beschreibung 2024 die Auswertungen von 2024 und den Jahren davor abbildet.

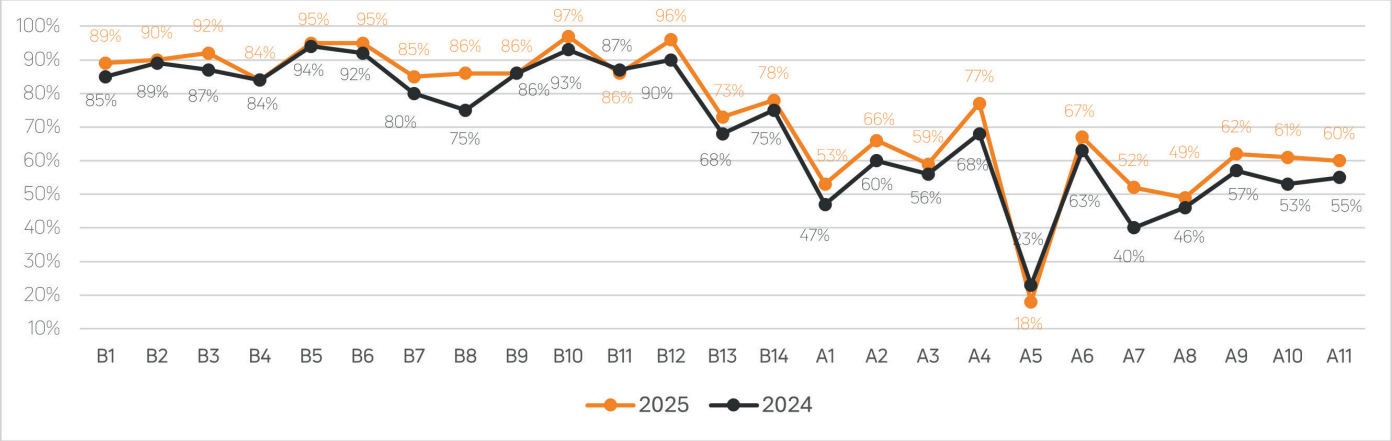
Die B- und A-Fragen wurden im Zeitverlauf auf Erfassungsquote verglichen.



Die Cyberresilienz steigt an.

Hinweis zur Datenverarbeitung und Anonymisierung
Im Rahmen dieser Analyse wurden ausschließlich anonymisierte Daten verwendet. Personenbezogene Informationen wurden entweder nicht erhoben oder vor der Auswertung vollständig entfernt bzw. so verändert, dass kein Rückschluss auf Einzelpersonen möglich ist. Die Einhaltung geltender Datenschutzbestimmungen, insbesondere der DSGVO, wurde bei allen Verarbeitungsschritten gewährleistet.

Jahresvergleich



Die Grafik beschreibt den Zeitraum 2024 (und die Jahre davor) bis 2025. In dieser sind alle Fragen der Basissicherheit (B-Fragen) und dem fortgeschrittenen Sicherheitslevel in der X-Achse abgebildet. Die Y-Achse bildet das validierte Endergebnis ab.

Die B-Fragen sowie die A-Fragen haben im Vergleich zu den Jahren davor eine höhere Erfüllungsquote.

Foto: Firefly

Basissicherheitslevel (B-Rating)

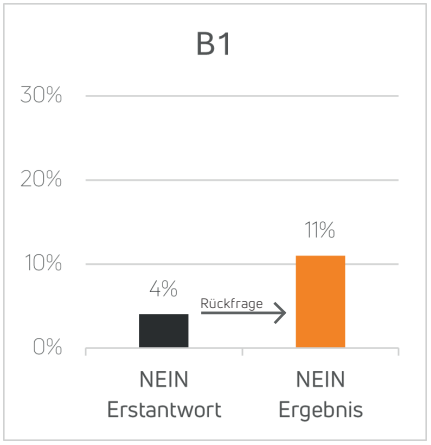
Das B-Rating bewertet das Basissicherheitsniveau der IT einer Organisation. Die Anforderungen beziehen sich auf einen grundlegenden Schutz, der von jeder Organisation eingehalten werden sollte. Diese sind allgemein formuliert, erfordern aber eine Mindestqualität, um die notwendigen Sicherheitsanforderungen zu garantieren.

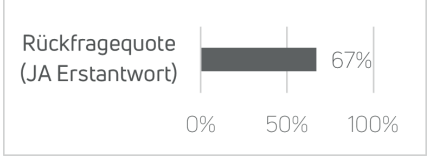
Auswertungsergebnisse

Die nachfolgende Auswertung bezieht sich auf einen konkreten Teil des CyberRisk Rating-Ablaufs. Der gesamte Ablauf einer Rating-Erstellung wird auf Seite 5 dargestellt.

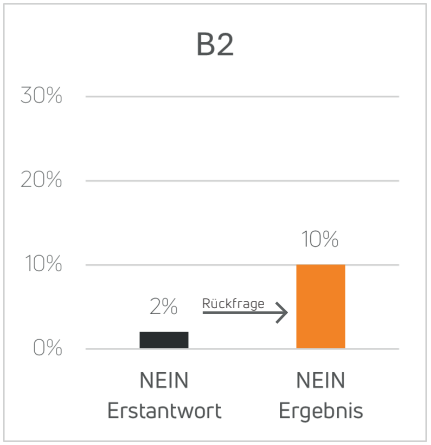
In der Auswertung wird die "*Nein*"-*Erstantwort* mit dem "*Nein*"-*Ergebnis* verglichen. Das bedeutet beispielsweise, dass Unternehmen die erste Basissicherheislevelfrage (B1) zu 4% mit "Nein" und zu 96% mit "Ja" beantworten. Nach Rückfrage der Antwort liegt das Ergebnis der Stichprobe bei 11% "Nein" und 89% "Ja".

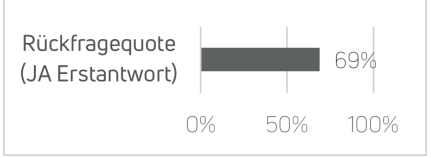
B1 - Haben Sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für Ihr Unternehmen gültig ist?



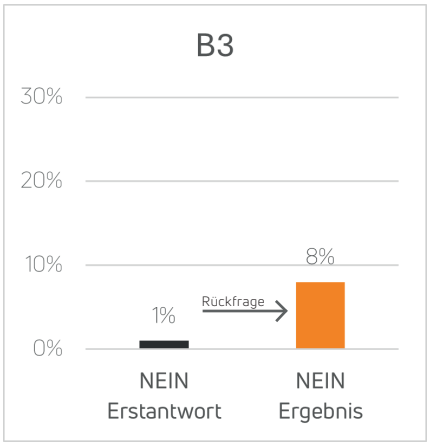


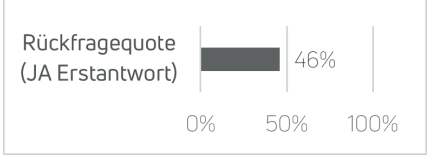
B2 – Schulen Sie Ihre Mitarbeiter regelmäßig in Informationssicherheit?



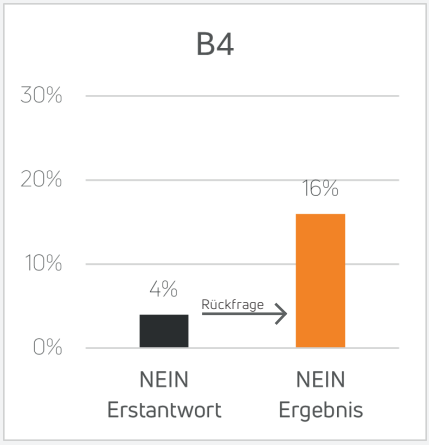


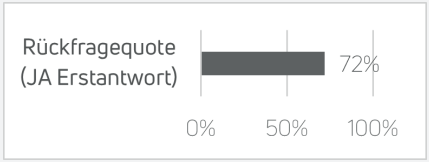
B3 - Gibt es in Ihrem Unternehmen eine oder mehrere benannte Personen, die für das Thema Informationssicherheit zuständig sind?



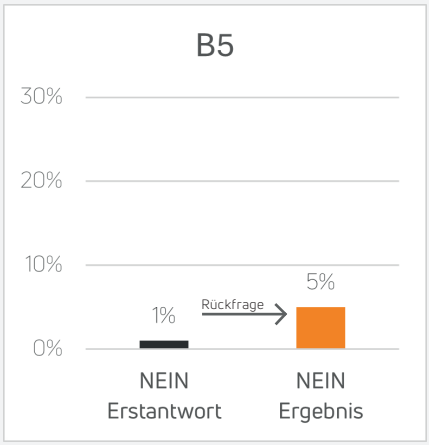


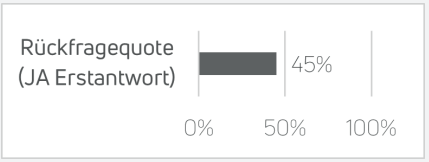
B4 - Pflegen Sie regelmäßig ein Verzeichnis all Ihrer IT-Assets und - Services (inkl. Cloud-Dienste) sowie der damit verbundenen Verantwortlichkeiten?



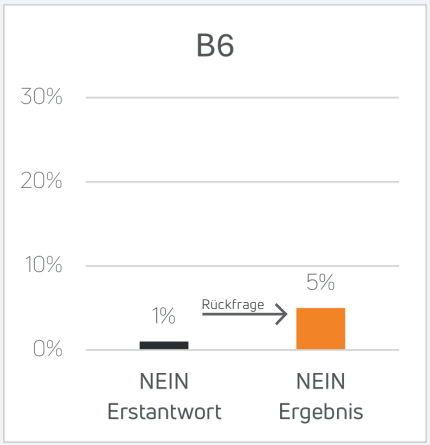


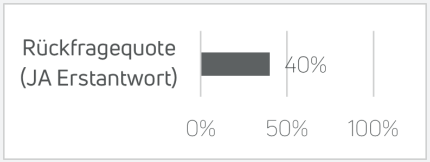
B5 - Verwalten Sie den Zugang zu Ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?





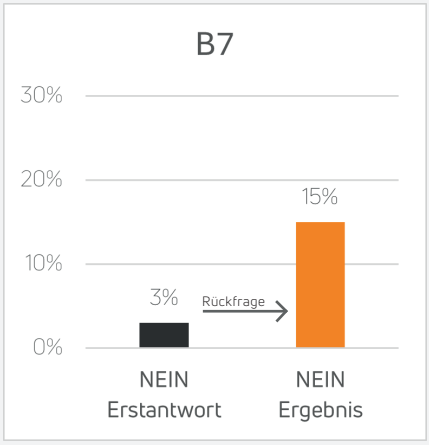
B6 - Verlangen Sie von Ihren Mitarbeitern, für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?

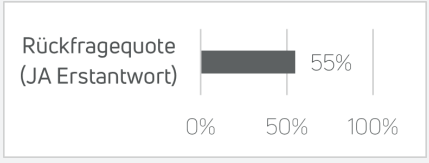




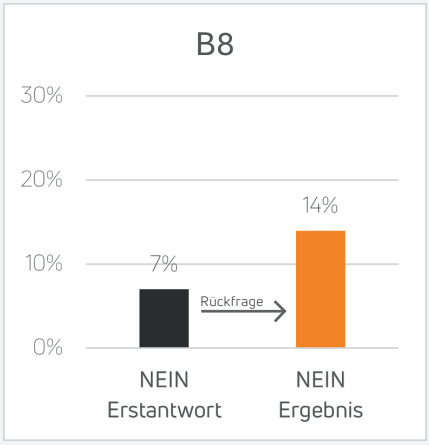
95% DER UNTERNHEMEN HABEN EIN ANGEMESSENES BERECHTIGUNGS-MANAGEMENT

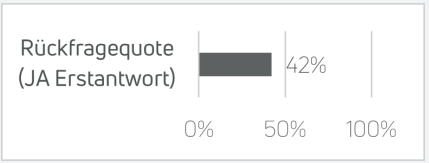
B7 - Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all Ihrer IT-Systeme?



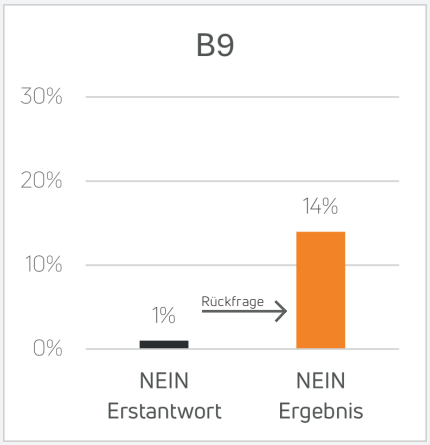


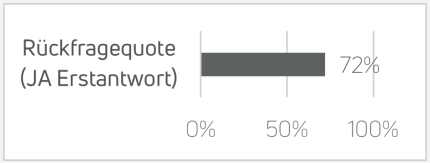
B8 – Überprüfen Sie - sofern vorhanden - individuell entwickelte, aus dem Internet zugängliche Anwendungen auf Sicherheitslücken vor Inbetriebnahme?



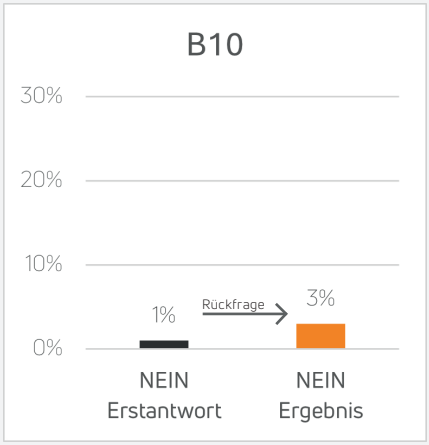


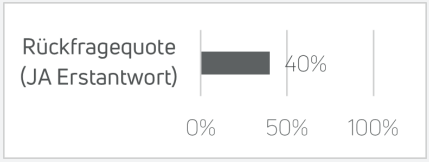
B9 - Aktualisieren Sie alle IT-Systeme und Anwendungen regelmäßig mit Sicherheitsupdates?



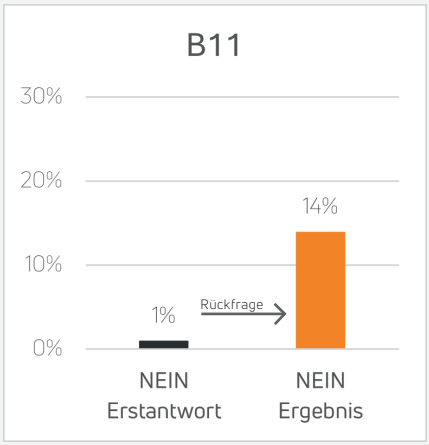


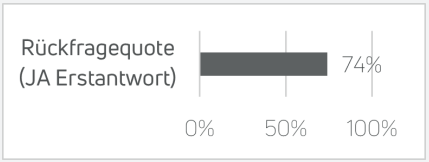
B10 - Sichern Sie Ihr Netzwerk vor unberechtigtem Zugriff von Außen ab?



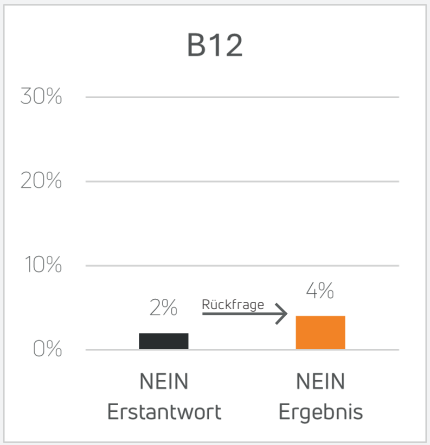


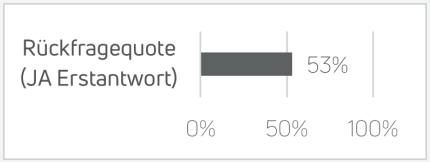
B11 - Überwachen Sie Ihre IT-Systeme auf Malware?





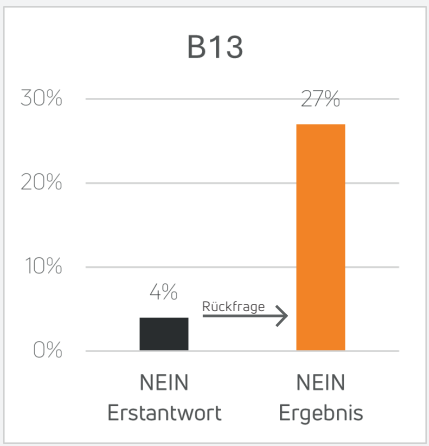
B12 - Verschlüsseln Sie sensible Daten bei der Übertragung im Internet?

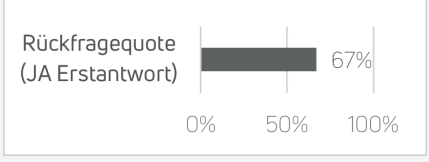




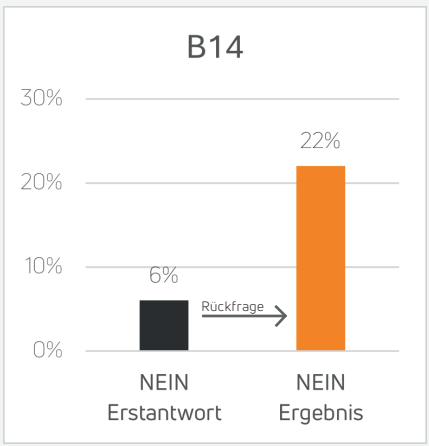
KNAPP JEDES VIERTE UNTERNEHMEN HAT KEINE AUSREICHENDE BACKUP- UND NOTFALLPLANUNG

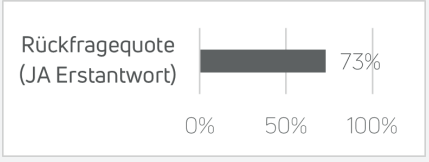
B13 - Protokollieren Sie die Nutzung Ihrer IT-Systeme, um Sicherheitsvorfälle nachvollziehbar zu machen?





B14 - Haben Sie einen Notfallplan, anhand dessen Sie auf einen IT-Sicherheitsvorfall reagieren?





Zwischenfazit B-Rating:

Die grundlegenden Sicherheitsanforderungen (B-Fragen) werden durchwegs zuverlässig erfüllt. Auch bei Rückfragen zeigen sich konsistente Standards. Das unterstreicht, dass IT-Sicherheit in vielen Unternehmen bereits fest etabliert ist.

In durchschnittlich 9,36 % der Fälle zeigt sich, dass Unternehmen ihre Erstantwort tendenziell zu optimistisch einschätzen.

Fortgeschrittenes Sicherheitslevel (A-Rating)

Das A-Rating bewertet den Anspruch eines fortgeschrittenen Sicherheitsniveaus einer Organisation. Es gilt für Organisationen, die aufgrund ihrer Tätigkeit einen höheren Sicherheitsanspruch haben. Die Bewertung erfolgt durch eine Selbstdeklaration der Organisation und entspricht der gleichen Methode wie jener des B-Ratings.

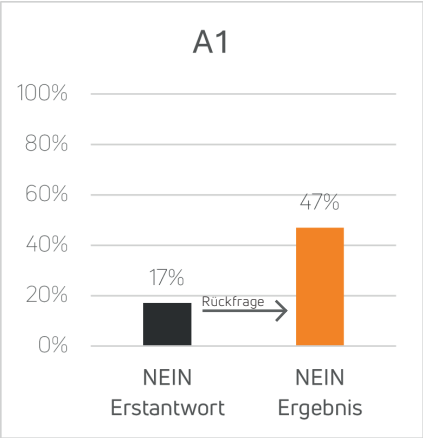
Auswertungsergebnisse

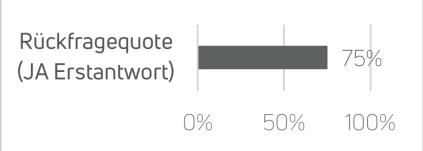
Die nachfolgende Auswertung bezieht sich auf einen konkreten Teil des CyberRisk Rating-Ablaufs. Der gesamte Ablauf des Ratings befindet sich auf Seite 5.

In der Auswertung wird die *"Nein"-Erstantwort* mit dem *"Nein"-Ergebnis* verglichen. Das bedeutet beispielsweise, dass Unternehmen die erste fortgeschrittene Sicherheitslevelfrage (A1) zu 17% mit "Nein" und zu 83% mit "Ja" beantworten. Nach Rückfrage der Antwort liegt das Ergebnis der Stichprobe bei 47% "Nein" und 53% "Ja".

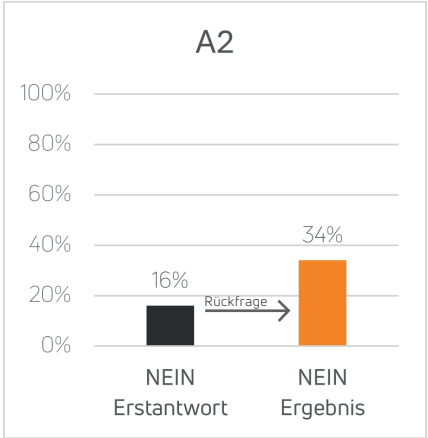
ÜBER EIN DRITTEL DER FORTGESCHRITTENEN UNTERNEHMEN HAT NOCH KEIN WIRKSAMES RESILIENZKONZEPT UMGESETZT ODER GETESTET

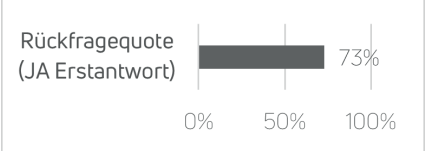
A1 - Überprüfen Sie IT-Systeme in Ihrem Netzwerk auf Sicherheitslücken?



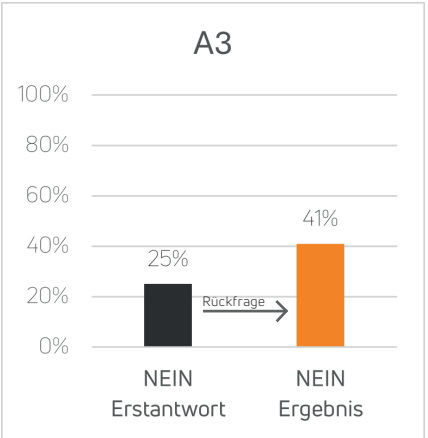


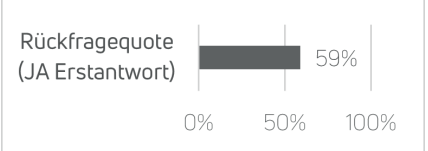
A2 - Haben Sie Mechanismen im Einsatz, die bei der Erstellung bzw. dem Erwerb von individuell entwickelter Software deren Sicherheit überprüfen?



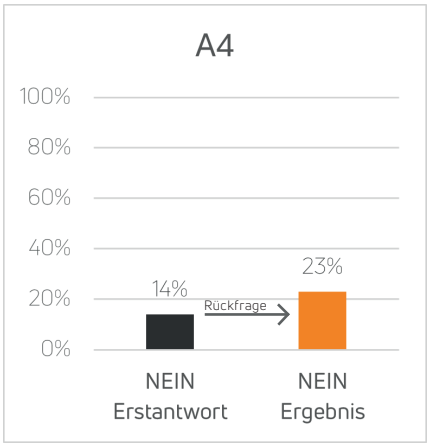


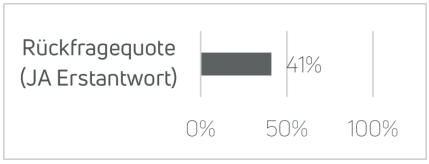
A3 - Führen Sie in Ihrer Systemlandschaft Penetration Tests durch?



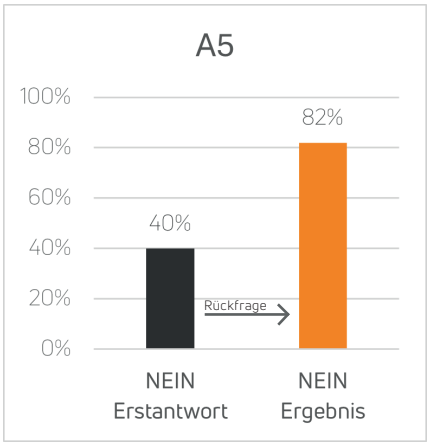


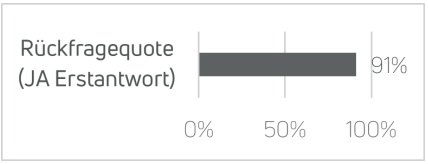
A4 - Überwachen Sie Ihre Systemlandschaft auf ungewöhnliche Aktivitäten und Anomalien?



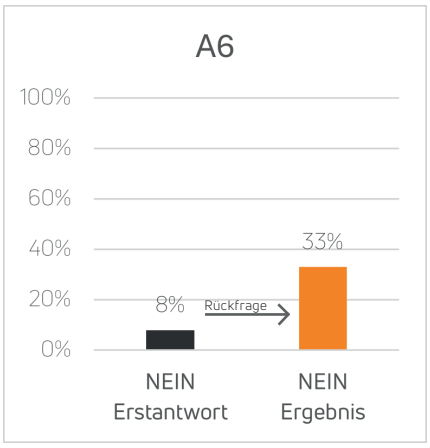


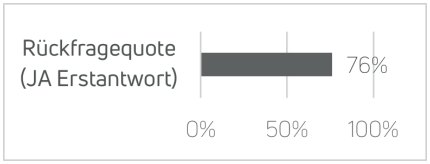
A5 - Haben Sie Whitelisting und Cloud Access Security Broker (CASB) im Einsatz, um die Ausführung nicht autorisierter Prozesse und Anwendungen zu unterbinden?





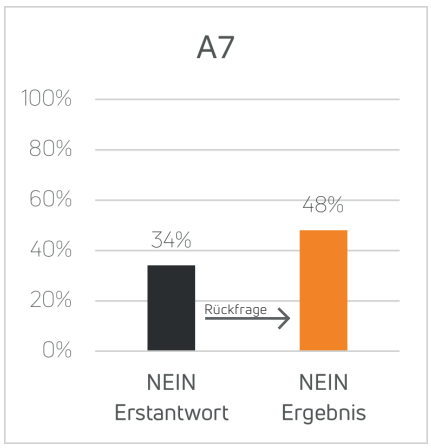
A6 - Schützen Sie Identitäten, Zugriffe und Berechtigungen in geeigneter und nachvollziehbarer Weise?

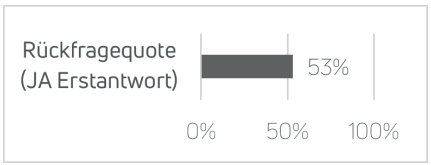




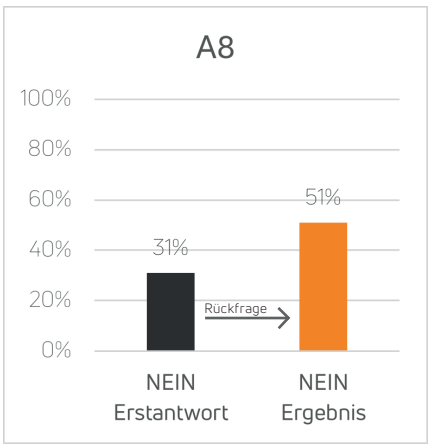
ÜBER 80 % HABEN WEDER WHITELISTING NOCH EINEN CLOUD ACCESS SECURITY BROKER IM EINSATZ (A5)

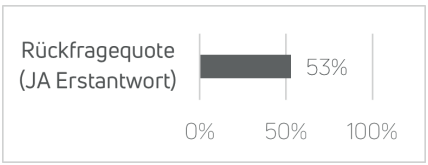
A7 - Haben Sie Technologie im Einsatz, die die Log Files Ihrer Systeme automatisiert korreliert und analysiert?



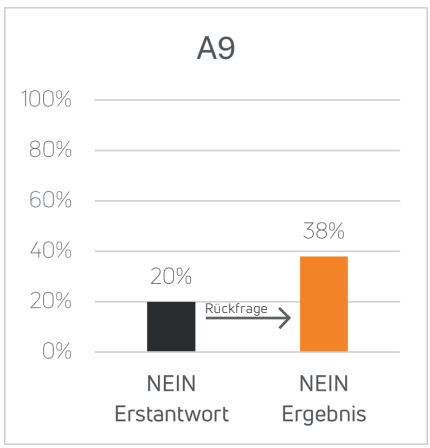


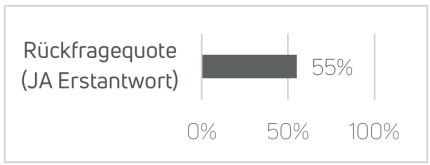
A8 - Haben oder nutzen Sie ein Security Operations Team?



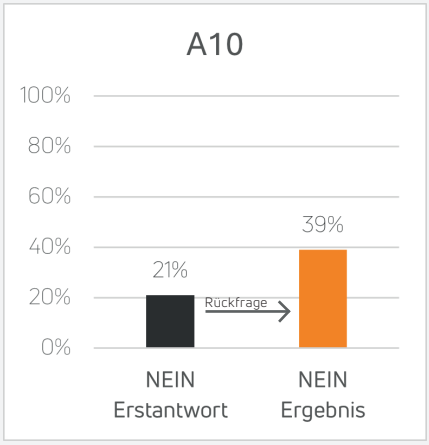


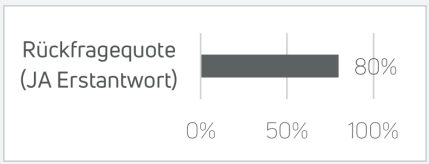
A9 - Können Sie bei einem schwerwiegenden Sicherheitsvorfall auf qualifizierte Ressourcen zurückgreifen?



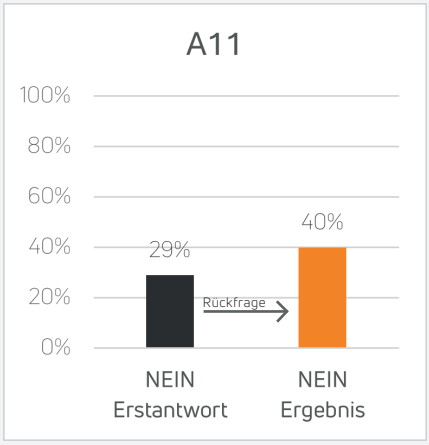


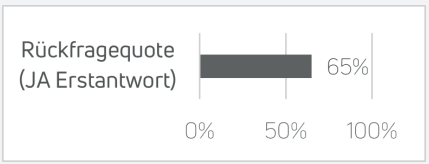
A10 - Stellen Sie über ein getestetes Resilienzkonzept oder eine resiliente Architektur Ihre Betriebskontinuität sicher?





A11 - Haben Sie einen Prozess zum Management Ihrer Lieferantenrisiken?





Zwischenfazit A-Rating

Kategorie A verdeutlicht, dass viele Unternehmen den überdurchschnittlichen Sicherheitsstandard bislang noch nicht erreichen.

Die Analyse der A-Fragen zeigt, dass Unternehmen ihre Leistungen in diesem Bereich im Schnitt um 20 % überschätzen.

Highlights der Auswertungen

Zur besseren Übersicht wurden die zentralen Erkenntnisse der Auswertung 2025 in kompakter und prägnanter Form zusammengefasst. Sie bieten einen Überblick über die wichtigsten Entwicklungen und Tendenzen des aktuellen Jahres. Darüber hinaus wurden relevante KPIs aus dem CyberRisk Report 2024 überarbeitet, aktualisiert und in einem direkten Vergleich mit den Zahlen von 2025 (Stand August) gegenübergestellt. Die daraus resultierenden Unterschiede und Veränderungen werden in den begleitenden Beschreibungen detailliert erläutert.

14%

der Unternehmen führen keine regelmäßigen Sicherheitsupdates durch. (B9)

90%

der Unternehmen schulen ihre Mitarbeiter regelmäßig in Informationssicherheit. (B2)

5%

der Unternehmen fordern von ihren Mitarbeitern keine Verwendung von Passwörtern mit einer sicheren Mindeststärke für alle Anwendungen. (B6)

3 von 10

Lieferanten sind nicht in der Lage, IT-Sicherheitsvorfälle in ihrem Unternehmen durch Protokollierung ihrer Systeme zuverlässig zu erkennen. (B13)

86%

der österreichischen Unternehmen überwachen ihre IT-Systeme aktiv auf Schadsoftware. (B11)

22%

der Unternehmen haben keinen Notfallplan, anhand dessen sie auf einen IT-Sicherheitsvorfall reagieren könnten. (B14)

60%

Nur 60% der Unternehmen besitzen einen Prozess zum Management ihrer Lieferantenrisiken. (A11)

25.295

Lieferanten sind in der CyberRisk Datenbank eingemeldet. Die Anzahl hat sich im Vergleich zum Vorjahr mehr als verdoppelt. (12.342)

A-Rating

38,5%

jener Lieferanten, für die ein A-Rating angefragt wurden, können den Anforderungen nicht gerecht werden.

B-Rating

20,7%

der Unternehmen weisen ein mangelndes Basissicherheitslevel (B-Rating: schlechter als 300 inkl. Assessments, welche abgelehnt oder zurückgezogen wurden) auf.

1 VON 3

Unternehmen verwendet keine Multifaktor-Authentifizierung insbesondere für von extern erreichbare Systeme. So kann der Schutz von Identitäten, Zugriffe und Berechtigungen nicht gewährleistet werden. (A6)

WEBSITE SECURITY

249.111

Unternehmen und deren Websiten werden monatlich gescannt.

DURCHSCHNITTLICHER WEBRISK INIDKATOR FÜR ÖSTERREICH

213,5

Der WebRisk Indikator für Österreich liegt im Wertebereich zwischen 100 und 700 im unteren Drittel (das Ergebnis wurde um 0-Summen bereinigt und gerundet). Somit ist der Durchschnitt im Vergleich zu 2024 (219,5) gesunken. Das bedeutet, dass Österreichs Websiten (etwas) sicherer geworden sind.

Fazit

Im Spannungsfeld zwischen einer stark steigenden Anzahl an Cyberangriffen und regulatorischen Maßnahmen auf europäischer Ebene sehen sich viele österreichische Unternehmen mit zahlreichen Herausforderungen konfrontiert. Die Umsetzung der Regulatorik ist jedenfalls ein wichtiger Schritt für eine flächendeckende Sensibilisierung zum Thema Cybersecurity, entscheidend wird die konkrete Umsetzung effektiver Maßnahmen innerhalb der Unternehmen sein. Diese ist ohne Wenn und Aber ein fundamentaler Bestandteil eines professionellen Risikomanagements der Gegenwart.

Der KSV1870 CyberRisk Rating Report 2025 zeigt, dass eine positive Tendenz klar erkennbar ist. Die vom CyberRisk Advisory Board erarbeiteten Anforderungen (CyberRisk Schema) werden von Lieferanten schrittweise deutlich besser erfüllt als noch vor einem Jahr, und erhöhen somit die Cyberresilienz flächendeckend. Darüber hinaus ist eine klare positive Tendenz erkennbar, dass vor allem Basisanforderungen zum Teil besser erfüllt werden als zum selben Zeitpunkt des Vorjahres. Dennoch: trotz einer positiven Entwicklung besteht in Summe nach wie vor ein hohes Verbesserungspotenzial. Die Unternehmen müssen weiterhin mit Nachdruck daran arbeiten, ihre Cybersicherheit zu stärken. Die zum Teil deutliche Differenz zwischen Eigenangaben und dem rückgefragten (validierten) Endergebnis zeigt, wie wichtig eine kritische Prüfung von intern erstellten Reports, KPIs und Maßnahmen ist. Zugleich bilden sie die Basis für weitere Verbesserung.

Als KSV1870 Nimbusec GmbH sind wir froh, zu sehen, dass gesetzte Maßnahmen, wie etwa das CyberRisk Schema, einen Mehrwert zur Erhöhung der Cyberresilienz von Unternehmen beitragen!

Foto: Anna Rauchenberger | Robert Staubmann

Robert Staubmann
Geschäftsführer der KSV1870 Nimbusec GmbH

DAS
CYBERRISK
RATING
by KSV1870

Der CyberRisk Manager by KSV1870 Nimbusec

Ihre Plattform für ein effizientes Cyberrisiko-Management von Lieferanten nach NIS2.

→ **EFFIZIENT**

Für viele Lieferanten, einfach koordinierbar, inkl. API-Integration.

→ **BEST PRACTICE LAUT NIS FACT SHEET**

Die Basis für Ihr Lieferantenmanagement nach NIS2 und DORA.

→ **ALL-IN-ONE**

In einer Plattform Nachweise verwalten, Lieferanten kontaktieren und Maßnahmen setzen.

Fragen?
Wir sind für Sie da.

Telefonisch
+43 (0) 732 / 860 626

Per E-Mail
office@nimbusec.com

POWERED BY
nimbusec
Part of **KSV1870**