

NIS2, WESHALB, WARUM? –

STUDIE ZUM AKTUELLEN KENNTNISSTAND UND
UMSETZUNGSGRAD VON NIS2 IN DEUTSCHLAND



In Zusammenarbeit mit unserem exklusiven Studienpartner

mimecast[®]



NIS2, WESHALB, WARUM? – STUDIE ZUM AKTUELLEN KENNTNISSTAND UND UMSETZUNGSGRAD VON NIS2 IN DEUTSCHLAND

Inhalt

Management Summary 3

1. Das Wissen zu NIS2 ist noch sehr lückenhaft 4
 2. Die meisten Unternehmen meinen, die NIS2-
Umsetzung fristgerecht zu schaffen 5
 3. Beim Gros der Unternehmen reicht die
vorhandene Security für NIS2 nicht aus..... 6
 4. Die Höhe der Sanktionen bei NIS2-Verletzung
ist oft noch eine Unbekannte 7
- Summary 8

Studiendesign

- Impressum 2
Studiensteckbrief 9
Stichprobenstatistik 9

Editorial 3

Studienpartner

- Mimecast 10

Impressum

Fragebogenentwicklung:
Bernd Hohlweg (Mimecast),
Halime-Merve Ersan (Mimecast),
Matthias Teichmann (Foundry)

**Endredaktion /
CvD Studienberichtsband:**
Matthias Teichmann

Analysen / Kommentierungen:
Oliver Schonschek, Bad Ems

**Hosting / Koordination
Feldarbeit:**
Armin Rozsa
(Foundry)

Studienpartner:
Mimecast Germany GmbH
Kistlerhofstraße 172
81379 München
Telefon: +49 89 904 200 800
www.mimecast.com/de

Grafik:
Jutta Weber-Vidal, Würzburg
www.erdenbuerger.de

Umschlaggestaltung unter
Verwendung einer Farbgrafik
von © shutterstock / Pyty

Lektorat:
Elke Reinhold, München

Ansprechpartner:
Matthias Teichmann
matthias.teichmann@foundryco.com

**Foundry
(formerly IDG Communications)**

Anschrift:
IDG Tech Media GmbH
Georg-Brauchle-Ring 23
80992 München
Telefon: +49 89 36086 0
Fax: +49 89 36086 118
E-Mail: info@idg.de

Vertretungsberechtigter:
Jonas Triebel, Geschäftsführer

Registergericht:
Amtsgericht München, HRB 99110

Umsatzsteueridentifikationsnummer:
DE 811 257 834

Weitere Informationen unter:
www.foundryco.com

Alle Angaben in diesem Ergebnisband wurden mit größter Sorgfalt zusammengestellt. Trotzdem sind Fehler nicht ausgeschlossen. Verlag, Redaktion und Herausgeber weisen darauf hin, dass sie weder eine Garantie noch eine juristische Verantwortung oder jegliche Haftung für Folgen übernehmen, die auf fehlerhafte Informationen zurückzuführen sind.

Der vorliegende Ergebnisberichtsband, einschließlich all seiner Teile, ist urheberrechtlich geschützt. Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen, auch auszugsweise, bedürfen der schriftlichen Genehmigung durch den Herausgeber.

Einleitung

Am 27.12.2022 wurde die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2-Richtlinie) im Amtsblatt L333 der Europäischen Union veröffentlicht. Sie stellt eine Weiterentwicklung der (ersten) NIS-Richtlinie aus dem Jahr 2016 dar und muss bis Oktober 2024 in nationales Recht umgesetzt sein. Hochrechnungen zufolge werden zirka 30.000 deutsche Institutionen und Unternehmen davon betroffen sein. Das sind deutlich mehr als nach bisherigem Recht.

Wie gut wissen Unternehmensentscheider und IT-Verantwortliche über NIS2 Bescheid, wie fortgeschritten sind entsprechende Umsetzungen bzgl. der nahenden Deadline?

Diese und weitere Fragen untersucht die Studie von CIO, CSO und Computerwoche in Kooperation mit Mimecast. Basis ist eine Kurzumfrage auf Basis von 108 Befragten, die im Juli 2024 durchgeführt wurde.

Die Key Findings
im Überblick

Management Summary



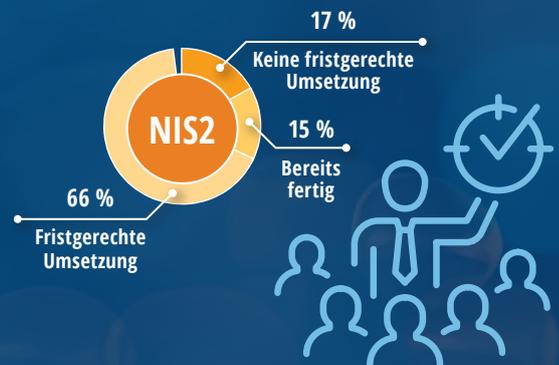
Nicht einmal jeder Zehnte kennt alle Inhalte von NIS2

Von fünf Fragen zu NIS2 können die Teilnehmer im Durchschnitt nicht einmal drei Fragen richtig beantworten. Sieben Prozent der Befragten gaben sogar bei jeder Frage eine falsche Antwort. Im Durchschnitt antworteten zudem 21 Prozent der Unternehmen mit „Ich weiß nicht“.



92 Prozent der Unternehmen benötigen ein dediziertes NIS2-Budget

24 Prozent der Befragten sehen den Investitionsbedarf bei bis zu 50.000 Euro, weitere 37 Prozent berichten von Investitionen von bis zu 100.000 Euro, während 31 Prozent der Unternehmen die Investitionen mit mehr als 100.000 Euro beziffern.



17 Prozent der Unternehmen sehen Zeitprobleme bei NIS2

15 Prozent der Befragten sagen, sie sind bereits mit der NIS2-Umsetzung fertig. 66 Prozent haben die Umsetzung begonnen und wollen diese innerhalb der Frist bis 17. Oktober 2024 abgeschlossen haben. Gleichzeitig sind die NIS2-Vorgaben aber nicht vollständig bekannt.

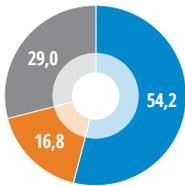


Die genauen Sanktionen bei NIS2 kennt nur jeder Fünfte

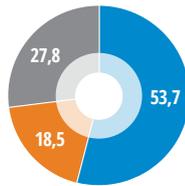
22 Prozent der Befragten halten die mögliche Sanktionshöhe für wichtige Einrichtungen bei Verstoß gegen NIS2 für niedriger, als sie ist. 33 Prozent denken, dass die NIS2-Sanktionen höher sind als die tatsächlichen bis zu sieben Millionen Euro Bußgeld oder 1,4 Prozent des Jahresumsatzes.

Nachfolgend sehen Sie fünf Aussagen rund um das Thema NIS2-Richtlinie. Welche dieser Aussagen sind wahr und welche sind nicht wahr?

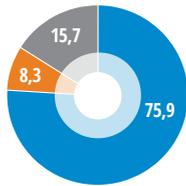
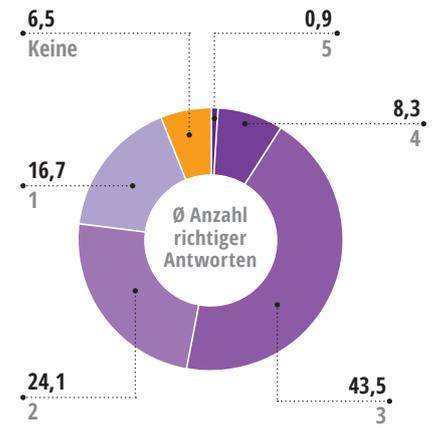
Angaben in Prozent. Basis: n = 108



„Werden seitens der Unternehmen keine angemessenen Cybersicherheitsmaßnahmen implementiert, werden gemäß NIS2-Richtlinie Unternehmen als Ganzes für Verstöße verantwortlich gemacht. Eine persönliche Haftung für Mitglieder der Geschäftsleitung ist nicht vorgesehen.“

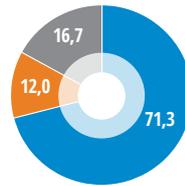


„Von der NIS2-Umsetzung sind in Deutschland etwa 30.000 Unternehmen betroffen, in denen schätzungsweise fast die Hälfte aller abhängig Beschäftigten arbeiten.“

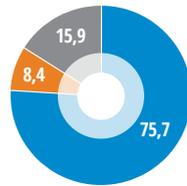


„Die NIS2-Richtlinie verlangt von Unternehmen Maßnahmen zur E-Mail-Sicherheit, einschließlich Verschlüsselung, Multi-Faktor-Authentifizierung, Phishing-Schutz sowie zur Sicherstellung der Geschäftskontinuität durch Backup- und Wiederherstellungspläne.“

● Wahr
● Nicht wahr
● Weiß nicht



„Die NIS2-Richtlinie gilt für alle Unternehmen, die Dienstleistungen in der EU erbringen oder dort tätig sind, wenn sie mehr als 50 Personen beschäftigen oder einen Jahresumsatz von mehr als 10 Mio. EUR haben.“



„Beispiele der von der NIS2-Richtlinie verlangten Mindeststandards an die Cybersicherheit sind unter anderem: Cyber-Risikomanagement, Incident Management, Business Continuity Management, Sicherheit in der Lieferkette, Schwachstellenmanagement, Training.“

Das Wissen zu NIS2 ist noch sehr lückenhaft

88 Prozent der Befragten scheinen nicht zu wissen, dass die NIS2-Richtlinie für bestimmte Sektoren und Branchen gilt. Nur 17 Prozent der Umfrageteilnehmer wissen von einer möglichen persönlichen Haftung der Geschäftsleitung bei Verletzung von NIS2. Und: Fast jeder Vierte (24 Prozent) kennt die geforderten Maßnahmen für das Risikomanagement nach NIS2 nicht genau.

Insgesamt sind nicht einmal zehn Prozent der Befragten in der Lage, mindestens vier der fünf Statements zu NIS2 korrekt als „wahr“ oder „unwahr“ einzustufen. Dabei liegen interessanterweise die größeren Unternehmen ab 1.000 Beschäftigten öfter falsch als die kleineren Unternehmen. Immerhin: Bei der Nennung der von NIS2 geforderten Mindeststandards sind es 77 Prozent der größeren und 74 Prozent der kleineren Unternehmen, die richtig liegen.

Besonders kritisch erscheint jedoch, dass die persönliche Haftung der Geschäftsleitung bei der Verletzung der NIS2-Vorgaben offensichtlich

lich mehrheitlich unbekannt ist. Diese persönliche Haftung soll im Sinne von NIS2 eigentlich dazu beitragen, dass die Cybersicherheit in den Unternehmen und Einrichtungen den „notwendigen Rückenwind“ durch das Management erfährt. Diese Rechnung geht allem Anschein nach nicht auf.

Ist das persönliche Haftungsrisiko der Leitung aber weitgehend unbekannt, droht dieser verstärkte „Rückenwind“ ausbleiben. Offensichtlich bedarf es noch deutlich mehr der Aufklärung und Sensibilisierung zur NIS2-Richtlinie, auch und gerade in der Management-Ebene.

Die meisten Unternehmen meinen, die NIS2-Umsetzung fristgerecht zu schaffen

81 Prozent der befragten Unternehmen sagen, sie seien mit der Umsetzung der Vorgaben von NIS2 bereits fertig oder würden dies fristgerecht bis zum 17.10.2024 erledigt haben. Elf Prozent der Befragten haben mit der Umsetzung begonnen, denken aber, sie erreichen die NIS2-Compliance nicht mehr bis zum Fristablauf. Sechs Prozent der Teilnehmer haben mit der NIS2-Umsetzung noch gar nicht begonnen.

Die kleineren Unternehmen mit weniger als 1.000 Beschäftigten sehen die zeitliche Umsetzung der neuen NIS2-Richtlinie eher in Gefahr als die größeren. Hier sagen immerhin 22 Prozent der Befragten, dass sie die Umsetzung von NIS2 nicht mehr schaffen können, wobei zwölf Prozent dieser Unternehmen damit begonnen haben, zehn Prozent noch nicht.

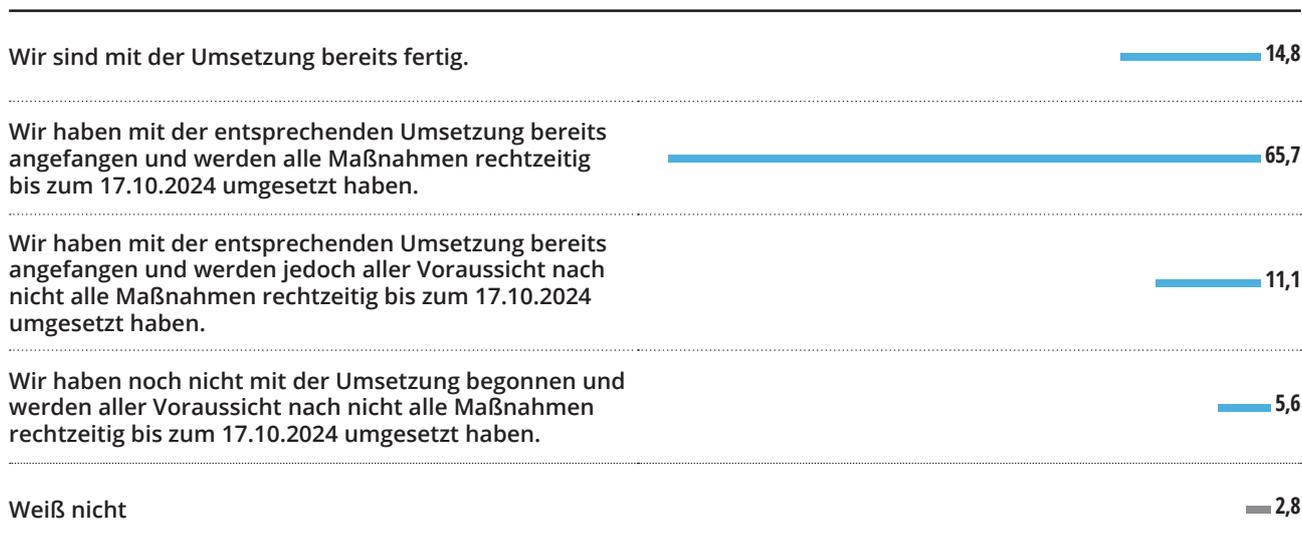
Interessant ist auch, dass der C-Level und IT-C-Level noch häufiger der Meinung sind, dass die NIS2-Umsetzung bereits erfolgt oder zeitlich kein Problem sei. Hier sagen dies 86 Prozent der Befragten. Die eher in die praktische Umsetzung involvierten Befragten aus IT-Leitung / IT-Fachbereichsleitung / IT-Bereich hingegen sind nur zu 76 Prozent dieser Ansicht.

Wichtig erscheint es jedoch, die Bewertung des Umsetzungsgrads von NIS2 in Beziehung zu setzen mit dem ebenfalls abgefragten Wissen um die NIS2-Vorgaben. Berücksichtigt man die zuvor betrachtete lückenhafte Kenntnis der NIS2-Anforderungen, relativiert dies die Aussagen zu dem scheinbar großen Fortschritt bei der Umsetzung von NIS2.

Wenn Unternehmen nicht genau wissen, was in NIS2 gefordert wird und für wen es gilt, dann könnte auch die Einschätzung, bereits alles umgesetzt zu haben oder dies zumindest fristgerecht zu schaffen, getrübt sein.

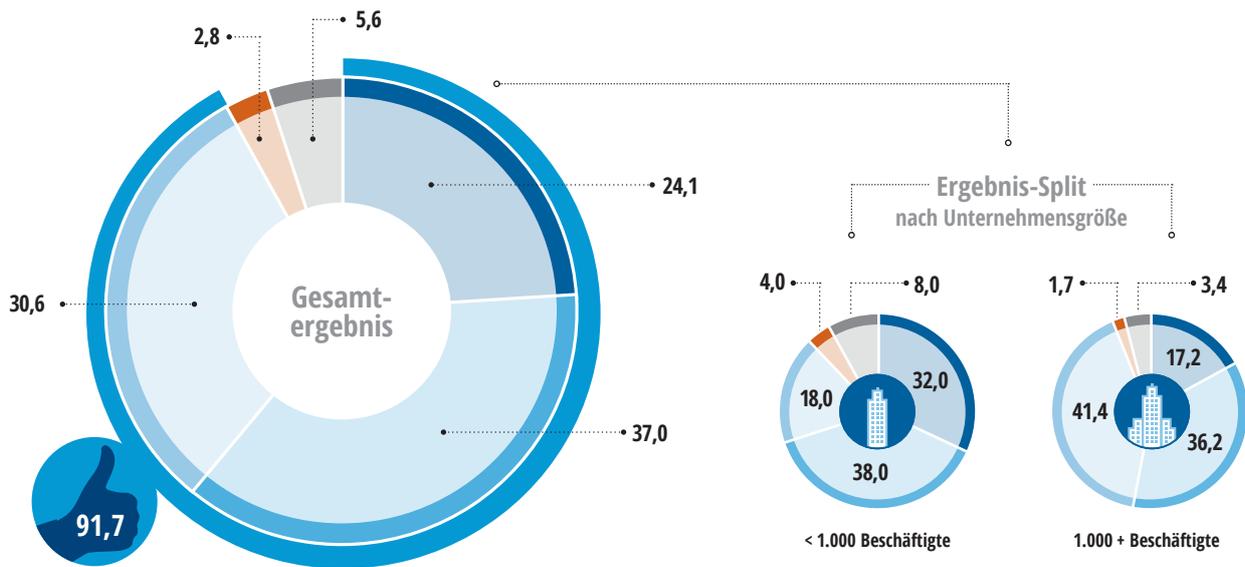
Wie weit ist Ihr Unternehmen bei der Umsetzung der NIS2-Richtlinie in Bezug auf die Deadline vom 17. Oktober 2024?

Angaben in Prozent. Basis: n = 108



Muss(te) Ihr Unternehmen Investitionen in die IT-Sicherheit tätigen, um die NIS2-Mindeststandards zu erfüllen?

Angaben in Prozent. Basis: n = 108



Beim Gros der Unternehmen reicht die vorhandene Security für NIS2 nicht aus

92 Prozent der Unternehmen müssen in IT-Security investieren oder haben dies bereits getan, um die NIS2-Vorgaben erfüllen zu können. Fast jeder dritte Befragte berichtet sogar von einem Investitionsbedarf von mehr als 100.000 Euro. Lediglich rund drei Prozent der Unternehmen sagen, sie hätten für NIS2 keinen Investitionsbedarf.

Offensichtlich reichten oder reichen den meisten Unternehmen die bereits vorhandenen Security-Infrastrukturen und -Maßnahmen nicht aus, wenn es um die Compliance mit den NIS2-Vorgaben geht. Entsprechende Investitionen sind über alle Unternehmensgrößenklassen hinweg notwendig. Sieben von zehn Unternehmen mit weniger als 1.000 Beschäftigten müssen bis zu 100.000 Euro investieren. Bei den Großunternehmen sind es knapp über 40 Prozent, in denen sogar Investitionen von über 100.000 Euro notwendig werden.

Interessant ist auch, dass es häufiger die kleineren Unternehmen sind, die meinen, keine Investitionen für NIS2 mehr tätigen zu müssen. Allerdings sind sich in diesen Unternehmen auch überdurchschnittlich viele Befragte unsicher, ob sie Security-Budget für die NIS2-Umsetzung benötigen oder gebraucht haben.

Generell lässt sich sagen: Auch wenn sich viele Unternehmen nicht im Klaren über die genauen Forderungen von NIS2 sind, wird von den meisten Befragten ein Bedarf für Security-Investitionen gesehen, oder diese wurden schon getätigt mit Blick auf NIS2.

- Ja, Investitionen bis EUR 50.000 notwendig
- Ja, Investitionen bis EUR 100.000 notwendig
- Ja, Investitionen über EUR 100.000 notwendig
- Nein, keine Investitionen notwendig
- Weiß nicht

Die Höhe der Sanktionen bei NIS2-Verletzung ist oft noch eine Unbekannte

Bei einer NIS2-Verletzung drohen den sogenannten wichtigen Einrichtungen Sanktionen von bis zu sieben Millionen Euro oder 1,4 Prozent des Jahresumsatzes. Nur jedes fünfte Unternehmen (21 Prozent) kennt die genaue Höhe. Im C-Level oder IT-C-Level sind es sogar nur 16 Prozent der Befragten. Etwas besser sieht es im IT-Bereich und in der IT-Leitung aus, wo immerhin 26 Prozent der Befragten die Höhe der möglichen NIS2-Sanktionen kennen.

Gerade die Leitungsebene des C-Levels und IT-C-Levels sollte sich mit den möglichen Sanktionen bei Verstößen gegen die neue Cybersicherheitsrichtlinie NIS2 befassen, denn sie trägt die Verantwortung und kann auch persönlichen Haftungsrisiken ausgesetzt sein.

Trotzdem kennen viele Befragte aus der Leitungsebene von Unternehmen und Einrichtungen die wirkliche Höhe der möglichen NIS2-Sanktionen nicht. Jeder Fünfte gibt unumwunden zu, es nicht zu wissen, knapp 22 Prozent dieser Befragten denken, die drohenden Bußgelder seien geringer, und 33 Prozent halten sogar noch höhere Sanktionen für möglich.



Daraus sollte man aber nicht schließen, dass die Leitungsebene deshalb der NIS2-Umsetzung mehr Gewicht geben würde. Vielmehr zeigte die Umfrage an anderer Stelle, dass gerade C-Level und IT-C-Level die Umsetzung von NIS2 bereits mehrheitlich als erledigt oder zeitlich machbar einstufen.

Deshalb sollte die sich offenbarende Unkenntnis über die Sanktionshöhen eher als Zeichen dafür gewertet werden, dass der Inhalt der NIS2-Richtlinie noch nicht genau genug bekannt ist und die Aufklärungsarbeit dazu nun dringend an Fahrt aufnehmen sollte.

Da sich die IT-Leitung und der IT-Bereich auch mit Details wie der Sanktionshöhe besser auszukennen scheinen, als es bei der Unternehmensleitung der Fall ist, empfiehlt sich eine Verbesserung der internen Kommunikation zu NIS2. Dies würde auch bei der Einschätzung der tatsächlich erreichten Umsetzung von NIS2 helfen.

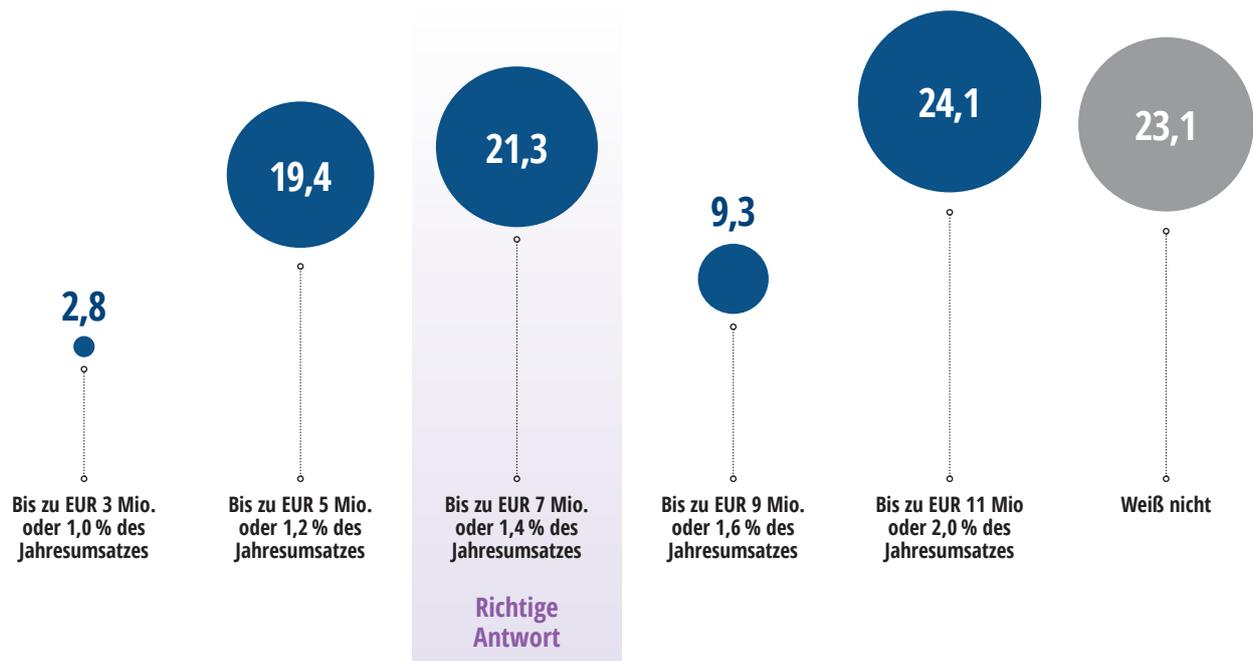
↘ Bitte beachten Sie die Ergebnisdarstellung auf der nächsten Seite.

In der NIS2-Richtlinie wird bei Unternehmen zwischen „Besonders wichtige Einrichtungen“ und „Wichtige Einrichtungen“ unterschieden. Besonders wichtige Einrichtungen unterliegen einer proaktiven Aufsicht, wichtige Einrichtungen einer reaktiven Aufsicht durch die Behörden.

Verstöße gegen die NIS2-Richtlinie können Bußgelder nach sich ziehen. Bis zu welcher Höhe können Bußgelder gegen sog. wichtige Einrichtungen verhängt werden?

Verstöße gegen die NIS2-Richtlinie können Bußgelder nach sich ziehen. Bis zu welcher Höhe können Bußgelder gegen sogenannte wichtige Einrichtungen verhängt werden?

Angaben in Prozent. Basis: n = 108



Summary:

Erhebliche Wissenslücken rund um NIS2 können mitunter gefährliche Folgen für Unternehmen und Unternehmer haben. Ob das nun die Zuversichtlichkeit in der Einhaltung der Deadline von NIS2 oder aber zu defensive NIS2-Budgetplanungen sind, schlussendlich müssen sich gerade persönlich haftende Gesellschafter über die Folgen und Sanktionen bei Nichteinhaltung von NIS2 viel klarer sein!

Gerade die unterschiedlichen Kenntnisstände zwischen C-Level und den IT-Verantwortlichen legen den intensiven Austausch der beiden Funktionen nahe, sodass wirklich alle NIS2-Vorgaben technisch abgehakt werden, entsprechende Investitionen zeitnah getätigt werden und somit die Deadline wirklich guten Gewissens eingehalten werden kann.

Studiensteckbrief

HerausgeberCIO, CSO und COMPUTERWOCHE
Exklusiver StudienpartnerMimecast
GrundgesamtheitenC-Level-und IT-C-Level-Führungskräfte sowie IT-Führungskräfte (IT-Leitung / IT-Fachbereichsleitung)
TeilnehmergenerierungPersönliche E-Mail-Einladung über die exklusive Unternehmensdatenbank von CIO, CSO und COMPUTERWOCHE und – zur Erfüllung der Quotenvorgaben – über externe Online-Access-Panels
Gesamtstichprobe108 abgeschlossene und qualifizierte Interviews
Untersuchungszeitraum9. bis 12. Juli 2024
MethodeOnline-Umfrage (CAWI)
Untersuchungszeitraum und DurchführungCustom Research Team von CSO, CIO und COMPUTERWOCHE in Zusammenarbeit mit Mimecast

Stichprobenstatistik

Branchenverteilung*	Energie	2,8 %
	Wasserversorgung & Abwasserentsorgung	3,7 %
	Herstellung und Vertrieb von Chemikalien	6,5 %
	Herstellung von Maschinen, Fahrzeugen sowie elektrischen / elektronischen Geräten.....	25,0 %
	Informations- und Kommunikationstechnologie (IKT) – Dienstleistungsmanagement.....	37,0 %
	Digitale Infrastruktur	14,8 %
	Digitale Anbieter (z.B. Onlinemarktplätze, Soziale Netzwerke).....	3,7 %
	Lebensmittelproduktion, -verarbeitung und -vertrieb	0,9 %
	Banken und Versicherungen & Finanzmarkt-Infrastruktur	13,0 %
	Transport, Logistik und Verkehr (inkl. Post- und Kurierdienste).....	12,0 %
	Raumfahrt / Weltraum-Bodeninfrastruktur.....	1,9 %
	Dienstleistungen für Unternehmen.....	0,9 %
	Öffentliche Verwaltungen.....	6,5 %
	Forschungssektor, Forschungsinstitute	0,9 %
	Herstellung von Medizinprodukten	1,9 %
	Gesundheit & Gesundheitswesen (z.B. Krankenhäuser, Gesundheitsdienstleister, Pharmazeutik, Medizinforschung)	2,8 %
Unternehmensgröße deutschlandweit	Weniger als 1.000 Beschäftigte.....	46,4 %
	1.000 Beschäftigte und mehr.....	53,7 %
Funktion im Unternehmen	C-Level / IT-C-Level	47,2 %
	IT-Leitung / IT-Fachbereichsleitung / IT-Bereich.....	52,8 %
Jährliche Aufwendungen in IT-Systeme	Weniger als 10 Millionen Euro	40,7 %
	10 Millionen Euro und mehr	57,4 %
	Weiß ich nicht / keine Angabe	1,9 %

* Mehrfachnennungen möglich

ÜBER MIMECAST

Mimecast ist eine KI-gestützte, API-fähige und vernetzte Human-Risk-Management-Plattform. Sie wurde entwickelt, um Unternehmen vor dem gesamten Spektrum von Cyberbedrohungen zu schützen. Dafür integriert sie moderne benutzerfreundliche Technologien mit Strategien für das Erkennen von Risiken und den Aufbau von Sicherheitskompetenz, die immer den Nutzer im Fokus behalten. Darauf ausgelegt, unsichtbare Risiken sichtbar zu machen und Dateneinblicke so aufzubereiten, dass sie als Entscheidungsgrundlage dienen können, eröffnet sie Unternehmen proaktive Handlungsmöglichkei-

ten. Sie hilft, Kommunikations- und Kollaborationslandschaften zu schützen, kritische Daten zu sichern, Mitarbeitende aktiv in das Risikomanagement einzubeziehen und eine Sicherheitskultur zu fördern, die mit Unternehmenszielen wie Geschäftskontinuität und Steigerung der Produktivität in Einklang steht. Über 42.000 Unternehmen weltweit vertrauen Mimecast, um der sich dynamisch entwickelnden Bedrohungslage einen Schritt voraus zu sein. Von internen Risiken bis hin zu externen Gefahren – Mimecast bietet Kunden mehr. Mehr Sichtbarkeit. Mehr Einblicke. Mehr Agilität. Mehr Sicherheit.

mimecast[®]

Ansprechpartner:

Bernd Hohlweg – Director Marketing DACH
bhohlweg@mimecast.com

Mimecast Germany GmbH
Kistlerhofstraße 172
81379 München
Telefon: +49 89 904 200 800
Website: www.mimecast.com/de