NIS2: SIND SIE BEREIT?

Ihr umfassender Leitfaden zu den Grundprinzipien und Verpflichtungen der neuen europäischen Cybersicherheitsrichtlinie NIS2 - einschließlich praktischer Schritte zur Erstellung eines effektiven Aktionsplans, um sicherzustellen, dass Sie gut vorbereitet sind.

Insight unterstützt Sie bei den ersten Schritten.

Insight

NIS2: ein kurzer Überblick

Die Europäische Union (EU) hat die NIS2-Gesetzgebung zur Verbesserung der Cybersicherheit und Cyberresilienz erarbeitet. Die Mitgliedstaaten haben bis zum 17. Oktober 2024 Zeit, diese Richtlinie in nationales Recht umzusetzen, das von den Unternehmen eingehalten werden muss.

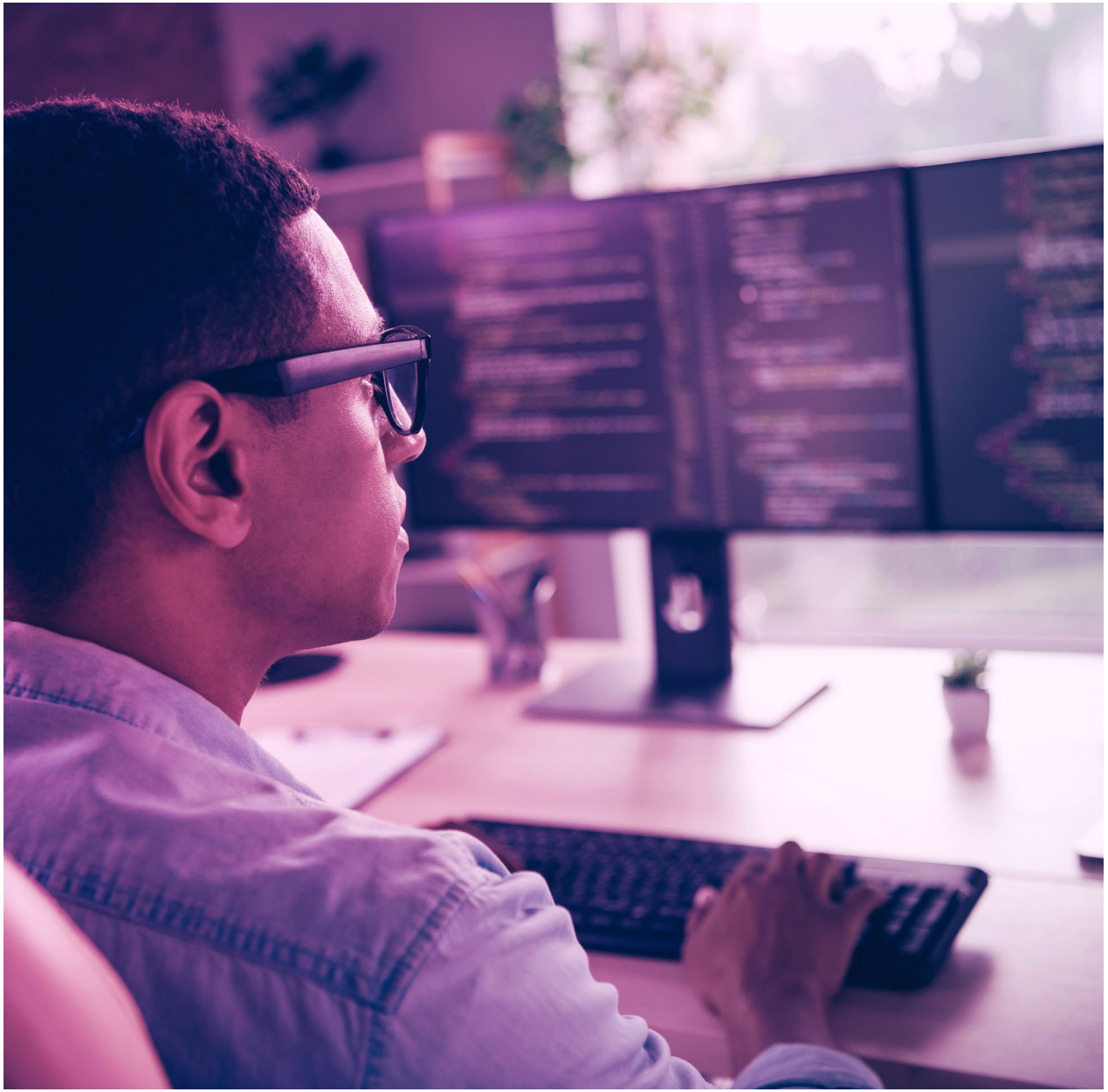
NIS2 gilt für „wesentliche" und „bedeutende" Unternehmen in bestimmten Branchen ab einer bestimmten Größe. Auch Unternehmen in der Lieferkette der betroffenen Unternehmen und Betreiber kritischer Anlagen müssen sich daran halten. Das Gesetz beinhaltet Pflichten wie Sorgfaltspflicht, Meldepflicht und Überwachung. Die Sorgfaltspflicht verlangt von den Unternehmen, eigene Risikoanalysen durchzuführen und Maßnahmen zu ergreifen, um die digitale Sicherheit und Kontinuität zu gewährleisten. Im Rahmen der Meldepflicht müssen Störungen innerhalb von 24 Stunden gemeldet werden. Die Aufsicht umfasst proaktive und reaktive Kontrollen bei kritischen Einrichtungen. Bei Nichteinhaltung können Bußgelder verhängt werden, und die Geschäftsführer haften persönlich und gesamtschuldnerisch für die Einhaltung der NIS2-Richtlinie.

Für alle Unternehmen, auch solche, die nicht direkt von NIS2 betroffen sind, ist es von entscheidender Bedeutung, ihre Widerstandsfähigkeit gegenüber Cyber-Bedrohungen kritisch zu bewerten. Jedes Unternehmen ist Risiken wie Reputationsschäden, Datendiebstahl und finanziellen Verlusten ausgesetzt. Die Umsetzung der NIS2-Richtlinie ist ein ausgezeichneter Ausgangspunkt für den Ausbau und die kontinuierliche Verbesserung der Cyber-Sicherheitsmaßnahmen.

NIS2 verstehen

NIS2 ist die neue europäische Richtlinie für Netzwerk- und Informationssicherheit, welche die NIS-Richtlinie von 2018 ersetzt und im Oktober 2024 in Kraft treten wird.
NIS2 verfolgt zwei Ziele: die Harmonisierung der Cyber-Resilienz-Praktiken in ganz Europa und die Verbesserung der Cyber-Sicherheit für Unternehmen und Organisationen.
Im Gegensatz zur ursprünglichen NIS-Richtlinie, die sich nur auf wesentliche Sektoren wie z.B. Wasser, Energie und Telekommunikation konzentrierte, gilt NIS2 für ein breiteres Branchen-Spektrum.

> "Um die NIS2-Richtlinie zu erfüllen, müssen Sie ermitteln, welche Systeme und Dienste in Ihrer Organisation als kritische Infrastrukturen gelten, und die damit verbundenen Risiken bewerten. Sobald Sie diese Informationen haben, können Sie die erforderlichen Maßnahmen festlegen und bestimmen, wie diese in Ihre Organisation integriert werden können."
>
> Dirk de Goede, Security Spezialist bei Insight



Wer ist von NIS2 betroffen?

Die NIS2-Leitlinie klassifiziert Organisationen nach ihrer Branche und ihrer Bedeutung für Gesellschaft und Wirtschaft. Es wird zwischen zwei Arten von Einrichtungen unterschieden: „wesentliche“ und „wichtige“ Einrichtungen, mit zusätzlichen Bestimmungen für Sonderfälle, wie z. B. Unternehmen innerhalb der Lieferkette.

Wesentliche Einrichtungen:	Wichtige Einrichtungen:
Energie	Postkurierdienste
Finanzmarktinfrastruktur	Ernährung
Digitale Infrastruktur	Abfallwirtschaft
Öffentliche Verwaltung	Digitale Anbieter
Gesundheit	Fertigungsindustrie
Banken	Chemie
Transport & Verkehr	Forschungseinrichtungen
IT Service Management	
Trinkwasserversorgung	
Raumfahrt	
Abwasserentsorgung	

Die folgenden Kriterien werden verwendet, um zu entscheiden, ob NIS2 für Ihr Unternehmen gilt:

Wesentliche Einrichtungen:

Große Unternehmen mit **über 250 Mitarbeitern, einem Nettoumsatz von mehr als 50 Mio. Euro und einer Bilanzsumme von über 43 Mio. Euro**. Diese sind für Wirtschaft und Gesellschaft von entscheidender Bedeutung und werden von der Regierung aktiv überwacht.

Wichtige Einrichtungen:

Mittelgroße Organisationen aus der Gruppe der wesentlichen Unternehmen und mittlere bis große Organisationen in anderen Schlüsselsektoren. Diese Unternehmen beschäftigen **mindestens 50 Mitarbeiter oder haben einen Jahresumsatz und eine Bilanzsumme von mehr als 10 Millionen Euro**. Sie unterliegen einer weniger strengen Aufsicht, werden aber auditiert, nach einem Vorfall gibt oder wenn es Anzeichen von Nichteinhaltung gibt.

Darüber hinaus gilt die NIS2 für:

- **Bestimmte kleinere Unternehmen**
- **Unternehmen innerhalb der Lieferkette von wesentlichen und bedeutenden Einrichtungen**
- **Einige weitere Ausnahmen**

Welche Verpflichtungen sind in der NIS2 festgelegt?

Die NIS2 umfasst drei Hauptverpflichtungen:

Verantwortungsbereich

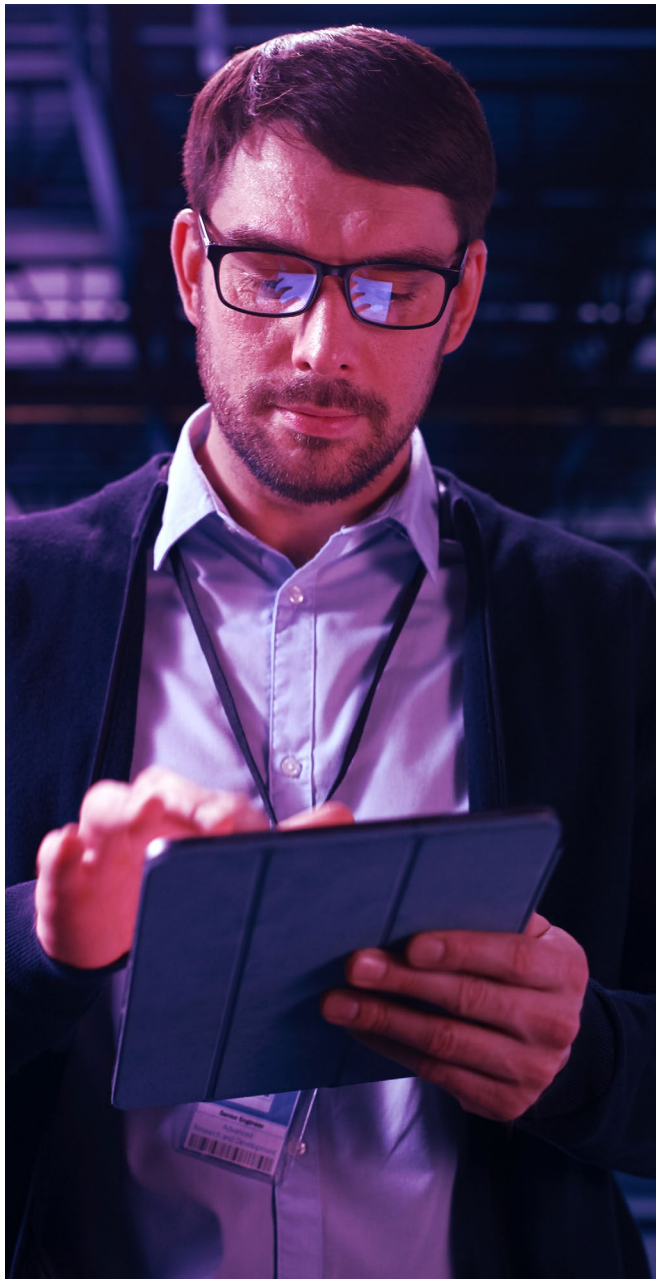
Organisationen müssen ihre eigenen Risikobewertungen durchführen und Maßnahmen zur Sicherung ihrer Dienste und zum Schutz von Informationen umsetzen.

Meldung von Vorfällen

Organisationen müssen Vorfälle, die wesentliche Dienste erheblich beeinträchtigen könnten, innerhalb von 24 Stunden der Aufsichtsbehörde melden. Cybervorfälle müssen auch dem Computer Security Incident Response Team (CSIRT) gemeldet werden. Ob ein Vorfall gemeldet werden muss, hängt von Faktoren wie der Dauer der Störung, der Anzahl der betroffenen Personen und den möglichen finanziellen Verlusten ab.

Überwachen

Unternehmen müssen strenge Aufsichtspflichten erfüllen, einschließlich regelmäßiger Bewertungen ihrer Cybersicherheitsmaßnahmen und Risikomanagementpraktiken. Darüber hinaus sind sie verpflichtet, mit den zuständigen Behörden zusammenzuarbeiten und diese zeitnah über wesentliche Vorfälle oder Veränderungen zu informieren, die ihre Sicherheit beeinträchtigen.



Was passiert, wenn Sie die Vorschriften nicht einhalten?

Sobald die NIS2 in nationales Recht umgesetzt ist, müssen alle Unternehmen innerhalb der angegebenen Kategorien und Sonderfälle die Vorschriften einhalten. Je nach Einstufung der Organisation können Konformitätsprüfungen proaktiv oder reaktiv durchgeführt werden.

Bußgelder:

Wenn eine Organisation die NIS2 nicht einhält, kann die Aufsichtsbehörde nach einer Inspektion ein Bußgeld verhängen. Jeder Mitgliedstaat legt die Höhe der Bußgelder selbst fest, die Höchstbeträge betragen jedoch:

- **Für wesentliche Einrichtungen:** Bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes
- **Für wichtige Einrichtungen:** Bis zu 7 Mio. Euro oder 1,4 % des weltweiten Jahresumsatzes

Gesamtschuldnerische Haftung:

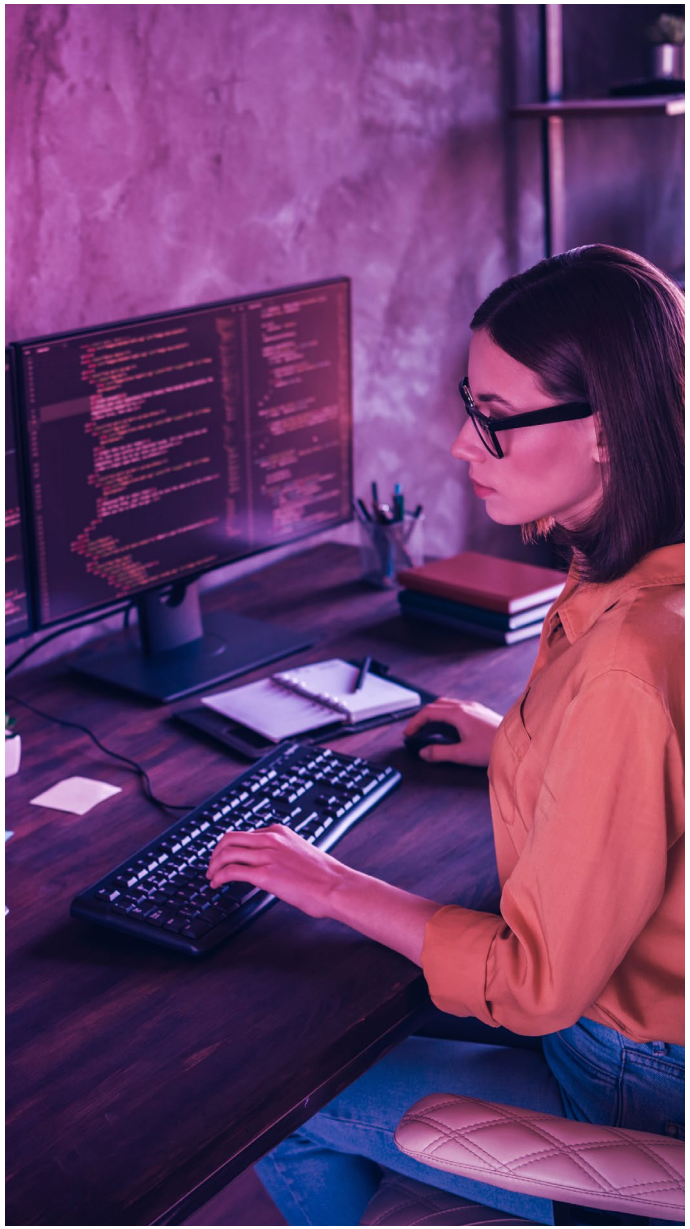
Jeder Geschäftsführer ist persönlich für die Einhaltung der NIS2 durch seine Organisation verantwortlich. Sie können diese Verantwortung nicht delegieren oder andere für Versäumnisse verantwortlich machen.

NIS2-Mindestanforderungen für das Cybersicherheitsrisikomanagement

Artikel 21 der NIS-Richtlinie2 enthält eine Liste von Maßnahmen zum Cyber-Sicherheits-Risikomanagement, die kritische Unternehmen zum Schutz ihrer Netz- und Informationssysteme umsetzen müssen.

Mindestanforderungen NIS2:

1. **Risikoanalyse:** Welche Systeme und Dienste sind für Ihr Unternehmen am wichtigsten und stellen somit das größte Risiko dar? Wie ist die Sicherheit Ihrer Softwareumgebung organisiert?
2. **Geschäftskontinuität:** Welche Verfahren gibt es für das Störfallmanagement, einschließlich eines robusten Backup-Systems? Welche Krisenmanagement- und Wiederherstellungsmaßnahmen werden durchgeführt?
3. **Sicherheit von Netzwerk- und Informationssystemen:** Wie sind Ihre Systeme konfiguriert und wie gehen Sie mit Schwachstellen um?
4. **Effektivität:** Wie wird die Wirksamkeit Ihrer Sicherheitsmaßnahmen geprüft? Gibt es hierfür etablierte Verfahren?
5. **Reaktionsplan für Sicherheitsvorfälle:** Wie werden Vorfälle behandelt und registriert?
6. **Sicherheit in der Lieferkette:** Welche potenziellen Risiken gibt es für Ihr Unternehmen durch externe Lieferanten und Dienstleistern?
7. **Cybersicherheit & menschliche Faktoren:** Wie gut sind Ihre Mitarbeiterinnen und Mitarbeiter über die IT- und Sicherheitsrichtlinien informiert? Wären weitere Schulungen und Awareness-Trainings sinnvoll?
8. **Kryptografie und Verschlüsselung:** Welche Richtlinien und Verfahren gibt es für den Einsatz von Kryptographie und Verschlüsselung?
9. **Identität und Zugriff:** Welche Sicherheitsaspekte gibt es in Bezug auf Personal, Zugriffsrichtlinien und Asset Management?
10. **Multi-Faktor-Authentifizierung:** Ist eine Multi-Faktor-Authentifizierung für Konten:
    - auf die über das Internet zugegriffen werden kann
    - mit administrativen Rechten und für kritische Systeme implementiert?



Ihre NIS2-Checkliste

Es ist wichtig, sich nicht nur auf die Mindestanforderungen zu konzentrieren. Wir wissen, dass für eine gründliche NIS2-Bewertung detailliertere Informationen erforderlich sind. Die folgende 25-Punkte-Checkliste wird empfohlen, um die vollständige Einhaltung der NIS2-Maßnahmen und die Bereitschaft dazu sicherzustellen.

Nr.	Checkliste:	✓
1.	Zutrittskontrollen	
2.	Situationsbezogene Awareness	
3.	Konfigurationsmanagement	
4.	Security Assessment und interne Audits	
5.	Kryptografie	
6.	Mitarbeitersicherheit/ Interne Bedrohungen	
7.	Identität, Autorisierung & Authentifizierung	
8.	Asset Management	
9.	Remote-Arbeit	
10.	Risikomanagement	
11.	Informationssicherheitsaspekte von BCP/BCDR	
12.	Gesetzliche und vertragliche Anforderungen	
13.	Compliance und Datenschutz	
14.	Vorfall-Management:	
15.	Wiederherstellungsplanung	
16.	Entwicklung und Tests von Software/Applikationen	
17.	Physische Sicherheit	
18.	Datenklassifizierung	
19.	Schulung & Sensibilisierung	
20.	Sicherheitsrichtlinien, -verfahren und -abläufe	
21.	Risikomanagement der Lieferkette/Sicherheit von Drittlieferanten	
22.	Schwachstellenbewertung	
23.	Patch Management:	
24.	Netzwerk & Kommunikation	
25.	Schutz vor Datenverlust	

Wie Insight helfen kann

Wir wissen, dass die Vorbereitung auf NIS2 für viele Unternehmen eine große Herausforderung darstellt und sind gerne bereit, sie dabei zu unterstützen. Wenn Sie Fragen zu NIS2 haben oder weitere Informationen zu den Maßnahmen in unserer Checkliste benötigen, wenden Sie sich bitte an uns.

Insight bietet einen integrierten Ansatz zur Erreichung der NIS2-Konformität. Wir bauen auf Ihren bestehenden Prozessen auf und stellen die Konformität mit anderen EU-Richtlinien und Verordnungen sicher, um den Übergang so reibungslos wie möglich zu gestalten.

Sehen Sie sich das Video an und erfahren Sie, wie wir Sie unterstützen können.

Sofortmaßnahmen

Benötigen Sie sofortige Hilfe in Ihrer spezifischen Situation? Insight bietet Dienstleistungen wie unseren NIS2 Awareness Workshop oder den NIS2 Assessment Service an, um Ihnen einen Vorsprung bei der Einhaltung der kommenden NIS2-Vorschriften zu verschaffen. Gemeinsam sorgen wir dafür, dass Ihre IT-Infrastruktur sicher und Ihre Unternehmensdaten geschützt sind.

Jedes Land hat sein eigenes nationales Cybersicherheitszentrum, das die Umsetzung der neuen NIS2-Richtlinie unterstützt und koordiniert. Nützliche Links zu lokalen Länderressourcen für NIS2:

Österreich

NIS Anlaufstelle - Anlaufstelle NISG

parlament.gv.at/gegenstand/XXVII/A/4129

Deutschland

NIS2 in Germany (NIS2UmsuCG) – OpenKRITIS

NIS 2 Directive, Transposition in Germany (nis-2-directive.com)

Niederlande

2.5 Improve Cybersecurity - Digital Government (nldigitalgovernment.nl)

Belgien

NIS2 | Centre for Cyber security Belgium

Italien

Authority and sanctions - ACN

Spanien

Key Data Privacy and Cybersecurity Laws | Spain | Global Data Privacy and Cybersecurity Handbook | Baker McKenzie Resource Hub

Adoption of the NIS2 Directive | INCIBE-CERT | INCIBE

Frankreich

https://cyber.gouv.fr/en

Irland

https://www.ncsc.gov.ie/

Großbritannien

(obwohl nicht direkt betroffen, plant Großbritannien, seine aktuellen NIS-Vorschriften

Government response to the call for views on proposals to improve the UK's cyber resilience - GOV.UK (www.gov.uk)

The Network and Information Systems (NIS) framework aims to enhance the cybersecurity resilience of critical infrastructure | Fieldfisher

Machen Sie den nächsten Schritt

Insight unterstützt Sie bei der Erfüllung Ihrer NIS2-Verpflichtungen. Wir bieten detaillierte Beratung und praktische Maßnahmen, die Ihr Unternehmen ergreifen muss, um sich auf NIS2 vorzubereiten.

Besuchen Sie unsere Webseite **at.insight.com** oder wenden Sie sich an Ihren Insight Account Manager, um zusätzliche Informationen und persönliche Beratung zu erhalten.

at.insight.com

MKT7148