NIS2:

SICHER UND KON-FORM

Ihr kompakter Leitfaden zu den wichtigsten Prinzipien und Anforderungen der neuen europäischen Cybersicherheitsrichtlinie – inklusive praxisnaher Schritte für einen erfolgreichen Aktionsplan. So sind Sie bestens vorbereitet.

Insight begleitet Sie auf Ihrem Weg ...

Insight | Microsoft

NIS2: Fit für die neue Richtlinie

Seit Oktober 2024 gilt in der European Union (EU) die neue NIS2-Richtlinie – mit strengeren Anforderungen an Sicherheit und Compliance. Sie betrifft Unternehmen in kritischen Sektoren sowie deren Lieferketten.

NIS2 gilt für „wesentliche“ und „wichtige“ Einrichtungen in bestimmten Sektoren ab einer bestimmten Unternehmensgröße. Auch Partner in der Lieferkette sowie bestimmte andere Organisationen müssen die Vorgaben einhalten. Das Gesetz beinhaltet Pflichten wie Sorgfaltspflicht, Meldepflicht und Aufsicht.
Die Sorgfaltspflicht verpflichtet Unternehmen, eigene Risikoanalysen durchzuführen und Maßnahmen zu ergreifen, um digitale Sicherheit und Geschäftskontinuität zu gewährleisten. Im Rahmen der Meldepflicht müssen Vorfälle innerhalb von 24 Stunden gemeldet werden, wenn es zu einer Dienstunterbrechung kommt.
Die Aufsicht umfasst proaktive und reaktive Kontrollen für zentrale Einrichtungen. Bei Nichteinhaltung können Geldstrafen verhängt werden – und Geschäftsführer sind persönlich verantwortlich sowie gesamtschuldnerisch haftbar für die Einhaltung der NIS2-Vorgaben.

Es ist entscheidend, dass alle Unternehmen – auch jene, die nicht direkt von NIS2 betroffen sind – ihre Widerstandsfähigkeit gegenüber Cyberbedrohungen kritisch prüfen. Jedes Unternehmen ist Risiken wie Reputationsschäden, Datendiebstahl und finanziellen Verlusten ausgesetzt. Die Umsetzung der NIS2-Leitlinien bietet einen hervorragenden Ausgangspunkt, um Cybersicherheitsmaßnahmen zu verbessern und kontinuierlich weiterzuentwickeln.
Da die neue NIS2-Richtlinie die Anforderungen an Sicherheit und Compliance deutlich erhöht, unterstützen Insight und Microsoft Unternehmen dabei, regulatorische Vorgaben mit einer umfassenden Cloud-Sicherheitsstrategie zu verbinden – um Resilienz aufzubauen, Sicherheit zu stärken und Compliance zu vereinfachen.

NIS2 verstehen

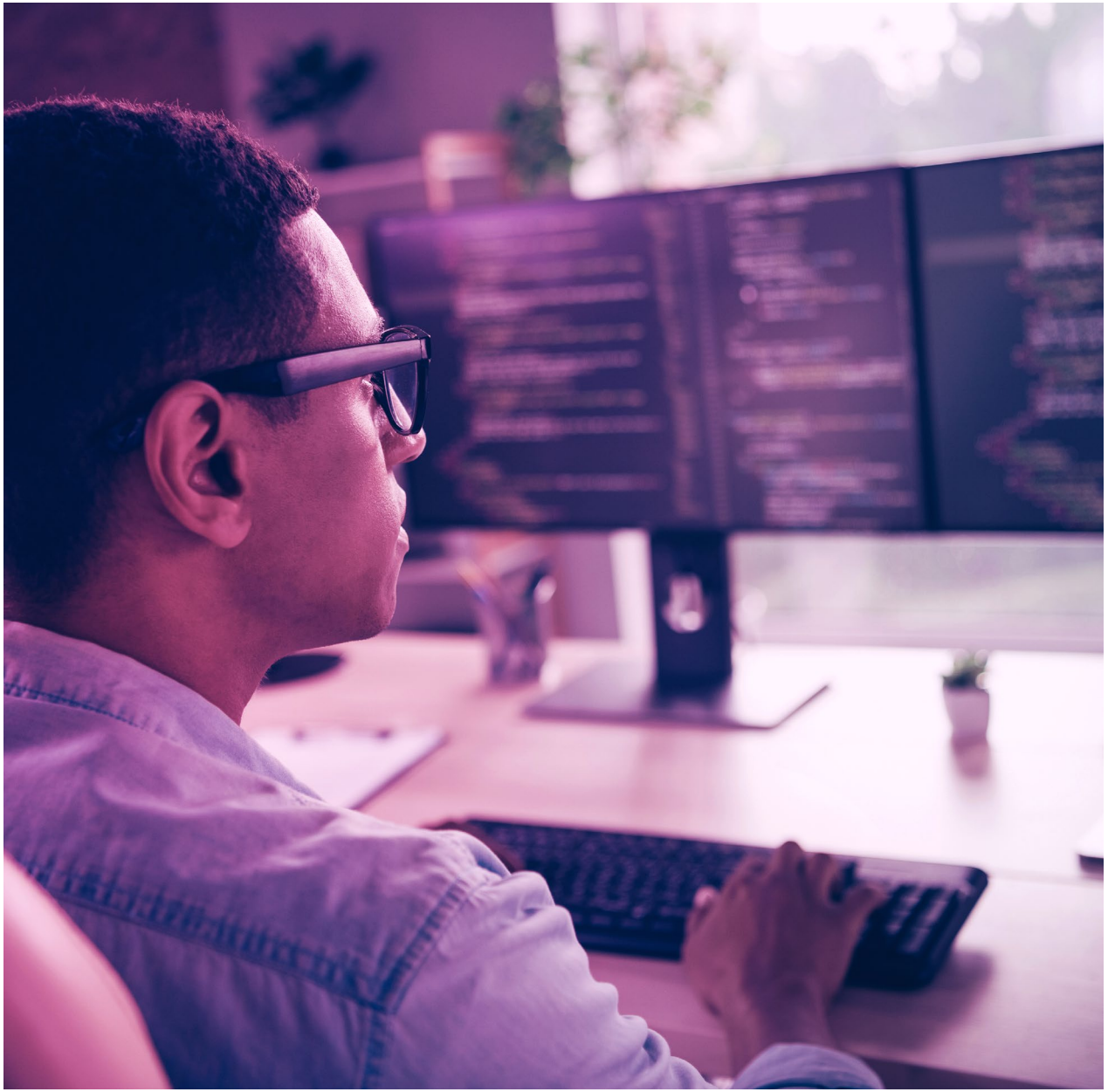
NIS2 ist die neue europäische Richtlinie für Netzwerk- und Informationssicherheit und ersetzt die NIS-Richtlinie von 2018. Sie trat im Oktober 2024 in Kraft.

Das Ziel von NIS2 ist zweifach:

- Cyber-Resilienz-Praktiken europaweit zu harmonisieren
- Cybersicherheit für Unternehmen und Organisationen zu verbessern

Im Gegensatz zur ursprünglichen NIS-Richtlinie, die sich nur auf wesentliche Sektoren wie Wasser, Energie und Telekommunikation konzentrierte, gilt NIS2 für eine deutlich breitere Palette von Unternehmen.

> "Um die NIS2-Richtlinien einzuhalten, müssen Sie ermitteln, welche Systeme und Dienste Ihres Unternehmens als kritische Infrastruktur gelten und die damit verbundenen Risiken bewerten. Sobald Sie diese Informationen haben, können Sie die erforderlichen Maßnahmen festlegen und entscheiden, wie Sie diese in Ihre Organisation integrieren."
>
> Dirk de Goede, Security Specialist bei Insight



Für wen gilt NIS2?

Die NIS2-Richtlinie stuft Organisationen anhand ihres Sektors sowie ihrer Bedeutung für Gesellschaft und Wirtschaft ein. Sie unterscheidet zwischen zwei Arten von Einrichtungen: „wesentliche“ und „wichtige“ Einrichtungen – mit zusätzlichen Regelungen für Sonderfälle, wie z.B. Partner in der Lieferkette.

Wesentliche Einrichtungen:	Wichtige Einrichtungen:
Energie	Post- und Kurierdienstleistungen
Finanzmarktinfrastruktur	Ernährung
Digitale Infrastruktur	Abfallwirtschaft
Öffentliche Dienstleistungen	Digitale Anbieter
Gesundheitswesen	Herstellende Industrie
Bankwesen	Chemie
Transport & Verkehr	Forschungseinrichtungen
IT-Service Management	
Trinkwasserversorgung	
Raumfahrt	
Abwasserentsorgrung	

Folgende Kriterien entscheiden, ob NIS2 für Ihre Organisation gilt:

Wesentliche Einrichtungen:

Große Unternehmen mit mehr als 250 Mitarbeitenden, einem Jahresumsatz von über 50 Millionen Euro und einer Bilanzsumme von über 43 Millionen Euro. Diese Organisationen sind für Wirtschaft und Gesellschaft von zentraler Bedeutung und werden von staatlichen Stellen aktiv überwacht.

Wichtige Einrichtungen:

Mittlere Unternehmen aus den Sektoren der wesentlichen Einrichtungen sowie mittelgroße bis große Unternehmen in anderen wichtigen Branchen. Diese Organisationen haben mindestens 50 Mitarbeitende oder einen Jahresumsatz und eine Bilanzsumme von jeweils über 10 Millionen Euro. Sie unterliegen einer weniger strengen Aufsicht, werden jedoch geprüft, wenn es Hinweise auf Nichteinhaltung gibt oder nach einem Vorfall.

Darüber hinaus gilt NIS2 auch für:

- **Bestimmte kleine Organisationen**
- **Partner in der Lieferkette von wesentlichen und wichtigen Einrichtungen**
- **Einige weitere Ausnahmen**

Welche Pflichten sind in NIS2 festgelegt?

NIS2 umfasst drei Hauptpflichten:

Sorgfaltspflicht

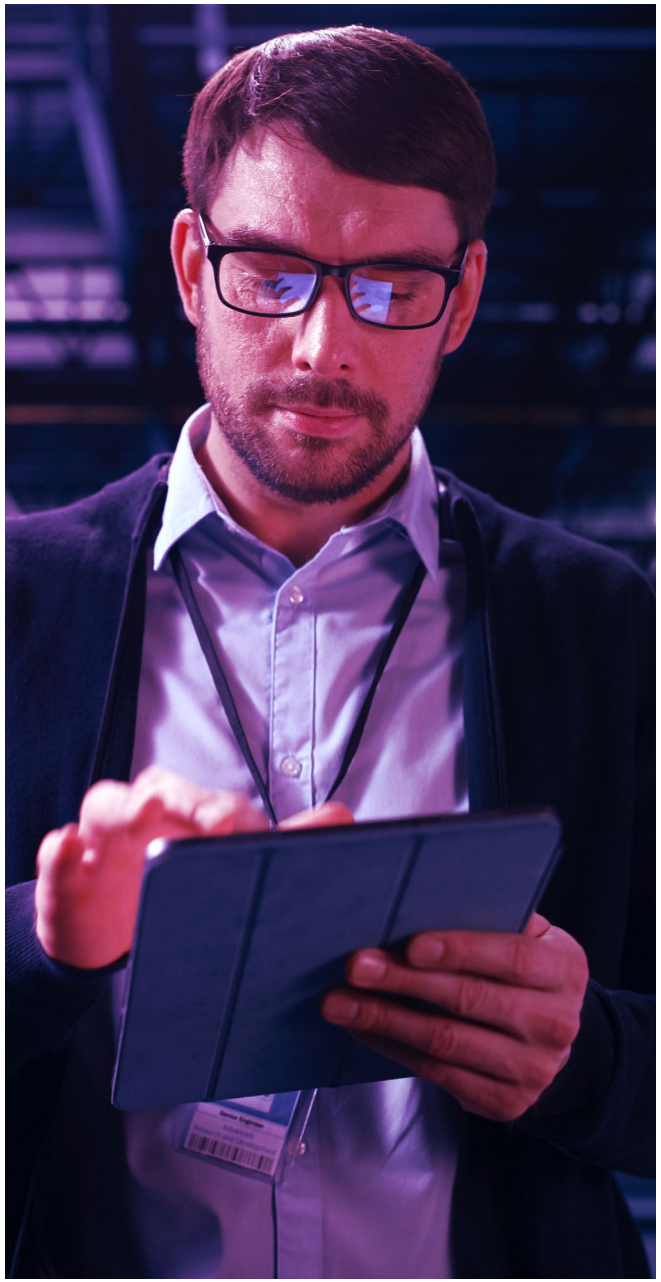
Organisationen müssen eigene Risikobewertungen durchführen und Maßnahmen umsetzen, um ihre Dienste zu sichern und Informationen zu schützen.

Meldung von Vorfällen

Organisationen müssen Vorfälle, die wesentliche Dienste erheblich beeinträchtigen könnten, innerhalb von 24 Stunden der Aufsichtsbehörde melden. Cybervorfälle müssen außerdem an das Computer Security Incident Response Team (CSIRT) gemeldet werden. Faktoren wie die Dauer der Störung, die Anzahl der betroffenen Personen und mögliche finanzielle Verluste bestimmen, ob ein Vorfall meldepflichtig ist.

Aufsicht

Organisationen müssen strenge Aufsichtspflichten einhalten, einschließlich regelmäßiger Bewertungen ihrer Cybersicherheitsmaßnahmen und ihres Risikomanagements. Sie sind außerdem verpflichtet, mit den zuständigen Behörden zusammenzuarbeiten und zeitnah Updates zu bedeutenden Vorfällen oder Änderungen zu geben, die ihre Sicherheit betreffen.



Was passiert, wenn Sie nicht compliant sind?

Sobald NIS2 in Ihrem Land in nationales Recht umgesetzt ist, müssen alle Organisationen in den festgelegten Kategorien und Sonderfällen die Vorschriften einhalten. Je nach Klassifizierung der Organisation können Compliance-Prüfungen proaktiv oder reaktiv durchgeführt werden.

Bußgelder:

Wenn eine Organisation NIS2 nicht einhält, kann die Aufsichtsbehörde nach einer Prüfung ein Bußgeld verhängen. Jeder Mitgliedstaat legt die Höhe der Geldstrafe selbst fest, jedoch gelten folgende Höchstgrenzen:

- **Für wesentliche Einrichtungen:** Bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes
- **Für wichtige Einrichtungen:** Bis zu 7 Millionen Euro oder 1.4% des weltweiten Jahresumsatzes

Gesamtschuldnerische Haftung:

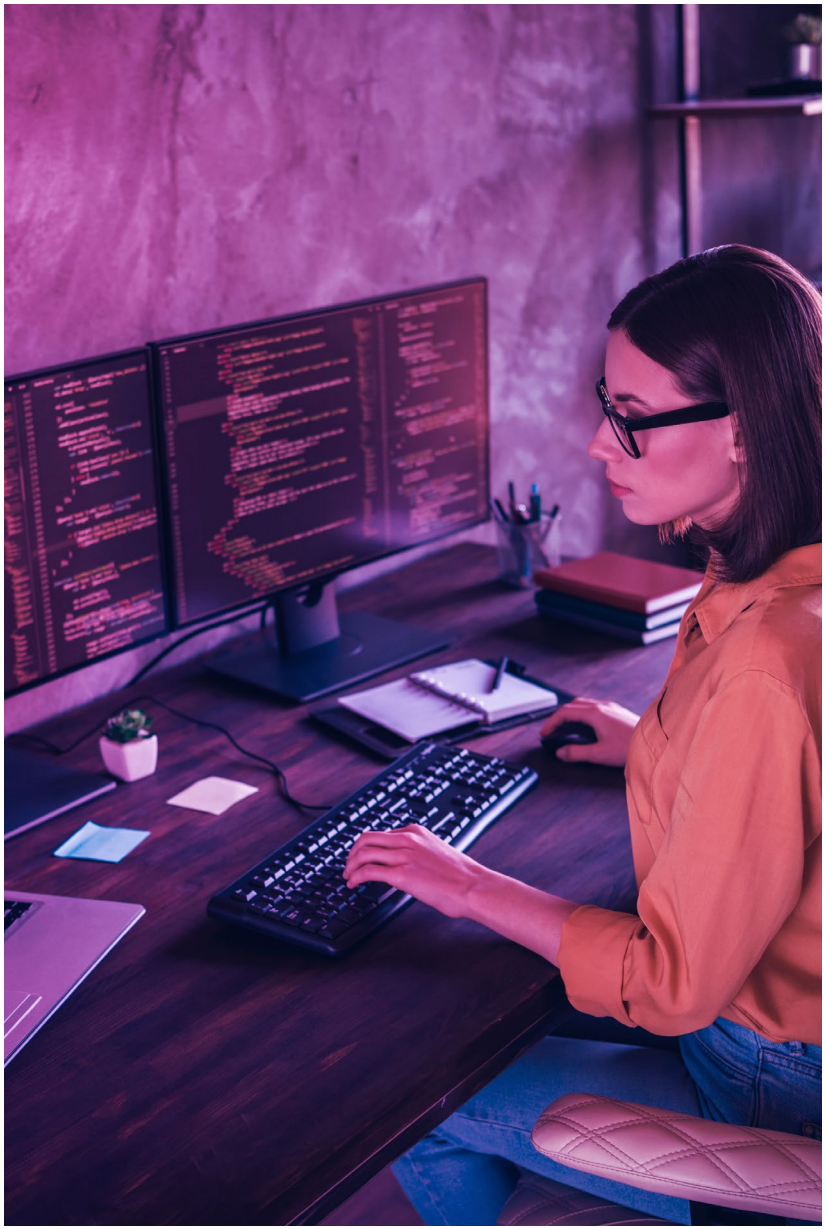
Jede Geschäftsführung ist persönlich dafür verantwortlich, dass ihre Organisation NIS2 einhält. Diese Verantwortung kann nicht übertragen werden, und es ist nicht zulässig, andere für Verstöße verantwortlich zu machen.

Mindestanforderungen der NIS2 für das Cybersicherheits-Risikomanagement

Artikel 21 der NIS2-Richtlinie enthält eine Liste von Maßnahmen zum Cybersicherheits-Risikomanagement, die wesentliche und wichtige Einrichtungen umsetzen müssen, um ihre Netz- und Informationssysteme zu schützen.

Mindestanforderungen nach NIS2:

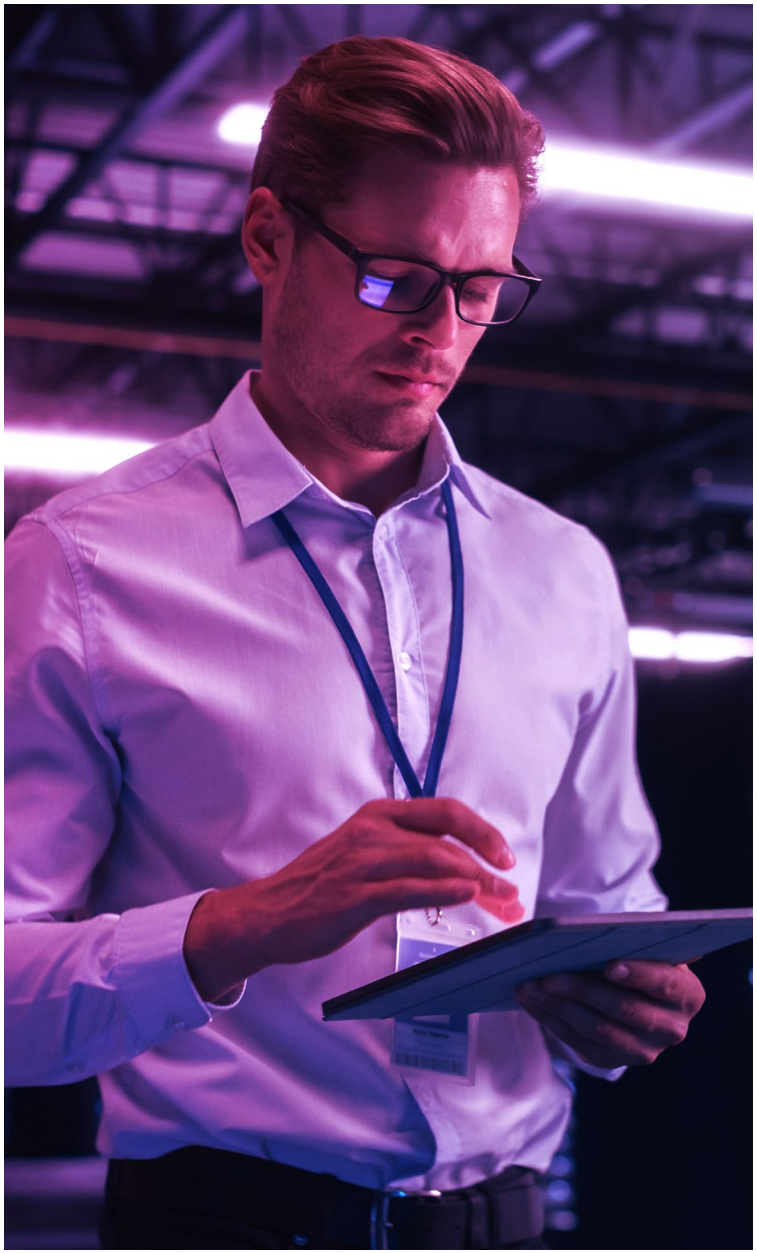
1. **Risikobewertung:** Welche Systeme und Dienste sind für Ihre Organisation am wichtigsten und stellen daher das größte Risiko dar? Wie ist die Sicherheit Ihrer Umgebung organisiert?
2. **Geschäftskontinuität:** Welche Verfahren bestehen für das Incident-Management, einschließlich eines robusten Backup-Systems? Welche Maßnahmen zur Krisenbewältigung und Wiederherstellung werden umgesetzt?
3. **Sicherheit von Netzwerk- und Informationssystemen:** Wie sind Ihre Systeme konfiguriert und wie werden Schwachstellen behoben?
4. **Wirksamkeit:** Wie wird die Wirksamkeit Ihrer Sicherheitsmaßnahmen getestet? Gibt es dafür festgelegte Verfahren?
5. **Plan zur Reaktion auf Sicherheitsvorfälle:** Wie werden Vorfälle behandelt und dokumentiert?
6. **Sicherheit in der Lieferkette:** Welche potenziellen Risiken bestehen für Ihre Organisation durch externe Lieferanten und Dienstleister?
7. **Sensibilisierung für Cybersecurity:** Wie wird die Personalsicherheit verwaltet? Sind alle mit der Sicherheitsrichtlinie vertraut und halten sich daran? Welche Schulungen werden für Mitarbeitende angeboten?
8. **Kryptografie und Verschlüsselung:** Welche Richtlinien und Verfahren bestehen für den Einsatz von Kryptografie und Verschlüsselung?
9. **Identität und Zugriff:** Welche Sicherheitsaspekte betreffen Personal, Zugriffspolitiken und Asset-Management?
10. **Multi-Faktor Authentifizierung:** Ist Multi-Faktor-Authentifizierung für Konten implementiert, die über das Internet zugänglich sind, für Konten mit administrativen Rechten sowie für kritische Systeme?



Ihre NIS2-Checkliste

Es ist wichtig, sich nicht ausschließlich auf die Mindestanforderungen zu konzentrieren. Bei Insight wissen wir, dass eine gründliche NIS2-Bewertung detailliertere Informationen erfordert. Die folgende Checkliste mit 25 Punkten wird empfohlen, um vollständige Konformität und Bereitschaft im Hinblick auf die NIS2-Maßnahmen sicherzustellen.

Nr.	Checkliste	✓
1.	Zugriffskontrolle	
2.	Situationsbewusstsein	
3.	Konfigurationsmanagement	
4.	Sicherheitsbewertung & interne Audits	
5.	Kryptografie	
6.	Personalsicherheit / Insider-Bedrohung	
7.	Identität, Autorisierung & Authentifizierung	
8.	Asset-Management	
9.	Remote-/Außendienst-Arbeit	
10.	Risikomanagement	
11.	Informationssicherheitsaspekte der BCP/BCDR	
12.	Rechtliche & vertragliche Anforderungen	
13.	Compliance & Datenschutz	
14.	Incident-Management	
15.	Wiederherstellungsplanung	
16.	Software-/Anwendungsentwicklung und -tests	
17.	Physische Sicherheit	
18.	Datenklassifizierung	
19.	Schulung & Sensibilisierung	
20.	Sicherheitsrichtlinien, Verfahren & Workflows	
21.	Risikomanagement in der Lieferkette/Sicherheit bei Drittanbietern	
22.	Schwachstellenmanagement	
23.	Patch-Management	
24.	Netzwerk & Kommunikation	
25.	Verhinderung von Datenverlust	



NIS2-Compliance mit Insight und Microsoft - sicher, strategisch, zukunftsorientiert

Die Umsetzung der NIS2-Richtlinie ist für viele Unternehmen ein komplexes und strategisch wichtiges Projekt. Insight begleitet Sie dabei als verlässlicher Partner – von der ersten Analyse bis zur erfolgreichen Umsetzung.

Als Microsoft Solutions Partner in den Bereichen Security, Modern Work und Azure verfügen wir über tiefgehendes Know-how in den modernsten Microsoft-Technologien. Wir verbinden diese Expertise mit einem erprobten Vorgehensmodell:

- Readiness-Checks & Roadmap-Entwicklung
- Implementierung & Integration
- Komplett gemanagte Sicherheitsservices

Unser Ziel geht über reine Compliance hinaus: Wir helfen Ihnen, NIS2-Anforderungen mit Ihren übergeordneten Geschäftsstrategien zu verknüpfen – für mehr Resilienz, Risikominimierung und Kostenoptimierung. Ob komplexe hybride IT-Landschaften, das Management von Drittanbieter-Risiken oder die Stärkung Ihrer Incident-Response-Fähigkeiten – wir entwickeln eine Compliance-Strategie, die langfristige Agilität und Wachstum unterstützt.

Mit Insight und Microsoft erhalten Sie einen ganzheitlichen Ansatz, um die Anforderungen der NIS2-Richtlinie effizient und sicher umzusetzen. Wir greifen Ihre bestehenden Prozesse auf, optimieren sie und stellen sicher, dass sie mit anderen relevanten EU-Richtlinien und Verordnungen harmonieren. So gelingt der Übergang reibungslos – ohne unnötige Unterbrechungen im Geschäftsbetrieb.

Jetzt handeln - für maximale Sicherheit

Brauchen Sie sofort Orientierung für Ihre konkrete Situation? Unsere maßgeschneiderten Services geben Ihnen den entscheidenden Vorsprung:

- NIS2 Awareness Workshop – vermittelt Wissen, schafft Verständnis und sensibilisiert Ihr Team.
- NIS2 Assessment Service – analysiert Ihre aktuelle Sicherheitslage und definiert klare Handlungsschritte.

Gemeinsam sorgen wir dafür, dass Ihre IT-Infrastruktur optimal geschützt ist und Ihre Geschäftsdaten jederzeit sicher bleiben.

Nützliche Ressourcen & Links zu NIS2:

Deutschland, Österreich & Schweiz

DE: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-2-Richtlinie/nis-2-richtlinie_node.html | www.bundesregierung.de

AT: https://www.bundeskanzleramt.gv.at/en/topics/cybersecurity/strategic-nis-office.html

CH: https://www.ncsc.admin.ch/ncsc/en/home.html

Insight

Bereit für den nächsten Schritt?

Mit Insight an Ihrer Seite meistern Sie den Weg zur NIS2-Compliance sicher und effizient. Wir geben Ihnen klare Handlungsempfehlungen und konkrete Maßnahmen, damit Ihr Unternehmen bestens vorbereitet ist.

Jetzt Kontakt aufnehmen

Jetzt informieren & durchstarten: Besuchen Sie unsere Webseiten und lassen Sie sich von Ihrem Insight-Experten auf dem Weg zur NIS2-Compliance begleiten.

at.insight.com | ch.insight.com | de.insight.com

MKT7148