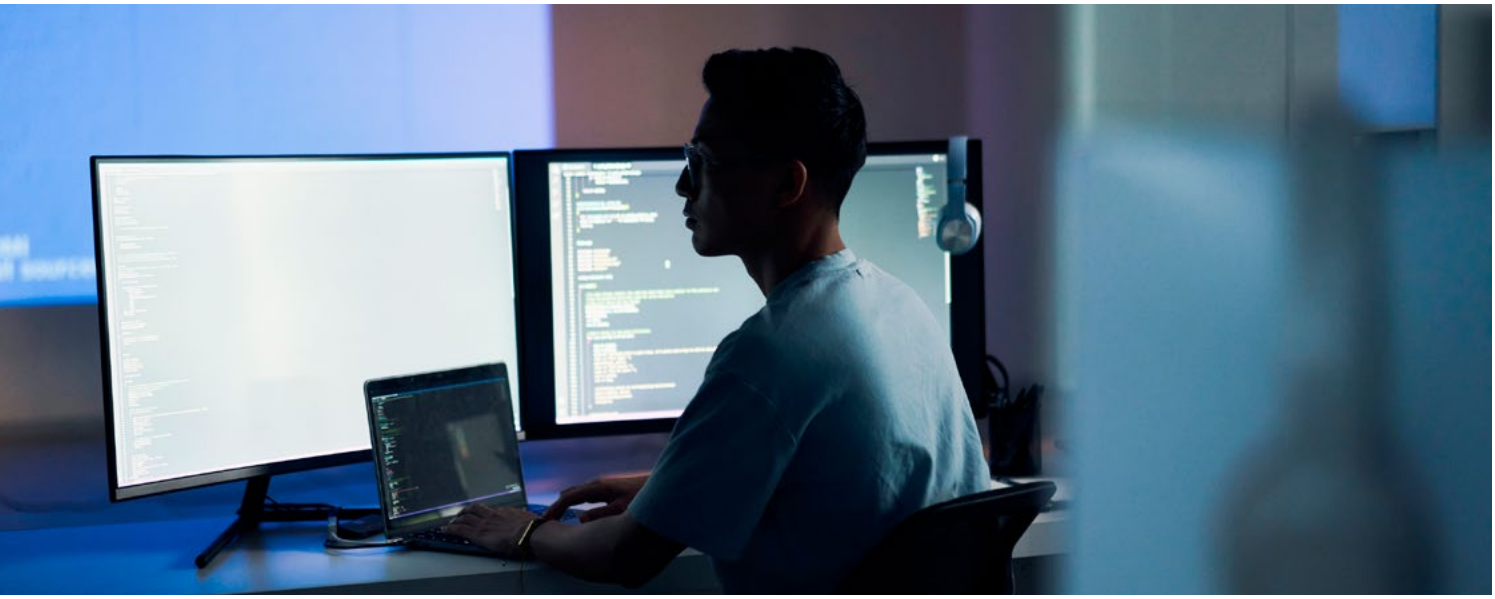
PROFI.info

PROFI SECURITY WORKSHOP
NIS/2 UND DORA FÜR IBM i

ANFORDERUNGEN
ENTSPANNT UMSETZEN

PROFI
Wir entwickeln mehr als IT



OPTIMALE VORBEREITUNG AUF DIE NIS/2-RICHTLINIE

Die NIS/2-Richtlinie (Network and Information Security) ist die überarbeitete Version der ursprünglichen NIS-Richtlinie, die im Jahr 2016 von der Europäischen Union verabschiedet wurde.

Hier sind einige der wichtigsten Punkte der NIS/2-Richtlinie:

- **Erweiterter Anwendungsbereich:** NIS/2 umfasst nun mehr Sektoren und Unternehmen, die als kritisch eingestuft werden, wie z. B. Gesundheitswesen, Energie, Verkehr und Finanzdienstleistungen.
- **Strengere Sicherheitsanforderungen:** Unternehmen müssen stärkere Sicherheitsmaßnahmen implementieren, einschließlich Risikomanagement, Vorfallmeldung und kontinuierlicher Überwachung.
- **Schutz personenbezogener Daten:** Die Richtlinie legt großen Wert auf den Schutz personenbezogener Daten und die Einhaltung der Datenschutz-Grundverordnung (DSGVO).

Anwendungsbereich NIS/2 und DORA

NIS/2 deckt eine breite Palette von Sektoren ab, die als kritisch für die Sicherheit und Stabilität der EU betrachtet werden, wie Energie, Verkehr, Gesundheitswesen und digitale Infrastruktur.

DORA konzentriert sich speziell auf den Finanzsektor und zielt darauf ab, die Betriebsstabilität digitaler Systeme in Finanzinstituten zu verbessern.

Die NIS/2-Richtlinie legt eine Reihe von Sicherheitsanforderungen fest, die Unternehmen und Organisationen in der IT einhalten müssen, um ein hohes Maß an Cybersicherheit zu gewährleisten.

Hier sind einige der wichtigsten Richtlinien:

- **Risikomanagement:** Unternehmen müssen ein umfassendes Risikomanagementsystem implementieren, um potenzielle Bedrohungen und Schwachstellen zu identifizieren und zu bewältigen.
- **Sicherheitsmaßnahmen:** Es müssen geeignete technische und organisatorische Maßnahmen ergriffen werden, um die Sicherheit von Netz- und Informations-

systemen zu gewährleisten. Dazu gehören unter anderem Firewalls, Verschlüsselung und Zugangskontrollen.
- **Kontinuierliche Überwachung:** Die IT-Systeme müssen kontinuierlich überwacht werden, um verdächtige Aktivitäten und potenzielle Sicherheitsvorfälle frühzeitig zu erkennen.
- **Schulung und Sensibilisierung:** Mitarbeiter müssen regelmäßig geschult und für die Bedeutung der Cybersicherheit sensibilisiert werden. Dies trägt dazu bei, menschliche Fehler zu minimieren und das Sicherheitsbewusstsein zu stärken.

Bei Nichteinhaltung der NIS/2-Richtlinie drohen erhebliche Strafen. Die Sanktionen können je nach Schwere des Verstoßes und der Art der betroffenen Einrichtung variieren. Hier sind einige der möglichen Strafen:

Bußgelder
Für besonders wichtige Einrichtungen können Bußgelder bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher Betrag höher ist.

Für wichtige Einrichtungen können Bußgelder bis zu 7 Millionen Euro oder 1,4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher Betrag höher ist.

Haftung der Geschäftsleitung
Die NIS/2-Richtlinie sieht vor, dass Mitglieder der Unternehmensleitung persönlich haftbar gemacht werden können, wenn sie ihren Cybersicherheitsverpflichtungen nicht nachkommen.

Weitere Informationen zu NIS/2 finden Sie in unserer **Checkliste**.

PROFI Security Workshop NIS/2 und DORA für IBM i
Um all diesen regulatorischen Vorgaben gerecht werden zu können, unterstützen wir Sie gerne bei der Durchführung eines mehrstufigen Aktionsplans:

1. Analyse des Systems anhand eines Software-Tools, das bereits erfolgreich im Großbanken-Umfeld im Einsatz ist und sämtliche Vorgaben der Richtlinien abdeckt. Das Tool analysiert durch ca. 1.300 SQL-Abfragen sämtliche sicherheitsrelevanten Werte des IBM i Betriebssystems und gibt detaillierte Reports mit Handlungsempfehlungen aus.
2. Erarbeitung einer Vorgehensweise zum Schliessen der Sicherheitslücken und Umsetzen der Empfehlungen aus dem Scan.
3. Unterstützung bei der Änderung der sicherheitsrelevanten Einstellungen im IBM i Betriebssystem
4. Schulung der Mitarbeiter in sicherheitsrelevanten Themen.

DIE PROFI ENGINEERING SYSTEMS AG

Die PROFI AG ist ein mittelständischer IT-Dienstleister mit Unternehmenssitz in Darmstadt. Das Unternehmen begleitet seine Kunden in allen Belangen der digitalen Transformation mit einem spezialisierten Portfolio von IT-Lösungen, Dienstleistungs- und Beratungsangeboten rund um die Themen Server- und Speichersysteme, Hybrid Cloud, Business Continuity, Cyber Resilience, IT-Automation, Virtualisierung, Digital Workplace, Software-Entwicklung und Managed Services.

Der Anspruch ist höchste Kompetenz, Zuverlässigkeit und Qualität, mit messbarem Erfolg und direktem Beitrag zur Wertschöpfung und Wettbewerbsfähigkeit der Kunden.

PROFI beschäftigt über 300 Mitarbeitende an bundesweit 12 Standorten. Seit vielen Jahren gehört das Unternehmen zu Deutschlands erfolgreichsten IT-Lösungsanbietern und pflegt langjährige Partnerschaften mit allen führenden IT-Herstellern.

Unsere IT-Lösungen für Ihren Erfolg

- **Business Continuity**
- **Cyber Resilience**
- **DevOps**
- **Digital Workplace**
- **Managed Services**
- **Netzwerk / IT Security**
- **Platforms**
- **SDDC / IT-Automation**
- **Software-Entwicklung**

03/2025

PROFI Engineering Systems AG
Otto-Röhm-Straße 18
64293 Darmstadt
Telefon: +49 6151 8290-0
Telefax: +49 6151 8290-7610
E-Mail: profi@profi-ag.de
www.profi-ag.de

UNSERE PARTNER

Gemeinsam mit unseren starken Partnern setzen wir Ihre optimalen Lösungen um.

PROFI
Wir entwickeln mehr als IT