Der Cyber Security Scheck

Zielsetzung
Cyber Security Schecks unterstützen österreichische KMUs, die zur Anwendung der Cybersicherheits-Richtlinie NIS2 verpflichtet sind, bei der Umsetzung von Cyber Security Maßnahmen zu NIS2.
Mit der NIS2-Richtlinie, die bis zum 17. Oktober 2024 umzusetzen ist, müssen viele Unternehmen verpflichtende Sicherheitsmaßnahmen und Meldepflichten im Bereich der Cybersicherheit implementieren. Der Cyber Security Scheck fördert die Umsetzung technischer Sicherheitsmaßnahmen zu NIS2 und hilft Ihnen dadurch die Sicherheit und Cyberabwehrfähigkeit ihrer Netz- und Informationssysteme zu stärken.

Was wird gefördert
Gefördert werden Kosten für Technologien sowie für Beratungsleistungen, die für die Umsetzung der technischen Sicherheitsmaßnahmen erforderlich sind.

Auf Ihre Bedürfnisse zugeschnitten berät und unterstützt Pilz in einem Stufenprozess*:

- **Industrial Security Compliance Check**
- **Risk Analysis**
- **Risk Assessment**
- **Detailed Design**

Wer wird gefördert
- Mittlere Unternehmen (50-249 Beschäftigte und < 50 EUR Mio Jahresumsatz oder < 43 Mio EUR Jahresbilanzsumme)
- Kleinunternehmen (< 50 Beschäftige und < 10 Mio EUR Jahresumsatz oder Jahresbilanz)
- Unternehmen mit einer Niederlassung in Österreich
- Unternehmen, die in den Anwendungsbereich der NIS 2 fallen
- Das kostenlose Webinar zum Wirkbereich der NIS 2 kann hier angefordert werden

Förderzeitraum und -umfang
- Der Förderzeitraum beträgt 12 Monate ab Projektstart.
- Die Förderung muss vor Umsetzung der Maßnahmen beantragt werden
- Das Förderansuchen muss bis spätestens 15.04.2024 bei der FFG eingereicht werden
- Der Projektstart hat bis 01.06.2024 zu erfolgen, frühestens jedoch mit der Einreichung des Förderantrags
- Die Förderung beträgt pro Cyber Security Scheck maximal EUR 10.000
- Die Förderquote beträgt maximal 40% der förderbaren Gesamtkosten des Projekts

Umsetzung in der Praxis | Ihre Vorteile
- \+ Die Förderung betrifft Sicherheitsmaßnahmen, die sie bis Oktober 2024 gesetzlich indiziert ohnedies umsetzen müssen. Andernfalls können Sie uU für die Pflichtverletzung haftbar gemacht werden.
- \+ Die Antragstellung über die Förderung ist ab sofort bis spätestens 15. April 2024 bei der FFG möglich.
- \+ Die geförderten Maßnahmen helfen Ihnen Schwachstellen in Ihrem Netzwerk zu erkennen und Vorkehrungen zu treffen, um die Verfügbarkeit Ihrer Maschinen und Anlagen auch bei einem Angriff zu gewährleisten.

Quellen
- Österreichische Förderagentur für wirtschaftsnahe Forschung, Entwicklung und Innovation (FFG) | Link
- Wirtschaftskammer Österreich | Link

Ihr Kontakt
Andreas Willert
Head of Industrial Security
Tel: +431 7986263-26 | Mobil: +43 664 8419467 | E-Mail: a.willert@pilz.at

PILZ
THE SPIRIT OF SAFETY

Stufenprozess zur sicheren Maschine

Der Stufenprozess im Pilz Cyber Security Check

01	Industrial Security Compliance Check	▸ Industrial Security Expertenvortrag ▸ OT-Security Compliance Overview & Quick Check NIS 2/MVO/CRA ▸ Live-Tech-Demo einer industrial Firewall am Beispiel der Pilz Security Bridge ▸ Anlagenbesichtigung & Besprechung kundenspezifischer Fragen auf Basis des Netzwerkplans ▸ Empfehlungen zur Umsetzung der IEC 62443 für den Schutz der Safety von Maschinen gegen Cyber-angriffe basierend auf der IEC TS 63074 ▸ Überblick über organisatorische Maßnahmen, damit die technischen Maßnahmen wirkungsvoll sind
02	Risk Analysis	▸ Industrial Security Compliance Check ▸ Bestimmung der Grenzen des in Betracht zu ziehenden Systems ▸ Ermittlung der Schutzziele jedes Assets anhand der zu erwartenden Schadenshöhe bei Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit
03	Risk Assessment	▸ Ermittlung sämtlicher Risiken für jedes Asset innerhalb jeder Lebensphase des Systems hinsichtlich der in Betracht gezogenen Schutzziele ▸ Empfohlene Herangehensweise zur Reduzierung des Risikos ▸ Ermittlung der Systemstabilität und Verwundbarkeiten (optional) ▸ Dokumentation der Schwachstellen und der entsprechenden Gefährdung
04	Detailed Design	▸ Ermittlung potentieller Gefährdungsmilderungsstrategien ▸ Festlegung des Security Levels nach 62443 für jedes Systemteil ▸ Definition und Spezifikation der Gegenmaßnahmen ▸ Gestaltung des Aufbaus der Geräte und des Einsatzes vorhandener Features im Hinblick auf die Gefährdungsreduzierung bzw. Einhaltung des Target Security Levels ▸ Dokumentation der Anforderungen der Umsetzungsempfehlungen

Ihr Kontakt
Andreas Willert
Head of Industrial Security
Tel: +431 7986263-26 | Mobil: +43 664 8419467 | E-Mail: a.willert@pilz.at

PILZ
THE SPIRIT OF SAFETY