ARS Akademie

WISSEN MACHT ERFOLG

Wie Informationssicherheit und NIS2 Ihr Geschäft verändern

Schutz vor Cyberbedrohungen - NIS2 in der Praxis

Kursinfos

Jetzt online buchen!

Seminar-ID: **332327**

Ort: **Wien, Online**

📣 Darum lohnt sich der Kurs

Die Anforderungen an Informationssicherheit und NIS2 verändern Geschäftsprozesse und Risikomanagement grundlegend. Dieses Seminar zeigt, wie Sie Ihr internes Kontrollsystem anpassen, geschäftskritische Assets schützen und die aktuellen EU-Regularien erfolgreich umsetzen.

Das nehmen Sie mit

In diesem Seminar werden Sie an die rechtlichen Herausforderungen der Cybergovernance Thematik herangeführt und erhalten Anregungen, wie Sie ihr Internes Kontrollsystem und Risikomanagement an die Herausforderungen der Cybersicherheit anpassen. Erhalten Sie zudem alle Informationen zu den aktuellen und kommenden NIS und NIS 2.0. Bestimmungen. Die gemeinsame Abendveranstaltung gibt dabei Raum zum Wissens- und Erfahrungsaustausch.

Ihr Programm im Überblick

- Informationssicherheit Rahmenbedingungen
  - Gesetzliche Anforderungen, Normen und Standards
    - EU-Regularien – NIS 2.0 Überblick
    - Parallelen zur DSGVO – potentielle Auswirkungen (persönlich und Unternehmen)
    - Internes Kontrollsystem und Risikomangement
    - Haftungsthemen
    - Mein Unternehmen als Bestandteil der Lieferkette bzw. eigene Produkte und Dienstleistungen mit Software
- Aktuelle Lage in KMUs
  - Warum es auch Sie betrifft – Klärung Betroffenheit
  - Resilienz von Unternehmen
  - KMUs sind kein Angriffsziel – oder doch ?
  - Verantwortung der Geschäftsführung
  - Notwendige Ressourcen
- GRC – Governance, Risk, Compliance und Unternehmensführung
  - Verbundene Themenstellungen – Risikomanagement, DSGVO, BCM, notwendige Zertifizierungen
  - Risikolandschaft von Unternehmen
    - BSI Gefahrenkatalog
    - Ausgewählte Beispiele und weiterführende Informationen
- Mindestanforderungen an Klein- und Mittelunternehmen

    - Basis ÖSCS – Österreichische Strategie für CyberSicherheit – Österreichisches Informationssicherheitshandbuch
    - Schlussfolgerungen aus „Best Practice“ – Leitfäden für KMUs
- Vom Warum zum WIE
    - Parameter und resultierende Anforderungen (z.B. Betrieb eigener IT, Cloudcomputing, Lieferant für kritische Infrastruktur…)
    - Interne Regelungen – Verantwortung, Dokumentation…
    - Grundlegende Basisanforderungen – „Cyberhygiene“
    - CRR – Cyberriskrating – Schema 2023 – welche Fragen und Anforderungen von Partnern an sie gestellt werden
    - Geschäftskritische Assets, Prozesse und Einbindung in Ökosysteme
- Worauf Sie keinesfalls verzichten können
    - Thematisierung im Unternehmen (Schulung, Evaluierung….)
    - Geeignete Bausteine zum Schutz ihrer Infrastruktur und Anwendungen (z.B. Rechtemanagement, Umgang mit Passwörtern usw.)
    - Business Continuity und Notfallsmanagement
    - Vorsorgemaßnahmen (Was tue ich wenn…..)
- Bausteine zur Bewältigung der resultierenden Anforderungen
    - Prozesse, Organisation, Technik
    - Überblick zu Produkten, Lösungen und Dienstleistungen mit besonderem Fokus auf die Anforderungen von KMUs
    - Weiterführendes Knowhow (Websites, Checklisten, IT-Markt…)
        - Österreichische Einrichtungen und internationale Einrichtungen rund um Cybersicherheit
            - Public / Private Partnership – Initiativen und Knowhow aus Österreich
- Technologie und Dienstleistungen
    - Intransparenter Lösungsmarkt
    - „Leistbare“ Technologien und Lösungsbausteine
    - Dienstleister – Matching Nachfrage und Angebot
- Förderungen

Interessant für

- Geschäftsführer, Eigentümer, Management
- Beauftragte für Informationssicherheit

Termine & Optionen

DATUM	DAUER	ORT	FORMAT	PREIS
08.04.2025-09.04.2025	1 Tag	Virtual Classroom	Online	€ 950,-
08.04.2025-09.04.2025	1 Tag	Wien	Präsenz	€ 950,-

Preise exkl. MwSt.

In Kooperation mit

Beratung & Buchung

Jeffrey Müller-Büchse
+43 1 713 80 24-38 bildungsmanagement@ars.at