


EU-Vorschriften zur Cybersicherheit – Anforderungen der NIS2-Richtlinie

EU Cyber Resilience Act: Sichere Hard- und Software

Beginn:	 Ostfildern	Veranstaltungsnr.: 36187.00.002	Präsenz
19.05.2025 - 09:00 Uhr		Leitung	EUR 720,00 (MwSt.-frei)
Ende:		<u>Dr. Thomas Liedtke</u>	Mitgliederpreis ⓘ
19.05.2025 - 16:30 Uhr			EUR 648,00 (MwSt.-frei)
Dauer:			
1,0 Tag			

in Zusammenarbeit mit:



BESCHREIBUNG



Energiewirtschaft, Automobil- und Maschinenbau, Medizintechnik, Krankenhäuser, Universitäten, Banken und Finanzämter – alle Sektoren haben eines gemeinsam: sie sind von essentieller Bedeutung für das Leben und die Wirtschaft in Deutschland. Als Schnittstelle von physischer Infrastruktur und digitaler Innovation sind sie aber auch Angriffsziele im Cyberraum. Besonders mit dem Fortschritt der Digitalisierung gewinnt eine umfassende Cyberresilienz und -sicherheit immer mehr an Bedeutung. Sie ist der beste Schutz, um drohende Gefahren, wie beispielsweise Ransomware oder Phishing, gezielt abzuwehren und den digitalen Wandel dauerhaft zu ermöglichen.

Die Erhöhung des Niveaus der Cybersicherheit in der Europäischen Union, über Unternehmen und die gesamte Lieferkette hinweg, ist das Ziel der neuesten NIS2-Richtlinie.

Durch die Modernisierung des bestehenden rechtlichen Rahmens, um mit einer zunehmenden Digitalisierung und einer sich entwickelnden Bedrohungslandschaft für die Cybersicherheit Schritt zu halten, erweitert diese Verordnung den Anwendungsbereich der Cybersicherheitsregeln auf neue Sektoren und Einrichtungen.

Mit zahlreichen Anwendungsfällen hilft Ihnen das Seminar, NIS2 und seine

Auswirkungen auf Unternehmen zu übersetzen und zu verstehen.

Ziel der Weiterbildung

Das Seminar zielt darauf ab, Ihnen Kenntnisse über die zunehmenden Gefahren schädlicher Angriffe und deren Vielfalt, einschließlich Malware, Phishing und Ransomware, zu vermitteln. Es legt den Fokus darauf, wie Sie ein höheres Maß an digitaler Sicherheit und Widerstandsfähigkeit gegen Cyberbedrohungen erreichen können, durch präventive und reaktive Maßnahmen. Bis zum 17.10.2024 müssen alle betroffenen Organisationen spezifische Sicherheitsmaßnahmen erweitern und umsetzen, um ihre Systeme zu schützen. Die Nichtumsetzung dieser Maßnahmen kann zu Geldstrafen von bis zu 10 Millionen Euro führen. Praxisnahe Tipps zur minimalen Umsetzung beinhalten regelmäßige Backups, Firewalls, Antivirenprogramme und Multi-Faktor-Authentifizierung. Durch diese Maßnahmen sollen Sie die Sicherheitslage verbessern und die Widerstandsfähigkeit gegen Cyberangriffe erhöhen.

IMMER TOP!

Unser Qualitätsversprechen



Seit über 65 Jahren gehört die Technische Akademie Esslingen (TAE) mit Sitz in Ostfildern – nahe der Landeshauptstadt Stuttgart – zu Deutschlands größten Weiterbildungs-Anbietern für berufliche und berufsvorbereitende Qualifizierung im technischen Umfeld. Unser Ziel ist Ihr Erfolg. Egal ob Seminar, Zertifikatslehrgang oder Fachtagung, unsere Veranstaltungen sind stets abgestimmt auf die Bedürfnisse von Ingenieuren sowie Fach- und Führungskräften aus technisch geprägten Unternehmen. Dabei können Sie sich stets zu 100 Prozent auf die Qualität unserer Angebote verlassen. Warum das so ist?

PROGRAMM

Montag, 19. Mai 2025

9.00 bis 12.15 und 13.15 bis 16.30 Uhr

Motivation

- Ziele und Motivation der NIS2
- Wer ist betroffen?
 - Betreiber kritischer Anlagen
 - wichtige Einrichtungen
 - mittlere Unternehmen, Großunternehmen

Anforderungen

- neue und erweiterte Anforderungen
- Mindestmaßnahmen (z.B. BCM, Sicherheit in der Lieferkette, Multi-Faktor-Authentifizierung, ...)
- Size-cap-Regel
- Risikomanagement-Maßnahmen
- Haftungsrisiken für die Geschäftsführung; strenge Aufsicht
- strenge Meldepflichten (24h für Sicherheitsvorfälle, 72h für Bewertungen)
- Schulungsverpflichtung für die Geschäftsführung
- Rechte und Rollenverteilung
- Sicherstellung der Wettbewerbsfähigkeit

EU Cyber Resilience Act (EU-Gesetz über Cyberresilienz)

- EU-Vorschriften zur Cybersicherheit gewährleisten sicherere Hard- und Software
- Sicherheitsrisiken von Produkten und Software mit digitalen Komponenten
- Verbraucherschutz
- Sicherheitsupdates für Produkte und Software
- Risikoanalyse, welche Produkte cybersicher sind, oder wie man sie einrichtet, sodass ihre Cybersicherheit geschützt ist
- harmonisierte Vorschriften für das Inverkehrbringen von Produkten oder Software mit digitalen Komponenten
- Rahmen von Cybersicherheitsanforderungen für die Planung, Gestaltung, Entwicklung und Wartung solcher Produkte mit Verpflichtungen, die in jeder Phase der Wertschöpfungskette zu erfüllen sind;
- Verpflichtung zur Sorgfaltspflicht für den gesamten Lebenszyklus solcher Produkte

Praxisbeispiel für eine Risikoanalyse

Zusammenfassung und Ausblick

- Alle Personen eines Unternehmens, die zur Cybersicherheit beitragen
- Alle Personen, die systematische Risikoanalysen durchführen und entsprechende Managementsysteme etablieren und Zertifizierungen erreichen müssen

REFERENT:INNEN



Dr. Thomas Liedtke

Dr. Thomas Liedtke ist

- seit vielen Jahren Mitglied der deutschen DIN-AK-Spiegelgruppe, welche für die Definition ISO/SAE 21434, ISO/PAS 5112 und weitere Cybersecuritystandards verantwortlich ist
- Mitglied des intacs Advisory Boards und Leiter der SPICE Cybersecurity Arbeitsgruppe
- Leiter der ZVEI Arbeitsgruppe Datensicherheit im Automobil
- Leadauditor für CSMS; ISMS; TISAX
- Berater für die Implementierung der Cybersecurity in Unternehmen

Publikationen

- Informationssicherheit: Möglichkeiten und Grenzen; SpringerLink publisher:

link.springer.com/book/10.1007/978-3-662-63917-7

- The New Cybersecurity Challenges and Demands for Automotive Organisations and

Projects – an Insight View link.springer.com/chapter/10.1007/978-3-031-42307-9_21

Weitere Veranstaltungen

[Automotive Cybersecurity ISO/SAE 21434: Sicherheitsstandards in der Automobilindustrie](#)

[Sicherheitsgerichtete Systeme entwickeln](#)

[Einführung in die Kryptographie: Methoden und praktische Anwendungen](#)

VERANSTALTUNGORT

Technische Akademie Esslingen

An der Akademie 5

73760 Ostfildern

Die TAE befindet sich im Südwesten Deutschlands im Bundesland Baden-Württemberg – in unmittelbarer Nähe zur Landeshauptstadt Stuttgart. Unser Schulungszentrum verfügt über eine hervorragende Anbindung und ist mit allen Verkehrsmitteln gut und schnell zu erreichen.



GEBÜHREN UND FÖRDERMÖGLICHKEITEN

Die Teilnahme beinhaltet [Verpflegung](#) sowie ausführliche Unterlagen.

Preis:

Die Teilnahmegebühr beträgt:

720,00 € (MwSt.-frei)

Fördermöglichkeiten:

Für den aktuellen Veranstaltungstermin steht Ihnen die [ESF-Fachkursförderung](#)

leider nicht zur Verfügung.

Für alle weiteren Termine erkundigen Sie sich bitte vorab bei unserer [Anmeldung](#).

Andere Bundesland-spezifische Fördermöglichkeiten finden Sie [hier](#).

Inhouse Durchführung:

Sie möchten diese Veranstaltung firmenintern bei Ihnen vor Ort durchführen? Dann fragen Sie jetzt ein individuelles [Inhouse-Training](#) an.