

Cyber-Sicherheit im Unternehmen

- NIS2-Richtlinien verstehen und umsetzen
- Wie Sie Hackerangriffe erkennen und Ihre Cybersecurity-Roadmap erstellen



MEET THE EXPERTS



SCHÜTZEN SIE IHR UNTERNEHMEN DURCH DIE UMSETZUNG DER NIS2-RICHTLINIE VOR CYBERBEDROHUNGEN UND SICH SELBST VOR RECHTLICHEN KONSEQUENZEN!

Ihr Risiko

- Die Einhaltung der NIS2-Richtlinie ist für viele Unternehmen verpflichtend. Eine Nicht-Umsetzung kann zu erheblichen rechtlichen Konsequenzen und hohen Bußgeldern führen.
- Wissen Sie, ob NIS-2 für Sie relevant ist?
- Wenn ja, stellen Sie sicher, dass Sie alle relevanten gesetzlichen Vorgaben im Bereich Cybersecurity erfüllen und somit Strafen vermeiden.
- **Es besteht akuter Handlungsbedarf!**



- Nutzen Sie das **kostenfreie Informationsangebot** zum Thema Cyber-Security und NIS-2
- Investieren Sie einen Nachmittag und erfahren Sie mehr über NIS-2 und welche Gefahren bei der Digitalisierung drohen und wie Sie ihnen begegnen können



Homeoffice, Cloud Computing, Industrie 4.0, Digitale Produktion.

Mit der **zunehmenden Digitalisierung** und Vernetzung von Maschinen und Anlagen werden Prozesse vereinfacht und Flexibilität, Produktivität und Qualität gesteigert. Kurz die **Wertschöpfung des Unternehmens verbessert sich**.

Aber auch das **Risiko Zielscheibe von Cyberangriffen zu werden, erhöht sich**. Deshalb stehen Unternehmen in einer zunehmend vernetzten Welt vor immer größeren Herausforderungen in der Cybersicherheit.

Die **NIS2-Richtlinie** (Network and Information Security Directive) der Europäischen Union zielt darauf ab, die Resilienz und Sicherheit von Netz- und Informationssystemen zu stärken. Für produzierende Unternehmen bedeutet dies, dass sie sich auf **neue Sicherheitsstandards einstellen und effektive Maßnahmen zur Abwehr von Cyberbedrohungen implementieren müssen**. Auf die Unternehmen kommen zusätzliche Anforderungen in der Umsetzung und Dokumentation zu.

Welche Risiken bestehen, was Unternehmen dagegen tun können und welche Sicherheitsüberlegungen Sie treffen müssen, wird von unterschiedlichsten Experten aus der Branche diskutiert und erörtert.

Diese Veranstaltung bietet Ihnen einen Einblick in die NIS2-Richtlinien und **zeigt praxisnahe Wege auf**, wie Sie diese erfolgreich umsetzen können, um Ihr Unternehmen optimal zu schützen.

Es erwarten Sie:

- spannende Diskussionsbeiträge,
- Tipps, worauf Sie bei der Umsetzung von IT-Sicherheitskonzepten achten müssen
- und die Möglichkeit mit Experten Ihre Fragen zu diskutieren.



Karl Friedrich Schmidt
Geschäftsführer
accelcon industrial Engineering GmbH

AGENDA

13:00 Eintreffen der Gäste

13:30 Begrüßung
Dr. Martin Thul,
Leiter Geschäftsstelle „We move it“ & Geschäftsführer CVC Südwest

13:40 Einleitung:
Im Visier der Hacker: Warum Cyberabwehr entscheidend ist
Karl Friedrich Schmidt

Vortrag:
14:00 **Was müssen von NIS-2 betroffene Unternehmen und Organisationen tun?**
Michael Harmann

14:45 Talk and Meet

Vortrag:
15:15 **Super GAU Cyber-Attack: Was kann ich im Vorfeld tun?**
Jens Hildenbeutel

Vortrag:
16:00 **Analyse der eigenen Verantwortlichkeiten und NIS 2 Readiness entlang der Lieferkette**
Jasper Bhaumick

16:45 Abschlussdiskussion, Come together



VORTRÄGE

Vortrag:

Was müssen von NIS-2 betroffene Unternehmen und Organisationen tun?

- In diesem Vortrag beleuchten wir den erweiterten Anwendungsbereich der NIS-2-Richtlinie und klären, welche Unternehmen von den verschärften Datenschutzvorgaben betroffen sind. Sie erfahren, welche Anforderungen auf Sie zukommen, wie die Meldepflicht für Sicherheitsvorfälle ausgestaltet ist und welche Konsequenzen Verstöße nach sich ziehen – inklusive möglicher Haftung und Sanktionen für die Geschäftsführung.

Vortrag:

Super GAU Cyber-Attack: Was kann ich im Vorfeld tun?

- Die Firma wurde Opfer eines Hackerangriffs. Alle Daten sind verschlüsselt, die Produktion steht still, und sowohl der Vertrieb, der Einkauf als auch die Verwaltung haben keinen Zugriff mehr auf ihre Unterlagen. In diesem Vortrag zeigen wir, wie solche Angriffe typischerweise ablaufen, und an welchen Punkten, sowie anhand welcher Verhaltensmuster solche Bedrohungen bereits frühzeitig erkannt und abgewehrt werden können.

Vortrag:

Analyse der eigenen Verantwortlichkeiten und NIS-2 Readiness entlang der Lieferkette

- In diesem Vortrag zeigen wir anhand eines Praxisbeispiels, wie Unternehmen ihre internen Verantwortlichkeiten im Rahmen der NIS-2-Richtlinie dokumentieren und die notwendigen Maßnahmen zur Umsetzung festhalten können. Zudem erläutern wir, wie die Lieferkette erfolgreich in das Risikomanagement integriert wird, um die NIS-2-Readiness auf allen Ebenen zu gewährleisten. Erfahren Sie praxisnah, wie Sie Risiken entlang der Lieferkette identifizieren und managen können.

CYBERSECURITY-EXPERTEN IM FOKUS: UNSERE REFERENTEN STELLEN SICH VOR...



Karl F. Schmidt

Geschäftsführer
Accelcon industrial
engineering GmbH
Germany

Digitale
Transformation
Lean Production
Digitaler Retrofit
IIoT-Beratung und
Implementierung
OEE-Implementierung



Michael Harmann

Auditor/Cyber-
Security Specialist

Chief Information Security
Datenschutz



Jens Hildenbeutel

Leiter IT-Service-Management
Verantwortlicher für Cyber-
Security
4S IT Solutions AG
Germany

Managed IT Security
Services
Security Awareness-
Trainings
IT-Services



Jasper Bhaumik

Vorstandsvorsitzender
Bizpando AG
Switzerland

B2B-Compliance-
Plattform für
Lieferkettensorgfalts-
pflicht
CSRD, CSDDD