

WORKSHOP

CYBERSICHERHEITS-
RICHTLINIE NIS 2

RECHT –
RISIKOMANAGEMENT –
MAßNAHMEN

WORKSHOP

CYBERSICHERHEITS-RICHTLINIE NIS 2

Recht – Risikomanagement – Maßnahmen

Mit der neuen Cybersicherheits-Richtlinie mit der Bezeichnung "NIS 2" gelten ab Oktober 2024 für viele Unternehmen bestimmter Sektoren verpflichtende Sicherheitsmaßnahmen und Meldepflichten bei Sicherheitsvorfällen.

Der Anwendungsbereich geht weit über die vom derzeit geltenden NIS-Gesetz betroffenen Unternehmen – vorwiegend Anbieter kritischer Infrastrukturen und digitaler Dienste – hinaus.

In Zukunft fallen beispielsweise auch mittlere und große Unternehmen in den Bereichen Post- und Kurierdienste, Abfallbewirtschaftung, Chemie, Lebensmittel oder verarbeitendes Gewerbe sowie die öffentliche Verwaltung unter diese Regelungen. Betroffene Einrichtungen müssen Mindeststandards für Cybersicherheit nachweisen können und Sicherheitsvorfälle binnen 24 Stunden melden.

Die Leitungsorgane müssen Schulungen nachweisen und haften persönlich für die Einhaltung der Risikomanagementmaßnahmen. Auch die Sicherheit in der Lieferkette ist zu beachten.

Es ist wichtig, dass sich betroffene Unternehmen rechtzeitig auf die Regelungen vorbereiten, um ihre internen Prozesse an die Vorgaben anzupassen. Dies ist nicht nur in Hinblick auf die rechtlichen Erfordernisse und hohen Strafdrohungen erforderlich, sondern sollte auch als Chance gesehen werden, das eigene Unternehmen vor drohenden Cyberattacken zu schützen.

Auch wenn die Empfehlung zur Etablierung eines Risikomanagementprozesses nicht neu ist und sich aus zahlreichen Informationssicherheitsstandards wie ISO 27001 bis hin zu Gesetzen wie der DSGVO ableiten lässt, erhält das Thema Risikomanagement mit der NIS 2 eine neue - zentrale - Bedeutung im Unternehmensalltag. So gilt ein effektives Risikomanagement als DIE Steuerungskomponente, die es der Unternehmensführung ermöglichen soll, fundierte Entscheidungen zu treffen.

Der zweite Teil konzentriert sich daher auf die Kernkomponenten und den Aufbau eines geeigneten Risikomanagementprozesses. Die richtige Vorgehensweise und die Vermeidung typischer Fallstricke werden ebenfalls thematisiert. Zudem werden praktische Erfahrungen und Hintergründe zu den in NIS 2 geforderten Sicherheitsmaßnahmen diskutiert. Dabei werden Themen wie die Verwaltung von Benutzerkonten und Berechtigungen, die angemessene Härtung von Geräten und Anwendungen, die Absicherung administrativer Zugriffe und Tätigkeiten sowie Aspekte der Netzwerksicherheit behandelt. Abschließend wird ein Überblick über die häufigsten Auditfeststellungen und die daraus resultierenden Maßnahmen gegeben.

Thema/Vortragende	Zeit
<p>Teil 1: Recht</p> <ul style="list-style-type: none"> • Überblick zur NIS 2-Richtlinie • Unterschiede vom derzeit geltenden NIS-Gesetz zu den neuen NIS 2-Bestimmungen • Welche Unternehmen sind von NIS 2 betroffen? • Welche Anforderungen stellt NIS 2 an Unternehmen? • Was müssen Vorstände/Geschäftsführer tun? • Welche Vorgaben gibt es in Bezug auf die Lieferkette? • Welche Strafen und Rechtsfolgen drohen bei nicht konformer Umsetzung? <p>Vortragende: Mag. Verena Becker, BSc</p>	<p>09:00-13:00 Uhr</p>
<p>Teil 2: Risikomanagement & Maßnahmen</p> <ul style="list-style-type: none"> • Kernkomponenten und Aufbau eines Risikomanagementprozesses • Möglichkeiten und Quellen zur Identifikation relevanter Risiken • Planung und Umsetzung geeigneter Sicherheitsmaßnahmen • Umgang mit Restrisiken • Kernkomponenten und Aufbau eines ISMS • Diskussion und Hintergründe zu wesentlichen in der NIS 2 geforderten Sicherheitsmaßnahmen <p>Vortragender: Markus Hellmann, MA BSc</p>	<p>13:00-17:00 Uhr</p>

ZIELGRUPPE

Der Workshop richtet sich insbesondere an Beraterinnen und Berater in den Bereichen Informationssicherheit, Risikomanagement und Informationstechnologie. Des Weiteren an Absolventinnen und Absolventen der incite-Lehrgänge „[DSGVO – Die EU-Datenschutzgrundverordnung](#)“ und „[Data & IT Security](#)“. Darüber hinaus an „[Zertifizierte Datenschutzbeauftragte](#)“ und „[Certified Data & IT Security Experts](#)“, sowie an alle Interessierten, die sich im Bereich NIS 2 weiterbilden möchten. Voraussetzung ist die Mitgliedschaft in der Fachgruppe Unternehmensberatung, Buchhaltung und Informationstechnologie Steiermark oder Fachvertretung Telekommunikations- und Rundfunkunternehmungen Steiermark.

ZIELE

- Ich kenne den grundlegenden Aufbau der NIS 2-Richtlinie.
- Ich kann beurteilen, ob ein Unternehmen von NIS 2 betroffen ist.
- Ich kenne den Unterschied zwischen einer wesentlichen und einer wichtigen Einrichtung.
- Ich weiß, welche Anforderungen auf betroffene Einrichtung mit NIS2 zukommen.
- Ich kenne die Anforderungen an die Unternehmensleitung.
- Ich weiß, welche Rechtsfolgen bei Nichteinhaltung der Vorschriften drohen.
- Verständnis für Ansätze und Methodologien im Bereich Riskmanagement
- Wissen um wesentliche in NIS 2 geforderte Sicherheitsmaßnahmen

STRUKTUR UND METHODIK

- Vortrag und Erfahrungsinput
- Praxisbeispiele
- Diskussion

ABSCHLUSS

Die

Absolventinnen und Absolventen des Workshops erhalten eine Teilnahmebestätigung.

TERMINE UND SEMINARORT

Termin	Seminarort	Anmeldung
11.9.2024	WIFI Graz	Eine Anmeldung ist hier möglich.

KOSTEN

Die Fachgruppe UBIT Steiermark und die Fachvertretung Telekommunikations- und Rundfunkunternehmungen Steiermark übernehmen für ihre Mitglieder 100% der Kurskosten in der Höhe von € 450,- und stellen Snacks und Getränke während des Workshops zur Verfügung.

Die im Kurspreis enthaltenen Kursmaterialien werden in digitaler Form zur Verfügung gestellt.

ANMELDUNG

Bitte melden Sie sich über unsere [Website](#) zu diesem Workshop an.

Anmeldeschluss ist zwei Wochen vor Beginn.

Wir weisen darauf hin, dass die Anmeldungen nach Datum des Einlangens berücksichtigt werden. Aufgrund der begrenzten Kursplätze wird eine rasche Anmeldung empfohlen.

Der Workshop findet mit mindestens acht und maximal 24 Teilnehmerinnen und Teilnehmern statt.

Die Anmeldung ist verbindlich. Bei einer Stornierung/unterlassenen Absage/Nichterscheinen ab dem 2.9.2024 behält sich die Fachgruppe Unternehmensberatung, Buchhaltung und Informationstechnologie vor, die Kurskosten in der Höhe von € 450,- brutto einzuheben.

Wenn Sie Fragen haben, kontaktieren Sie uns bitte!

Wenn Sie Fragen haben, kontaktieren Sie uns bitte.

Patrick Halper, BA

05 90900-3798

patrick.halper@incite.at



Vortragende:



©Nadine Studeny Photography

Mag. Verena Becker, BSc (WU)

ist als Cybersicherheitsexpertin in der Bundessparte Information und Consulting in der Wirtschaftskammer Österreich tätig. Sie ist Juristin und Betriebswirtin mit Schwerpunkt Informationssicherheit. Weiters ist sie Cofounderin von Women4Cyber Austria, Mitglied der ENISA Ad Hoc Working Group on Enterprise Security und Information Security Managerin nach ISO/IEC 27001:2022.



Markus Hellman, MA BSc

ist ehemaliger Polizeibeamter und Experte für Integrierte Managementsysteme und verfügt über 10 Jahre Erfahrung im Polizeidienst, insbesondere in den Bereichen Risikomanagement und Verfassungsschutz. Seine akademische Ausbildung umfasst den Studiengang Sicherheitsmanagement an der FH Campus Wien und den Studiengang Risikomanagement an der FH Campus Wien. Zusätzlich verfügt er über Zertifizierungen in den Bereichen Risikomanagement, Wirtschaftsprüfung und Interne Revision.