incite
DIE UBIT.AKADEMIE

LEHRGANG

DATA & IT SECURITY

Ausgabedatum: 11.11.2025

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung · Buchhaltung · IT

LEHRGANG

DATA & IT SECURITY

IT-Sicherheit und Datenschutz kompakt

Angriffe auf digitale IT-Infrastrukturen stellen zusehends ein immer mehr ernstzunehmendes Risiko dar. Die Zahl der unerlaubten Zugriffe steigt jährlich an. Cyberattacken zählen in Österreich und weltweit zu den größten Risiken für Unternehmen. Aufgrund der Abhängigkeit von einer funktionierenden IT sind Unternehmen gefordert ihr geistiges Eigentum, ihre Kundinnen- und Kundendaten und ihre Geschäftsgeheimnisse vor Angriffen zu schützen.

Seit 25. Mai 2018 gilt die EU-Datenschutz-Grundverordnung (EU-DSGVO). Diese neue Verordnung soll Bürger:innen mehr Rechte und die Kontrolle über ihre personenbezogenen Daten einräumen. Für alle österreichischen Unternehmen ohne Ausnahme -, auch KMU - ergeben sich viele datenschutzrechtliche Verpflichtungen. Unternehmen müssen selbst eine Risikoeinschätzung vornehmen und in Sachen Schutz personenbezogener Daten entsprechende Maßnahmen setzen. Die Nichtbeachtung dieser vielen Bestimmungen kann mit einer Geldstrafe bis zu € 20 Mio. oder bei Konzernen mit bis zu 4 % des weltweiten Umsatzes sanktioniert werden.

Die neue EU-Cybersicherheits-Richtlinie „NIS2" muss bis 17. Oktober 2024 in Österreich umgesetzt werden. Ab diesem Zeitpunkt gelten für viele Unternehmen bestimmter Sektoren und deren Dienstleister und Lieferanten konkrete Mindeststandards für Cybersicherheit und Meldepflichten bei Sicherheitsvorfällen. Knowhow im Bereich Informations- und Datensicherheit ist damit ein Muss für jedes Unternehmen, qualifizierte Expertinnen und Experten werden dringend gesucht.

Dieser Lehrgang wurde gemeinsam mit der Wirtschaftskammer Österreich Bundessparte Information und Consulting, der Österreichischen Computergesellschaft (OCG), dem Zentrum für sichere Informationstechnologie – Austria (A-Sit), in Kooperation mit dem Kuratorium Sicheres Österreich (KSÖ), SBA-Research und anderen Expert:innen auf diesem Gebiet entwickelt.

ZIELGRUPPE

Dieser Lehrgang richtet sich an UBIT-Mitglieder, IT-Dienstleister:innen und Unternehmensberater:innen und alle Interessierten, die ihr Wissen im Bereich Daten- und Informationssicherheit erweitern möchten.

ZIEL

Die Absolventinnen und Absolventen des Lehrgangs sind durch ihr im Lehrgang erworbenes Wissen in der Lage, Risiken in Unternehmen und von Behörden zu minimieren (z.B. Verhinderung von Gesetzesverstößen, Bußgeldern, u.v.m.) sowie Imageverluste und Kosten als Folge von Datenschutzverstößen oder Defiziten im Bereich Informationssicherheit zu vermeiden.

Der Lehrgang bietet einen umfassenden Mix zwischen rechtlichen Grundlagen, technischen und organisatorischen Maßnahmen und der Lehre aus der IT-Betriebsführung und gewährleistet dadurch den größtmöglichen Lernerfolg für die Teilnehmerinnen und Teilnehmer und Nutzen im Unternehmen.

STRUKTUR UND METHODIK

- Vortrag, Diskussionen im Plenum und in Arbeitsgruppen
- 7 Live-Webinare, 28 Unterrichtseinheiten
- Einbringung und Aufarbeiten von Fallstudien der Teilnehmerinnen und Teilnehmer bzw. der Trainerin und des Trainers

ABSCHLUSS
Die Absolventinnen und Absolventen erhalten eine Teilnahmebestätigung.

Option: Ergänzende Zertifizierung „Data & IT Security Expert" bei Erfüllung der Zulassungskriterien gem. Zertifizierungshandbuch.

SEMINARORT
Distance-Learning via Online-Tool Zoom

KOSTEN
Die Kosten für den Lehrgang betragen **1.560,00 Euro** (zzgl. USt.).
Die im Kurspreis enthaltenen Kursmaterialien werden in digitaler Form zur Verfügung gestellt.
Sie erhalten vor Kursbeginn eine Rechnung an die von Ihnen angegebene Rechnungsadresse.
Die Zahlung erfolgt bis spätestens 14 Tage vor Kursbeginn. Die Teilnahme ohne Bezahlung des Teilnahmebeitrages ist nicht möglich.
Bankverbindung: Raiffeisen-LB NÖ-Wien, IBAN: AT92 3200 0000 1040 1289, BIC: RLNWATWW

FÖRDERMÖGLICHKEITEN

JETZT QR – CODE SCANNEN UND GLEICH ANMELDEN!

ANMELDUNG
Bitte melden Sie sich über unsere Termin-Website zu dem Lehrgang Data und IT Security an.
Anmeldeschluss ist vier Wochen vor Lehrgangsbeginn.
Wir weisen darauf hin, dass die Anmeldungen nach Datum des Einlangens berücksichtigt werden.
Aufgrund der begrenzten Seminarplätze wird eine rasche Anmeldung empfohlen.
Der Lehrgang findet mit mindestens acht und maximal 26 Teilnehmerinnen und Teilnehmern statt.

DAS PROGRAMM IM DETAIL

Rechtliche Vorgaben: Grundlagen des Datenschutzrechts
- Einführung in die Datenschutzgrundverordnung (DSGVO)
- Begriffsbestimmungen (Personenbezug, Daten, Verarbeitung, sensible Daten)
- Rollen im Datenschutz (Verantwortliche, Auftragsverarbeiter, Betroffene)
- Spielregeln im Datenschutz (Grundsätze, Rechtmäßigkeit, Einwilligung,
- Das österreichische Datenschutzgesetz (DSG) und Spezialregeln in Österreich

Vertiefendes Datenschutzwissen Allgemein
- Betroffenenrechte (Informationen, Löschung, Auskunft)
- Dokumentation im Datenschutz
- Risikoanalysen, Datenschutzfolgenabschätzungen und Meldepflichten
- Internationaler Datentransfer

Vertiefendes Datenschutzwissen: Datensicherheit Einführung
- Was bedeutet Datensicherheit lt. DSGVO?
- Privacy by Design / Privacy by Default
- Data Breach Notification

Vertiefendes Datenschutzwissen: ePrivacy

- Datenschutzkonforme Webseiten
- Tracking, Cookies, Webseitenanalysen
- Unerbetene Nachrichten (Spam, Cold Calling)

Cybersicherheits-Richtlinie NIS2

- Überblick über die NIS-Gesetzgebung und die NIS2-Richtlinie
- Anwendungsbereich/Betroffenheit
- Risikomanagementmaßnahmen im Unternehmen
- Meldepflichten
- Aufsicht und Strafen

Datenschutz- und IT-Compliance

- Umsetzungsplanung der DSGVO
- Bestellung einer oder eines Datenschutzbeauftragten
- Verfahrensverzeichnis
- Datenschutz-Folgenabschätzung
- Data Protection by Default und by Design
- Data Breach Notification Duty
- Internationaler Datenverkehr
- Technische und organisatorische Maßnahmen
- Haftung und Sanktionen
- Aufsichtsbehörde

Grundlegende Überlegungen: IT-Sicherheitsstrategie & Risikomanagement

- Identifikation strategischer Sicherheitsziele und Ableitung einer IT-Sicherheitsstrategie
- Erhebung unternehmensrelevanter Geschäftsprozesse und der diese unterstützenden IT-Infrastruktur
- Klassifikation von Unternehmenswerten
- Sicherheitsaspekte bei Outsourcing, Cloud Computing & Zusammenarbeit mit Externen
- Kernkomponenten und Aufbau eines Risikomanagementprozesses
- Möglichkeiten und Quellen zur Identifikation relevanter Bedrohungen für die IT-Infrastruktur
- Planung und Umsetzung geeigneter Sicherheitsmaßnahmen
- Umgang mit Restrisiken
- Exkurs ISMS
- Überblick über relevante Standards und verfügbare Tools
- Praxisbeispiele

Expertenstatement zur Cyberkriminalität

Netzwerksicherheit – Endpointmanagement

- Überblick Cyberkriminalität
- Nutzungsverbot nicht betrieblicher Software
- Grundlagen netzwerktechnischer Sicherheitsmaßnahmen (Firewalls, WLAN, ...)
- Einsatz eines Verschlüsselungsproduktes für Arbeitsplatzsysteme
- Auswahl von Passwörtern/ Zwei-Faktor-Authentifizierung
- Technischer Virenschutz und Notfallmaßnahmen
- Rechtsstruktur auf Arbeitsplatzrechnern
- Gefahrenquelle Wechselmedien

- Kurzüberblick relevanter Normen und Standards für KMUs

DSGVO & NIS 2 - Umsetzung von risikominimierenden Maßnahmen

- Verpflichtende Maßnahmen nach DSGVO
- Verpflichtende Maßnahmen nach NIS 2

Betriebsführung von IT-Systemen

- Verfahren für die Verwaltung von IT-Systemen
- Überwachung von Systemen
- Umgang mit Personal
- Sicherheitssensibilisierung und -schulung
- Abwehr von Social Engineering Angriffen
- Unabhängige Sicherheitsüberprüfungen

Identitäts und Berechtigungsmanagement

- Verwaltung von Identitäten und Berechtigungen
- Authentifizierungsmechanismen
- Prüfung und Audits
- Single Sign-On, Identity Federation und Cloud Services

Supply-Chain Management und sichere Software

- Umgang mit Lieferanten und Dienstleistern
- Bewertung der Sicherheit von Softwareprodukten
- Umgang mit Schwachstellen
- Einsatz von Kryptographie

Datensicherung & Notfallmanagement

- Datensicherungskonzept und -planung
- Sicherungsverfahren
- Datenlöschung / Entsorgung von Daten
- Umgang mit Sicherheitsvorfällen
- Notfallvorsorge

Physische Infrastruktur

- Baulich-organisatorische Maßnahmen
- Zutrittskontrollen, Schlüsselverwaltung
- Stromversorgung, Klimatechnik, Brandschutz

KMU.Digital

Vortagende

Mag. Ursula Illibauer

Mag. Ursula Illibauer ist seit April 2015 als Juristin in der Bundessparte Information und Consulting der Wirtschaftskammer Österreich beschäftigt. Zu ihren Aufgabengebieten zählen insbesondere Konsumentenschutzrecht, E-Commerce Recht und Datenschutz. Hauptaugenmerk liegt hierbei in der Beratung von Unternehmen sowie in der Gesetzesbegutachtung. Sie ist zudem Vortragende und auch publizistisch tätig.

Dipl.-Ing. Philipp Reisinger, BSc

Philipp Reisinger (CISA, CISSP) ist Consultant bei SBA-Research – einem Forschungszentrum für Informationssicherheit und IT-Sicherheitsdienstleister.
Seine primären Tätigkeitsgebiete sind die Beratung von Unternehmen zu organisatorischen Aspekten der Informationssicherheit, ISO 27001 Zertifizierungsbegleitung sowie die Durchführung von Audits, Risikoanalysen und Sicherheitsbewusstseinsschulungen. Außerdem ist er als Trainer und Lektor aktiv.

Ing. DI Thomas Bleier MSc

ist Eigentümer und Geschäftsführer der B-SEC better secure KG mit den Schwerpunkten IT-Security Assessments, Audits und Trainings – insbesondere im Bereich industrieller Automatisierungstechnik (OT/ICS). Neben seiner Tätigkeit als Auditor im Bereich Informationssicherheit ist er als Security-Trainer und FH-Lektor tätig.

©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 und Board Member des Frauennetzwerks Women4Cyber Austria, Mitglied der ENISA Ad Hoc Working Group on Enterprise Security, zertifizierte Information Security Managerin und ausgebildete Wirtschaftstrainerin.

Ing. Joseph M. Riedinger

leitete die Cybercrime Unit des Landeskriminalamts Niederösterreich und sammelte umfassende Erfahrung in digitaler Forensik und der Bearbeitung von Cyberkriminalität. Er war Konsulent des Bundeskriminalamtes und Berater für die Finanzmarktaufsicht Österreichs. Zusätzlich ist er als Lektor an der Fachhochschule Wiener Neustadt tätig und hält Vorträge zu "Digitale Forensik & Cybercrime" an verschiedenen Akademien und Veranstaltungen im Banken-, Gewerbe- und Industriesektor sowie für die WKO. Als Gründer und Eigentümer der Unternehmen COGITO-IT Datacenter Systemhaus GmbH und TECHNOLUTION Cyber Security Consulting GmbH betreut Ing. Riedinger hochsensible Kunden im Bereich Netzwerk und Security. Er lebt damit also direkt am Puls der Informationstechnologie und ihren Gefahren!

Mag. Michael Schützenhofer, CMC

Michael Schützenhofer ist Wirtschaftsinformatiker und Humanist. Nach Stationen als Programmierer, IT-Lehrer, IT-Dienstleister, IT-Leiter und zuletzt Geschäftsführer einer Marken- und Digitalagentur wechselte er in die Unternehmensberatung und kehrte auch wieder in die Lehre zurück. Sein Beratungsschwerpunkt liegt in der strategischen Unternehmensführung mit Fokus auf Digitalisierung und KI. Dabei motiviert er zum Denken "out of the box". Daneben unterrichtet er an Fachhochschulen und Akademien und begeistert Menschen mit Keynotes zu diesen Themen.

Art	Termin 1 Am Vormittag + Gastvorträge am Nachmittag	Termin 2 Am Nachmittag
ONLINE	13.04. 9:30-13:00 • Grundlegende Überlegungen: IT-Sicherheitsstrategie & Risikomanagement **Vortragender:** Dipl.-Ing. Philipp Reisinger, BSc	07.09. 13:30-17:00 • Grundlegende Überlegungen: IT-Sicherheitsstrategie & Risikomanagement **Vortragender:** Dipl.-Ing. Philipp Reisinger, BSc
	13.04. 13.30-15.00 • KMU.Digital **Vortragender**: Mag. Michael Schützenhofer, CMC	08.09. 13:30-17:00 • Netzwerksicherheit – Endpointmanagement **Vortragender:** Dipl.-Ing. Philipp Reisinger, BS
	14.04. 9:30-13:00 • Netzwerksicherheit – Endpointmanagement **Vortragender:** Dipl.-Ing. Philipp Reisinger, BS	14.09. 13:30-17:00 • NIS 2 Anforderungen und Rahmenbedingungen • DSGVO & NIS 2 – Umsetzung risikominimierender Maßnahmen • Betriebsführung von IT-Systemen **Vortragende:** Ing. DI Thomas Bleier MSc Mag. Verena Becker, BSc (WU
	15.04. 9:30-13:00 • Rechte und Pflichten aus der DSGVO • Datenschutz- und IT-Compliance **Vortragende:** Mag. Ursula Illibauer	15.09. 13:30-17:00 • Identitäts- und Berechtigungsmanagement • Supply-Chain Management und sichere Software • Datensicherung & Notfallmanagement • Physische Infrastruktur **Vortragender:** Ing. DI Thomas Bleier MSc
	16.04. 9:30-13:00 • Rechte und Pflichten aus der DSGVO • Datenschutz- und IT-Compliance **Vortragende:** Mag. Ursula Illibauer	23.09. 17:00-19:00 • Expertenstatement **Gastvortrag**: Ing. Joseph M. Riedinger
	20.04. 9:30-13:00 • NIS 2 Anforderungen und Rahmenbedingungen • DSGVO & NIS 2 – Umsetzung risikominimierender Maßnahmen • Betriebsführung von IT-Systemen **Vortragende:** Ing. DI Thomas Bleier MSc Mag. Verena Becker, BSc (WU)	28.09. 13.30-15.00 • KMU.Digital **Vortragender**: Mag. Michael Schützenhofer, CMC
	21.04. 9:30-13:00 • Identitäts- und Berechtigungsmanagement • Supply-Chain Management und sichere Software • Datensicherung & Notfallmanagement • Physische Infrastruktur **Vortragender:** Ing. DI Thomas Bleier MSc	29.09. 13:30-17:00 • Rechte und Pflichten aus der DSGVO • Datenschutz- und IT-Compliance **Vortragende:** Mag. Ursula Illibauer
	22.04. 17:00-19:00 • Expertenstatement **Gastvortrag**: Ing. Joseph M. Riedinger	30.09. 13:30-17:00 • Rechte und Pflichten aus der DSGVO • Datenschutz- und IT-Compliance **Vortragende:** • Mag. Ursula Illibauer

Ihre Ansprechpersonen

KURSANMELDUNG:

Mgr. Zuzana Rajcsányi-Buchtová, Akad. M&S (WU)
Telefon: 05 90900 – 3797
E-Mail: zuzana.buchtova@incite.at
MS Bookings Beratungstermin gleich buchen

ZERTIFIZIERUNGEN:

Carolin Eder
Telefon: 05 90900 – 3794
E-Mail: carolin.eder@incite.at

UBIT.Akademie incite

Wiedner Hauptstraße 57, 1040 Wien
www.incite.at
E-Mail: office@incite.at
Telefon: 05 90 900 – 3792
Linktree