Seminar

CYBERSECURITY KOMPAKT & NIS2

Informationssicherheit rechtlich, organisatorisch und technisch
Cybersicherheitsgesetz, NIS2

Referenten

Ing. Franz **Hoheiser-Pförtner**, MSc / Ing. Dr. iur Christof **Tschohl**

Details

Zeit

Dienstag, 18.06.2024 09:00-13:00 Uhr vor Ort: Florianigasse 55/10, 1080 Wien

Ort

vor Ort:
Florianigasse 55/10, 1080 Wien
Research Institute – Digital Human Rights Center

Zertifizierung

Die Veranstaltung wird von Austrian Standards als Weiterbildungsveranstaltung für die Rezertifizierung als Datenschutzbeauftragte*r anerkannt.

Inhalt

Organisationen der kritischen Infrastruktur sind elementarer Bestandteil unseres Lebens und gewährleisten die Grundversorgung unserer Gesellschaft. In ihren Prozessen setzen diese Organisation wesentlich auf die Nutzung vernetzter Technologien sowie Informations- und Kommunikationssysteme.

Das Seminar bietet ein workshopbasiertes Training zu ***„Cyber Security (NIS2)“,*** in dem anhand konkreter Fallbeispiele aus der realen Welt verschiedene sicherheitskritische Szenarien in Zusammenhang mit der Digitalisierung, Vernetzung und Interoperabilität zentraler gesellschaftlicher Infrastruktur durchgespielt werden. Unter Heranziehung spezifischer Policies und Werkzeuge erarbeiten die Teilnehmer*inne unter Vorgaben der Trainer passende Lösungen für die einzelnen Phasen des Krisenszenarios. Auf diese Weise werden Lücken (Gaps) im System anschaulich aufgezeigt und richtige Strategien und Vorgangsweisen dargestellt.

Ihr persönlicher Nutzen

- Ziel des Seminars ist es Ihnen eine praktische Hilfestellung zur Identifizierung und Vermeidung von sicherheitstechnischen Risiken zu geben sowie robuste (resiliente) IT-Infrastrukturen zu implementieren und zu managen ***(Welche Aufgaben hat ein Krisenstab und wie stellt man ihn zusammen? Was sind die Eckpfeiler effektiver Vorbereitung? Was sind die größten Herausforderungen eines Krisenmanagements?).***
- Es werden umfassende Details zur rechtskonformen Implementierung von Sicherheitsstandards für IT-Netzwerken vorgestellt ***(ISO 27000-Serie „Informationssicherheitsmanagement“, ÖNORM D 4900-Serie „Risikomanagement für Organisationen und Systeme“, ONR 17091 „Krisenmanagement - Strategische Grundsätze“ usw).***
- Sie werden mit technischen und organisatorischen Maßnahmen und Strategien zur Gewährleistung der IT-Resilienz vertraut gemacht ***(Welche Dokumente müssen bei einer NIS2-Prüfung vorliegen? Welche Rollen spielen bestehende Zertifizierungen und Risikomanagement? Wie können sich Unternehmen in organisatorischer und technischer Hinsicht auf eine NIS2-Prüfung vorbereiten?).***
- Sie erhalten einen umfassenden Überblick zu aktuellen rechtlichen Fragen der Netz- und Informationssicherheit ***(Europäische und innerstaatliche Rechtsgrundlagen - Verordnungen, Richtlinien und Gesetze; Normative Sicherheitsanforderungen und Zusammenspiel von Netz- und Informationssystemsicherheitsgesetz (NISG) und Datenschutzgrundverordnung (DSGVO); Data Breach Notification gem NISG und DSGVO; Rechtsakt zur EU-Cybersicherheit und Ausblick auf NIS II).***

Zielgruppe

- Unternehmen und Betreiber von Diensten in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur sowie Personen aus der öffentlichen Verwaltung
- Personen, die mit der Umsetzung NIS-Vorgaben konfrontiert sind wie Mitarbeiter von IT-Abteilungen, Netzwerktechniker, Risikomanager, Chief Information Security Officer sowie Juristen und Gerichtssachverständige

Programm

5 min	**Begrüßung & Vorstellung** **Christof Tschohl, Franz Hoheiser-Pförtner,**
1 h 55 min	**Phase 1: Rahmen** – Grundlagenvermittlung: rechtlich, technisch und organisatorisch – Prozesse, Leitfäden und Policies – Abläufe, Dynamiken, Reaktionen – Strategische Grundsätze
15 min	**Kaffeepause**
25 min	**Phase 2: Praxis-Beispiele** – Sicherheitsvorfälle und Meldepflichten – Dokumentation und Zertifizierungen – Krisenszenarien und Resilienz
20 min	**Phase 3: Diskussion und Reflexion** – Reflexion der Ergebnisse – Fragen und Diskussion – Ausblick und Verabschiedung

Referenten

Franz Hoheiser-Pförtner

Ing. Franz Hoheiser-Pförtner, MSc. beschäftigt sich seit vielen Jahren mit dem Thema Informationssicherheit im Gesundheitswesen. Wobei Prävention und Sicherheitsmanagement aus seiner Sicht zwei wichtige Säulen für die ganzheitliche Betrachtung von Hygienemaßnahmen in digitalen Prozessen sind. Im Gesundheitswesen ist Saftey für (be)handelten Menschen immer schon ein wichtiges Thema und wird immer mehr auch durch Security erweitert.

Er ist Gründungsmitglied und Vorstandsmitglied der "Cyber Security Austria" (CSA), die die Cybersicherheit der strategischen Infrastruktur Österreichs fördert. Seit 2012 fördert die CSA die Ausbildung junger Talente durch die "Austria Cyber Security Challenge" und seit 2014 durch die "European Cyber Security Challenge".

Neben seiner beruflichen Laufbahn unterrichtet er an Fachhochschulen, Informationssicherheit und Cybersicherheit für E-Health-Anwendungen und technische Perspektiven. Das Resilienz-Management für klinische und nicht-klinische Gesundheitsprozesse ist eine seiner Schwerpunkte bei wissenschaftlichen und beruflichen Aktivitäten.

Christof Tschohl

Ing. Dr. Christof Tschohl ist wissenschaftlicher Leiter und Gesellschafter des Research Institute – Digital Human Rights Center. Er ist Nachrichtentechniker, promovierter Rechtswissenschaftler, Vorstandsmitglied in der Datenschutz-NGO „noyb“, Arbeitskreisleiter in der Österreichischen Computergesellschaft (OCG) sowie Mitglied der Fachgruppe Grundrechte der österreichischen Richtervereinigung und im CERT-Beirat der Republik Österreich.

Anmeldung

Teilnahmegebühr
Preis pro Person: 420,- € (exkl. USt.)

Ermäßigung
20 % für Network-Member (network.fair.data) – www.networkfairdata.at

10 % für Frühbuchende bis eine Woche vor dem Event.
Geben Sie bei Buchung bitte den **Gutscheincode mit dem Datum ihres Events** an:

Code: "**Cyber18Juni**" bei Buchung bis 11.06.2024

Buchung unter
www.researchinstitute.at/academy

Der Kurs findet ab 5 Teilnehmer*innen statt und ist auf 20 Personen beschränkt.

Customer Service

Für Fragen zum Seminar, der Buchung oder Rabatten:

T: +43 699 107 010 74
M: office@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center

Büro: Florianigasse 55/10, 1080 Wien
Telefon: +43 1 524 3 524 – 0
E-Mail: kontakt@researchinstitute.at

FN: 355966f, HG Wien, **UID:** ATU66270867
Sitz: Amundsenstraße 9, 1170 Wien

Erste Bank AG
IBAN: AT112011129541798300
BIC: GIBAATWWXXX

Nach Eingang der Anmeldung erhalten Sie eine Anmeldebestätigung sowie Ihre Rechnung per E-Mail. Die Teilnahmegebühr muss spätestens 14 Tage vor Beginn der Veranstaltung auf unserem Konto eingelangt sein. Bitte beachten Sie, dass der Einlass zur Veranstaltung nur gewährt werden, wenn die Zahlung bei der Research Institute AG & Co KG eingelangt ist oder am Veranstaltungstag direkt erfolgt. Sollte es Ihnen nicht möglich sein den Veranstaltungstermin wahrzunehmen, können Sie Ihren Seminarplatz selbstverständlich weitergeben bzw eine:n Vertreter:in entsenden. Für weitere Details siehe unsere Allgemeinen Geschäftsbedingungen abrufbar unter: https://researchinstitute.at/agb.