ditis TRAINING CENTER
SKILLED FOR THE DIGITAL FUTURE

ditis Veranstaltungskatalog 2022

Ausbildungen, Best-Practice Workshops und Online-Seminare

ditis Training-Center für Datenschutz, Cyber-Security und digitale Produktentwicklung

Ihr Mehrwert – Skilled for the Digital Future

Unsere Trainings verbinden individuelle Beratung mit praxisorientierten Workshops und Ausbildungen.

In unseren Veranstaltungen erfahren Sie von Praktikern für Praktiker, wie Sie Fragestellungen aus dem Alltag rund um Datenschutz, Informationssicherheit, IT-Security und die digitale Produktentwicklung fachlich kompetent lösen.

Die Veranstaltungen sind in sich abgeschlossen und einzeln buchbar.

Veranstaltungsort

Präsenzveranstaltungen finden im Voith Trainingscenter in Heidenheim statt. Im Einzelfall abweichende Veranstaltungsorte werden im Vorfeld bekanntgegeben.

Aufgrund der aktuellen Pandemiesituation werden bis auf weiteres alle Veranstaltungen online durchgeführt.

Workshop-Dauer

Sofern nicht anders angeben, beginnen die Workshops um 9:00 Uhr und enden um 17:00 Uhr.

Bewirtung

Bei Präsenzveranstaltungen ist die Bewirtung für die Dauer der Veranstaltung enthalten.

Übernachtung

Für die mehrtägigen Veranstaltungen empfehlen wir Ihnen gerne ein Hotel zur individuellen Buchung.

Kostenfreie Online-Seminare

Zu unseren regelmäßig stattfindenden Online-Seminaren können Sie sich direkt auf unserer Homepage unter www.ditis.de im Bereich Veranstaltungen anmelden.

1 Veranstaltungsübersicht

1.1 Best-Practice Workshops

Kurs-Nr.	Titel	Datum
IS-01	Was bedeutet das neue IT-Sicherheitsgesetz 2.0 für die Zulieferindustrie und den Maschinenbau?	21.03.2022
DPS-01	So wäre aus der Schwachstelle „Log4Shell“ kein Problem geworden: Security Requirements Engineering – Sicher Software entwickeln	27. - 28.04.2022
ISM-03	Ransomware und der Incident Response Plan – in der Theorie wissen alle Bescheid: Wir üben den Ernstfall.	28.04.2022
DS-03	Microsoft Teams für Datenschützer – Einführung und Betrieb datenschutzfreundlich gestalten	03.05.2022
IS-02	Industrial Hacking – Cybersecurity 4.0	04.05.2022
DPS-01	So wäre aus der Schwachstelle „Log4Shell“ kein Problem geworden: Security Requirements Engineering – Sicher Software entwickeln	17. - 18.05.2022
IS-01	Was bedeutet das neue IT-Sicherheitsgesetz 2.0 für die Zulieferindustrie und den Maschinenbau?	18.05.2022
IS-03	Industrial Product Security - Risiken und Chancen bei der Entwicklung von cybersicheren Produkten für die Industrie 4.0	18.05.2022
IS-02	Industrial Hacking – Cybersecurity 4.0	06.07.2022
IS-03	Industrial Product Security - Risiken und Chancen bei der Entwicklung von cybersicheren Produkten für die Industrie 4.0	20.07.2022
IS-02	Industrial Hacking – Cybersecurity 4.0	07.09.2022
IS-03	Industrial Product Security - Risiken und Chancen bei der Entwicklung von cybersicheren Produkten für die Industrie 4.0	21.09.2022
DPS-01	So wäre aus der Schwachstelle „Log4Shell“ kein Problem geworden: Security Requirements Engineering – Sicher Software entwickeln	27. – 28.09.2022
IS-02	Industrial Hacking – Cybersecurity 4.0	02.11.2022

Kurs-Nr.	Titel	Datum
IS-03	Industrial Product Security - Risiken und Chancen bei der Entwicklung von cybersicheren Produkten für die Industrie 4.0	16.11.2022
DPS-01	So wäre aus der Schwachstelle „Log4Shell“ kein Problem geworden: Security Requirements Engineering – Sicher Software entwickeln	16. – 17.11.2022
DS-02	Aufbautraining: Datenschutzaspekte in Microsoft 365	Auf Anfrage
DS-04	Aufbautraining: Datenschutzaspekte zu Microsoft SharePoint & OneDrive - Der Standardspeicherort mit internationalen Fragezeichen?	Auf Anfrage
DS-05	Videokonferenzsysteme aus datenschutzrechtlicher Sicht bewerten: Funktionen, Vertragsgestaltung, Sicherheitskriterien	Auf Anfrage
ISM-01	Ready for ISMS – Das umfassende und praxisnahe Training für Informationssicherheitsverantwortliche	Auf Anfrage
ISM-05	SO/IEC 27701 – Integriertes Managementsystem für Datenschutz und Informationssicherheit	25.11.2022

1.2 Ausbildung mit optionaler Prüfung

Kurs-Nr.	Titel	Datum
DPS-02	Ausbildung zum „Data Privacy Software Engineer“	17. – 20.10.2022
DPS-03	Prüfung zum „Data Privacy Software Engineer“	21.10.2022

1.3 Kostenfreie Online-Seminare

Zu unseren regelmäßig stattfindenden Online-Seminaren zu Themen rund um Datenschutz, Informationssicherheit, IT-Security und Digitaler Produktsicherheit können Sie sich direkt auf unserer Homepage www.ditis.de im Bereich Veranstaltungen anmelden.

Online-Seminar	Datum
IEC 62443 für Hersteller im Maschinen- und Anlagenbau – Übersicht und Vorgehensweise	Termine und Anmeldung über unsere Homepage
Was bedeutet Privacy und Security by Design für die Entwicklung digitaler Produkte?	Termine und Anmeldung über unsere Homepage
ditis InfoSec-Manager Automotive – Betrieb eines Managementsystems nach ENX TISAX	Termine und Anmeldung über unsere Homepage
TISAX® 5.0 - Inhalte, Änderungen und Handlungsempfehlungen	Termine und Anmeldung über unsere Homepage
Was bedeutet UNECE R155/R156 und ISO/SAE 21434 für Zulieferer der Automobilindustrie?	Termine und Anmeldung über unsere Homepage

2 Detaillierte Beschreibung

2.1 Best-Practice Workshops

Kurs-Nr.	Beschreibung
DS-01	„Microsoft 365 Einführung - Was tun als Datenschutzbeauftragter?“ Ihr Unternehmen steht vor der Entscheidung Microsoft 365 einzuführen oder steht kurz vor der Umsetzung. Bei der Einführung neuer Lösungen, gerade wenn sie so komplex sind wie Microsoft 365 gibt es neben den von Microsoft genannten Vorteilen jedoch einiges zu beachten, damit Ihr Unternehmen den Anforderungen der DSGVO gerecht wird. Wir geben Ihnen einen Überblick über Module und Services, die relevanten datenschutzrechtlichen Anforderungen und beantworten Ihre Fragen dazu. Sie erhalten konkrete Hinweise zur Vertragsgestaltung mit Microsoft und Dienstleistern sowie Muster-Checklisten für die Begleitung bei der Einführung von Microsoft 365. Inhalte des Trainings • Überblick Microsoft 365 (Module und Services: z.B. Teams, OneDrive, SharePoint, Graph, Delve…) • Cloud-Strategie, Geolokation der Verarbeitungen, Verschlüsselung, rechtliche Rahmenbedingungen • Relevante datenschutzrechtliche Anforderungen bei der Einführung • Aktuelle Ansichten der Aufsichtsbehörden • Konkrete Vertragsgestaltung mit Microsoft und Dienstleistern bei der Einführung • Eckpfeiler des Projektablaufs bei der Einführung von Microsoft 365 beginnend bei der Cloud-Strategie bis zum Betrieb • Microsoft 365 im Verzeichnis der Verarbeitungstätigkeiten • Einbindung der Mitbestimmung z.B. Leistungs- und Verhaltenskontrolle) • Fragen & Diskussionen Zielgruppe: Datenschutzbeauftragte, Datenschutzkoordinatoren, Verantwortliche für die Einführung von M365 Dauer: 1 Tag Kurssprache: Deutsch Kosten: 420 EUR pro Teilnehmer Die Teilnehmer erhalten nach Anschluss der Veranstaltung eine Teilnahmebescheinigung.

Kurs-Nr.	Beschreibung

DS-02	**Aufbauseminar: Datenschutzaspekte in Microsoft 365 - Auditierung, Drittstaatentransfer, Rechtsgrundlagen, Löschung und Berechtigungen, Dokumentation, Einblick in das Admin-Center für DSBs**
	
	M365 ist in Ihrem Unternehmen bereits bekannt, Sie verfügen bereits über Grundkenntnisse der datenschutzrechtlichen Betrachtung von M365 und haben erste praktische Schritte in der Dokumentation unternommen.
	
	Dieser Kurs vermittelt Ihnen vertiefte Kenntnisse zu ausgewählten Detail-Themen wie z.B. Drittstaatentransfer, Auditierung und Connected Experiences.
	
	Ergänzend geben wir Hinweise für datenschutzfreundliche Gestaltungsmöglichkeiten. Darüber hinaus zeigen wir Ihnen, welche Prüfschritte bei der Bewertung von Microsoft als Dienstleister erforderlich sind. Dies umfasst sowohl die vertragliche Gestaltung als auch Dokumente im Trust-Center. Ferner werfen wir einen Blick in die Administrationswelt von M365.
	
	Inhalte des Trainings
	
	• Vertragliche Grundlagen im Kontext M365: Was gilt es hier zu beachten?
	• Drittstaatentransfer:
	  ○ Wie ist die aktuelle Lage?
	  ○ Ergänzende Dokumentationsanforderungen
	• Einsatz einzelner Dienste an einem ausgewählten Beispiel:
	  ○ Verarbeitungsverzeichnis
	  ○ Rechtsgrundlagen
	• Einblick in die Administrationswelt von M365 für Datenschützer, inkl. Compliance Center und ausgewählter Datenschutzaspekte zu
	  ○ Lösch- und Aufbewahrungsfristen
	  ○ Berechtigungen
	• Herausforderungen beim Einsatz von Connected Experiences
	  ○ Vertragliche Einordnung
	  ○ Datenschutzrelevante Einstellmöglichkeiten
	
	Zielgruppe:
	
	Datenschutzbeauftragte, Datenschutzkoordinatoren
	
	Dauer: 1 Tag
	
	Kurssprache: Deutsch
	
	Kosten: 420 EUR pro Teilnehmer
	
	Die Teilnehmer erhalten nach Anschluss der Veranstaltung eine Teilnahmebescheinigung.

Kurs-Nr.	Beschreibung
DS-03	**Microsoft Teams für Datenschützer – Einführung und Betrieb datenschutzfreundlich gestalten** Der breite Funktionsumfang von Teams gestattet die Nutzung in nahezu jedem Unternehmensprozess. Hierbei steht der Datenschutz vor der Herausforderung, durch entsprechende Vorgaben die Nutzung datenschutzfreundlich zu gestalten. Das Seminar vermittelt Ihnen dazu die notwendigen Kenntnisse. Die Berücksichtigung von Datenschutzaspekten in Microsoft Teams erfordert die Einbindung und Koordination verschiedener Bereiche im Unternehmen, u.a. IT, Fachabteilungen, Datenschutzorganisation und Betriebsrat. In diesem Seminar erhalten Sie das notwendige Rüstzeug, um diese Themen mit allen Beteiligten auf Augenhöhe zu diskutieren. Die umfangreichen Konfigurationsmöglichkeiten von Teams sind wesentlicher Bestandteil einer datenschutzfreundlichen Nutzung. Daher beschränkt sich die Veranstaltung nicht nur auf die Sicht von Datenschutzbeauftragten und Anwender, sondern wirft auch einen Blick auf die zugehörigen Admin-Center. **Inhalte des Trainings** • Überblick über den Funktionsumfang von Microsoft Teams aus der Sicht des Datenschutzes • Microsoft Teams als Bestandteil von Microsoft 365 (Vertragsgestaltung, Ansichten der Aufsichtsbehörden) • Microsoft Teams Dokumentationsanforderungen (Verzeichnis der Verarbeitungen, Abgrenzung Administration zu Verarbeitungen der Fachabteilungen) • Unternehmensvorgaben zur Nutzung von Microsoft Teams (Nutzerrichtlinie) • Datenschutzrelevante Einstellungen in den zugehörigen Admin-Centern inkl. deren Auswirkungen • Zusammenarbeit mit externen Teilnehmern (Arten der Zusammenarbeit, Berechtigungen) • Berücksichtigung von Microsoft Teams in Betriebsvereinbarungen (z.B. Anlage zur BV Microsoft 365) • Umgang mit Apps (Einschränkungsmöglichkeiten, Risiken) **Zielgruppe:** Datenschutzbeauftragte, Datenschutzkoordinatoren, Verantwortliche für die Einführung von M365 **Dauer:** 1 Tag **Kurssprache:** Deutsch **Kosten:** 420 EUR pro Teilnehmer Die Teilnehmer erhalten nach Anschluss der Veranstaltung eine Teilnahmebescheinigung.

Kurs-Nr.	Beschreibung
DS-04	**Aufbauseminar: Datenschutzaspekte zu Microsoft SharePoint & OneDrive - Der Standardspeicherort mit internationalen Fragezeichen?** Kein Speicherdienst wird vergleichbar kontrovers diskutiert und ist dennoch derart allgegenwärtig. Durch die automatische Einbindung bei einer Einführung von M365 entstehen Aufgaben für Datenschützer und Informationstechniker. Dieser Aufbau-Workshop soll helfen zu verstehen, warum. Als Standardinformationsplattform ist SharePoint bei den meisten M365 (Enterprise) Versionen bereits on-premise oder als Online-Dienst im Einsatz. Der Aufbau-Workshop dient dem Erweitern der datenschutzorientierten Betrachtung dieses vielseitigen Tools und nimmt den Zusammenhang zu OneDrive in den Fokus. Zielgruppe Datenschutzbeauftragte, Datenschutzkoordinatoren Dauer: 2 Stunden Kurssprache: Deutsch Kosten: 145 EUR pro Teilnehmer Die Teilnehmer erhalten nach Anschluss der Veranstaltung eine Teilnahmebescheinigung.
DS-05	**Videokonferenzsysteme aus datenschutzrechtlicher Sicht bewerten: Funktionen, Vertragsgestaltung, Sicherheitskriterien** Videokonferenzen erfreuen sich nicht zuletzt auf Grund des vermehrten mobilen Arbeitens immer größerer Beliebtheit. Auch die Einsparung von Reisezeiten begünstigte die Nutzung. Die Corona-Pandemie führte jedoch dazu, dass Systeme oftmals ohne ausreichende Prüfung in Betrieb genommen wurden. In diesem Seminar möchten wir Ihnen aus Sicht des Datenschutzes Grundlagen zur Beschaffung, Einrichtung und Nutzung von Videokonferenzsystemen vermitteln. Dabei blicken wir auf die verschiedenen Funktionen, welche die Dienste neben der eigentlichen Video- und Tonübertragung bereitstellen und prüfen, mit welcher Rechtsgrundlage diese eingesetzt werden können. Welche Systeme, wie beispielsweise FaceTime oder Threema sind alternativ zu den typischen Dienstleistern wie LogMeIn, Zoom oder Teams ebenfalls geeignet? Wir geben Ihnen Hinweise zur Vertragsgestaltung, insbesondere bei der Beauftragung von Dienstleistern in einem Drittland. Was sagen die Aufsichtsbehörden zu dem Thema allgemein bzw. zu den einzelnen Dienstleistern? Mit einem Verweis auf ein Mindestmaß an technischen und organisatorischen Maßnahmen wie beispielsweise Verschlüsselung und Schutz der eigenen Konferenz wird das Seminar abgerundet. Zielgruppe Datenschutzbeauftragte, Datenschutzkoordinatoren Dauer: 2 Stunden Kurssprache: Deutsch Kosten: 145 EUR pro Teilnehmer Die Teilnehmer erhalten nach Anschluss der Veranstaltung eine Teilnahmebescheinigung.

Kurs-Nr.	Beschreibung

ISM-01	**Ready for ISMS – Das umfassende und praxisnahe Training für Informationssicherheitsverantwortliche**
	
	IT-Security-Expertise, Awareness-Guru, Schulterschluss zum Datenschutz, Pressestelle und Rechte Hand der Geschäftsführung - die Verantwortung für Informationssicherheitsmanagement im Unternehmen umfasst viel mehr auf der täglichen Agenda als einfach nur die "Security-Flagge" hochhalten.
	
	Wir zeigen Ihnen in einem kompakten Seminar, was diese Verantwortung an Regelaufgaben umfasst und wie sie mit Anfragen und Spezialthemen aus Fachbereichen umgehen können. Sie erhalten konkrete Hinweise zur Umsetzung normativer Anforderungen und zur Umsetzung im betrieblichen Alltag.
	
	Inhalte des Trainings
	
	• Überblick über Gestaltung von Informationssicherheitsmanagementsystemen
	  ○ Inhalte des ISMS, Schnittstellen / Abgrenzung zu anderen Managementsystemen
	  ○ Normen, Gesetze, Branchenstandards
	  ○ Rolle und Verantwortung im ISMS
	• Ansätze für die Gestaltung regelmäßiger Aufgaben im ISMS
	  ○ Planung und Überwachung von Zielen und Schwerpunkten
	  ○ Maßnahmendefinition / Nachverfolgung
	  ○ Schutzbedarfsfeststellungen und Risikomanagement
	  ○ Interne und externe Audits
	  ○ Dienstleistermanagement
	  ○ Schulungen und Awareness
	  ○ Managementberichte
	  ○ Aktualisierung von Regelungen und Dokumentationen
	• Normative Anforderungen zu Anfragen / Themen aus allen Fachbereichen
	  ○ Projektmanagement / Änderungsmanagement
	  ○ Sicherheitsvorfälle und Meldung Richtung Behörden / Kunden
	  ○ IT-Sicherheit
	  ○ Personalsicherheit
	  ○ Gebäudemanagement
	• Fragen & Diskussionen
	
	Zielgruppe
	
	Informationssicherheitsbeauftragte, Informationssicherheitskoordinatoren
	
	Dauer: 3 Tage
	
	Kurssprache: Deutsch
	
	Kosten: 1.920 EUR pro Teilnehmer
	
	Die Teilnehmer erhalten nach Anschluss der Veranstaltung eine Teilnahmebescheinigung.

Kurs-Nr.	Beschreibung
ISM-02	Ransomware – eine reale Bedrohung für Unternehmen: Prävention und Management des Ernstfalls. Das Schreckgespenst Ransomware ist in aller Munde – wir sprechen in dieser Veranstaltung mit: • Geschäftsführern ehemals betroffener Unternehmen, • Cybersicherheitsexperten, • Großschadensspezialisten • Krisenmanager darüber. Zielgruppe: IT-Leiter, CIO, CISO, Informationssicherheitsbeauftragte Dauer: 3,5 Stunden Kurssprache: Deutsch Kosten: 380 EUR pro Teilnehmer
ISM-03	Ransomware und der Incident Response Plan – in der Theorie wissen alle Bescheid: Wir üben den Ernstfall. Das Seminar untergliedert sich in zwei Phasen: **Teil 1: Die Vorbereitung auf den Ernstfall** Auf Basis unserer Praxiserfahrung zeigen wir die wichtigsten technischen und organisatorischen Bestandteile auf, die für die erfolgreiche Bewältigung des Ernstfalls Ransomware in der Praxis benötigt werden und die Teil eines funktionierenden Incident Response Plans sein müssen. **Teil 2: Die Übung des Ernstfalls** Auf Basis der in Teil 1 aufgezeigten technischen und organisatorischen Bestandteile durchlaufen wir die einzelnen Phasen eines Ransomware-Vorfalls. So lernen Sie die Fallstricke des Ernstfalls kennen, bevor er eintritt. Unsere Referenten betrachten das Thema aus der Sicht der: Organisation: Tobias Adrian (Informationssicherheitsmanagement - ditis) Technik: Johannes Eberleh (Cybersicherheitsexperte – ditis) Zielgruppe: IT-Leiter, CIO, CISO, Informationssicherheitsbeauftragte Dauer: 4,5 Stunden Kurssprache: Deutsch Kosten: 420 EUR pro Teilnehmer

Kurs-Nr.	Beschreibung
ISM-05	**ISO/IEC 27701 – Integriertes Managementsystem für Datenschutz und Informationssicherheit** Datenschutz und Informationssicherheit – im Kern geht es beiden Disziplinen um den Schutz von Daten und sensiblen Informationen. Doch scheinbar ewig verlaufen die Anstrengungen, parallel zueinander diese Ziele zu erreichen anstatt harmonisiert. Trotz unterschiedlicher Vorschriften, Standards und Gesetze ergibt sich eine Vielzahl an Schnittstellen, um dieser dynamischen Entwicklung zu begegnen. Der neue ISO-Standard zum Datenschutz, die ISO/IEC 27701 ist die erste zertifizierbare Norm für Datenschutzmanagementsysteme, die auf Basis eines ISO/IEC 27001-Zertifikats als „Add-on“ zum Informationssicherheitsmanagementsystem erlangt werden kann. Natürlich müssen Unternehmen, die am europäischen Markt aktiv sind, die gesetzlichen Anforderungen aus der DSGVO einhalten. Warum also eine Zertifizierung des Datenschutzmanagements, wenn es über die gesetzliche Anforderung bereits vorgeschrieben ist? Die Zertifizierung nach ISO/IEC 27701 verleiht einen Vorsprung vor dem Wettbewerb und kann am Markt nachweisen, dass Datenschutz und Informationssicherheit für Sie Priorität haben. Es ist zu erwarten, dass Branchengrößen eine ISO/IEC 27701-Zertifizierung ihrer Lieferanten für die Zusammenarbeit voraussetzen. Für Unternehmen, die bereits ein zertifiziertes Informationssicherheitsmanagement betreiben, ist die Erweiterung mit Hilfe unseres Datenschutzmanagementsystems mit geringem Aufwand zu erreichen. Informieren Sie sich jetzt in unserem Online-Seminar und lassen Sie sich von unseren Experten einen Überblick geben über: • Aufbau eines integrierten Datenschutz- und Informationssicherheitsmanagementsystems • Möglichkeiten, Vorteile und Ablauf der Zertifizierung • Unsere Unterstützung für Sie bei der Zertifizierung Zielgruppe: DSB, ISB, CIO, CISO, Managementsystem-Beauftragte, verantwortliche Manager Dauer: 2 Stunden Kurssprache: Deutsch Kosten: 220 EUR pro Teilnehmer

Kurs-Nr.	Beschreibung
DPS-01	**Workshop: So wäre aus der Schwachstelle „Log4Shell“ kein Problem geworden: Security Requirements Engineering – Sicher Software entwickeln** Um Ihre digitalen Produkte vor Angriffen zu schützen, müssen Sie wissen, wer die Angreifer sind, wie sie vorgehen und was deren Ziele sind. Dazu wird systematisch und methodisch eine vollständige Bedrohungsmodellierung durchgeführt – mit dem Ziel, die Auswirkungen der erkannten Bedrohungen zu reduzieren oder sogar zu eliminieren. In unserem zweitägigen Workshop lernen Sie die theoretischen Grundlagen der Bedrohungsanalyse und die unterschiedlichen Werkzeuge des Security Requirements Engineerings kennen. Mit praktischen Übungen untermauern wir das erlernte Wissen, damit Sie dieses bei ihren täglichen Aufgaben rund um die digitale Produktentwicklung anwenden können. Am ersten Tag werden folgende Themen behandelt: • Security Requirements Engineering – Warum? • Kennen Sie den Unterschied zwischen Bedrohung, Schwachstelle und Gefährdung? • Was ist Security - oder wie entwickeln wir ein sicheres Produkt? • Einsatzort und Sicherheitsumfeld des Produktes – wo soll das Produkt eingesetzt werden? • Was kann schon schief gehen? - Grundlagen und Ablauf einer Bedrohungsanalyse • Wie sicher soll das Produkt sein? Am zweiten Tag erwartet Sie unser Praxisteil, an dem Sie das bereits erlernte Wissen an einem Beispiel anwenden: • Definition von Assets • Analyse des Schutzbedarfs • Bedrohungsanalyse mit Hilfe von S.T.R.I.D.E. • Bewertung von Bedrohungen • Dokumentation von Sicherheitsanforderungen • Ausarbeitung von Abwehrmaßnahmen Zielgruppe: Projektverantwortliche (Projektleiter, Product-Owner, Scrum-Master), Produktmanager, Mitarbeiter / Verantwortliche Entwicklung, Mitarbeiter / Verantwortliche System- oder Softwarearchitektur, Datenschutzverantwortliche für das Produkt Dauer: 2 Tage Kurssprache: Deutsch Kosten: 1.900 EUR pro Teilnehmer Die Teilnehmer erhalten nach Anschluss der Veranstaltung eine Teilnahmebescheinigung.

Kurs-Nr.	Beschreibung
IS-01	**Was bedeutet das neue IT-Sicherheitsgesetz 2.0 für die Zulieferindustrie und den Maschinenbau?** Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist in der Version 2.0 nicht mehr nur für Betreiber kritischer Infrastrukturen relevant. Die Novellierung enthält Erweiterungen und Verschärfungen insbesondere für den Maschinen- und Anlagenbau. Wir haben die Auswirkungen der neuen Gesetzeslage analysiert und die dringenden Handlungsfelder bestimmt. In unserem Workshop erhalten Sie konkrete und praktische Hilfestellung zur vorgeschriebenen Umsetzung. Wir erläutern und diskutieren mit Ihnen u.a. diese Themen: • Grundlagen und wesentliche Inhalte zu IT-SiG 2.0 und NIS2 (Ausblick auf nationale und europäische Gesetzeslage) • Wer ist betroffen? Was sind kritische Komponenten? Neue Sektoren betreffen Komponentenhersteller und Zulieferer • Risiko und Bußgelder steigen drastisch (Meldepflichten und Verantwortlichkeiten) • Was tun? Praktische Handlungsempfehlungen zur Umsetzung von Sofortmaßnahmen und langfristige Strategie Unser Referent Bernd Gehring ist als Arbeitskreissprecher im VDMA-Arbeitskreis „Industrial Security“ tätig und berät bei Voith und vielen unserer Kunden die Verantwortlichen bei der Umsetzung der geforderten Sicherheitsthemen. Zielgruppe: IT-Verantwortliche, CTO, CIO, CISO Dauer: 3 Stunden Kurssprache: Deutsch Kosten: 380 EUR pro Teilnehmer Die Teilnehmer erhalten nach Anschluss der Veranstaltung eine Teilnahmebescheinigung.

Kurs-Nr.	Beschreibung
IS-02	Industrial Hacking – Cybersecurity 4.0 Cyber-Risiken in vernetzten Industrieumgebungen oder: wie einfach es ist, ein Kraftwerk zu hacken Wir berichten aus unserem Praxisalltag und den Erfahrungen, die wir beim Aufdecken von Sicherheitslücken und der Absicherung von industriellen Anlagen gemacht haben. • Grundlagen und Einführung in das Thema • Beispiele aus der Praxis • Risiken beim Einsatz von Legacy-Systemen • Angriffsmethoden (Hacking, Phishing, Social Engineering) • Abwehrmethoden (SIEM, SOAR, Anomaly-Detection) • Diskussion und Erfahrungsaustausch Zielgruppe: IT-Verantwortliche, CTO, CIO, CISO Dauer: 1 Stunden Kurssprache: Deutsch Kosten: 120 EUR pro Teilnehmer
IS-03	Industrial Product Security Risiken und Chancen bei der Entwicklung von cybersicheren Produkten für die Industrie 4.0 - Wie werden Maschinen und Anlagen cyberfit gemacht? Als Tochter eines Maschinenbauunternehmens kennen wir die Herausforderungen der Digitalisierung aus erster Hand. Wir sprechen über aktuelle Cyberrisiken, die sich über den kompletten Product-Life-Cycle eines Industrieprodukte erstrecken und diskutieren mögliche Ansätze zur Produktion von sicheren Komponenten und Anlagen. • Grundlagen und Einführung in das Thema • Security-by-Design und Default • Sicherheit in der Softwareentwicklung in der Automatisierung • Gesetzliche Anforderungen (KRITIS, Sicherheitsgesetze, Normen) • Praxisbeispiele bei der Entwicklung von cyberresilienten Maschinen und Anlagen • Diskussion und Erfahrungsaustausch Zielgruppe: IT-Verantwortliche, CTO, CIO, CISO Dauer: 1 Stunden Kurssprache: Deutsch Kosten: 120 EUR pro Teilnehmer

2.2 Ausbildung mit optionaler Prüfung

Kurs-Nr.	Beschreibung
DPS-02	Ausbildung zum „Data Privacy Software Engineer“

Anforderungen an den Datenschutz sind in unterschiedlichsten Gesetzen festgeschrieben und müssen auch in digitalen Services und Produkten umgesetzt werden. Zunehmend verlangen Betreiber und Kunden eine Bestätigung bezüglich der Umsetzung der Datenschutzvorgaben.

Schon bereits im Design und der Entwicklung von digitalen Services und Produkten sind Datenschutz-Grundsätze zu beachten. Nur so können digitale Services und Produkte auch im Anschluss datenschutzkonform betrieben werden. Man spricht hier von „Privacy by Design“. Mit unserer Ausbildung zum „Data Privacy Software Engineer“ möchten wir Sie in die Lage versetzen,

- ein Verständnis für die „Privacy by Design“-Anforderungen zu entwickeln – aus der Perspektive unterschiedlicher Stakeholder (Datenschutzbeauftragter, Kunde, Nutzer)
- einen Überblick über Methoden und Werkzeuge im Bereich „Privacy by Design“ zu bekommen
- „Privacy by Design“-Konzepte im Entwicklungsalltag zielgerichtet einsetzen zu können

Inhalte des Trainings

Als Mitglied eines Entwicklungsteams lernen Sie von Praktikern digitale Services und Produkte unter Security- und Privacy-Aspekten zu designen und zu entwickeln. Die Referenten liefern Ihnen die organisatorischen und methodischen Grundlagen und trainieren mit Ihnen gemeinsam auf Basis von Praxisbeispielen das Erlernte im Entwicklungsalltag umzusetzen.

Themenblöcke

Tag 1: Grundlagen des Datenschutzes aus Sicht der Entwicklung

Tag 2: Technischer und organisatorischer Datenschutz

Tag 3: Methodische Grundlagen zu „Privacy by Design“

Tag 4: Praktische Übungen zu „Privacy by Design“

Tag 5: Optionale Prüfung (siehe 2021-DPS-03)

Zielgruppe:

Projektverantwortliche (Projektleiter, Product-Owner, Scrum-Master), Produktmanager, Mitarbeiter / Verantwortliche Entwicklung, Mitarbeiter / Verantwortliche System- oder Softwarearchitektur, Datenschutzverantwortliche für das Produkt

Dauer: 4 Tage

Kurssprache: Deutsch und Englisch

Kosten: 3.300 EUR pro Teilnehmer

Die Teilnehmer erhalten nach Anschluss der Veranstaltung eine Teilnahmebescheinigung.

Kurs-Nr.	Beschreibung
DPS-03	Prüfung zum „Data Privacy Software Engineer“ Im Anschluss an die 4-tägige Ausbildung wird in einer Abschlussprüfung das Wissen abgefragt. Mit Bestehen der Prüfung erhalten Sie ein Zertifikat. Dauer: 2 Stunden Kurssprache: Deutsch und Englisch Kosten: 300 EUR pro Teilnehmer

Anmeldeformular

Zur Anmeldung senden Sie dieses Formular bitte ausgefüllt an uns zurück:

Vorname: _____

Name: _____

Firma: _____

_____

Straße: _____

PLZ / Ort: _____

Telefon: _____

E-Mail: _____

Alle Preise verstehen sich netto zzgl. der gesetzlichen Umsatzsteuer.

Sofern Sie über ein Dienstleistungskontingent bei ditis verfügen, kann die Teilnahme mit dem Kontingent verrechnet werden.

Die Teilnehmerzahl für die Workshops ist begrenzt. Die Mindestteilnehmerzahl für die Durchführung der Workshops beträgt drei Personen.

Verbindliche Anmeldung

Kurs-Nr.	Titel		
Termin	Name des Teilnehmers	E-Mailadresse	Gebühr

Teilnahmebedingungen

Bitte beachten Sie, dass die Anmeldung für die Veranstaltungen jeweils eine Woche vor Veranstaltungsbeginn geschlossen wird, spätere Anmeldungen können nur im Ausnahmefall berücksichtigt werden. Kostenfreie Stornierungen sind bis 14 Tage vor Beginn des Workshops möglich, bei späteren Absagen werden 20% der Teilnahmegebühr in Rechnung gestellt. Es gelten ausschließlich unsere AGB, die unter www.ditis.de eingesehen werden können.

Datum und Unterschrift:_____

Bitte per E-Mail senden an: vertrieb@ditis.de

Für Rückfragen stehen wir Ihnen unter info@ditis.de bzw. telefonisch unter +49 7321 37 5230 gerne zur Verfügung.

ditis Systeme – The Security Company
Zweigniederlassung der JMV SE & Co. KG
Lise-Meitner-Straße 15

89081 Ulm