

# **IT-SICHERHEIT**

# **DATENSCHUTZ**

Genauere Informationen dazu finden Sie auch in unserem Katalog 2020  
KAPITEL 19: IT-SICHERHEIT | DATENSCHUTZ.....ab Seite 350

# IT-SICHERHEIT UND DATENSCHUTZ

19



Cybersecurity – Die Hürden des Alltags überwinden	352
Neue Anforderungen der Bundesnetzagentur (BNetzA)	353
Der Risikofaktor Mensch im Cybercrime	354
Keine Panik bei Datenpannen	355
Marketing DSGVO-Check Teil I: Webseite und Newsletter daten- schutzkonform gestalten	356
Marketing DSGVO-Check Teil II: Marketingaktivitäten datenschutzkonform gestalten	357
Datenschutzaspekte in der Personalabteilung	358
Datenschutz ganz praktisch – sicher arbeiten mit PC und Smartphone	359

## CYBERSECURITY – DIE HÜRDEN DES ALLTAGS ÜBERWINDEN

» Seminarreihe IT-Sicherheit in der Energieversorgung



Seminartyp **Impuls**



Bietigheim-Bissingen

» Auch als **Inhouse-Seminar** verfügbar!



09.07.2020

1 Seminar-Tag



von 8<sup>30</sup> bis ca. 16<sup>30</sup> Uhr



min. 6 Personen, maximal 12 Personen



520,- Euro

Preisangabe pro Tag inkl. Verköstigung,  
Handoutunterlagen als PDF und Zertifikat

### Workshopinhalt · Workshopziel

Sie arbeiten als Informationssicherheitsbeauftragter in Ihrem Stadtwerk und sind zuständig für den Betrieb und die Weiterentwicklung Ihres Informationssicherheitsmanagementsystems (ISMS)? Sie stehen jedoch regelmäßig vor der Herausforderung, dass Ihre definierten Prozesse und Richtlinien zum Schutz der Informationen nicht eingehalten und gelebt werden?

Neue Projekte werden gestartet ohne Sie darüber in Kenntnis zu setzen und Anforderungen an die Informationssicherheit an die Informationssicherheit in Ihrem Stadtwerk aus? Oder funktioniert der Betrieb Ihres Managementsystems nur wenn Sie ständiger Antreiber sind und viele der Themen begleiten und selbst übernehmen?

Um diese Herausforderungen meistern zu können, bieten wir Ihnen verschiedene Methoden und Hilfestellungen, um Ihr Informations-Sicherheitsmanagementsystem in Ihrem Stadtwerk stärker zu etablieren. Zudem zeigen wir Ihnen wie Sie sich als Informationssicherheitsbeauftragter durchsetzen können und das Thema Informationssicherheit auf ein neues Level heben, um mit gutem Gefühl und Rückendeckung Ihr Informations-sicherheitsmanagementsystem betreiben und weiterentwickeln zu können.

- Aufbau prägender Awareness-Kampagnen
- Die Motivation der Mitarbeiter erhöhen Informationen schützen zu wollen
- Erlernen wie Hacker denken
- Aufbau spielerischer Trainings für Ihre Mitarbeiter
- Informationssicherheit interessant gestalten
- Was ist eigentlich Informationssicherheit? Wie jeder Mitarbeiter versteht was mit diesem Begriff gemeint ist
- Unterschiede zwischen Informationssicherheit und Datenschutz vermitteln
- Reale Risiken im Arbeitsalltag erkennen und vermitteln
- Folgen von Hackerangriffen vermitteln
- Vorbild sein

### Methodik

Trainerinput, moderierte Gruppendiskussion, dialogorientierter Vortrag, Praxisbeispiele, Übungen

Wir setzen auf praxisnahe Fallbeispiele und langjährige Erfahrungen aus verschiedenen Kundenprojekten.



Die Inhalte werden bei einer Inhouse-Buchung individuell nach dem Bedarf konzipiert.

## NEUE ANFORDERUNGEN DER BUNDESNETZAGENTUR (BNETZA)

» Seminarreihe IT-Sicherheit in der Energieversorgung

### Workshopinhalt · Workshopziel

Das IT-Sicherheitsgesetz ist schon seit 2015 in Kraft und spätestens seit 2018 sind alle davon betroffenen Stadtwerke danach zertifiziert.

Jedoch sind mit der neuen Auflage der ISO/IEC 27019 auch neue Anforderungen an die Energieversorger entstanden, welche zur Aufrechterhaltung Ihrer Zertifizierung zwingend bis zum 31.12.2020 erfüllt und in Ihr bestehendes Informationssicherheitsmanagementsystem mit aufgenommen werden müssen.

Für eine fristgerechte Erfüllung der neuen Anforderungen ist es notwendig sich frühzeitig mit deren Planung und Umsetzung auseinanderzusetzen.

In unserem Workshop besprechen wir mit Ihnen die Neuerungen und Änderungen der überarbeiteten ISO/IEC 27019, wie bspw. Qualifikationsanforderungen Ihrer Mitarbeiter, Regelungen zum Arbeiten im Außendienst oder Home Office, neue Anforderungen zur Sicherung Ihres Leitstands, die Absicherung kritischer Netzwerke und vieles mehr.

Mit unserem praxisorientierten Ansatz helfen wir Ihnen mit Beispielen und Umsetzungsempfehlungen dabei die neuen Anforderungen in Ihrem Stadtwerk zu erfüllen. Am Ende des Workshops verfügen Sie über die Änderungen und

Neuerungen der Norm sowie passender Umsetzungsmöglichkeiten.

- Aufzeigen der neuen Anforderungen
- Handlungs- und Umsetzungsempfehlungen
- Integration der neuen Anforderungen in Ihr Informationssicherheitsmanagementsystem
- Maßnahmen für die Praxis
- Aufrechterhaltung der Zertifizierung

### Methodik

Trainerinput, moderierte Gruppendiskussion, dialogorientierter Vortrag, Praxisbeispiele, Übungen



Die Inhalte werden bei einer Inhouse-Buchung individuell nach dem Bedarf konzipiert.



Seminartyp **Impuls**



Bietigheim-Bissingen

» Auch als **Inhouse-Seminar** verfügbar!



16.06.2020

1 Seminar-Tag



von 8<sup>30</sup> bis ca. 16<sup>30</sup> Uhr



min. 6 Personen, maximal 12 Personen



520,- Euro

Preisangabe pro Tag inkl. Verköstigung,  
Handoutunterlagen als PDF und Zertifikat

- » Änderungen und Neuerungen
- » Praxis
- » Zertifizierung

Informationssicherheitsbeauftragte (ISB) und Chief Information Security Officer (CISO), die ihre Expertise aufbauen müssen, Führungskräfte, die das Know-How brauchen.



- » Informationssicherheit
- » Prozesse und Projekte
- » Expertise auf- und ausbauen

ZIELgruppe

Informationssicherheitsbeauftragte (ISB) und Chief Information Security Officer (CISO), die ihre Expertise aufbauen müssen, Führungskräfte, die das Know-How brauchen.

## DER RISIKOFAKTOR MENSCH IM CYBERCRIME

» Seminarreihe IT-Sicherheit in der Energieversorgung



Seminartyp **Impuls**



Die Teilnehmer wählen Ort und Datum aus  
» Auch als **Inhouse-Seminar** verfügbar!



von 8<sup>30</sup> bis ca. 16<sup>30</sup> Uhr



min. 8 Personen, maximal 12 Personen



520,- Euro

Preisangabe pro Tag inkl. Verköstigung,  
Handoutunterlagen als PDF und Zertifikat

### Workshopinhalt - Workshopziel

Die Bedrohungen durch Cybercrime wachsen stetig und scheinen kaum aufzuhalten. Angriffsmethoden von Hackern ändern sich ständig und erschweren den Schutz der Informationen in Ihrem Stadtwerk.

Während Sie mit Hilfe von technischen und organisatorischen Maßnahmen versuchen sich bestmöglich gegen Hackerangriffe zu schützen, steigt die Anzahl von Social-Engineering Angriffen auf Ihre Mitarbeiter. Auch hier versuchen die Angreifer mit ständig neuen Tricks das Vertrauen Ihrer Mitarbeiter zu erlangen um an Ihre Informationen zu gelangen.

Um Ihr Stadtwerk effektiv gegen Social-Engineering-Angriffe zu schützen ist es wichtig, dass Ihre Mitarbeiter sich als Teil Ihres Informationssicherheitsmanagementsystems sehen und sich Ihrer Verantwortung bewusst sind. Mit entsprechend prägenden A-wareness-Kampagnen bleibt das Thema Informationssicherheit in den Köpfen Ihrer Mitarbeiter verankert und diese sind sich den drohenden Risiken bewusst.

Regelmäßige Trainings, sowie möglichst reale Angriffsbeispiele sind ebenso ein Bestandteil wie die Anpassung an die sich ständig ändernden Angriffsmethoden. Wie genau kann das gut funktionieren, dass alle Mitarbeiter der Organisation abgeholt werden?

- Aufbau prägender Awareness-Kampagnen
- Die Motivation der Mitarbeiter erhöhen Informationen schützen zu wollen
- Erlernen wie Hacker denken
- Aufbau spielerischer Trainings für Ihre Mitarbeiter
- Informationssicherheit interessant gestalten
- Was ist eigentlich Informationssicherheit? Wie jeder Mitarbeiter versteht was mit diesem Begriff gemeint ist
- Unterschiede zwischen Informationssicherheit und Datenschutz vermitteln
- Reale Risiken im Arbeitsalltag erkennen und vermitteln
- Folgen von Hackerangriffen vermitteln
- Vorbild sein

### Methodik

Trainerinput, moderierte Gruppendiskussion, dialogorientierter Vortrag, Praxisbeispiele, Übungen.

In unseren Workshops setzen wir auf praxisnahe Fallbeispiele und langjährige Erfahrungen aus verschiedenen Kundenprojekten.



Die Inhalte werden bei einer Inhouse-Buchung individuell nach dem Bedarf konzipiert.

## KEINE PANIK BEI DATENPANNEN

» Seminarreihe IT-Sicherheit in der Energieversorgung



### Workshopinhalt - Workshopziel

In unserer digitalen Welt ist es schnell passiert: personenbezogene Daten sind verloren gegangen, wurden versehentlich an falsche Empfänger versandt oder wurden durch einen Angriff von außen abgefangen. Nun heißt es Ruhe bewahren und wie in einem routinierten Krankenhausbetrieb die Behandlung der entstandenen Verletzung einleiten. Das geht jedoch nicht ohne Vorbereitung. Bereits im Vorfeld müssen die Voraussetzungen geschaffen werden, damit solche Vorfälle frühzeitig erkannt, aufgeklärt und behandelt werden. Nur wenn diese Voraussetzungen geschaffen sind, werden effektiv und effizient die richtigen Maßnahmen zur Behandlung ergriffen.

In unserem Workshop lernen Sie die gesamte Kette der notwendigen Abläufe kennen, die Ihr Unternehmen im Falle eines Datenschutzvorfalls durchlaufen muss. Dies umfasst die Qualifikation und Behandlung von Vorfällen sowie die Erarbeitung einer Strategie zur Vermeidung künftiger Vorfälle. Sie lernen, unter welchen Voraussetzungen eine Meldung an die zuständige Aufsichtsbehörde erfolgen muss und wie diese innerhalb der geforderten 72 Stunden-Frist erfolgen kann. Zur Vereinfachung der vorgeschriebenen Dokumentation zeigen wir Ihnen diese Schritte am Beispiel eines Tools, dem „diti's Datenschutzmanager“.

Dieser Workshop vermittelt auch die erforderlichen technischen Vorbereitungen zur Aufklärung eines Vorfalls, damit Sie

belastbare Informationen erhalten über bspw. Definition des Zeitraums, der Menge der betroffenen Daten und dem betroffenen Personenkreis. Dies kann mithilfe der Durchführung forensischer Untersuchungen erreicht werden. Diese sind nur möglich und datenschutzkonform einsetzbar, wenn bereits im Vorfeld des Ereignisses entsprechende Vorbereitungen, wie z.B. die Definition von Vorgaben zum korrekten Umgang mit und zur Auswertung von Logdateien, getroffen wurden.

- Benötigte Vorbereitungen und Abläufe zur Behandlung von Datenpannen
- Qualifikation von Datenpannen
- Meldepflicht und datenschutzrechtliche Hintergründe
- Vorbereitungsmaßnahmen zur Aufklärung von Datenpannen mithilfe technischer und forensischer Untersuchungen
- Erfüllung der Dokumentationspflichten

### Methodik

Trainerinput, moderierte Gruppendiskussion, dialogorientierter Vortrag, Praxisbeispiele.

In unseren Workshop setzen wir auf praxisnahe Fallbeispiele und langjährige Erfahrungen aus verschiedenen Kundenprojekten.



Die Inhalte werden bei einer Inhouse-Buchung individuell nach Ihrem Bedarf konzipiert.



Seminartyp **Impuls**



Die Teilnehmer wählen Ort und Datum aus  
» Auch als **Inhouse-Seminar** verfügbar!  
2-tägiges FlexSeminar



von 8<sup>30</sup> bis ca. 16<sup>30</sup> Uhr



min. 1 Person, maximal 12 Personen



Investition abhängig von Teilnehmerzahl



» Datenpannen  
» Vermeidung von Vorfällen  
» Datenschutzkette



Vorfallbeauftragte, Datenschutzverantwortliche, Ressourcenverantwortliche, Informationssicherheitsbeauftragte und alle Mitarbeiter, die sich mit Datenpannen auskennen müssen.

## MARKETING DSGVO-CHECK TEIL I: WEBSEITE UND NEWSLETTER DATEN-SCHUTZKONFORM GESTALTEN

» Seminarreihe IT-Sicherheit in der Energieversorgung



Seminartyp **Impuls**



Bietigheim-Bissingen

» Auch als **Inhouse-Seminar** verfügbar!



09.07.2020

1 Seminar-Tag



von 8<sup>30</sup> bis ca. 16<sup>30</sup> Uhr



min. 6 Personen, maximal 9 Personen



520,- Euro

Preisangabe pro Tag inkl. Verköstigung,  
Handoutunterlagen als PDF und Zertifikat

### Workshopinhalt · Workshopziel

Der Internetauftritt ist für die Außenwirkung Ihres Energieversorgers von besonderer Bedeutung und die digitale Visitenkarte.

Immer mehr Kunden werden online gewonnen und regelmäßige Newsletter tragen maßgeblich zur Kundengewinnung und Kundenbindung bei.

Zahlreiche Tools können auf die Webseite und in den Newsletter eingebunden werden und versprechen durch Analysen und Onlinewerbung eine zielgruppengenaue Ansprache, mehr Neukunden oder eine verbesserte „Customer Experience“.

Die Aufgabe, diese Dienstleister datenschutzkonform einzubinden stellt die Webseitenbetreiber mit zunehmender Vorschriftendichte vor Herausforderungen.

Wir machen den DSGVO-Check für Webseite und Newsletter. Ziel ist es, Ihnen praktisches Handwerkszeug zu vermitteln, damit Sie Ihren Internetauftritt und Newsletter aus der Sicht des Datenschutzes analysieren, Schwachstellen aufdecken und konkrete Maßnahmen ergreifen können.

Dabei betrachten wir insbesondere, welche Anforderungen es an die Datenschutzerklärung gibt und geben Hinweise zu deren Gestaltung.

- Datenschutzrechtliche Anforderungen an Webseite und Newsletter
- Vermittlung der Analyseschritte zur Bewertung einer datenschutzkonformen Webseite
- Häufige Schwachstellen und wie diese erkannt werden können
- Korrekte Ausgestaltung einer Datenschutzerklärung

### Methodik

Trainerinput, dialogorientierter Vortrag, viele Praxisbeispiel, Arbeitsblätter. In unseren Workshops setzen wir auf praxisnahe Fallbeispiele und langjährige Erfahrungen aus verschiedenen Kundenprojekten.



Die Inhalte werden bei einer Inhouse-Buchung individuell nach dem Bedarf konzipiert.



- » Website und Sicherheit
- » Wettbewerbsfaktor
- » Online Visitenkarte

**ZIEL** gruppe

Marketingleiter, Webseiten-Verantwortliche aus Vertrieb und Marketing, Datenschutzverantwortliche, die das Know How in den eigenen Reihen aufbauen wollen.

## MARKETING DSGVO-CHECK TEIL II: MARKETINGAKTIVITÄTEN DATENSCHUTZKONFORM GESTALTEN

» Seminarreihe IT-Sicherheit in der Energieversorgung

### Workshopinhalt · Workshopziel

Ihre Marketingaktivitäten beschränken sich nicht nur auf Webseite und Newsletter?

Dann sind Sie im DSGVO-Check Teil II richtig. Ob Gewinnspiel, Social Media Marketing, Messeveranstaltung oder Veranstaltungen mit Kooperationspartnern – das unternehmerische Ziel ist die Generierung von Neukunden, die Bindung von Bestandskunden oder das Zurückgewinnen von ehemaligen Kunden.

Mithilfe von datenschutzrechtlichen Leitplanken wird jedoch sichergestellt, dass die Kunden nicht zu buchstäblich „gläsernen“ Kunden werden.

Daher gilt es aus Sicht des Datenschutzes eine Balance zwischen den Zielen des Unternehmens und den rechtlichen Rahmenbedingungen zu finden.

Wir machen den DSGVO-Check für Ihre weiteren Marketingaktivitäten. Wir zeigen in unserem Workshop Möglichkeiten, wie Sie Ihre Marketingaktivitäten datenschutzkonform gestalten können, was Sie bspw. bei der Durchführung von Gewinnspielen beachten müssen und welche Hürden im Social Media Marketing zu nehmen sind.

- Überblick über die gesetzlichen Anforderungen aus DSGVO und BDSG an Marketingaktivitäten
- Datenschutzrechtliche Herangehensweise und Praxisbeispiele zum datenschutzkonformen Einsatz von Marketingmaßnahmen am Beispiel von:
  - Social Media
  - Gewinnspiele
  - Messen und Veranstaltungen mit Kooperationspartnern
  - u.v.m.

### Methodik

Trainerinput, dialogorientierter Vortrag, Praxisbeispiel, Arbeitsblätter. In unseren Workshops setzen wir auf praxisnahe Fallbeispiele und langjährige Erfahrungen aus verschiedenen Kundenprojekten.



Die Inhalte werden bei einer Inhouse-Buchung individuell nach dem Bedarf konzipiert.



Seminartyp **Impuls**



Die Teilnehmer wählen Ort und Datum aus

» Auch als **Inhouse-Seminar** verfügbar!  
2-tägiges FlexSeminar



von 8<sup>30</sup> bis ca. 16<sup>30</sup> Uhr



min. 1 Person, maximal 9 Personen



Investition abhängig von Teilnehmerzahl



- » Website und Sicherheit
- » Wettbewerbsfaktor
- » Online Visitenkarte

**ZIEL** gruppe

Marketingleiter, Webseiten-Verantwortliche aus Vertrieb und Marketing, Datenschutzverantwortliche, die das Know How in den eigenen Reihen aufbauen wollen.

## DATENSCHUTZASPEKTE IN DER PERSONALABTEILUNG

» Seminarreihe IT-Sicherheit in der Energieversorgung



Seminartyp **Impuls**



Bietigheim-Bissingen

» Auch als **Inhouse-Seminar** verfügbar!



03.08.2020

1 Seminar-Tag



von 8<sup>30</sup> bis ca. 16<sup>30</sup> Uhr



min. 6 Personen, maximal 9 Personen



520,- Euro

Preisangabe pro Tag inkl. Verköstigung,  
Handoutunterlagen als PDF und Zertifikat

### Workshopinhalt · Workshopziel

Von der Bewerbung, dem Onboarding und der aktiven Betreuung im Arbeitsverhältnis bis zum Austritt von Mitarbeitern, um diese Prozesse durchführen zu können benötigt die Personalabteilung grundsätzlich eine Vielzahl personenbezogener Informationen.

Dabei reicht das Spektrum der Personalprozesse von risikoarmen Themen, deren Herausforderung in ihrer Anzahl liegt, bis hin zu Prozessen mit hoch sensiblen Gesundheitsdaten.

Darum haben die Verarbeitungen der Personalabteilung auch zum Teil höhere Anforderungen aus der Datenschutzgrundverordnung (DSGVO) und dem deutschen Bundesdatenschutzgesetzes (BDSG) zu erfüllen.

Damit die Personalabteilung bei der Vielzahl der Vorgaben und Anforderungen nicht den Überblick verliert, dient dieser Workshop dazu Ihnen die datenschutzkonforme Ausgestaltung von Personalprozessen anhand verschiedener Praxisbeispiele aus den Bereichen Recruiting-Systeme, Personal- und BEM-Akte und Onboarding vorzustellen. Ebenso wird dargestellt, wie Sie Betriebsvereinbarungen im Datenschutz nutzen können.

- Überblick über die gesetzlichen Anforderungen aus DSGVO und BDSG an die Personalabteilung
- Vorstellung von Schlüsselprozessen in der Personalarbeit und deren datenschutzkonforme Ausgestaltung
- Herangehensweise an Prozesse mit besonders sensiblen personenbezogenen Daten und höheren datenschutzrechtlichen Anforderungen
- Einsatz von Betriebsvereinbarungen für Personalprozesse

### Methodik

Trainerinput, dialogorientierter Vortrag, viele Praxisbeispiel, Arbeitsblätter. In unseren Workshops setzen wir auf praxisnahe Fallbeispiele und langjährige Erfahrungen aus verschiedenen Kundenprojekten.



Die Inhalte werden bei einer Inhouse-Buchung individuell nach dem Bedarf konzipiert.

## DATENSCHUTZ GANZ PRAKTISCH - SICHER ARBEITEN MIT PC UND SMARTPHONE

» Seminarreihe IT-Sicherheit in der Energieversorgung

### Workshopinhalt · Workshopziel

Sie sind geschult und "sensibilisiert" für Datenschutz? Aber bedeutet Datenschutz konkret? Wie funktioniert er im täglichen Arbeiten?

Mehr als die Hälfte aller Datenpannen werden durch das Verhalten der Person vor dem PC verursacht!

Die Fehlerquellen sind vielfältig. Sie reichen vom leichtfertigen Umgang mit Passwörtern bis zur ungeprüften Weiterleitung von Mail-Anhängen. Ebenso spielt die ungeprüfte Verwendung von USB-Sticks und anderen Speichermedien eine große Rolle.

Und was bringt moderner IT-Datenschutz, wenn die Mitarbeiter unsicher sind, wie sie mit einer Erpressermail umgehen sollen und auf welchen Link man nicht drücken soll, was man wie am Telefon noch weitergeben darf? Diese Unsicherheit ist gefährlich. Sie kann im Ernstfall auch Bußgelder nach sich ziehen.

Sie lernen, Ihre Daten an Smartphone und PC effektiv zu schützen, sicher und souverän am PC zu arbeiten, Gefahren zu erkennen, Risiken einzuschätzen und Abhilfe zu schaffen.

- Mitarbeiter sind die Firewall ihrer Organisation
- Mitreden können - Datenschutz und Informationssicherheit

- So schützen Sie Ihren Arbeitsplatz
- Richtiger Umgang mit Passwörtern
- Bedrohungen auf Computer und Smartphone
- 1x1 der Verschlüsselung
- Computer sichern, sperren, schützen
- Sicher surfen
- Digitale Spuren
- Digitale Netze und der Datenschutz
- Sicher unterwegs sein und bleiben
- Datenschutz-konform mit Informationen umgehen
- Richtiger Umgang mit sensiblen Informationen
- Was darf ich, was darf ich nicht?
- 7 goldene Regeln für sicheres Arbeiten

### Methodik

Trainerinput, dialogorientierter Vortrag, viele Praxisbeispiel, Arbeitsblätter.

Nach dem Seminar erhalten Sie Checklisten und einen Maßnahmenkatalog zur Verfügung gestellt. Mit echten Vorfällen aus der Praxis, praktischen Übungen und aktuellen Informationen.



Die Inhalte werden bei einer Inhouse-Buchung individuell nach dem Bedarf konzipiert.



Seminartyp **Impuls**



Die Teilnehmer wählen Ort und Datum aus

» Auch als **Inhouse-Seminar** verfügbar!  
2-tägiges FlexSeminar



von 8<sup>30</sup> bis ca. 16<sup>30</sup> Uhr



min. 1 Person, maximal 9 Personen



Investition abhängig von Teilnehmerzahl



- » Datenschutz im Fachbereich
- » Expertise für Datenschutz
- » Zukunftsthema

ZIELgruppe

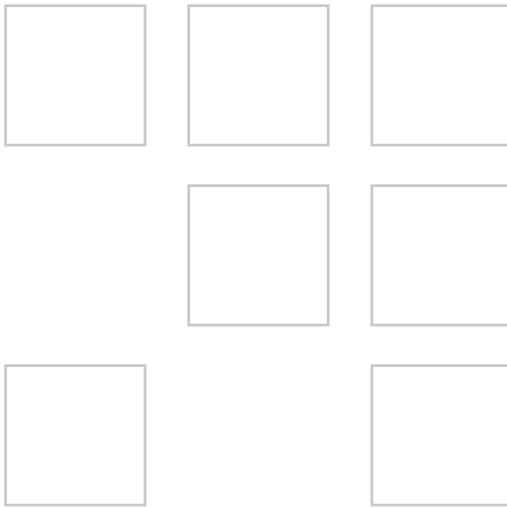
Alle Mitarbeiter und Entscheider im Fachbereich Personal, die das Know How in den eigenen Reihen aufbauen wollen.



- » Digitale Kompetenz für Alle
- » Richtiger Umgang mit Daten
- » Sicherer digitaler Umgang

ZIELgruppe

Alle Mitarbeiter, die ihre digitale Kompetenz festigen müssen sowie Anwendungssicherheit brauchen bzw. vermitteln müssen.



**StadtwerkeAkademie**

Eisenhutstraße 6  
72072 Tübingen

Fon 07071 157-3091

Fax 07071 157-369

info@stadtwerkeakademie.de

Aktuelle Infos und Online-Anmeldung  
unter [www.stadtwerkeakademie.de](http://www.stadtwerkeakademie.de)

Wir beraten Sie gerne!