Version 1.0

Einführung in die IT-Sicherheit

Mitarbeiterschulung

Sofort einsetzbares PowerPoint-Folien-Package für eine Mitarbeiter-Schulung zur IT-Sicherheit

Infos und Bestellmöglichkeit www.datakontext.com!

HISOLUTIONS

DATAKONTEXT

AGENDA

- Einführung
- Informationssicherheit – IT-Sicherheit – Datenschutz
- Vertraulichkeit, Integrität und Verfügbarkeit
- Security – Wie geht das?
- Relevante Bedrohungen
- Typische Angriffe
- Wichtige Maßnahmen
- Umgang mit IT-Sicherheitsvorfällen
- Quiz

BEISPIEL 2: „ANRUF VOM CHEF“

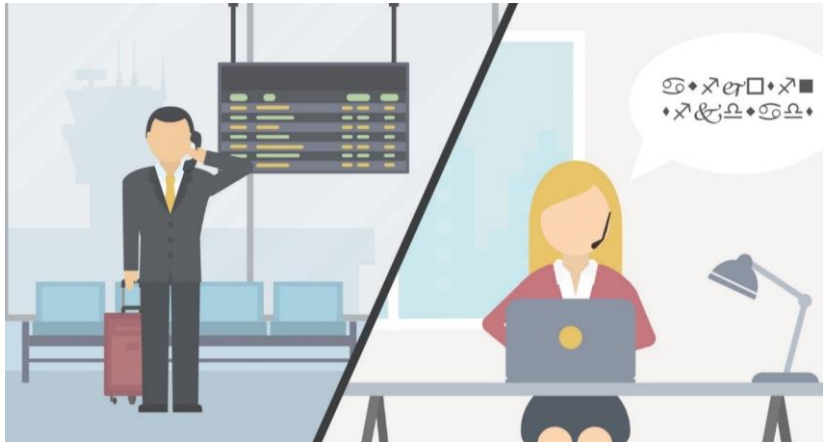
Der Chef ruft an. Vielleicht auch der CFO, auf jeden Fall ist es dringend. Die Verbindung ist schlecht, klar, er ist im Ausland unterwegs.

Und muss dringend sofort eine Überweisung anstoßen, sonst ist der Auftrag verloren.

In Ihnen weckt sich Zweifel. Das ist doch nicht im Rahmen der Prozesse?

Aber der Chef hat ja am Morgen schon eine E-Mail geschrieben, also wird das schon seine Richtigkeit haben?

Mit leichten Bauchschmerzen weisen Sie den Transfer an. Das Geld ist weg.

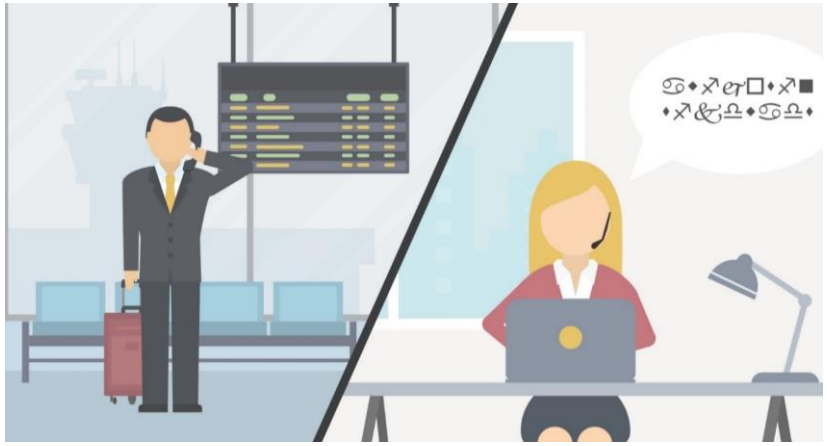


BEISPIEL 2: „ANRUF VOM CHEF“

Was ist passiert?

Sie sind dem sogenannten „CEO Fraud“, auch „Business Email Compromise“ (BEC) genannt, aufgesessen.

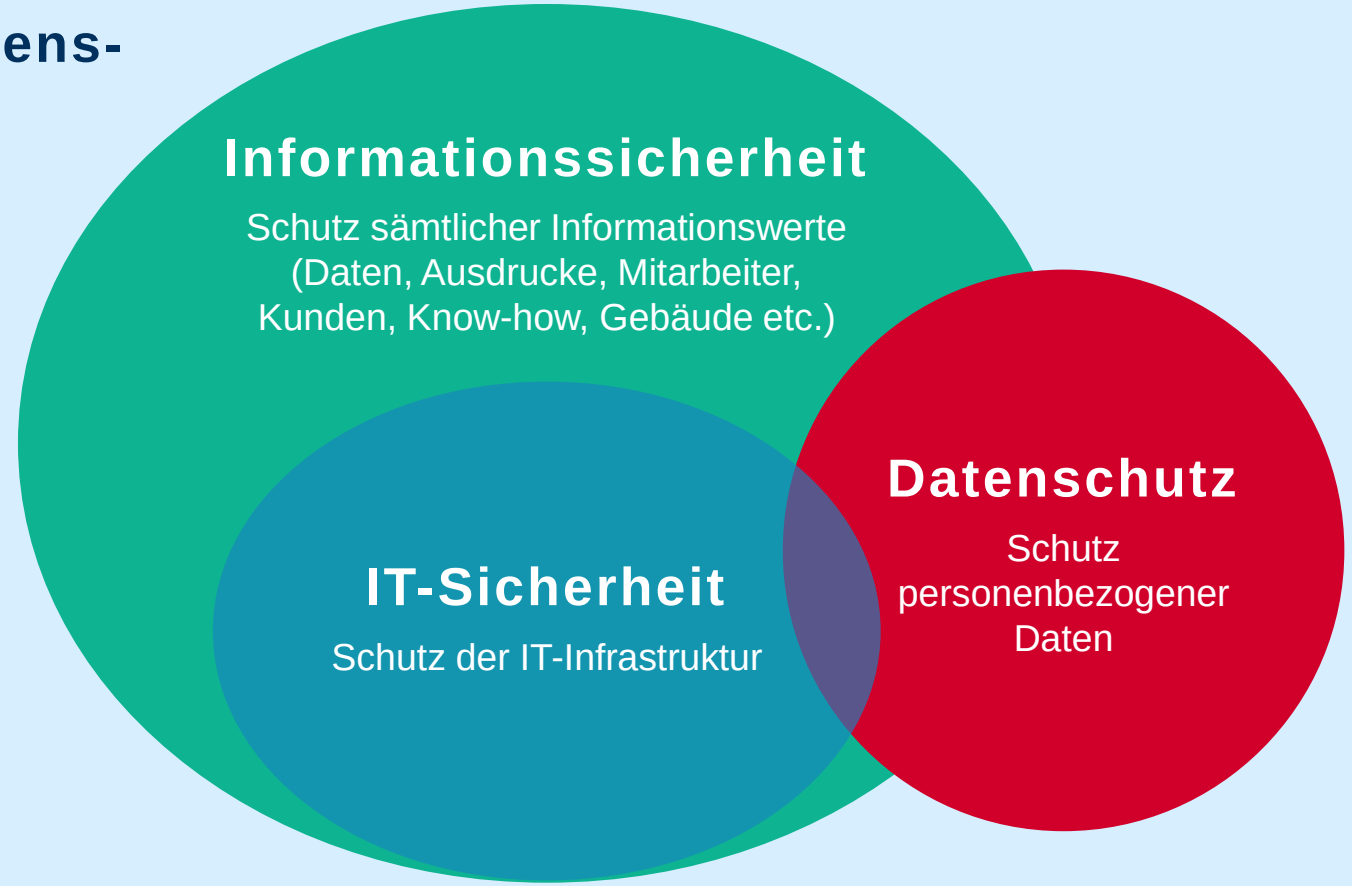
E-Mail wie Anruf waren gefälscht, der Chef hatte nichts damit zu tun.



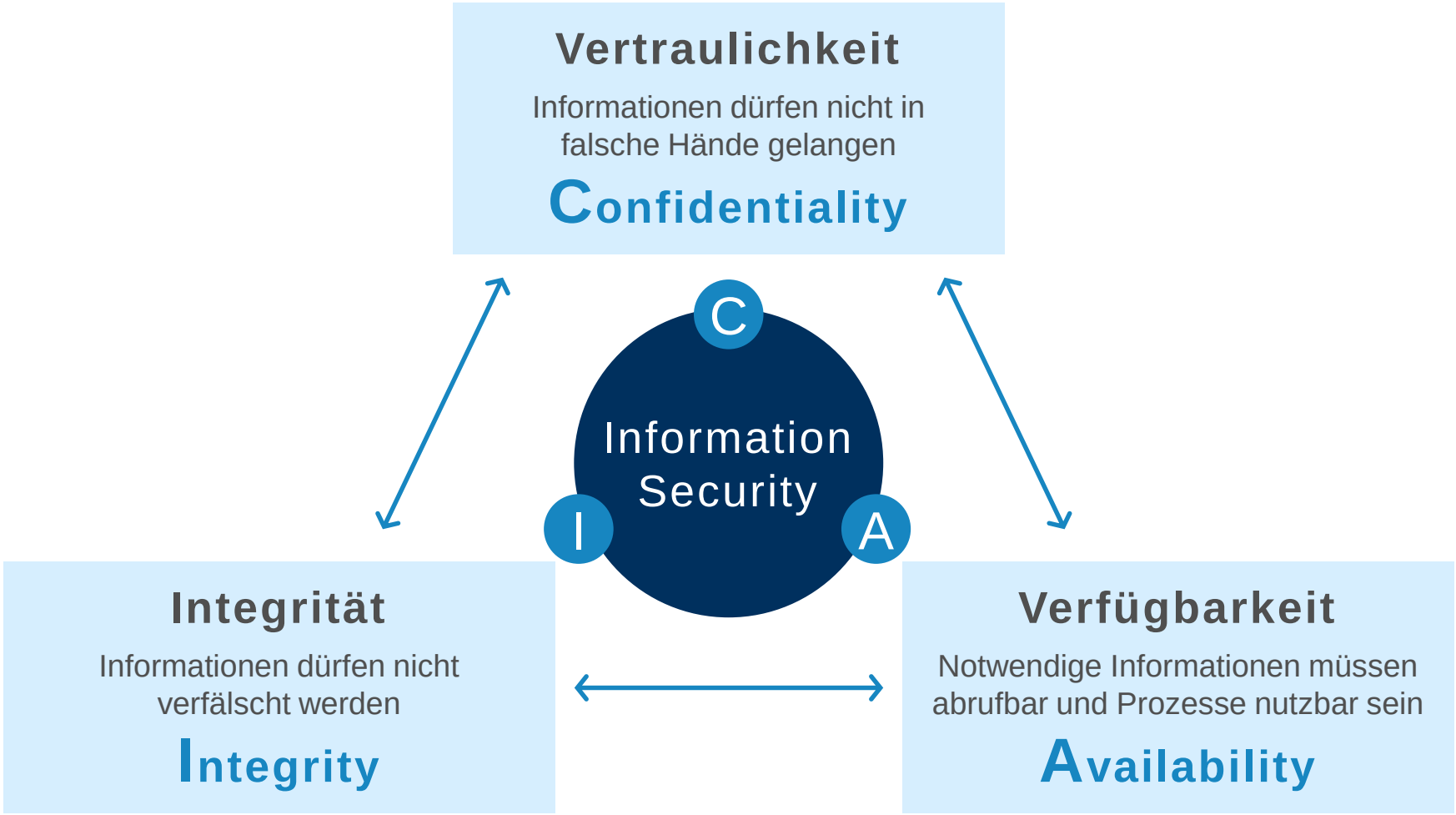
INFORMATIONSSICHERHEIT, IT-SICHERHEIT, DATENSCHUTZ

Unternehmens-sicherheit

inklusive Arbeitsschutz, Personenschutz, Safety, physische Sicherheit, …



VERTRAULICHKEIT, INTEGRITÄT, VERFÜGBARKEIT



INFORMATIONSSICHERHEIT GEHT NUR GEMEINSAM

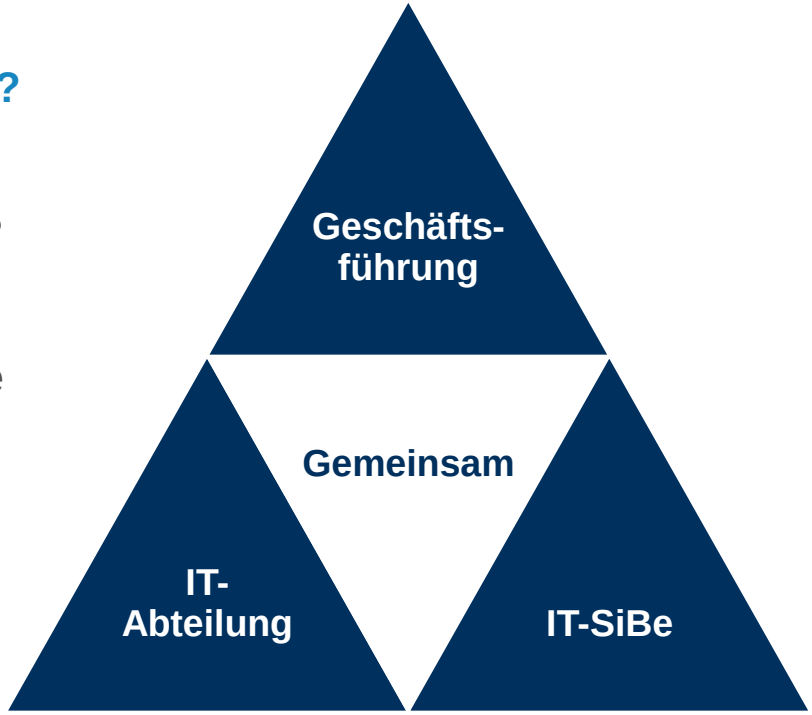
Wer macht denn nun aber eigentlich Informationssicherheit in einem Unternehmen?

Die Geschäftsführung? Die IT-Abteilung?
Der Informationssicherheitsbeauftragte (IT-SiBe)?

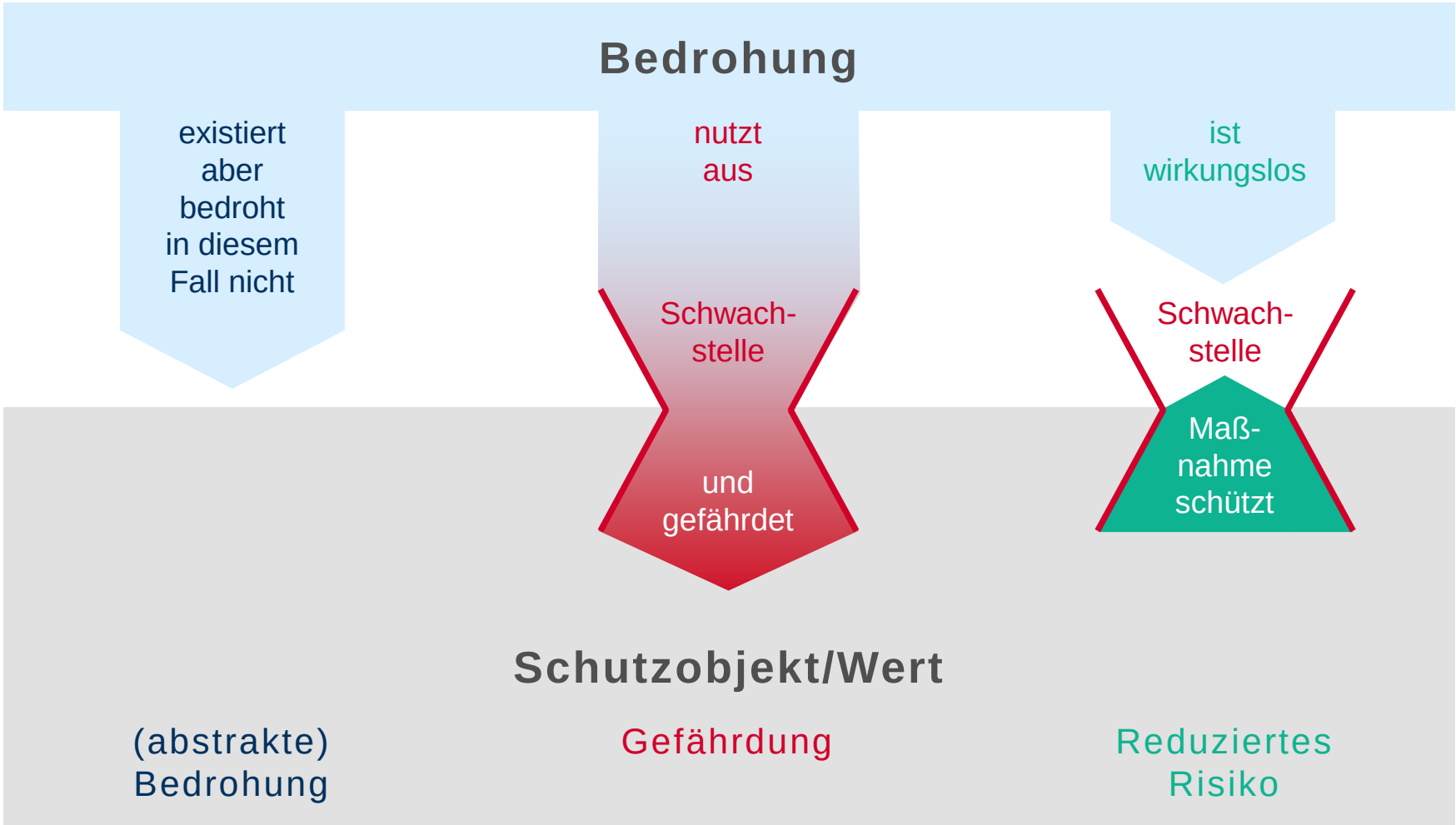
Alles richtig! Aber bei der Informationssicherheit müssen alle an einem Strang ziehen, da die Kette immer nur so stark ist wie ihr schwächstes Glied.

Alle Mitarbeiter tragen ihren Teil dazu bei, dass Informationen und Prozesse geschützt werden.

Also auch Sie!



SECURITY – WIE GEHT DAS?



SOCIAL ENGINEERING – BEISPIELE

1. **Telefon:** Ein „neuer Kollege“ ruft an, um mal eben sein Passwort zurücksetzen zu lassen
2. **E-Mail:** Der „Chef“ bittet um dringende Überweisung (CEO-Fraud), der „Dienstleister“ um umgehende Einrichtung eines weiteren VPN-Zugangs
3. **Messenger:** Die „Personalabteilung“ nutzt heute WhatsApp, um alle Mitarbeiter zu bitten, im verlinkten „Mitarbeiterportal“ schnell ihre AD- und E-Mail-Passworte zu ändern – aufgrund eines „Sicherheitsvorfalls“
4. **Persönlich:** Ein Fremder stellt sich als Dienstleister/Partner/Kollege vor und schlüpft mit Ihnen in einen Sicherheitsbereich oder beginnt ein Gespräch über ein internes Projekt, über das er Informationen im Netz gefunden hat.

WAS KANN MAN TUN GEGEN PHISHING UND SOCIAL ENGINEERING?

1. Gesundes Misstrauen gegenüber aller eingehenden Kommunikation: E-Mails, SMS, Messaging, Anrufe, persönliche Ansprache …
2. Im Zweifel lieber einmal zu viel plausibilisieren (Passt das? Kann das sein? Macht das Sinn gerade?) oder intern nachfragen. KEINE SORGE: Dafür muss man nicht unfreundlich werden. ☺
3. Seiten im Browser immer besser über ein Lesezeichen (Bookmark) oder durch manuelle Eingabe der Domain aufrufen als durch einen Klick.
4. Auf einen anderen Kommunikationskanal wechseln, z. B. bei Anruf eines „Kollegen“ per Festnetz diesen mobil übers Firmen-Verzeichnis (Telefonbuch) zurückrufen.
5. Ggf. die IT-Sicherheit bitten, eine Nachricht zu überprüfen.

GRUNDREGEL

Melden Sie jedes auffällige Verhalten der IT!

QUIZFRAGEN

Was ist Informationssicherheit?

- Schutz von Informationen während der Übertragung
- Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Prozessen
- Schutz vor Hackern und Spionen
- Schutz vor zu viel Informationen

QUIZFRAGEN

Was ist Informationssicherheit?

- Schutz von Informationen während der Übertragung
- Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Prozessen
- Schutz vor Hackern und Spionen
- Schutz vor zu viel Informationen

INFORMATIONEN ZUM AUTOR

David Fuhr
Dipl. Math.
CISSP, CISA, ISO 27001 Lead Auditor

Principal
Head of Research
HiSolutions AG

Blog: research.hisolutions.com

Sofort einsetzbares PowerPoint-Folien-Package für eine Mitarbeiter-Schulung zur IT-Sicherheit

Schulen Sie ohne lange Vorbereitungszeit und nutzen Sie das vortragsfertige Power-Point-Set für die Sensibilisierung Ihrer Mitarbeiter zur IT-Sicherheit. Der integrierte Referenten-Leitfaden liefert Ihnen Hintergrundinformationen und umfangreiche Vortragshinweise.

Mit Beispielen zu typischen Cyberangriffen wie Spam, Phishing, Social Engineering und Schadsoftware leiten Sie Ihre Mitarbeiter zu korrektem Verhalten an und schärfen das Bewusstsein für Gefahren von außen. Sie vermitteln ihnen auf anschauliche Weise, wie sie sicher mit Daten und IT umgehen. Sie erhalten Handlungsanweisungen, was bei Sicherheitsvorfällen zu tun ist. Mit einem Abschlusstest können Sie das erlernte Wissen überprüfen. Es werden keine besonderen IT-Kenntnisse vorausgesetzt.

Die Folien lassen sich an Ihr Corporate Design anpassen.

Gut geschulte Mitarbeiter sind ein zentraler Bestandteil im IT-Sicherheitskonzept eines jeden Unternehmens.

Titeldetails:
Daten/Download (Power-Point-Folien mit Trainer-Leitfaden)
ISBN: 978-3-89577-847-6
Auflage: Version 1.0

Infos und Bestellmöglichkeit www.datakontext.com!

HISOLUTIONS

DATAKONTEXT