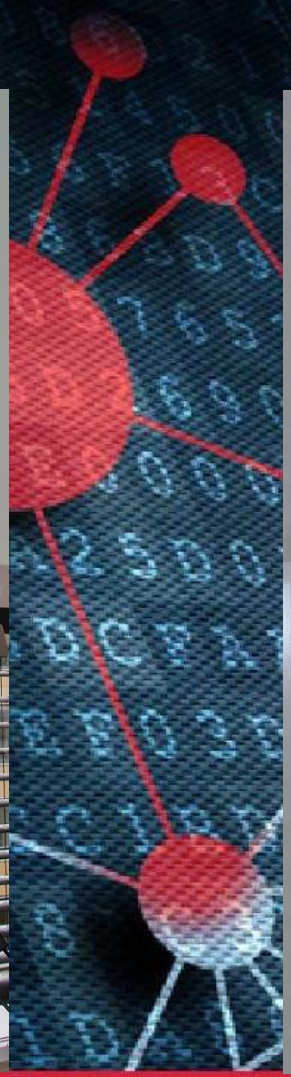
Andreas Scholtz

Martin Stolle



4. Kommunaler IT-Sicherheitskongress 2017

„Umsetzung der Leitlinie für Informationssicherheit des IT-Planungsrats in Kommunalverwaltungen“

SECURITY VON DRUCKINFRASTRUKTUREN AUS DER RECHTLICHEN SICHT

Was soll mir denn passieren?

Andreas F. Scholtz
Berater, Wirschaftsjurist

MC² MANAGEMENT CONSULTING GMBH

Modernisierung von Druck- und Dokumenteninfrastrukturen

ANALYSE

Wirtschaftlichkeitsanalysen
Analyse von Geschäftsprozessen
Bestandsaufnahmen
Sicherheitslagebilder
Security Analyse
Emissionsberechnung

BERATUNG

Konzepterstellung
Fleet Design
Business Case
Technische Beratung
Strategieentwicklung
Print-Policy Workshops
Security Workshops

BESCHAFFUNG

Ausschreibungen
GWB, VgV etc.

Erstellung von RfI, RfP
Begleitung von
Ausschreibungsprozessen
Bieterverhandlungen

IMPLEMENTIERUNG

Projektmanagement
Rolloutplanung & -steuerung
Technische Validierung
Begleitung von POC
Dokumentation

CONTROLLING

Vertragsmanagement
Fleet Management
SupplyWatch
FleetWatch
Ongoing Optimizing

MC² MANAGEMENT CONSULTING GMBH

Engagement

Allianz für Cyber-Sicherheit

Bundesamt für Sicherheit in der Informationstechnik

initiative wirtschaftsschutz

DVNW Deutsches Vergabenetzwerk

WAS SOLL MIR DENN PASSIEREN?

Sicherheitsmaßnahmen haben eine rechtliche Relevanz

https://www.datenschutzbeauftragter-info.de/debeka-zahlt-1-3-mio-eur-bussgeld-wegen-datenschutzverletzungen/; (2015)

DRUCKER UND MULTIFUNKTIONSGERÄTE: KEIN RECHTSFREIER RAUM

(unterlassene) Sicherheitsmaßnahmen haben eine rechtliche Relevanz

DIE INFORMATION

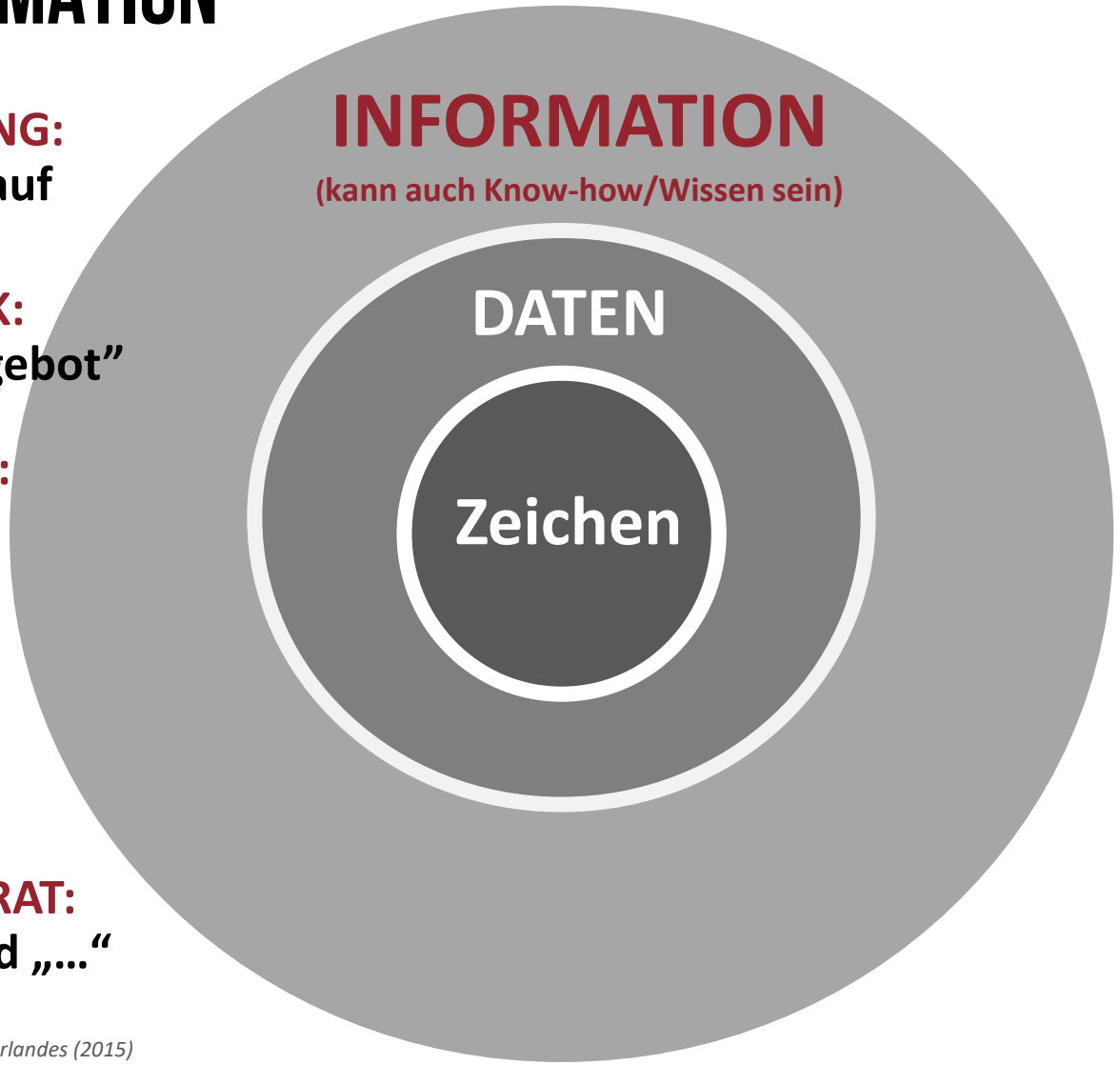
ENTSCHEIDUNG:
Produkteinkauf

PRAGMATIK:
“günstigstes Angebot”

SEMANTIK:
2,30 €

SYNTAX:
2,30

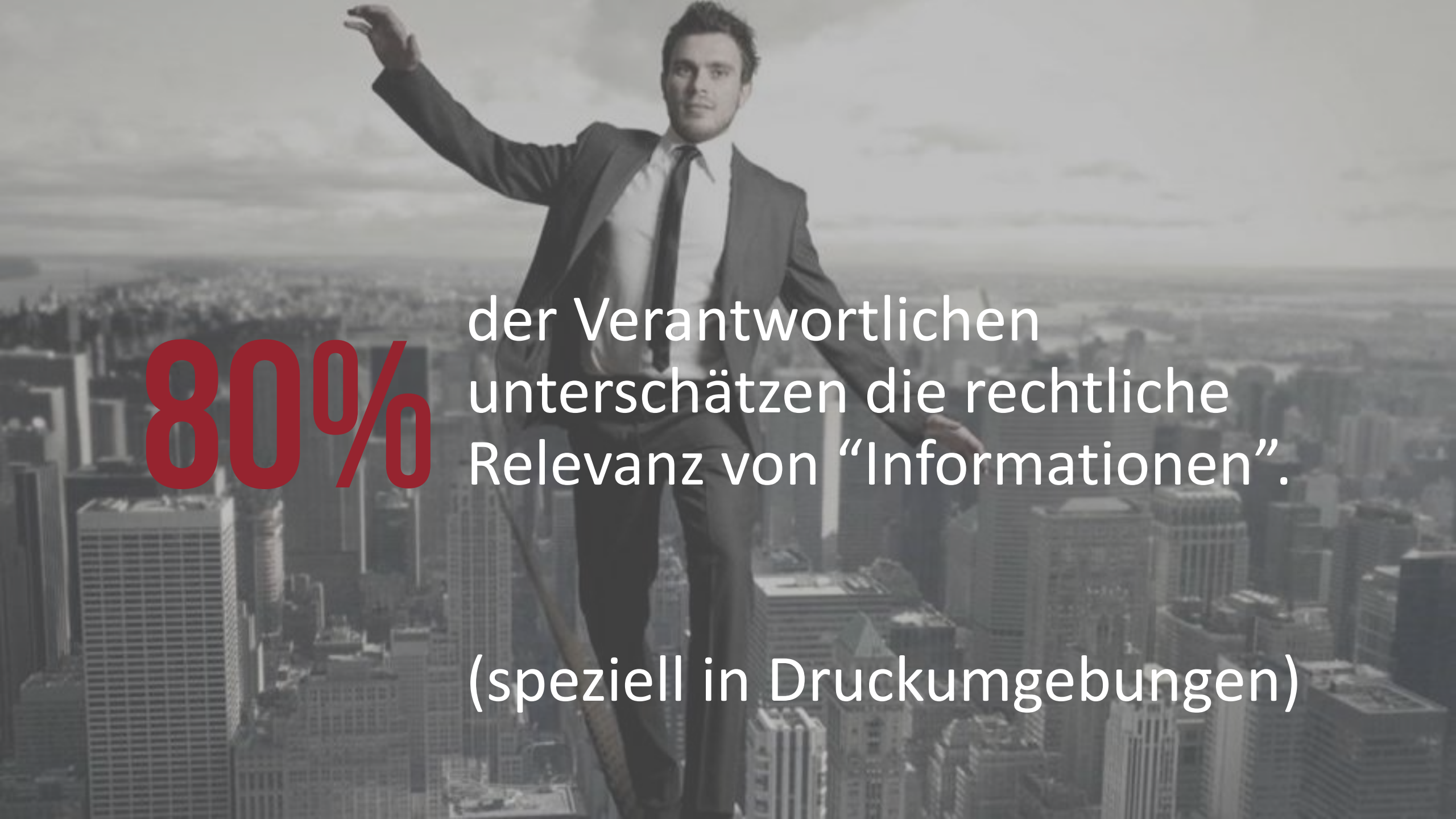
ZEICHENVORRAT:
„2“, „3“, „0“ und „…“



„[…] Information ist die Teilmenge von Wissen, die von einer bestimmten Person oder Gruppe in einer konkreten Situation benötigt wird und häufig nicht explizit vorhanden ist […]“

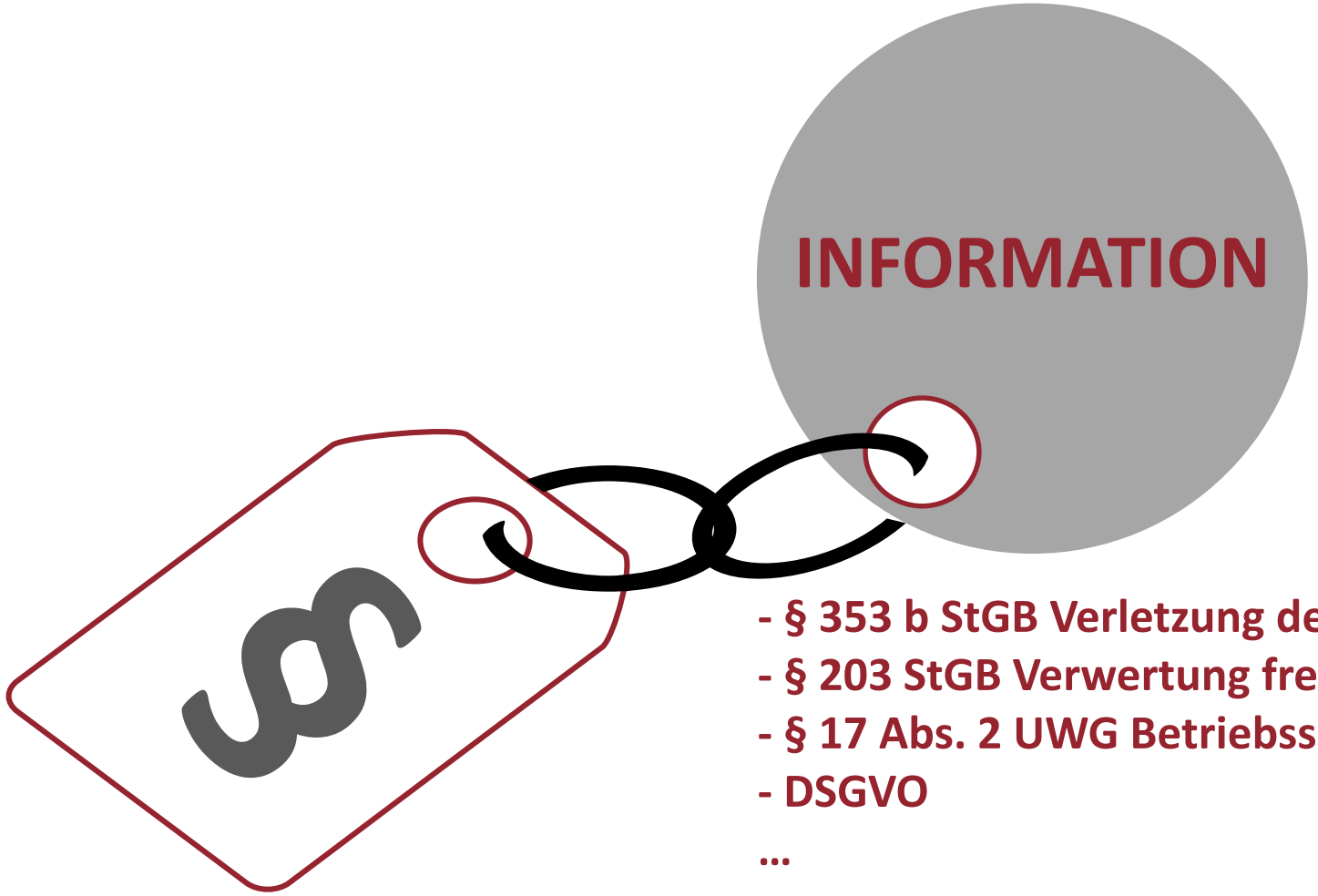
*„Information ist der (geglückte) Transfer von Wissen […]“**

**) o. V. auf: Universität des Saarlandes (2015)*
***) eigene Darstellung in Anlehnung an Hildebrandt (2011)*


80%
der Verantwortlichen
unterschätzen die rechtliche
Relevanz von “Informationen”.
(speziell in Druckumgebungen)

DIE INFORMATION

Hat einen „juristischen Anhänger“



- § 353 b StGB Verletzung des Dienstgeheimnisses
- § 203 StGB Verwertung fremder Geheimnisse
- § 17 Abs. 2 UWG Betriebsspionage
- DSGVO

…

INFORMATIONSTRÄGER

Ein „Dreigestirn“

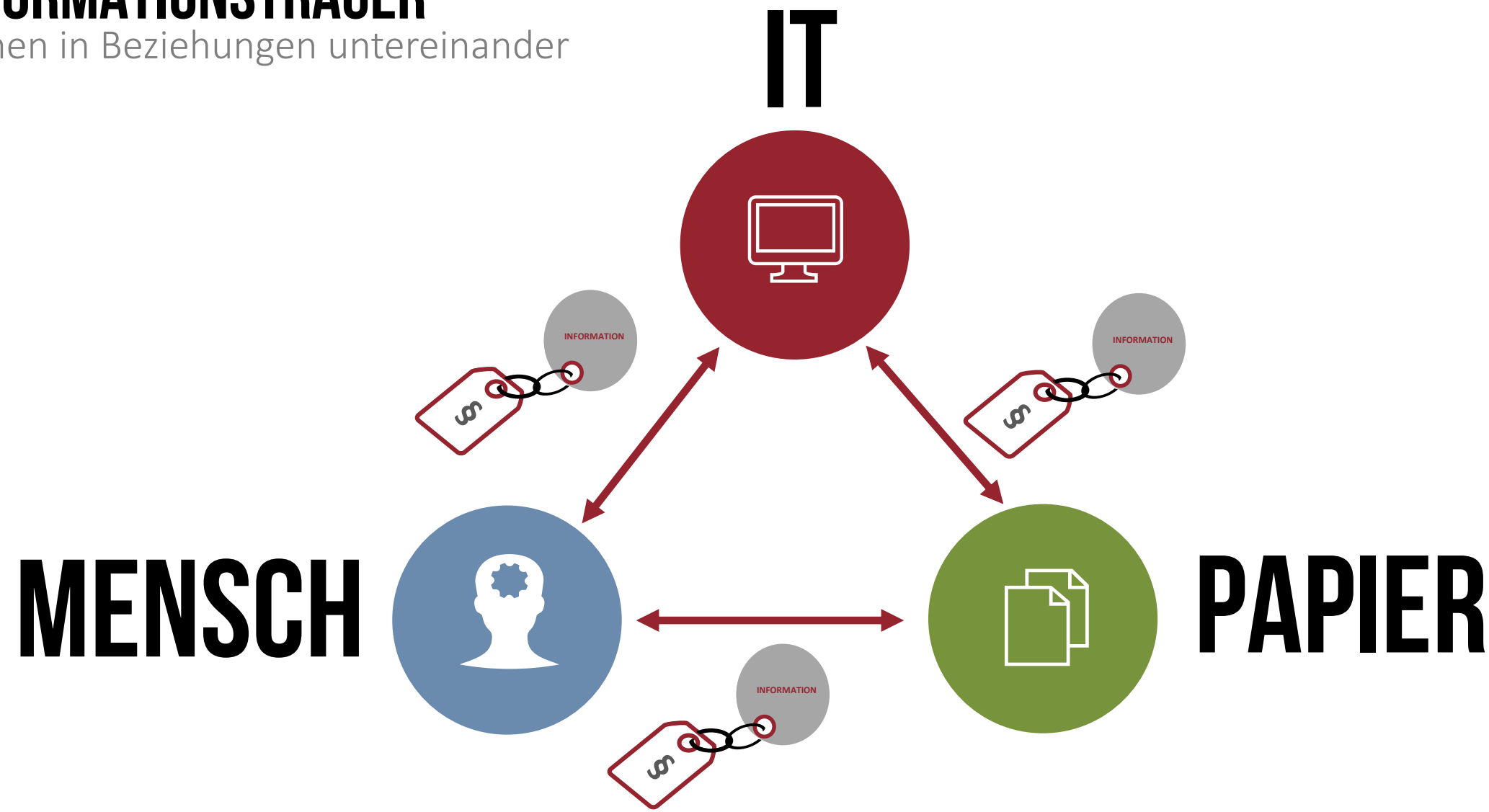
IT

PAPIER

MENSCH

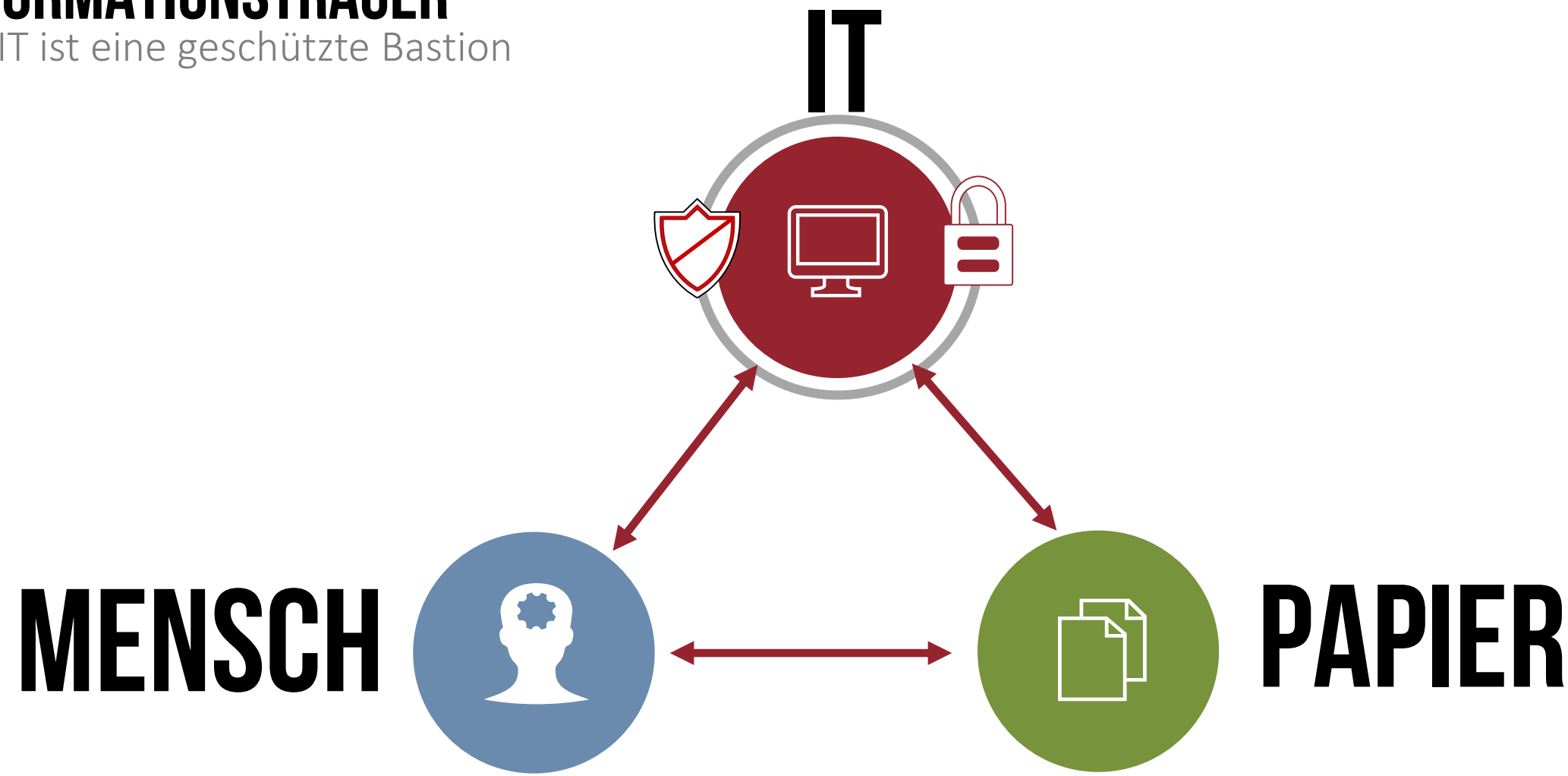
INFORMATIONSTRÄGER

Stehen in Beziehungen untereinander



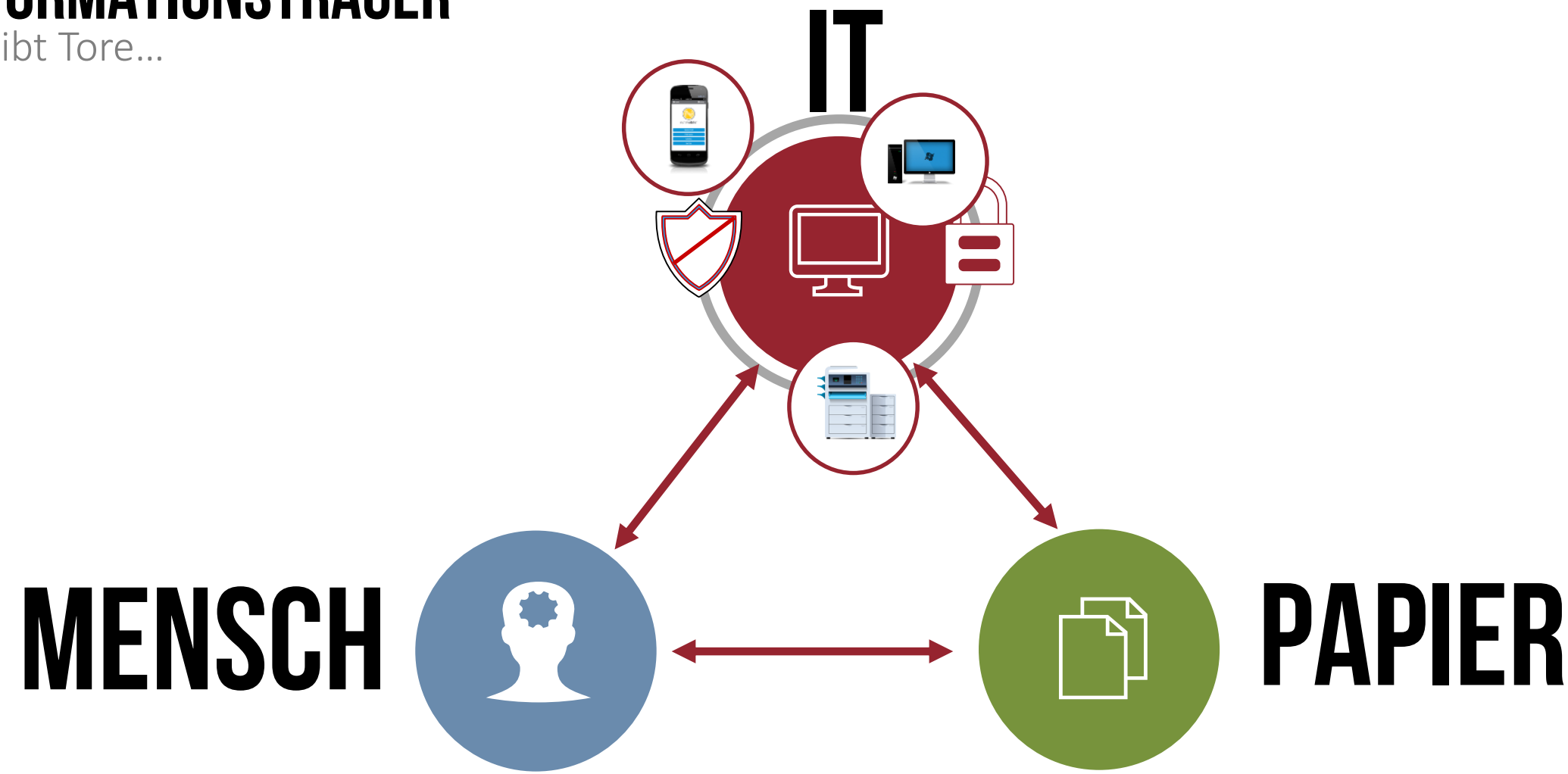
INFORMATIONSTRÄGER

Die IT ist eine geschützte Bastion



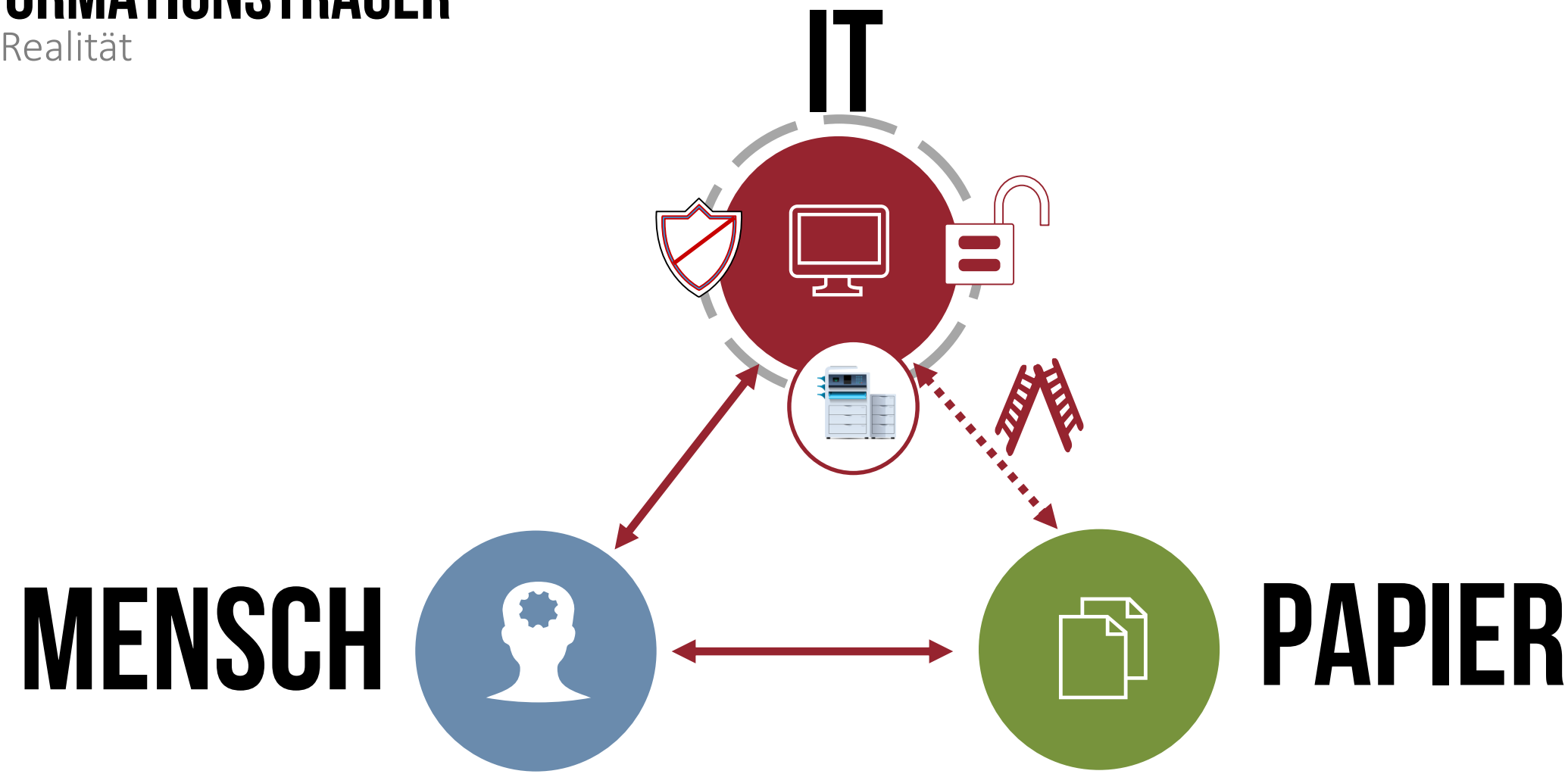
INFORMATIONSTRÄGER

es gibt Tore…



INFORMATIONSTRÄGER

Die Realität



EINFALLSTOR DRUCKER

WAS IST DIE “SPIELWIESE” FÜR IT + RECHT?

Europa, Deutschland, Organisation

ORGANISATIONEN
(Öffentliche Verwaltung
und Unternehmen)

HERAUSFORDERUNGEN (IN DEUTSCHLAND)

Vielschichtig

- **Verschärfte Sicherheitslage** in Deutschland
- **Zunahme** von **Angriffen auf die IT**
  (Cyberangriffe, Netzwerke, Druckinfrastrukturen)
- Zunahme von **Digitalisierung** (z.B. eGovernment etc.)
- **Abhängigkeit** von **IT-Systemen**
  (in wirtschaftlichen und gesellschaftlichen Bereichen)
- **Abhängigkeit** vom **Internet**
- **Neue Technologien/Innovationen:** Internet der Dinge, Maschine-to-Maschine, Telechirurgie …

GESETZGEBER SCHAFFEN RAHMEN

Regulatorische Beispiele

- **EU:** EU-Cybersicherheitsstrategie, NIS-Richtlinie (RL zur Netz- und Informationssicherheit), Zentrale (EU)-DSGVO …
- **Deutschland:** z.B. neues IT-SiG seit 26.07.2015 (Artikelgesetz)
  - ändert auch Vorschriften des BSI-Gesetzes
  - Einwirkung auf das Telekommunikationsgesetz (TKG) usw.

  Ziele:
  - Einhaltung eines Mindestniveaus an IT-Sicherheit
  - Zentrale Stelle für Meldungen von Verstößen über das BSI
  - Schutz (personenbezogener) Daten

Intension der Legislative

- Abwehr und Schutz von Schädigungen bereits bei der Umsetzung von Standardmaßnahmen

DIE MÄRKTE REAGIEREN

Regularien

Bsp. Presse

IT-SICHERHEIT / VERSICHERUNGSSCHUTZ

Risiko-Richtlinien

An den Attacken aus dem Cyberspace will künftig auch die deutsche Versicherungswirtschaft verdienen. Sie bastelt zurzeit an Musterbedingungen für neue IT Security-Versicherungspolicen und hat in einem ersten Schritt nun Standards für Sicherheitsmaßnahmen und -berater im deutschen Mittelstand veröffentlicht.

Wer steckt hinter dieser Attacke aus dem Cyberspace? Ein einzelner Hacker? Die organisierte Kriminalität? Der US-Geheimdienst? Oder ein chinesischer Wettbewerber? Diese Fragen zuverlässig beantworten zu können, dürfte in Zukunft wichtiger werden. Zumindest für die mittelständischen Unternehmen, die sich gegen Schäden versichern wollen, die durch Angriffe auf ihre IT verursacht werden.

„Die am Markt vorhandenen Deckungskonzepte konzentrieren sich überwiegend auf den industriellen und großgewerblichen Bereich", sagt Christian Ponzel, Sprecher des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. (GDV). „In diesen Segmenten

VdS-Geschäftsführer ***Robert Reinemann:*** *„Um die hohe Qualität bei der Umsetzung des VdS-Standards zu sichern, spielen die Cyber Security-Berater eine Schlüsselrolle."*

verfügen die Versicherungsnehmer im Regelfall über IT-Einheiten, die Schadenereignisse erkennen und die Beweise sichern können. Experten sprechen in diesem Zusammenhang auch von IT-Forensik. Insbesondere bei mittelständischen Unternehmen wird aus unserer Sicht das

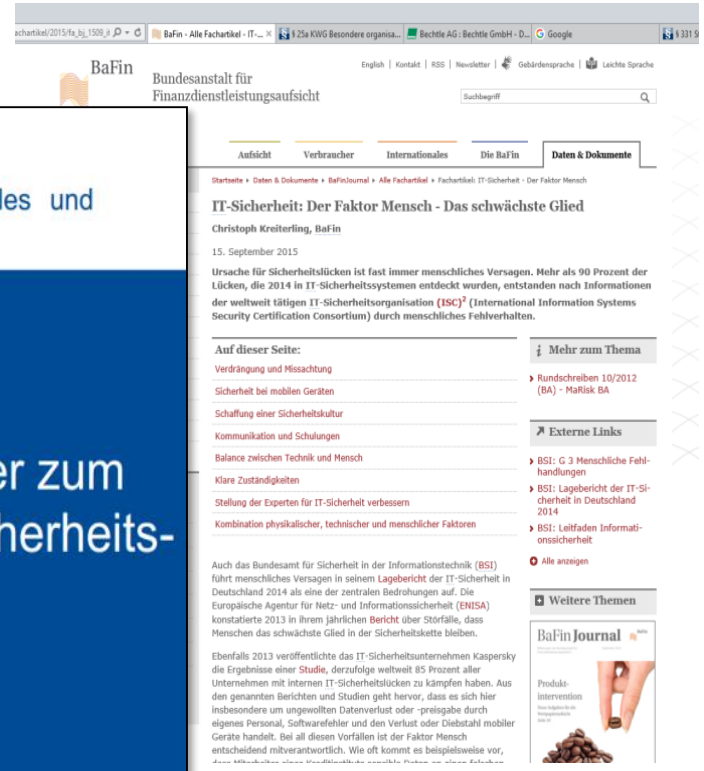
10

Quelle Infomarkt 2015

Aktionen von Aufsichtsbehörden

Rechnungshöfe des Bundes und der Länder

Grundsatzpapier zum Informationssicherheits-management



KONFRONTATION MIT LEGALEN PROBLEMATIKEN IN DER ORGANISATION

Beispielbereiche

BEISPIEL UNGESCHÜTZTE INFORMATIONEN

KEVIN MITNICK: GROSSMEISTER DES SOCIAL-ENGINEERING

geboren: 6. August 1963
FBI: „gefährlichster Hacker“

„Arbeitsnachweise“:

- mehr als 100 mal im Netzwerk des US Verteidigungsministeriums
- mehrfach im Netzwerk der NSA
- Statement Staatsanwalt: „„Mitnick kann einen Nuklearkrieg starten, indem er ins Telefon pfeift“

„Ohne großes technisches Know-how“
Mehrmals langjährig inhaftiert
Im Anschluss 3 Jahre IT-Nutzungsverbot

U.S. Department of Just
United States Marshals Serv

WANTED
BY U.S. MARSHALS

TICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
ited States Marshals Service NCIC entry number: (NIC/ W721460021).

AME: .....MITNICK, KEVIN DAVID
S (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

SCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

DDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

ANTED FOR: VIOLATION OF SUPERVISED RELEASE
RIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

ATE WARRANT ISSUED: NOVEMBER 10, 1992

SCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
HICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

arrested or whereabouts known, notify the local United States Marshals Office. (Telephone: 213-894-2485).
no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSM0000.

INFORMATIONS-LECKS

FÜHRUNGSPERSONEN TRAGEN VERANTWORTUNG

Hauptaufgaben

)"Wenn er nichts gewusst hat, ist er schuld!"

Dieselaffäre, Kommentar zu Winterkorn

1. **Organisation**
2. **Dokumentation**
3. **Kontrolle**

*)http://www.n-tv.de/wirtschaft/Ich-bin-sprachlos-article15976471.html , (2015)

FÜHRUNGSPERSONEN TRAGEN VERANTWORTUNG

Beispiele

FINANZDIENSTLEISTER

§ 25a KWG Besondere organisatorische Pflichten; Verordnungsermächtigung
Ein Institut muss über eine ordnungsgemäße Geschäftsorganisation verfügen […]
Besondere organisatorische Pflichten; Verordnungsermächtigung

Abs. 4 eine angemessene personelle und technisch-organisatorische Ausstattung des Instituts;

Abs. 5 […] die Festlegung eines angemessenen Notfallkonzepts, insbesondere für IT-Systeme […];

BEHÖRDEN

§ 75 Abs. 1 BBG
Pflicht zum Schadensersatz
[…] Beamtinnen und Beamte, die vorsätzlich oder grob fahrlässig die ihnen obliegenden Pflichten verletzt haben, haben dem Dienstherrn, dessen Aufgaben sie wahrgenommen haben, den daraus entstehenden Schaden zu ersetzen […];

§ 48 BeamtStG (Beamtenstatusgesetz) Pflicht zum Schadensersatz Beamtinnen und Beamte, die vorsätzlich oder grob fahrlässig die ihnen obliegenden Pflichten verletzen, haben dem Dienstherrn, dessen Aufgaben sie wahrgenommen haben, den daraus entstehenden Schaden zu ersetzen. Haben mehrere Beamtinnen oder Beamte gemeinsam den Schaden verursacht, haften sie als Gesamtschuldner. *>> gilt i. V. m. den jeweiligen Landesgesetzen;*

GMBH

§ 43 Abs. 1 GmbHG Treue, Sorgfalt und Sicherheit (GmbH)
[…] Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden. […]

- Status internes Risikomanagement im Unternehmen?
- IT-Sicherheit „up-to-date“?

z. B. Risiko bei Schädigungen Dritter: bei entstandenen Schaden
§ 823 BGB bei schuldhaften, rechtswidrigen Verhaltens (durch Tun oder Unterlassen) Schadensersatz bis in das Privatvermögen des Geschäftsführers;

AKTIENGESELLSCHAFT

§ 93 Abs. 2 S.1 AktG
[…] Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. […];

HEALTHCARE

§ 203 StGB
Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart […]
bis 2 Jahre bzw. Geldstrafe;

FÜHRUNGSPERSONEN TRAGEN VERANTWORTUNG

Beispiele

Verantwortung kann delegiert werden**,** dennoch: **Verantwortungsdelegation** schützt **nicht vor Strafen!**

§ 130 OWiG …geeignete Fachkräfte können kritische Aufgaben übernehmen, dennoch keine Entbindung von der Kontrolle durch Führungskräfte!

§ 130 Abs. 3 OWiG aufpassen – bei Pflichtverletzung können gem. **§ 30 OWiG**, Geldbußen drohen:

- bis 5 Mio. Euro bei Fahrlässigkeit
- bis 10 Mio. Euro bei Vorsatz

Spezielle Funktionsträger (Garantenpflicht):

§ 13 StGB
Wer es unterlässt, einen Erfolg abzuwenden, der zum Tatbestand eines Strafgesetzes gehört, ist nach diesem Gesetz nur dann strafbar, wenn er rechtlich dafür einzustehen hat […]

Dennoch: „[…] Pflicht, Rechtsverstöße und insbesondere Straftaten sind zu verhindern […]“ (BGH vom 17.07.2009, Az. 5 StR 394/08).

Das größte Risiko ist die eigene Untätigkeit!

- **Dokumentation:** Missstände fixieren, Tätigkeitsberichte, Verfahrensbeschreibungen, Risikomanagementsystem…
- **Reporting:** „Melden macht frei“ >> Risiko nach oben delegieren
- **Einbeziehung zuständiger Stellen:** Datenschutzbeauftragter, Betriebsräte…
- **Rechtliche Gestaltung:** Legitimation durch Betriebsvereinbarungen, Unternehmensrichtlinien…
- **Informieren durch:** Sensibilisierung / Schulung
- **Funktionsbeschreibung:** Aufgaben- u. Zuständigkeitsbereiche regeln

(FÜHRUNGS-)PERSONEN TRAGEN VERANTWORTUNG

Beispiele Datenschutzgrundverordnung (EU-) DSGVO

EU-DSGVO am 25.5.2016 in Kraft getreten, ersetzt ab 25.5.2018 das nationale Datenschutzrecht

- **Maßnahmen** gem. **Art. 25**: „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ ;*[…] der Verantwortliche trifft technische und organisatorische Maßnahmen […]*

- **Verantwortlichkeiten** werden erweitert gem. **Art. 26**: „Gemeinsam für die Verarbeitung Verantwortliche“ *[…] legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche […]*

- **Dokumentationspflichten** werden deutlich ausgeweitet gem. **Art. 30**: „Verzeichnis von Verarbeitungstätigkeiten “ ;*[…] Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen […]*

- Erweiterte **Bußgeldtatbestände**: bspw. Pflichten der Verantwortlichen und der Auftragsverarbeiter gem. **Art. 8, 11, 25** bis **39, 42, 43** etc.

- Möglichen **Bußgelder** erhöhen sich drastisch gem. **Art. 83**: **10 Mio. / 20. Mio. Euro** oder im Falle eines Unternehmens **2 % bzw. 4 %** seines weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres

Die neue DSGVO: http://www.datenschutz.bund.de

WEITERE NORMEN UND MÖGLICHE RECHTSFOLGEN

Beispiele

- Schadensersatz aus Vertrag § 280 BGB (Pflichtverletzung)
- Mitverschulden nach § 264 BGB, z.B. bei Mitwirkungspflichten
- Schadensersatz nach § 823 BGB (Organisationsverschulden)
- Verrat eines Geschäftsgeheimnisses § 17 UWG
- Bußgelder nach Datenschutzrecht
- Abmahnung wegen unlauterem Handeln, z.B. § 7 UWG (SPAM)
- Informations- bzw. Meldepflichten, § 42a BDSG, § 109a TKG, § 15a TMG, § 44b AtG, § 11 EnWG, § 8n BSIG
- Verlust des Versicherungsschutzes
- Probleme bei der Finanzierung
- Strafrecht / Bußgeld (§ 130 Abs. 1 i.V.m. § 30 OWiG)
- Negativer Prüfungsvermerk im Jahresabschluss (AG, GmbH, GmbH & Co.KG)
- …

MÖGLICHE RECHTSFOLGEN

Zusammenfassung

- Freiheitsstrafen
- Schadensersatzansprüche
- Ausfall der Versicherung
- Imageschäden

FAZIT

Eines Profis

„Es gibt zwei Arten von Organisationen:
solche, die schon **gehackt wurden**,
und solche **die es noch werden**.“

Robert Mueller, Direktor des FBI

KONTAKT

Ihre Ansprechpartner

Andreas Scholtz, LL.B.

Senior Business Consultant

T: +49 163 601 11 62

M: scholtz@mc-2.de

Dipl.-Ing. (FH) Martin Stolle

Senior Consultant

T: +49 170 563 85 62

M: stolle@mc-2.de

www.mc-2.de

+49 641 966 23 60

Ludwig Rinn Straße 14-16
35452 Heuchelheim