MASSNAHMEN ZU ANGEMESSENEM DATENSCHUTZ & DATENSICHERHEIT

first frame networkers
IT, die Sie weiterbringt

VORGABEN BEZÜGLICH MASSNAHMEN

first frame networkers
IT, die Sie weiterbringt

- Art. 7 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
  - Privacy by Default, datenschutzfreundliche Voreinstellungen
    Voreinstellungen sind so gesetzt, dass die Bearbeitung auf das Nötige beschränkt wird.
  - Privacy by Design
    Die Datenbearbeitung ist technisch und organisatorisch so ausgestaltet, dass die Datenschutzvorschriften eingehalten werden.
- Art. 8 Datensicherheit
  - Die Massnahmen entsprechen dem Umfang und dem durch die Bearbeitung entstehenden Risiko und dem Stand der Technik. Sie ermöglichen es, eine Verletzung der Datensicherheit zu vermeiden.
  - Mindestanforderungen werden vom Bundesrat definiert (revVDSG)

DATENSCHUTZ & DATENSICHERHEIT

first frame networkers
IT, die Sie weiterbringt

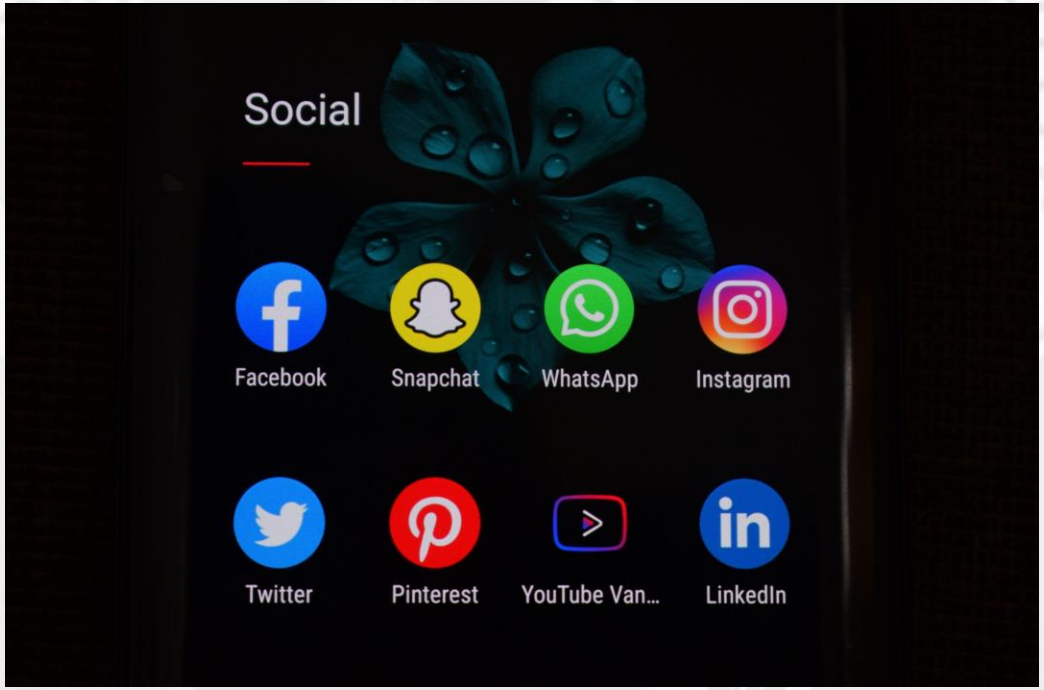
	Zielsetzung	Definition
Datenschutz	Vorhersagbarkeit (Predictability)	Zuverlässige Annahmen von betroffenen Personen, Verantwortlichen und Bearbeitern über Zweck und Resultat der Datenbearbeitung ermöglichen
	Verwaltbarkeit (Manageability)	Dokumentierte & granulare Datenbearbeitung, bspw. durch Funktionstrennung Verhindert dolose Handlungen, erlaubt Fehlern einzugrenzen.
	Trennbarkeit (Disassociability)	Bearbeitung von Daten ohne Zuordnung zu Personen
Datensicherheit	Vertraulichkeit (Confidentiality)	Schutz vor Offenlegung
	Integrität (Integrity)	Schutz vor unsachgemässer Änderung oder Zerstörung; Inkl. Nichtabstreitbarkeit der Bearbeitung und Authentizität der Daten
	Verfügbarkeit (Availability)	Sicherstellen des rechtzeitigen und zuverlässigen Zugangs zu Daten

VORHERSAGBARKEIT

first frame networkers
IT, die Sie weiterbringt

Die Datenbearbeitung verfolgt einen bestimmten Zweck und liefert für alle Beteiligten vorhersagbare Resultate.

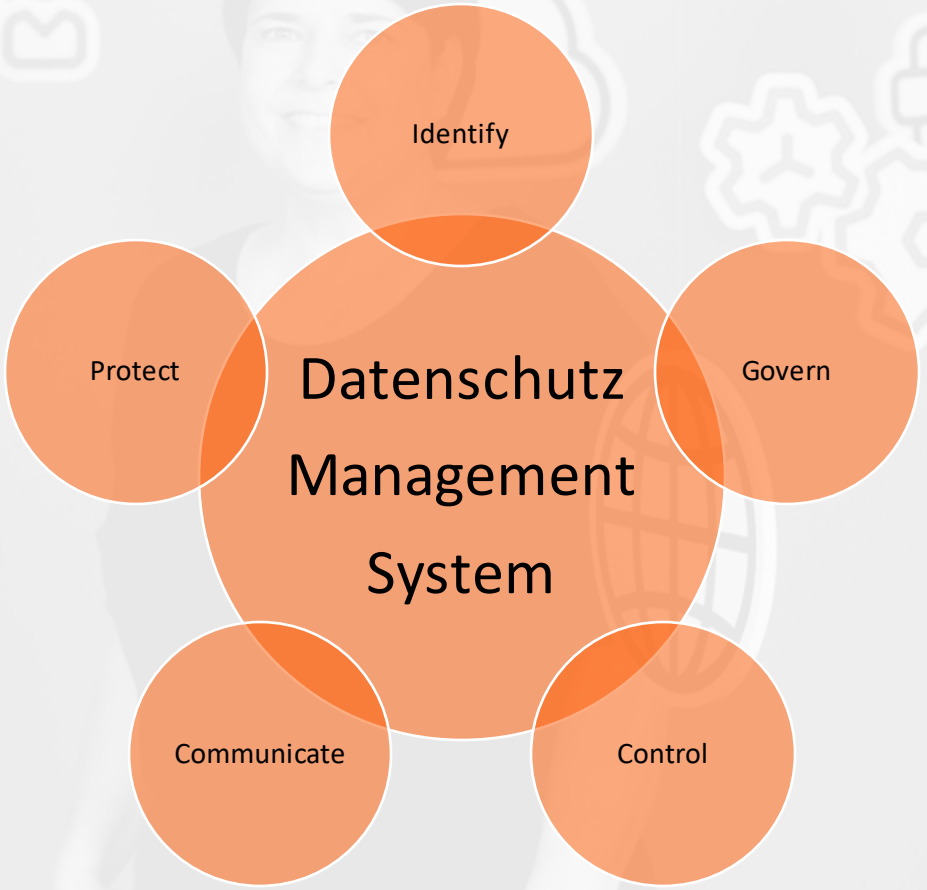
Beteiligte sind Betroffene, Verantwortliche, Auftragsbearbeiter! & Kriminelle?



VERWALTBARKEIT

first frame networkers
IT, die Sie weiterbringt

Prozesse werden dokumentiert, Interessenkonflikte durch Funktionstrennung und Rollenzuteilung vermieden und Bearbeitungsschritte protokolliert.



TRENNBARKEIT

first frame networkers
IT, die Sie weiterbringt

Datenbearbeitung erfolgt ohne Zuordnung zu Personen oder Geräten (Smartphone, Computer, …)

VERFÜGBARKEIT

first frame networkers
IT, die Sie weiterbringt

golem.de IT-NEWS FÜR PROFIS
HOME TICKER VIDEOS VORGELESEN FORUM | ANMELDEN
Golem.de jetzt werbefrei lesen TOP-THEMEN: CES 2021 Auto Netzpolitik mehr...
RE: STELLENMARKT AKADEMIE SHIFOO IT-KÖPFE GEHALTSCHECK | SERVICES: GOLEM-PC PREISVERGLEICH T

ADOBE

Flash-Abschaltung legt Züge in China lahm

Trotz des vor drei Jahren von Adobe angekündigten Endes von Flash ist die Software noch im Einsatz. Oder auch nicht.

25. Januar 2021, 11:43 Uhr, Werner Pluta

(Bild: Xiquinhosilva/Wikipedia/CC-BY 2.0)

Bahnhof von Dalian: Nichts ging mehr.

Vorhersagbarkeit <-> Verfügbarkeit

Quelle: https://www.golem.de/news/adobe-flash-abschaltung-legt-zuege-in-china-lahm-2101-153650.html

VERTRAULICHKEIT

first frame networkers
IT, die Sie weiterbringt

IT INSIDE IT
Das Portal für IT-Verantwortliche

News Inserieren Auf ein Bier Digital Channels Forum

Technologie Partner

Gold Sponsoren

< Zurück zur Startseite

Daten aus Cyber-Attacke auf Stadler Rail veröffentlicht

STADLER RAIL, SECURITY, ATTACKE, CYBERCRIME,

Von Philipp Anz, 29. Mai 2020 14:28 Letzte Aktualisierung: 02. Juni 2020 15:37

Hacker haben Daten aus dem Angriff von Anfang Mai online gestellt. Stadler erklärt, nicht auf die Erpressung einzugehen.

Vertraulichkeit <-> Verwaltbarkeit

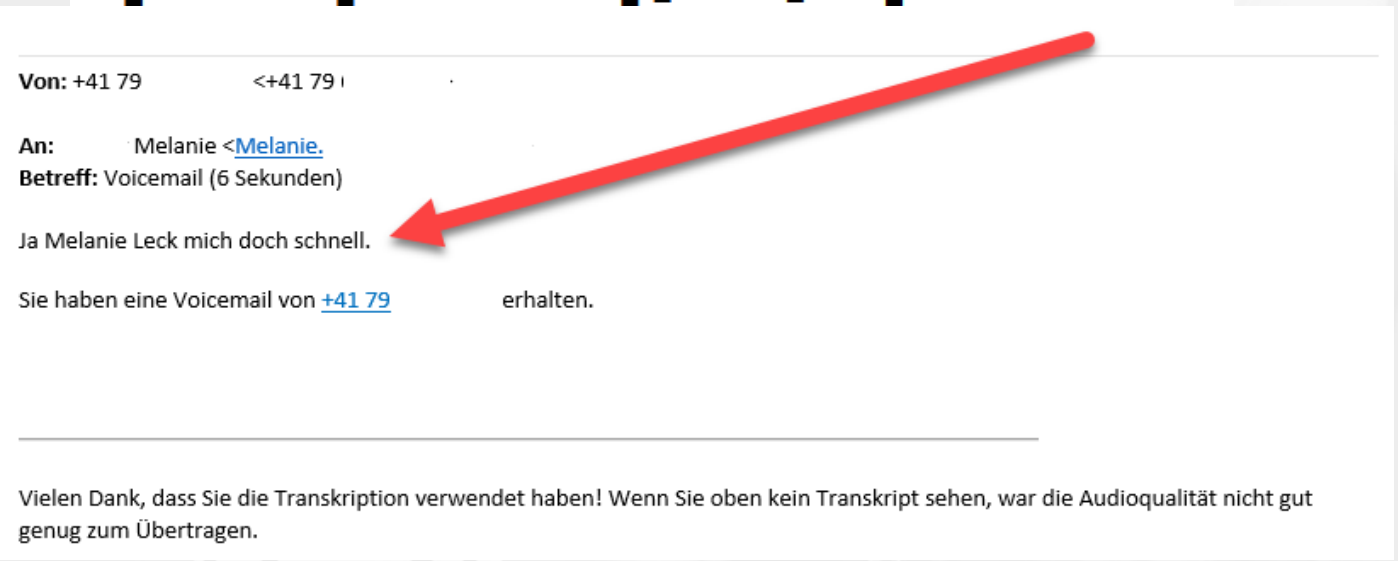
Vertraulichkeit <-> Trennbarkeit

INTEGRITÄT, SCHUTZ VOR VERÄNDERUNG

first frame networkers
IT, die Sie weiterbringt

Schockierte Bank-Coop-Kundin

«Erhielt Kontoauszüge von



Von: +41 79 <+41 79

An: Melanie <Melanie.
Betreff: Voicemail (6 Sekunden)

Ja Melanie Leck mich doch schnell.

Sie haben eine Voicemail von +41 79 erhalten.

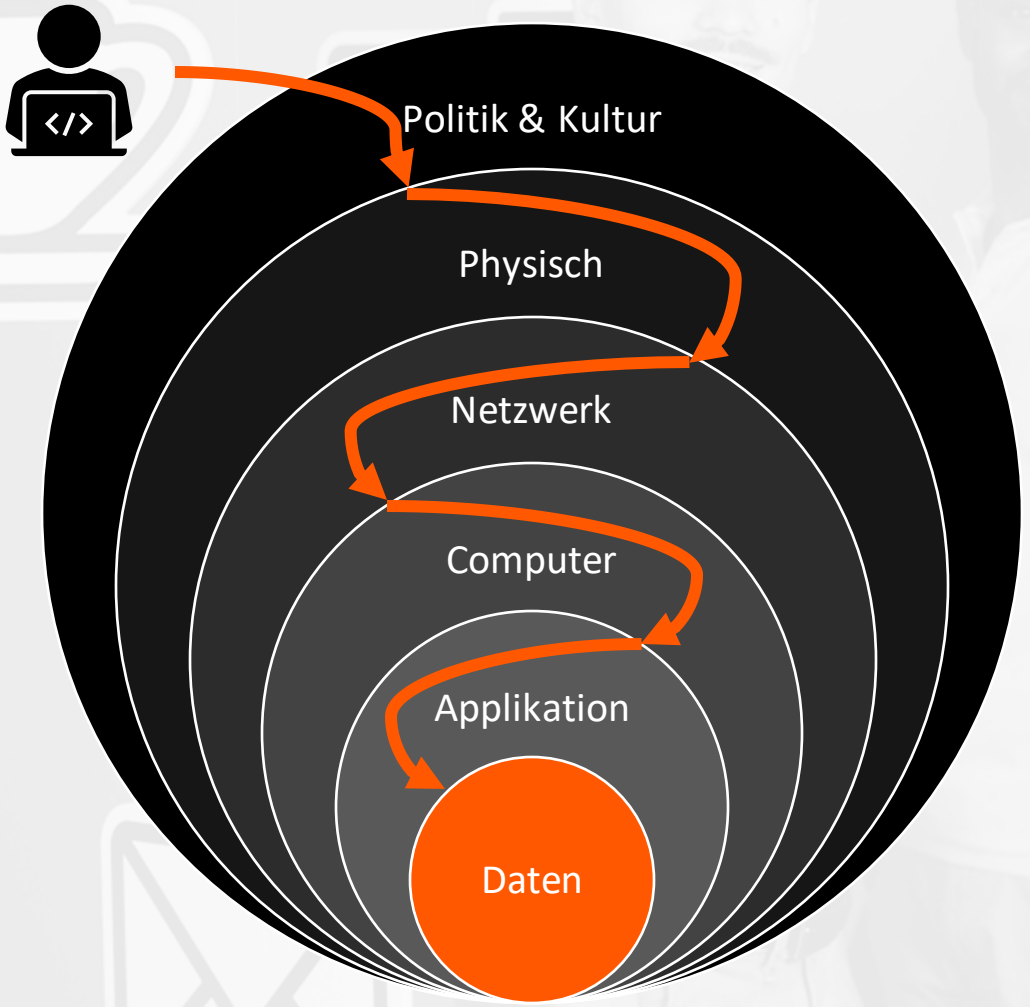
Vielen Dank, dass Sie die Transkription verwendet haben! Wenn Sie oben kein Transkript sehen, war die Audioqualität nicht gut genug zum Übertragen.

Daten dürfen nicht unsachgemäss verändert werden, die Authentizität der Daten muss gewährleistet sein und die Bearbeitung muss nachvollziehbar erfolgen.

Dies gilt auch für Algorithmen,
die Kurznachricht lautete ursprünglich:
«Ja Melanie, lüt mer doch schnell ah, Danke »

SICHERHEIT IM ZWIEBELSCHALENPRINZIP

first frame networkers
IT, die Sie weiterbringt



Weisungen, Schulungen, Risikomanagement, Firmenkultur

Geschäftsprozesse, Sicherheitszonen, Funktionstrennung

Netzwerktrennung, Event Erkennung und Alarmierung

Aktualisierung von Betriebssystem und Treiber, Verschlüsselung, Endpoint Security (EDR)

Software-Patches, Web- und Spam-Filter, Schutz von Webapplikationen, Isoliertes Websurfen

Berechtigungsmanagement, Datei- / Datenbank-Verschlüsselung

TYPISCHE ORGANISATORISCHE MASSNAHMEN

first frame networkers
IT, die Sie weiterbringt

- Dokumentierte Verfahren und Vorgaben
  Geschäftsprozesse und Weisungen mit geregelten Verantwortlichkeit
  Interne Audits zur kontinuierlichen Verbesserung
- Schulungen
  Geschäftsprozesse, Sicherheitsverfahren, Datenschutzverfahren
- Auftragsbearbeiter in Pflicht nehmen und überwachen
  Vertragliche Vereinbarungen, Audits
- Datenschutz & Sicherheitsmanagement unter Anwendung von Standards & Normen
  DMS & ISMS, Sicherheitsorganisation, Risikomanagement, …
- Durchführen von Wirksamkeitsprüfungen

STANDARDS UND NORMEN

first frame networkers
IT, die Sie weiterbringt

first security framework

Identifizieren		Schützen		Erkennen		Reagieren		Wiederherstellen	
Gesamtzustand Identifizieren	**1**	**Gesamtzustand Schützen**	**3**	**Gesamtzustand Erkennen**	**1**	**Gesamtzustand Reagieren**	**3**	**Gesamtzustand Wiederherstellen**	**2**
Inventar der Werte	2	Ausgebildete Benutzer	2	Achtsame Mitarbeiter	2	Notfallpläne	3	Business Continuity Management	2
Sicherheitspolitik	1	Segmentierte Netzwerke	3	Überwachte Dienste	1	Krisenstab	2	Verbesserung durch Lernen	4
Risiko Management	1	Identity, Access & Credential Mgmt	3	Überwachte Netzwerkübergänge	0	Notfall Team	4	Kommunikation von Vorfällen	3
Sicherheitsrichtlinien	0	Privilegierte Accounts & Active-Directory	2	Indicator of Compromise erkennen	3	Analytik	4	Desaster Datacenter	0
Sicherheitsorganisation	0	Geschützte Computer	4	Fallen: Canaries & Honeypots	0			Desaster Site	0
Sicherheitskommunikation	1	Geschützte Smartphones	4	Alarmierung	2			Forensik	2
Datenschutz	1	Geschützte Server	5	Penetration-Test	0				
Lieferantenmanagment	3	Geschützte Web-Applikationen	4						
Objektive Wirksamkeitsüberprüfung	0	Datensicherung	5						
		Physischer Schutz	2						
		Definierte Prozesse im Unternehmen	3						
		Prozesse der ICT-Dienstleister	4						

Legende: Massnahme: inexistent 0 - 5 vollständig umgesetzt

Trend Umsetzungsstand: ◦ erstmals beurteilt, → bleibt gleich, ↗ verbessert, ↘ reduziert

Prüfung vom DATUM

© first frame networkers ag

Version 10, 30.09.2020

ISO IEC

TYPISCHE TECHNISCHE MASSNAHMEN

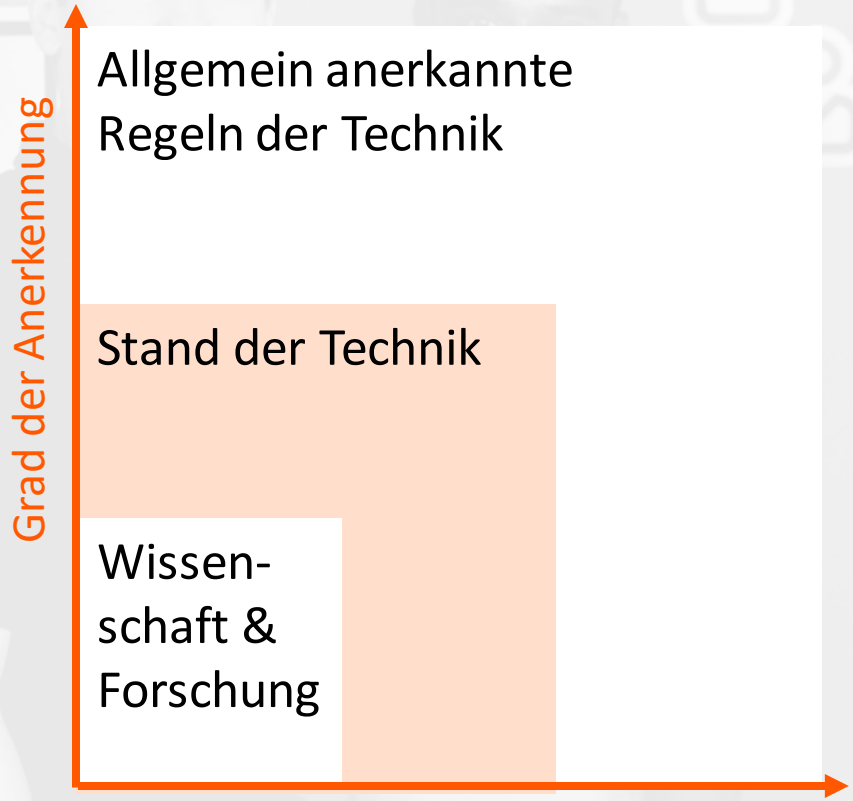
first frame networkers
IT, die Sie weiterbringt

- Zugangskontrolle für Zutritt und Zugriff
  Mit angemessenen Authentifizierungsverfahren, auch für Dritte
- Verschlüsselung (während Speicherung, auf dem Transportweg)
  Schlüsselverwaltung erfolgt durch Verantwortliche: Bring your own Key
- Datensicherung gemäss 3-2-1-Ø Regel
  3 Kopien auf 2 unterschiedlichen Medien, wovon 1 an externem Speicherort und nicht mit Windows-Credentials zugänglich,
  Ausführung und Konfigurationsänderung von Backupjobs aktiv überwachen
- Übliche Informationssicherheitsmassnahmen gemäss Stand der Technik
  -> Wirksamkeitsprüfungen durchführen!

STAND DER TECHNIK

first frame networkers
IT, die Sie weiterbringt

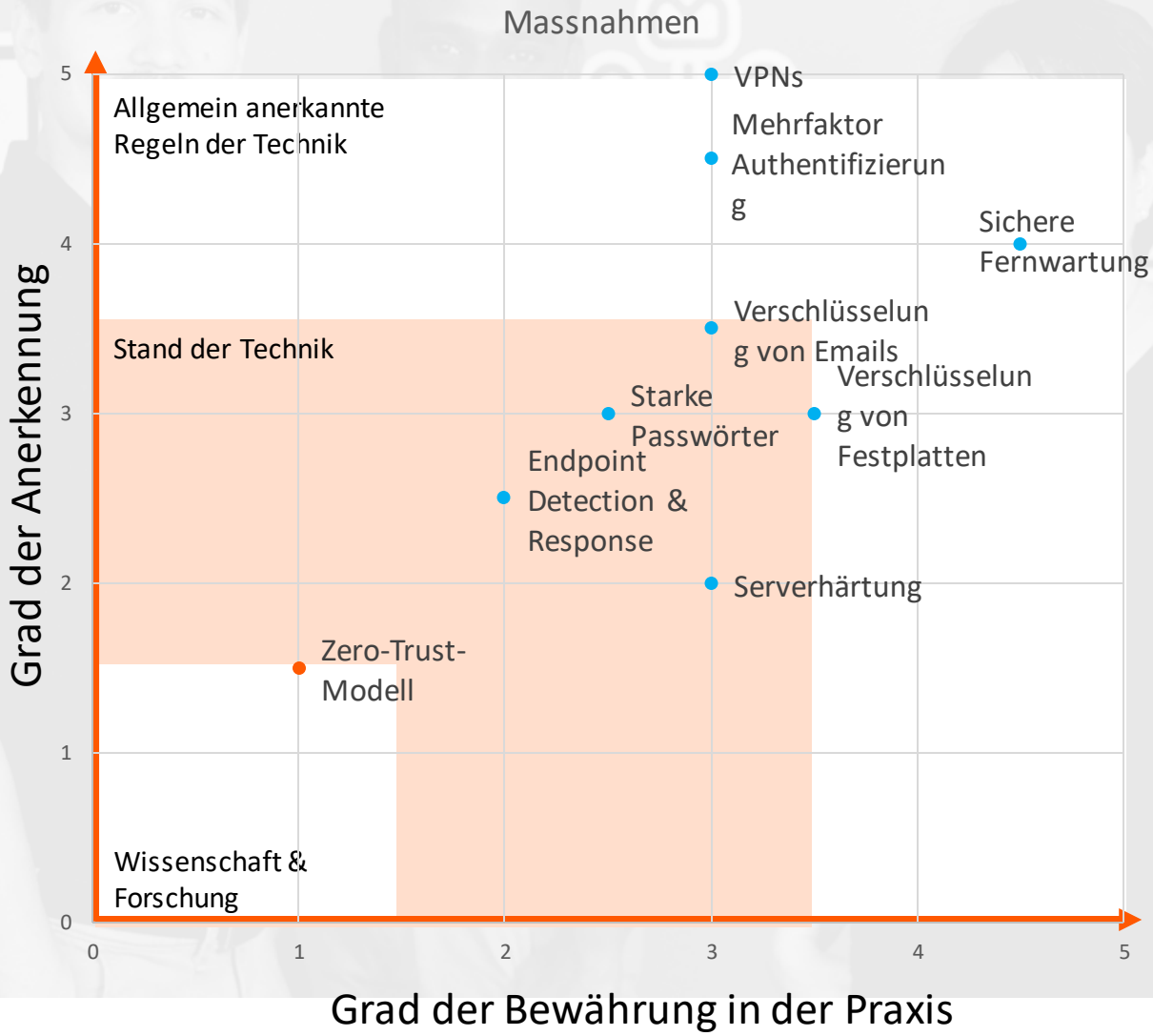
- Wiss. Publikation vs. Massenmedien?
- Bezug auf Normen?
- Empfehlung von Verbänden?
- Regelmässige Eignungsprüfung?



- Innovationsgrad?
- Erprobung Labor vs. Massenmarkt?
- Periodizität der Aktualisierung durch Hersteller?

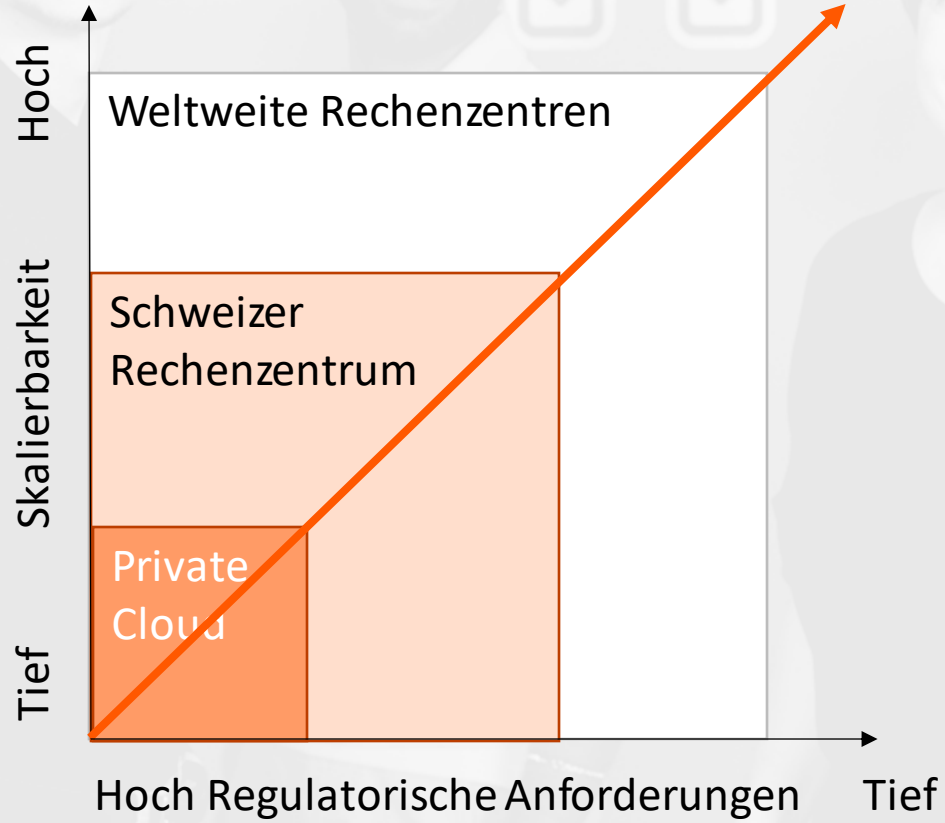
STAND DER TECHNIK

first frame networkers
IT, die Sie weiterbringt



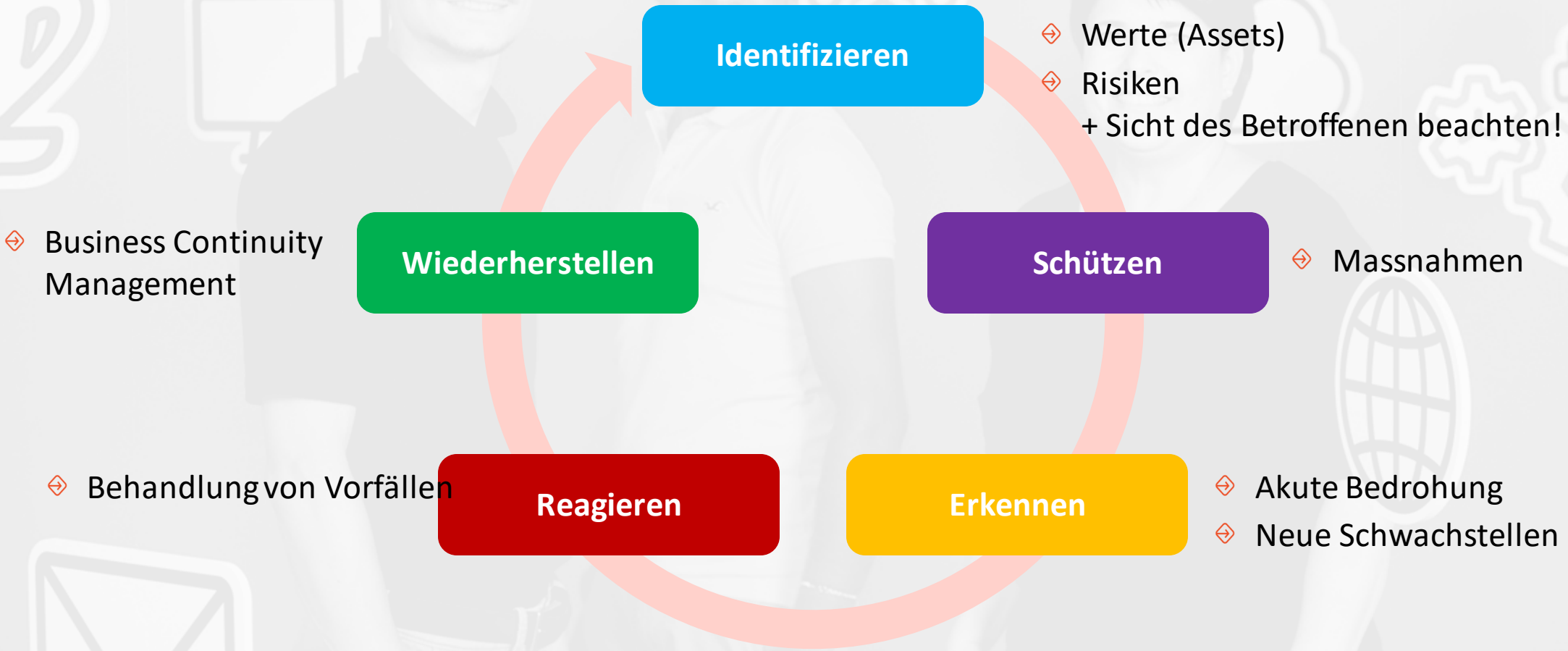
BEKANNTGABE VON PERSONENDATEN INS AUSLAND

first frame networkers
IT, die Sie weiterbringt



INFORMATIONSSICHERHEIT EIN STÄNDIGER PROZESS

first frame networkers
IT, die Sie weiterbringt



RISIKOMANGEMENT DURCH DATENSCHUTZ FOLGENABSCHÄTZUNG

first frame networkers
IT, die Sie weiterbringt

- **A** • Prüfung der Erforderlichkeit einer DSFA
- **B** • Datenschutz-Folgenabschätzung (DSFA)
- **1** • Beschreibung der Datenbearbeitung
- **2** • Prüfung der Einhaltung des Datenschutzrechts und Dokumentation der Massnahmen
- **3** • Risiken für betroffene Personen
- **C** • Risikobeurteilung

PFLICHTEN DIE NACH (TECHNISCHEN) LÖSUNGEN RUFEN

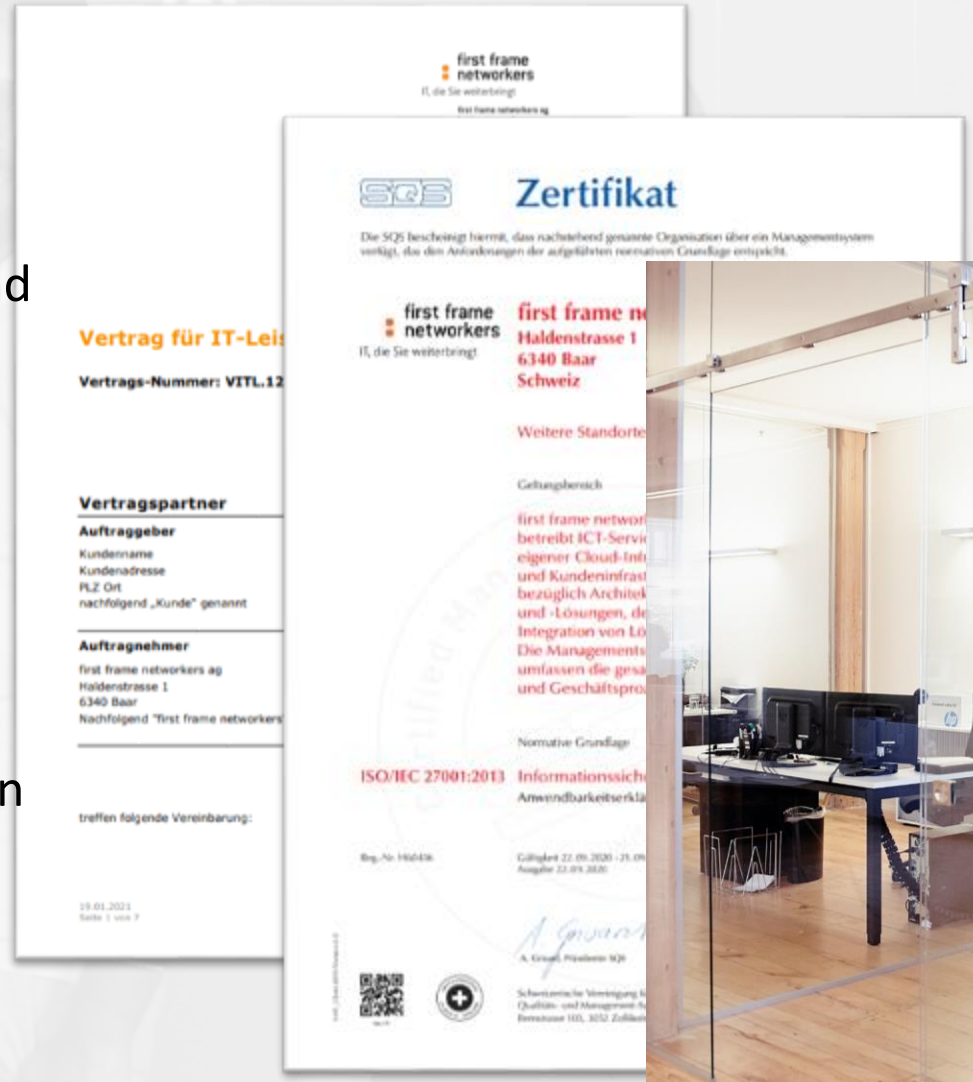
first frame networkers
IT, die Sie weiterbringt

- Meldepflicht (Art. 24)
  revDSG nennt keine Frist (rasch), DSGVO: 72h
  Analyse des Vorfalls wichtig
  - Zentrales Logging
- Rechte der betroffenen Person (Art. 32)
  Verbieten der Bearbeitung, Untersagen der Bekanntgabe an Dritte, Löschung oder Vernichtung
  - Systeme zur Bearbeitung müssen entsprechende Funktionen bereitstellen
    Desaster Recovery Konzepte müssen das Nachführen von Löschungen erlauben
- Verzeichnis der Bearbeitungstätigkeiten
  - Elektronische Unternehmensdokumentation, Prozessmanagement, Recordsmanagement, …
    -> Metadaten unterstützen, hilft auch bei der Risikoanalyse

UMGANG MIT AUFTRAGSBEARBEITERN

first frame networkers
IT, die Sie weiterbringt

- Bestimmungen zum Datenexport einhalten
- Verantwortlicher muss durch Instruktion und Kontrolle sicherstellen, dass der Auftragsbearbeiter
  - nur die definierte Datenbearbeitung durchführt,
  - dies Datenschutzkonform erfolgt,
  - seinen Verantwortlichkeiten und Pflichten nach DSG nachkommen kann.
- Unterauftragsbearbeiter melden lassen



WIE WÄHLE ICH SINNVOLLE MASSNAHMEN?

first frame networkers
IT, die Sie weiterbringt

- Risiko durch die Bearbeitung **für den Betroffenen**
  Hohes Risiko (besonders schützenswerte Daten, besonders umfassende Bearbeitung) -> Schutzmassnahmen gemäss Datenschutz-Folgenabschätzung
- Einhalten von Prinzipien
  - Datensparsamkeit
    Aufteilung auf Teilprozesse, mit Funktionstrennung & Pseudonymisierung oder Anonymisierung
  - Datensicherheit
    Sicherheitsmassnahmen nach dem Stand der Technik
- Auftragsbearbeiter in die Pflicht nehmen
  Vertrag, Zertifizierungen, Audits
- Orientierung an Standards und Normen

ISO 29151 & ISO 27701	als Erweiterung zu ISO 27001
NIST Privacy Framework Core	und NIST Cyber Security Framework Core
Privacy Implications Guide	zu CIS Critical Security Controls

FAZIT

first frame networkers
IT, die Sie weiterbringt

- Datenschutz muss interdisziplinär angegangen werden.
  Geschäftsanforderungen, juristische Gesichtspunkte und technische Möglichkeiten müssen in Einklang gebracht werden.
- Massnahmen müssen nachvollziehbar und bedienbar sein.
  Je komplizierter und einschränkender eine Massnahme um so eher wird sie umgangen: «Ich muss arbeiten können!»
- Die Anforderungen ergeben sich aus dem Risiko und müssen unabhängig von den Ressourcen erfüllt werden.
  Der Scope ist immer Verantwortliche(r) und Auftragsbearbeiter und Unterauftragsbearbeiter!
- Informationssicherheit ist eine Grundlage für Datenschutz.
- Technik kann begeistern, wenn sie auf einem organisatorisch stabilen Sockel steht.

LINKLISTE

first frame networkers
IT, die Sie weiterbringt

- Revidiertes DSG: Perma | https://perma.cc/QD2G-F5DS
- Handreichung zum «Stand der Technik»: TeleTrusT-Handreichung "Stand der Technik in der IT-Sicherheit«
- Leitfaden Technische und organisatorische Massnahmen des Datenschutzes: Technische und organisatorische Massnahmen des Datenschutzes (admin.ch)
- Datenschutz Self Assessment Tool: www.dsat.ch
- NIST Cybersecurity Framework | Privacy Framework
- Center for Internet Security ®: https://www.cisecurity.org/