

DATENSCHUTZ

Nur Schall und Rauch?

Wenn Daten gesundheitsschädlich
werden...



BitHawk

AGENDA

Überblick Datenschutzgesetz

Ursula Uttinger, Terrence Schweizer

Datenschutzgesetz & IT-Sicherheit in der Praxis

Ursula Uttinger, Terrence Schweizer

FACTS & FIGURES

4

Standorte in der
Schweiz

200

Mitarbeiter

52

Millionen
CHF Umsatz

15

Auszeichnungen
seit 2015

über

40

Service Management
Kunden

über

1200

Überwachte
Serversysteme

140

Zertifizierte technische
Spezialisten

über

800

Kunden

STRATEGISCHE PARTNER



Silver Services
Partner

Silver Sales
Partner



Gold Cloud Productivity
Gold Cloud Platform
Gold Small and Midmarket Cloud Solutions
Gold Datacenter
Gold Windows and Devices
Gold Messaging
Gold Communications
Gold Collaboration and Content
Silver Enterprise Mobility Management



ÜBER 15 AUSZEICHNUNGEN SEIT 2015

INITIATIVE MITTELSTAND

BEST OF

2015 / 2016 / 2017

ISG PROVIDER LENS

LEADER

SWITZERLAND
2015 - 2019

SWISS ARBEITGEBER

7 Platz

AWARD 2018

2015

MICROSOFT

Partner of the Year

2016 / 2017

CISCO

Partner of the Year

2017

CITRIX

Partner of the Year

ÜBER 800 KUNDEN VERTRAUEN UNS



Überblick Datenschutzgesetz

Datenschutzgesetz & IT-Sicherheit in der Praxis

Ursula Uttinger
Juristin (lic. iur.)
Datenschutzspezialistin

Terrence Schweizer
Dipl. El. Ing ETH
CDO BitHawk AG



BitHawk

Warum dieses Format?



Warum dieses Format?

Die DSGVO erfordert ein kooperatives Zusammenspiel zwischen Recht und Technik!

RECHT	TECHNIK
Rechtswissenschaft Werte und Prinzipien	Naturwissenschaft Formale Methoden und Beweise
Rechtstexte Auslegung und Interpretation	Normen und Standards Bestimmt und eindeutig
Viele Grautöne	Schwarz/Weiss

Was ist Datenschutz?





Brussels, Belgium

1972: «Blue Marbel» aufgenommen von der Apollo 17 Besatzung.



BitHawk



WIKIPEDIA:

Umweltschutz bezeichnet die Gesamtheit aller Maßnahmen zum Schutze der Umwelt, um die Gesundheit des Menschen zu erhalten.

**Hans-Dietrich Genscher «erster Deutscher Umweltminister», 1974 – 1992
Er hat den Begriff Umweltschutz aus den USA in die Deutsche Presse gebracht.**

Selbstmord einer 13-Jährigen: In Sozialen Medien laufen Schuldzuweisungen - was tun?

von Andreas Maurer — Schweiz am Wochenende • Zuletzt aktualisiert am 9.9.2017 um 05:48 Uhr



Datenschutz bezeichnet die Gesamtheit aller Maßnahmen zum Schutze der persönlichen Daten, um die Gesundheit des Menschen zu erhalten.

Personendaten weg, Geld weg, Chefjob weg

Es klingt wie ein Albtraum: Zuerst wird über den Chef der schwedischen Securitas der Konkurs verhängt, dann verliert er alle Ämter. Schuld ist ein Betrüger, der seine Personendaten stahl.

Ingrid Meissl Årebo, Stockholm
13.7.2017, 20:18 Uhr





Recht auf OptIn

Recht auf Auskunft

Recht auf Vergessen



BitHawk



Senate Judiciary & Commerce Committees
Joint Hearing

C-SPAN
c-span.org

Welche
Datenschutzgesetze
gibt es?



BitHawk

Welche Datenschutzgesetze gibt es?

CH - DSG

- Jeder Kanton: gesetzliche Grundlage – unterschiedliche Namen
- Je nachdem Gemeinde
- Spezialgesetze
 - Bankgeheimnis, Amtsgeheimnis, Berufsgeheimnis
 - Verordnung Videoüberwachung im öffentlichen Verkehr

International:

- DSGVO = GDPR
- DSG FL
- OECD-Richtlinie
- Kanada, Israel, Neuseeland, Uruguay, Argentinien

Für wen gilt was?



BitHawk

Für wen gelten diese Gesetze?

Bundesgesetz über den Datenschutz (DSG)

- CH: natürlich und juristische Personen geschützt
- Datenbearbeitung durch private Personen und/oder Bundesorgane
- Achtung Föderalismus! Kantonale/kommunale Gesetze bei kantonalen/kommunalen Organen

DSGVO

- Unternehmen der EU
- Bei Schweizer Unternehmen: Art. 3 DSGVO:
 - Niederlassung oder Auftragsdatenbearbeitung in der EU
 - Anbieten von Waren oder Dienstleistungen in der EU
 - Verhaltensbeobachtung von Personen in der EU

Wie kann die EU auf ein CH-Unternehmen zugreifen?

- Niederlassung in der EU
- Korrespondenzadresse in der EU
- Via CH-Gerichte

Praktisches Beispiel

Gärtner CH



Praktisches Beispiel

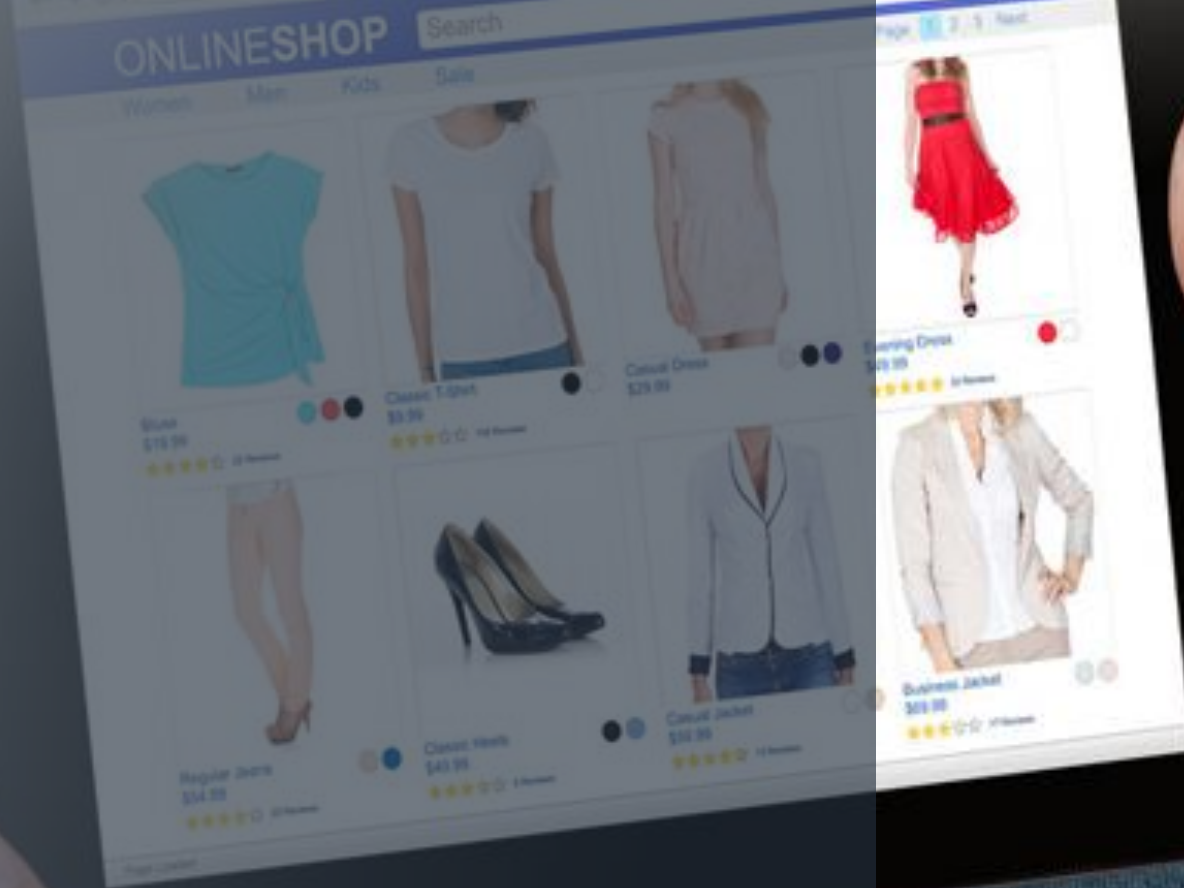
Beratungsbüro CH



BitHawk

Praktisches Beispiel

Onlinehändler CH



BitHawk

[illegible]

Was bedeuten die wichtigsten Grundsätze des Datenschutzes?



BitHawk

Datenschutz-Grundsätze

- Rechtmässigkeit
- Treu und Glauben
- Verhältnismässigkeit
- Zweckbindung
- Transparenz
- Richtigkeit
- Datensicherheit



Einige Punkte aus der DSGVO



Begriffe – neu (Art. 4)

- Profiling: Verhalten von Personen soll analysiert bzw. Vorhergesagt werden
- Pseudonymisierung: ohne weitere Informationen können personenbezogene Daten nicht einer bestimmten Person zugewiesen werden
- Genetische Daten / Biometrische Daten / Gesundheitsdaten

DSGVO	
Kapitel 1 (Art. 1 – 4)	▼
Allgemeine Bestimmungen	
Kapitel 2 (Art. 5 – 11)	▼
Grundsätze	
Kapitel 3 (Art. 12 – 23)	▼
Rechte der betroffenen Person	
Kapitel 4 (Art. 24 – 43)	▼
Verantwortlicher und Auftragsverarbeiter	
Kapitel 5 (Art. 44 – 50)	▼
Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen	
Kapitel 6 (Art. 51 – 59)	▼
Unabhängige Aufsichtsbehörden	
Kapitel 7 (Art. 60 – 76)	▼
Zusammenarbeit und Kohärenz	
Kapitel 8 (Art. 77 – 84)	▼
Rechtsbehelfe, Haftung und Sanktionen	
Kapitel 9 (Art. 85 – 91)	▼
Vorschriften für besondere Verarbeitungssituationen	
Kapitel 10 (Art. 92 – 93)	▼
Delegierte Rechtsakte und Durchführungsrechtsakte	
Kapitel 11 (Art. 94 – 99)	▼
Schlussbestimmungen	

Verpflichtungen (Kapitel 4)

- Datenschutzfreundliche Voreinstellungen
- Vertreter in der EU
- Verzeichnis von Verarbeitungstätigkeiten
- Meldung von Verletzungen von Datenschutz
- Datenschutzfolgeabschätzungen
- In Ausnahmefällen: Datenschutzbeauftragten

DSGVO	
Kapitel 1 (Art. 1 – 4)	▼
Allgemeine Bestimmungen	
Kapitel 2 (Art. 5 – 11)	▼
Grundsätze	
Kapitel 3 (Art. 12 – 23)	▼
Rechte der betroffenen Person	
Kapitel 4 (Art. 24 – 43)	▼
Verantwortlicher und Auftragsverarbeiter	
Kapitel 5 (Art. 44 – 50)	▼
Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen	
Kapitel 6 (Art. 51 – 59)	▼
Unabhängige Aufsichtsbehörden	
Kapitel 7 (Art. 60 – 76)	▼
Zusammenarbeit und Kohärenz	
Kapitel 8 (Art. 77 – 84)	▼
Rechtsbehelfe, Haftung und Sanktionen	
Kapitel 9 (Art. 85 – 91)	▼
Vorschriften für besondere Verarbeitungssituationen	
Kapitel 10 (Art. 92 – 93)	▼
Delegierte Rechtsakte und Durchführungsrechtsakte	
Kapitel 11 (Art. 94 – 99)	▼
Schlussbestimmungen	

Rechte (Kapitel 3)

- Transparente Information
- Informationspflicht bei Erhebung der Daten
- Auskunftsrecht
- Berichtigung und Löschung
- Widerspruchsrecht bei automatisierter Bearbeitung

DSGVO	
Kapitel 1 (Art. 1 – 4)	▼
Allgemeine Bestimmungen	
Kapitel 2 (Art. 5 – 11)	▼
Grundsätze	
Kapitel 3 (Art. 12 – 23)	▼
Rechte der betroffenen Person	
Kapitel 4 (Art. 24 – 43)	▼
Verantwortlicher und Auftragsverarbeiter	
Kapitel 5 (Art. 44 – 50)	▼
Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen	
Kapitel 6 (Art. 51 – 59)	▼
Unabhängige Aufsichtsbehörden	
Kapitel 7 (Art. 60 – 76)	▼
Zusammenarbeit und Kohärenz	
Kapitel 8 (Art. 77 – 84)	▼
Rechtsbehelfe, Haftung und Sanktionen	
Kapitel 9 (Art. 85 – 91)	▼
Vorschriften für besondere Verarbeitungssituationen	
Kapitel 10 (Art. 92 – 93)	▼
Delegierte Rechtsakte und Durchführungsrechtsakte	
Kapitel 11 (Art. 94 – 99)	▼
Schlussbestimmungen	

Busse (Kapital 8)

- Haftung
- Schadenersatz
- Busse: bis 10 Mio. bzw. bis zu 2% weltweiter Umsatz bei kleineren Verstößen; ansonsten 20 Mio. bzw. bis zu 4% weltweiter Umsatz

DSGVO	
Kapitel 1 (Art. 1 – 4)	▼
Allgemeine Bestimmungen	
Kapitel 2 (Art. 5 – 11)	▼
Grundsätze	
Kapitel 3 (Art. 12 – 23)	▼
Rechte der betroffenen Person	
Kapitel 4 (Art. 24 – 43)	▼
Verantwortlicher und Auftragsverarbeiter	
Kapitel 5 (Art. 44 – 50)	▼
Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen	
Kapitel 6 (Art. 51 – 59)	▼
Unabhängige Aufsichtsbehörden	
Kapitel 7 (Art. 60 – 76)	▼
Zusammenarbeit und Kohärenz	
Kapitel 8 (Art. 77 – 84)	▼
Rechtsbehelfe, Haftung und Sanktionen	
Kapitel 9 (Art. 85 – 91)	▼
Vorschriften für besondere Verarbeitungssituationen	
Kapitel 10 (Art. 92 – 93)	▼
Delegierte Rechtsakte und Durchführungsrechtsakte	
Kapitel 11 (Art. 94 – 99)	▼
Schlussbestimmungen	

Vergleich DSG und DSGVO

CH steht Revision an

- CH Gesetz aufgesplittet
- Anpassungen Schengen erfolgt
- Fahrplan für Teil 2 unklar

Wahrscheinlich wird vieles mehr oder weniger übernommen.

Was sind die wichtigsten Unterschiede?

- Sanktionen
- Risikofolgeabschätzung
- Informationspflichten
- Datenverarbeitungsverzeichnis
- Profiling
- Meldepflicht bei Datenschutzverletzungen
- Keine Pflicht betrieblicher Datenschutzbeauftragter – mit Ausnahmen

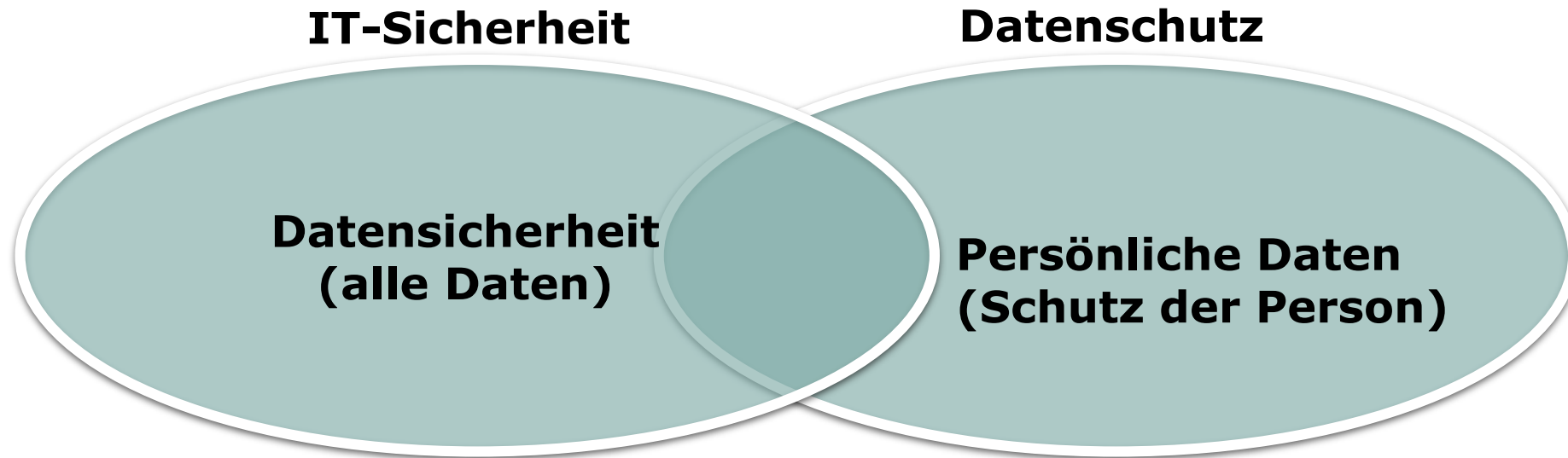


IT-Sicherheit vs Datenschutz



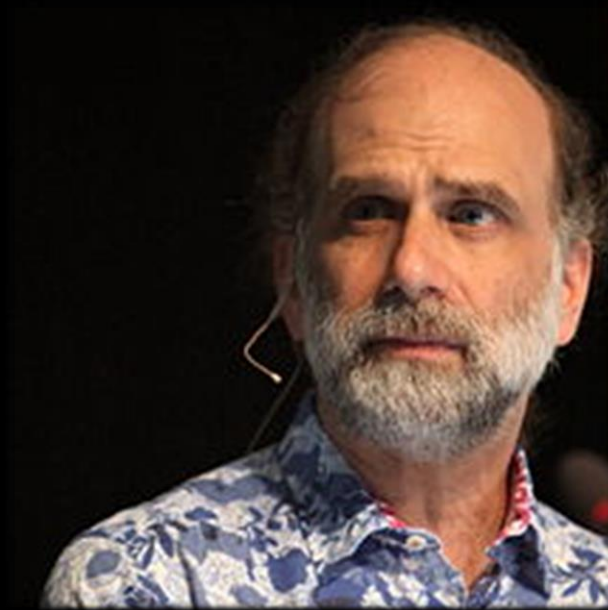
BitHawk

Was versteht ein Ingenieur unter Datensicherheit?



Was versteht ein Jurist unter Datensicherheit?

- Datensicherheit = Teil von Datenschutz
- Datensicherheit = Grundsatz der Datenbearbeitung
- Datensicherheit = organisatorisch & technisch



“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”

Bruce Schneier

American cryptographer, computer security professional, privacy specialist and writer



BitHawk

Zahlreiche Statistiken belegen, dass etwa die Hälfte der sicherheitsrelevanten Vorfälle durch Mitarbeiter im Unternehmen ausgelöst werden.

In den wenigsten Fällen geschieht dies absichtlich, meistens ist es Unachtsamkeit, mangelnde Ausbildung oder Leichtfertigkeit.

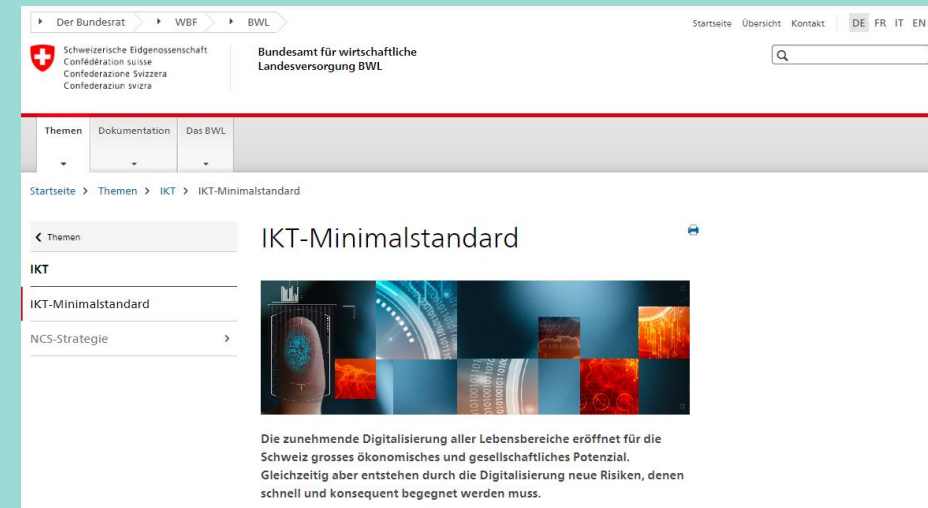


Wie kann man IT-Sicherheit managen?

Über 5000 Seiten
(Nachschlagewerk)



107 vereinfachte Kontrollfragen
Jetzt auch in Deutsch!





[English](#) | [Français](#)

Cybersecurity-Schnelltest für KMU

Wie gut ist Ihr Unternehmen vor Angriffen aus dem Cyberspace geschützt und darauf vorbereitet? Testen Sie jetzt, ob Sie die Minimalstandards für KMU erfüllen!

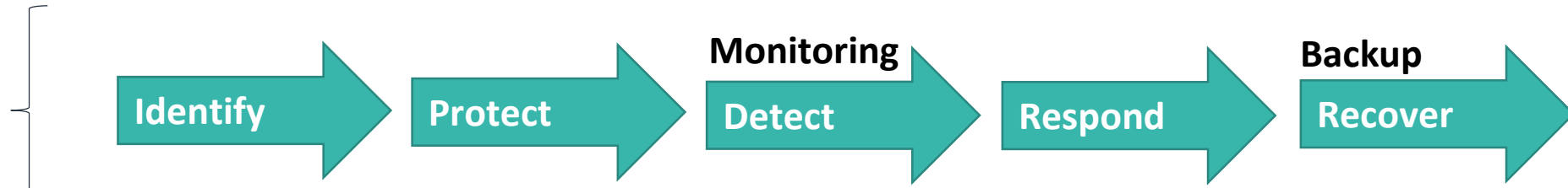


<https://ictswitzerland.ch/themen/cyber-security/check/>

NIST: Sicherheit als Prozess

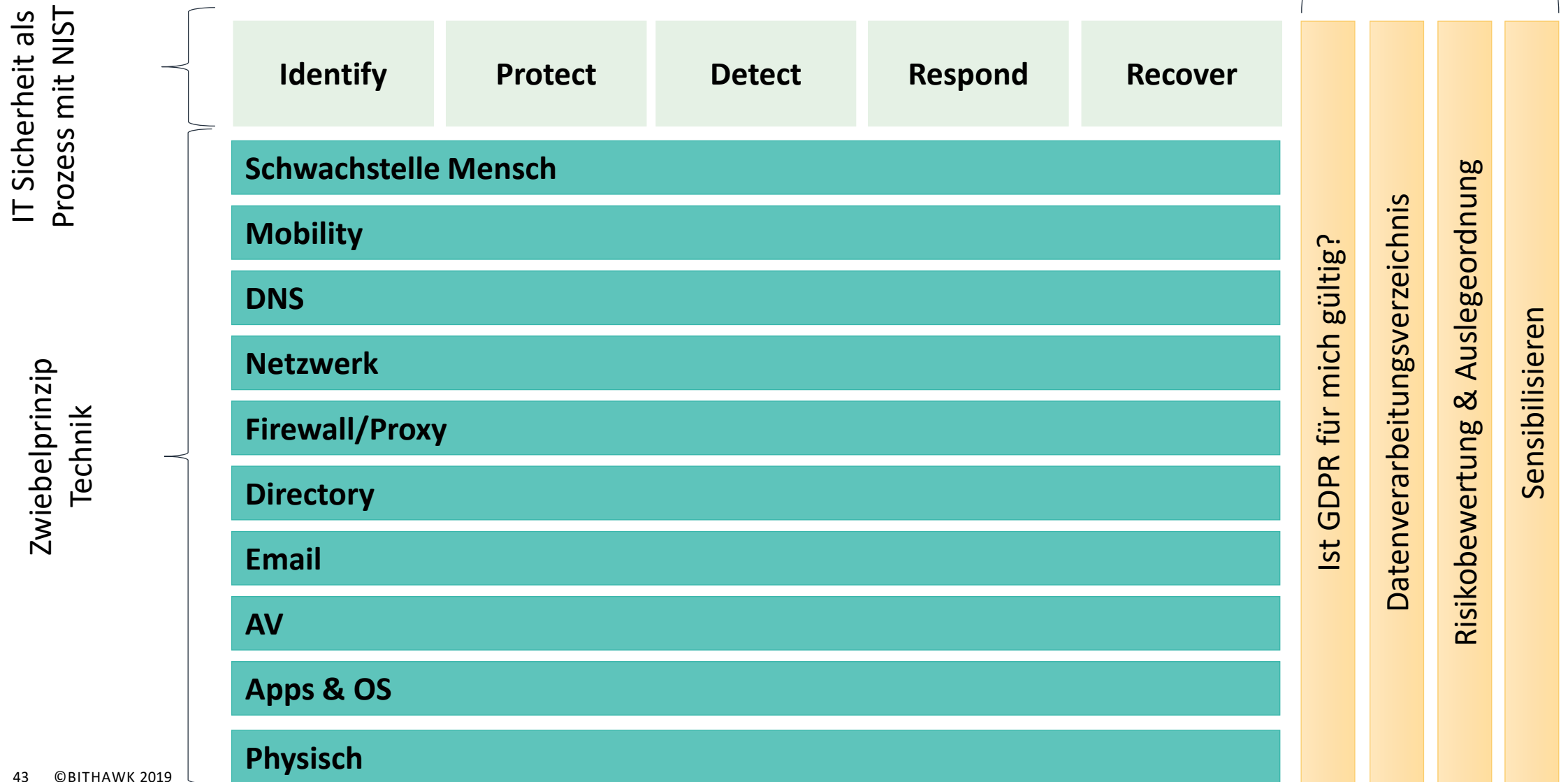


Prozesssicht

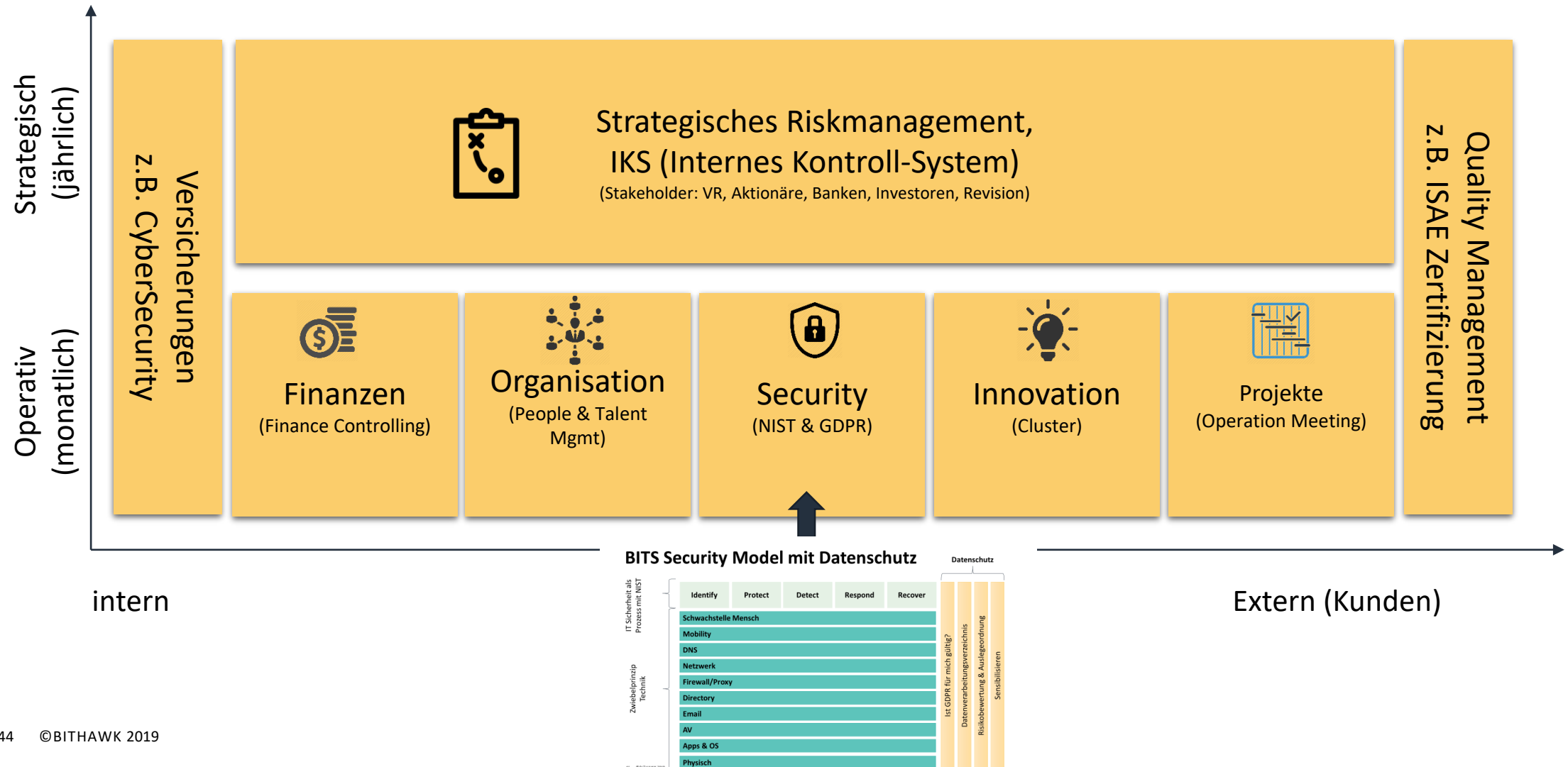


- **Identify** Verstehen was geschützt werden muss.
- **Protect** Entwicklung & Implementierung von Sicherheitsmechanismen.
- **Detect** Entwicklung und Implementierung von Prozessen & Funktionen um Attacken zu erkennen.
- **Respond** Klare Prozesse um auf Attacken zu reagieren.
- **Recover** Dokumentierte und getestete Prozesse um sich von einer Attacke schnell zu erholen.

Security Reifegrad Model mit Datenschutz



Riskmanagement Model



Was mache ich
nun ganz praktisch?



BitHawk

Was soll ich nun ganz praktisch tun?

1. Sind die Datenschutzgrundsätze umgesetzt?
2. Ist die DSGVO anwendbar?
3. Verzeichnis der Datenverarbeitung und Risikobewertung / Auslegeordnung erstellen
4. Braucht es eine Sensibilisierung und wer muss sensibilisiert werden?
5. Wie stelle ich sicher, dass Projekte mit dem Datenschutz vereinbar sind?
6. Wie organisiere ich die permanente Compliance mit Datenschutz?

Datenschutz-Grundsätze

- Rechtmässigkeit
- Treu und Glauben
- Verhältnismässigkeit
- Zweckbindung
- Transparenz
- Richtigkeit
- Datensicherheit



1. DSGVO anwendbar?

- Art. 3 DSGVO
- Praktische Beispiele aus Teil 1



2. Verzeichnis Datenverarbeitung und Risikobewertung/ Auslegeordnung erstellen

- Anstelle von Liste der Datensammlungen

2. Beispiel: Verzeichnis von Verarbeitungstätigkeiten

- Verantwortlicher
- Zweck der Verarbeitung
- Betroffenen Personen (MA, Interessenten, Lieferanten, Kunden, Patienten etc.)
- Betroffenen Daten (Namen, Email, Geburtsdatum, Geschlecht etc.)
- Zugriffberechtigte (Sales, HR, alle MA etc.)
- Datenübermittlung (Keine, Drittland, Organisation)
- Wann und wie werden die Daten gelöscht?
- Verweis auch technische und organisatorische Massnahmen

2. Risikobewertung

- Worst-Case Szenario
- Eintrittswahrscheinlichkeit dieses Worst-Case Szenario
- Auswirkung auf betroffene (zu Schaden kommende) Person (!)
- Wie kann ich den Schaden minimieren?
- Szenarien unter Beobachtung halten
- Reifegrad-Modell anwenden
- Aber: absolute Sicherheit nie möglich



3. Sensibilisierung

(permanentes Change Management)

- Schulungen
- Interne Informationsveranstaltungen
- Artikel in internen Medien/Portalen
- Weisungen/Reglemente etc.
- Ansprechperson definieren



BitHawk

4. Projekte und Datenschutz

- Jedes Projekt auf Datenschutzrelevanz prüfen
- Allenfalls prüfen, wie man Projekte entsprechend anpassen kann
- Jedes Projekt kann datenschutzkonform gestaltet werden – aber man muss frühzeitig daran denken!



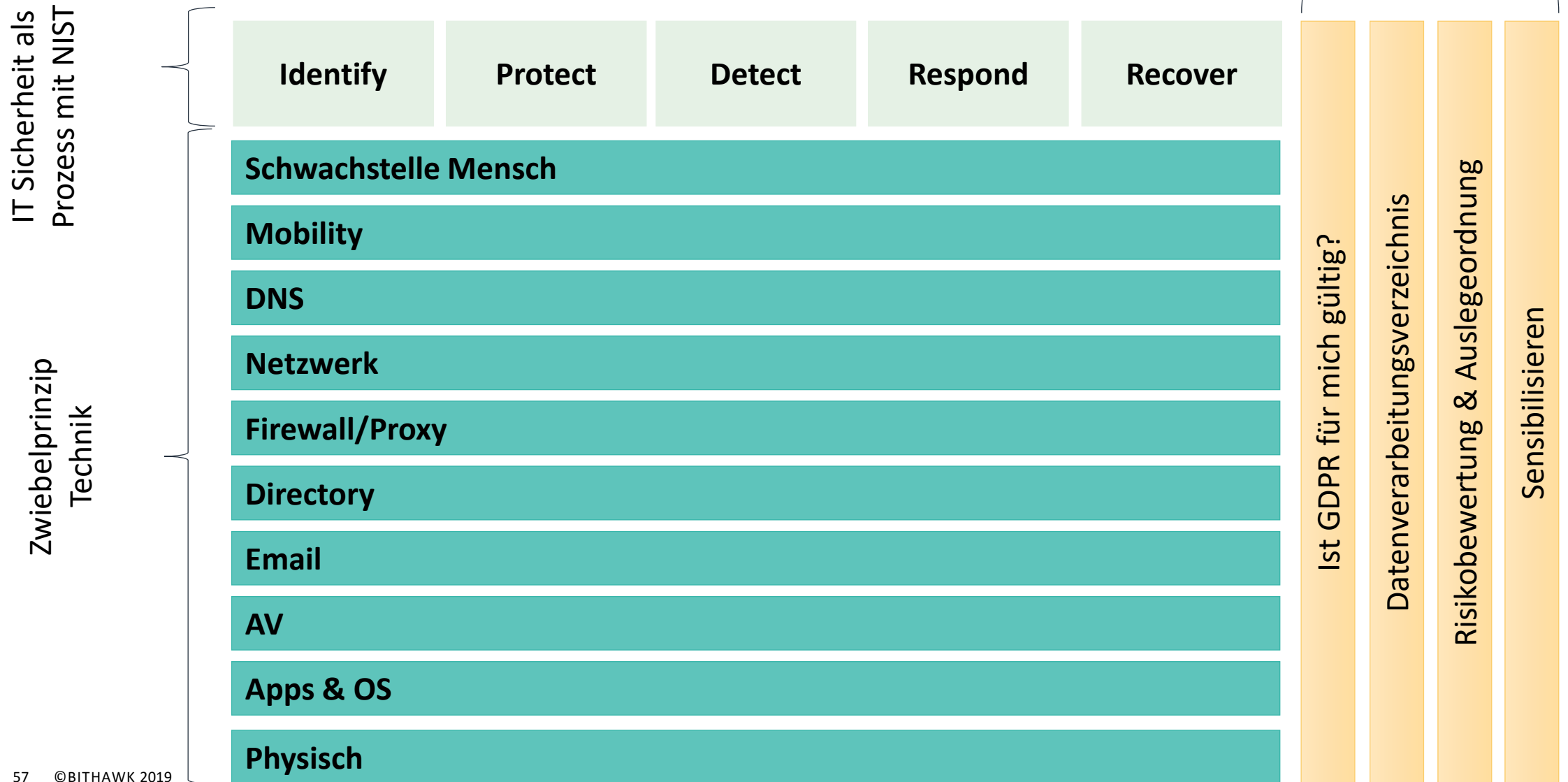
5. Compliance

Regelmässig...

- Intern überprüfen, wie Einhaltung der Vorgaben ist Hinterfragen, ob Daten noch relevant sind und Grundsätze
- eingehalten werden
- Verbesserungsprozess bezüglich Datenschutz installieren Risiko-Bewertung aktualisieren Datensicherheit – Stand der Technik prüfen



Security Reifegrad Model mit Datenschutz



Wo kann nun die Technik ganz praktisch helfen?

- Directory → Identity Management und Authentisierung (MFA, Windows Hello)
- Apps & OS → Verschlüsselung (OS, VMs, Backup), Azure Information Protection (classify, label, protect), Threat Protection
- Detect (Monitoring) → Log Analytics, Security Auditing and Logging
- E-Mail → Verschlüsselung, Data Loss Prevention, Threat Protection
- Prozesse → ServiceNow (Prozesssicherheit (Dokumentation) und Auditierbarkeit)

KEY TAKE AWAYS

Datenschutz erfordert ein kooperatives
Zusammenspiel von Legal & Technik

IT Sicherheit ist nicht gleich
Datenschutz - geht aber immer zusammen

Nicht in Aktionitis verfallen –
aber Datenschutz ernst nehmen

Die Praxis wird zeigen wie die EU mit
dem neuen Datenschutzgesetz umgeht.

Empfohlene Links

- BSI IT Grundschutz https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- GDPR <http://www.netzwoche.ch/news/2016-09-02/gdpr-warum-schweizer-firmen-jetzt-handeln-muessen>
- Video Cisco Ransomware <https://www.youtube.com/watch?v=4gR562GW7TI>
- Video Datenschutz mit Dave <https://youtu.be/F7pYHN9iC9I>
- Video Datenschutz mit Zuckerberg <https://youtu.be/fWJ-S7iLd8M>
- NIST US National Vulnerability Database <https://nvd.nist.gov/>
- Datenbank mit gehackten Accounts aus dem Darknet <https://haveibeenpwned.com/>
- NIST Cybersecurity Framework <https://www.nist.gov/cyberframework>
- Schweizer Übersetzung NIST https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
- ICT Cybersecurity für KMU <https://ictswitzerland.ch/themen/cyber-security/check/>

**Besten Dank für
Ihre Aufmerksamkeit**