TEMET
end-to-end IT security

EPD: Chancen und Risiken der informationellen Selbstbestimmung

Information Security in Healthcare Conference

Track "Governance"

Thomas Kessler
TEMET AG

07.06.2018
14:15 – 14:55

Über den Referenten

Thomas Kessler
Dipl. Physiker ETH
MAS ZFH in Business Administration

Gründer, Partner
In der IT Security tätig seit 1991

Spezialgebiete
Security Architecture and Strategy
Strong Authentication
Identity Provider (IdP)

Kontakt
Tel: +41 79 508 25 43
E-Mail: thomas.kessler@temet.ch

Über die TEMET AG

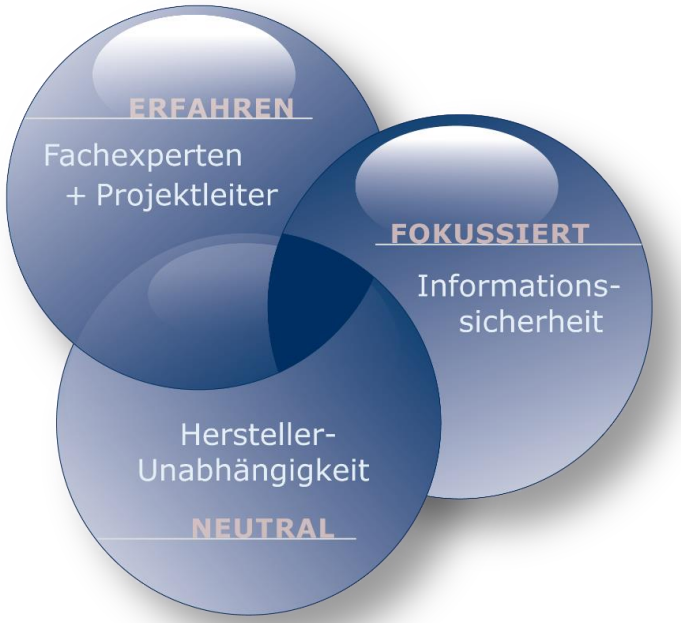
TEMET
end-to-end IT security

Mission

- Wir planen, konzipieren und realisieren Sicherheitsprojekte

Alleinstellungsmerkmale

- Wir vereinen fachliche Expertise mit Projektleiterkompetenz
- Wir konzentrieren uns auf die Informationssicherheit
- Wir sind neutral und nur unseren Kunden verpflichtet



Unternehmen

- Gründung im März 2010
- Inhabergeführte Aktiengesellschaft
- 12 Information Security Consultants
- Über 75 Kunden, welche höchste Anforderungen an die nachhaltige Gewährleistung ihrer Informationssicherheit stellen

Ausgewählte EPD Referenzprojekte

TEMET
end-to-end IT security

- Seit April 2018: Mandat als DSDS-V** der angehenden EPD Stammgemeinschaft Nordwestschweiz (SG NW)
- *2017, Universitätsspital Basel: Review der Sicherheitsaspekte beim EPD-Anbindungskonzept
- 2017: Spital: Ausarbeitung eHealth & mHealth Sicherheitsarchitektur
- *2016, Gesundheitsdepartement Basel-Stadt: Definition der Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) für die Informations-sicherheit im EPD.
- *2015, BAG: Bedrohungs- und Risikoanalyse für das Elektronische Patientendossier (EPD). Teilnahme an Expertenworkshops im Rahmen der Ausarbeitung des Ausführungsrechts für das EPDG (insb. TOZ***)
- 2014, EPD-Plattformanbieter: Konzeption des Authentication Layers mit verschiedenen Authentifizierungsverfahren (inkl. Prozesse)

*: Öffentlich vorgestellte Projekte anlässlich der eHealth Foren 2016/2017/2018

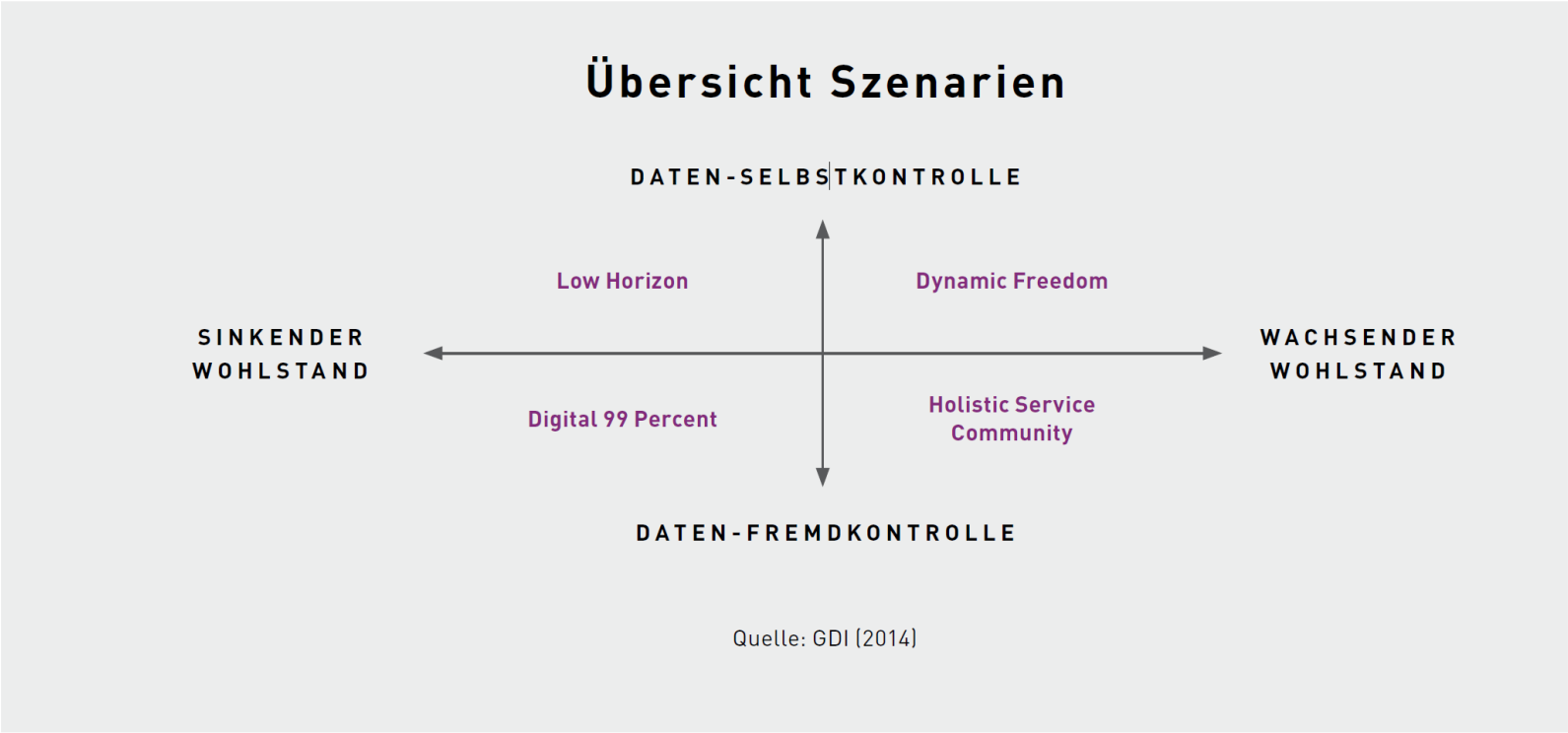
**: DSDS-V: Datenschutz- und Datensicherheitsverantwortlicher gemäss Art. 12 Abs. 2 EPDV
***: TOZ: Technische und Organisatorische Zertifizierungsvoraussetzungen

Agenda

- Informationelle Selbstbestimmung und das EPD
  - EPD Funktionalitäten für die Daten-Selbstkontrolle
- Konsequenzen für die Informationssicherheit
  - «Grundschutz» und «Selbstschutz»

Wer hat die Kontrolle über unsere Daten?

In einer von Swisscom beauftragten GDI Studie von 2014 ist dies eine der beiden Leitfragen, an denen sich die Definition gesellschaftlicher Zukunftsszenarien orientiert.



Quelle: "Die Zukunft der vernetzten Gesellschaft" (Gottlieb Duttweiler Institute GDI, 2014, p55)

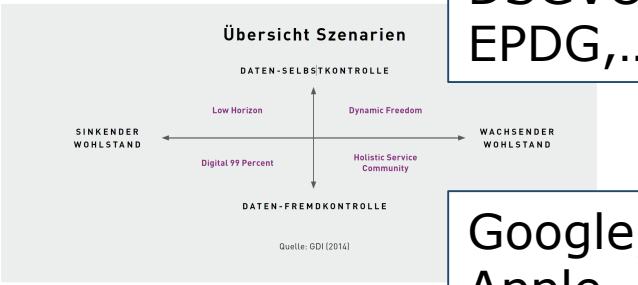
Einleitung (2/3)

- Das GDI Szenario „Hoher Wohlstand, hohe Selbstkontrolle“ lässt uns optimistisch in die gesellschaftliche Zukunft blicken:
  - Globale, gemeinschaftliche Orientierung der Gesellschaft;
  - Ökonomisch unabhängige, offen aufeinander zugehende Bürger in einer transparenten, nicht gespaltenen Gesellschaft;
  - Streben nach Lebensqualität statt Streben nach Reichtum und Besitz;
  - Kreativität und Innovationskraft als identitätsstiftende Eigenschaften.
- Aber auch das GDI Szenario „Hoher Wohlstand, geringe Selbstkontrolle“ hat seinen (gefährlichen…) Reiz:
  - Segmentierung anhand der Zugehörigkeit zu Corporate States. Diese bietet Komfort (Convenience), Sicherheit und Sinn;
  - Komfort: Filter bewältigen die Informationsflut, Datenhistorie hilft zu entscheiden;
  - Sicherheit: Totale Überwachung sowie Vernetzung mit Gleichgesinnten machen sicher – und führen zu konformem Verhalten;
  - Sinn: Corporate States ermöglichen Konsum und Status, bieten eine Freiheit im gesetzten Rahmen;
  - Es herrscht Gruppendruck und gibt einen sozialen Anschlusszwang.

Zitiert aus: “Die Zukunft der vernetzten Gesellschaft“ (Gottlieb Duttweiler Institute, 2014, pp 58/59)

Einleitung (3/3)

- Regulatoren / Gesetzgeber in Europa unterstützen die Daten-Selbstkontrolle nach Kräften, z.B.:
  - DSGVO (EU)
  - PSD2 (EU)
  - EPDG (CH)
- Die entgegenwirkenden Kräfte sind stark und argumentieren mit Komfort und Geborgenheit
  - Technosphären
  - Soziale Medien
- Der Ausgang ist ungewiss
- Welche Rolle spielt die Security?



DSGVO, EPDG,…

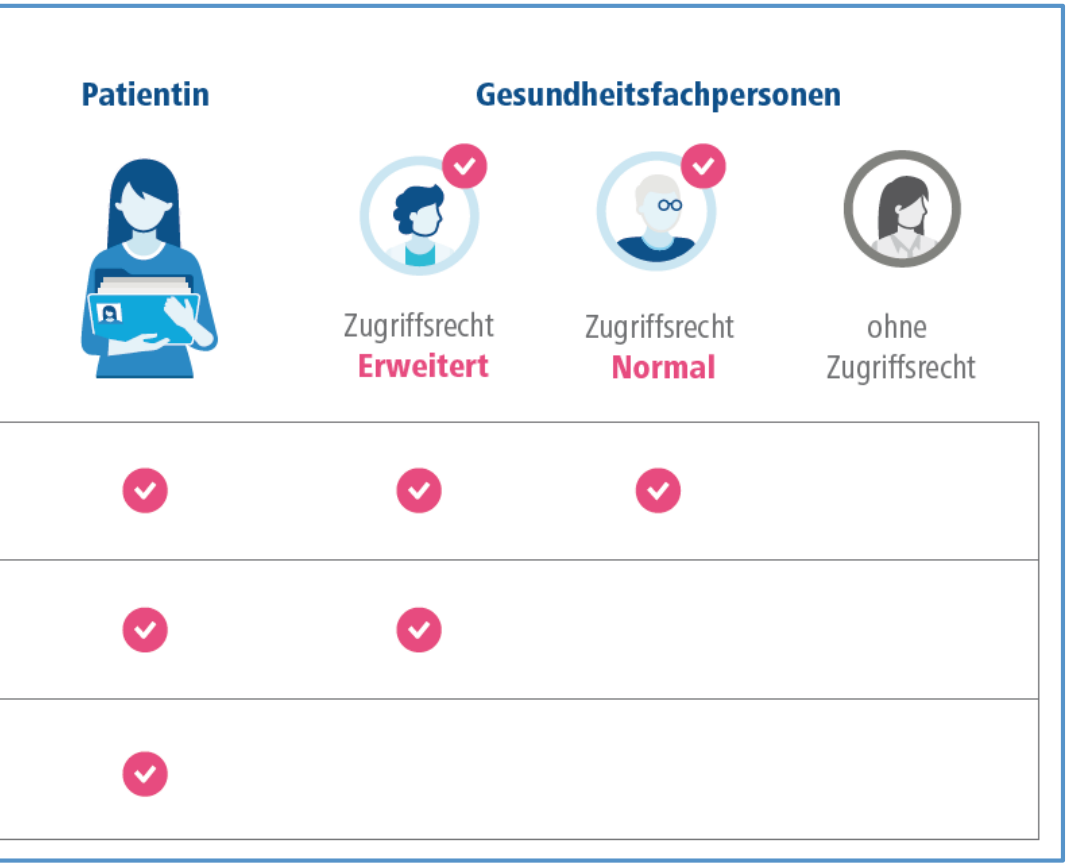
Google, Apple,…

Daten-Selbstkontrolle im EPD

- Die „Doppelte Freiwilligkeit“: Das Eröffnen und das Führen eines elektronischen Patientendossiers ist sowohl für den Patienten als auch für die ambulanten Leistungserbringer freiwillig.
- EPD Zugriffskontrolle: Patientinnen und Patienten können…
  - … alle in ihrem EPD abgelegten Dokumente selber und jederzeit einer von drei Vertraulichkeitsstufen zuordnen;
  - … einer Gesundheitsfachperson (GFP) ein normales oder erweitertes Zugriffsrecht erteilen oder diese ganz vom Zugriff auf ihr EPD ausschliessen;
  - … einer Gruppe von GFP ein (immer befristetes) Zugriffsrecht erteilen;
  - … die Verwaltung ihres EPD stellvertretend einer Vertrauensperson übergeben. Dies kann eine Person aus dem privaten Umfeld sein oder eine GFP (z.B. Pfleger);
  - … eine Gesundheitsfachperson ermächtigen, dass sie ihr eigenes Zugriffsrecht auf weitere GFP oder Gruppen von GFP überträgt;
  - … sich darüber informieren lassen, wenn neue GFP einer zugriffsberechtigten Gruppe von GFP beitreten;
  - … im EPD Zugriffsprotokoll jederzeit einsehen, wer zu welchem Zeitpunkt Dokumente abgerufen oder neue Dokumente im EPD abgelegt hat;
  - … die Grundeinstellungen jederzeit ändern.

Zugriffsrechte im EPD

Erteilung von Zugriffsrechten unter Berücksichtigung der Datenklassifizierung jedes einzelnen Dokuments:



Quelle: "EPD Informationsbroschüre für die Bevölkerung" (eHealth Suisse, 2018)

Wichtige Spezialfälle

- Notfallzugriff: Gesundheitsfachpersonen ohne Zugriffsrecht können im Notfall auf das EPD zugreifen.
  - Standardmässig können sie normal zugängliche Dokumente abrufen. Patienten können diese Einstellung ändern, indem Sie auch eingeschränkt zugängliche Dokumente freigeben oder aber den Notfallzugriff grundsätzlich ausschliessen.
- Ausschluss: Patientinnen können verlangen, dass bestimmte Dokumente nicht in Ihrem EPD erfasst werden, oder können bereits abgelegte Dokumente wieder selbst löschen.
- Versionierung: Wenn Gesundheitsfachpersonen bestehende Dokumente aktualisieren, bleiben frühere Versionen im EPD verfügbar.
- Widerruf der Einwilligung: Patienten können ihre Einwilligung für das EPD jederzeit und ohne Begründung widerrufen. In diesem Fall wird das EPD mit allen enthaltenen Dokumenten gelöscht.
- Ablage eigener Dokumente: Patienten können eigene Dokumente im EPD ablegen, wenn diese aus ihrer Sicht wichtig sind.

Erste und zweite Reflexion

Das EPD wird zum Lackmustest für die informationelle Selbstbestimmung:

- Das alles bedeutet viel Arbeit für die Patienten und Patientinnen!
- Werden sie diese leisten wollen und können?
- Werden sie die erforderlichen Hilfsmittel und Unterstützung erhalten?

- Oder anders gefragt: Sind wir reif für die informationelle Selbstbestimmung?

Optik der Informationssicherheit

Was sich der Sicherheitsverantwortliche (als «Profi» in Sachen IT-Security) so denkt:

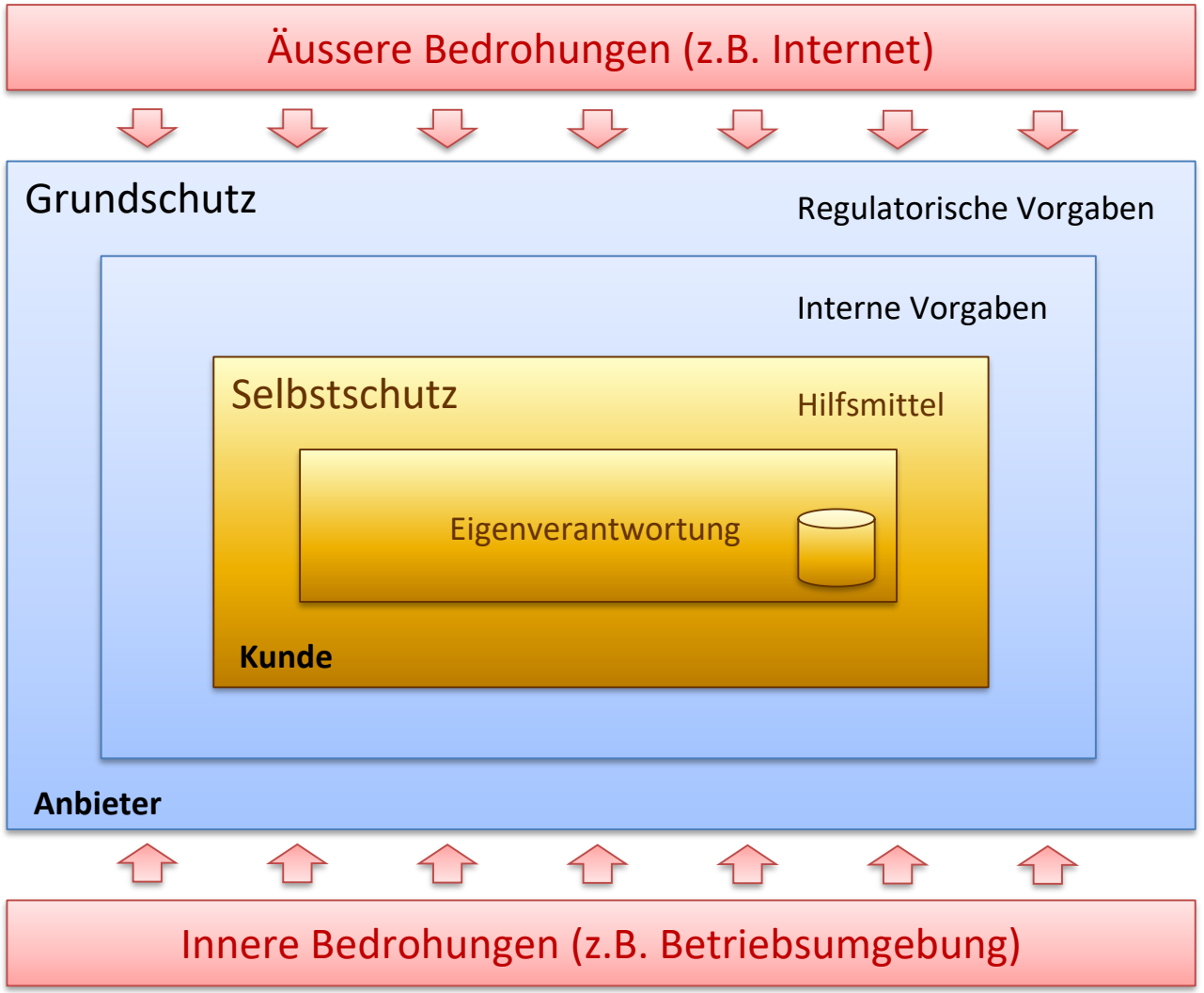
- Kann der Patient (als «Amateur») die Konsequenzen seines Tuns richtig einschätzen?
- Misst die Patientin der Informationssicherheit die nötige Bedeutung zu?
- Was passiert, wenn der Patient durch Eigenverschulden zu Schaden kommt?

⇨ Der Sicherheitsverantwortliche neigt, aus seinem Verantwortungsgefühl heraus, zum GDI Szenario der «Holistic Service Community»

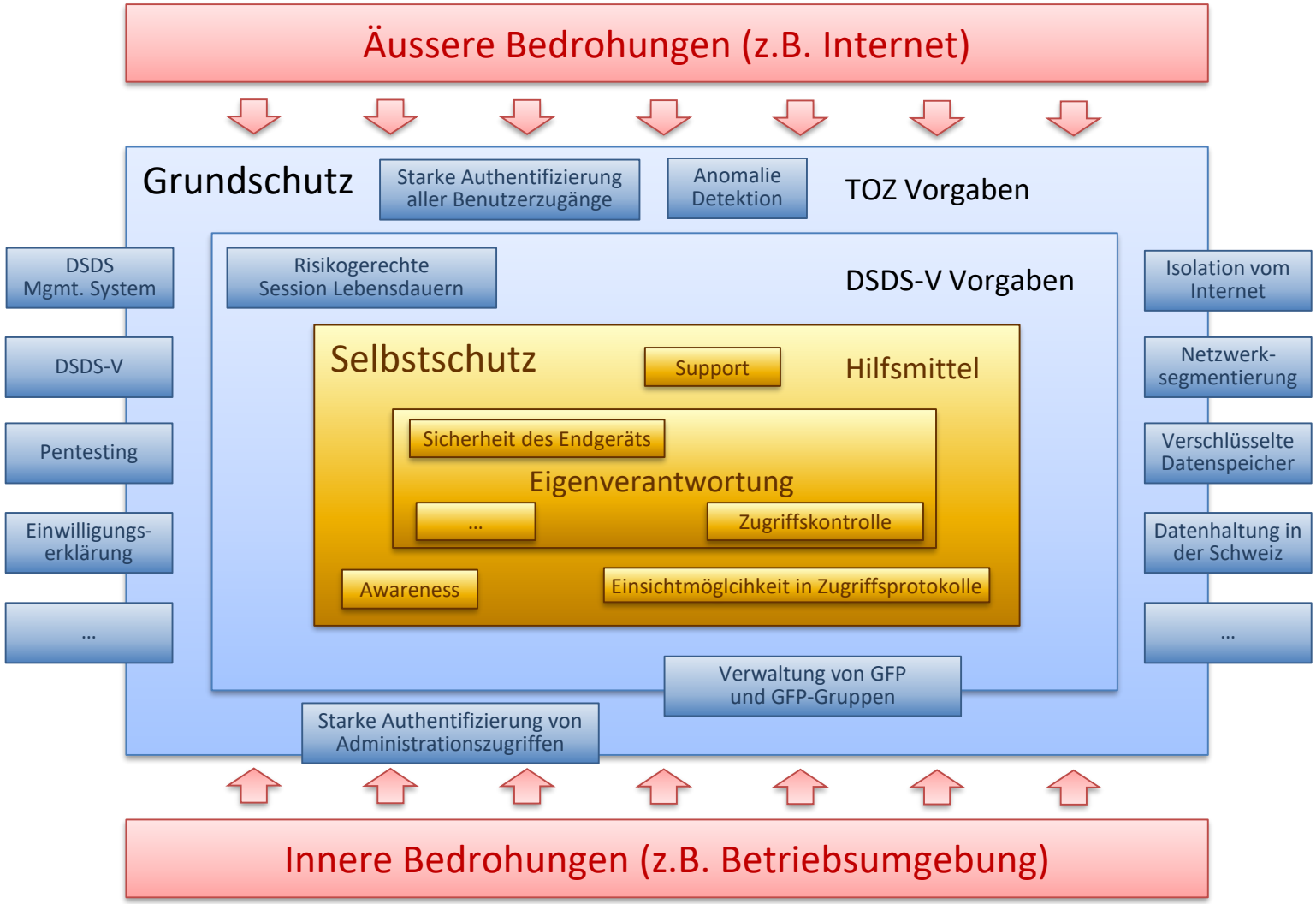
Verschärfte Fragestellungen für den CISO

- Darf der Anbieter seinen Kunden erlauben, auf grundlegende Sicherheitsmassnahmen zu verzichten?
- Muss er dies sogar tun, um die Datenhoheit des Kunden nicht über Gebühr einzuschränken?
- Und wenn nicht, wo liegen die Grenzen des Vertretbaren?

Eine differenziertere Betrachtung



Beispiele anhand des EPD (TOZ Vorgaben)



Ein neues Selbstverständnis des CISO

TEMET
end-to-end IT security

- Der Anbieter muss sicherstellen, dass der Service ordnungsgemäss erbracht wird («Grundschutz»)
  - Erfüllen externer regulatorischer Vorgaben
  - Definieren ergänzender interner Vorgaben
- Der Anbieter bietet den Kunden angemessene Unterstützung für die Daten-Selbstkontrolle
  - Entsprechende Dienstleistungen könnten auch von Dritten (z.B. Patientenorganisationen) erbracht werden
- Der Kunde nimmt seine Daten-Selbstkontrolle nach eigenem Gutdünken wahr

- Was gehört zum nicht verhandelbaren Grundschutz und was in die Eigenverantwortung?
  - Insbesondere dort, wo diese Frage nicht vom Regulator beantwortet wird (TOZ «Lücken» und Interpretationsspielraum)

Schlusswort (1/2)

- Daten-Selbstkontrolle (Entscheidungsfreiheit, Aufwand) und Daten-Fremdkontrolle (Bequemlichkeit, Geborgenheit) liegen im Clinch
- Die Gesetzgeber (in Europa) haben sich auf die Seite der informationellen Selbstbestimmung geschlagen (DSGVO, PSD2, EPDG)
- Bequemlichkeit ist eine stark entgegenwirkende Kraft

- Der Ausgang dieser Entwicklung ist ungewiss

Schlusswort (2/2)

- Und wo steht der Sicherheitsverantwortliche?
  - Wie üblich: Mitten drin im Getümmel!

- Beim DSDS-V gibt das EPDG Gesetz vor, dass er sich auf die Seite der Daten-Selbstkontrolle schlägt
- Ansonsten ist es einerseits eine persönliche Frage sowie andererseits eine Frage der Firmenkultur
- Prognose: Die Informationssicherheit wird vermehrt zum differenzierenden Merkmal und Teil der Marke
  - Qualität des «Grundschutzes»
  - Abgrenzung zwischen «Grundschutz» und «Selbstschutz»
  - Gewissermassen vergleichbar mit der Automobilbranche

Besten Dank
für Ihre Aufmerksamkeit!

TEMET AG
Basteiplatz 5
8001 Zürich
044 302 24 42
info@temet.ch
www.temet.ch