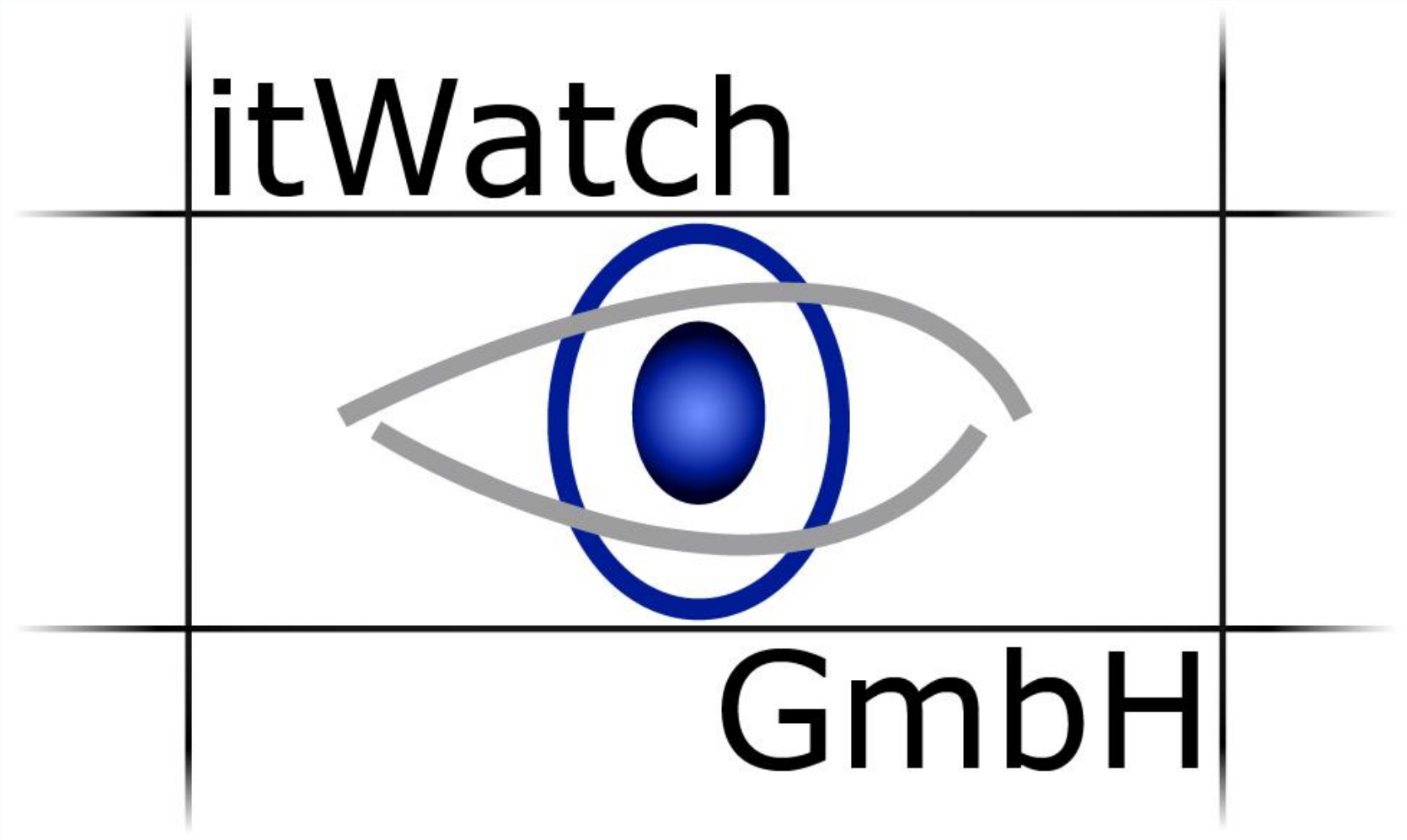
Ihre Sicherheit …
… unsere Mission



Ihre Sicherheit …
… unsere Mission

„Schutz im Cyberraum -
Spagat zwischen Wunsch und Wirklichkeit?“

Konferenz „IT-Sicherheit im Krankenhaus“
Keynote von Ramon Mörl | GF der itWatch GmbH

Kurzvorstellung Ramon Mörl

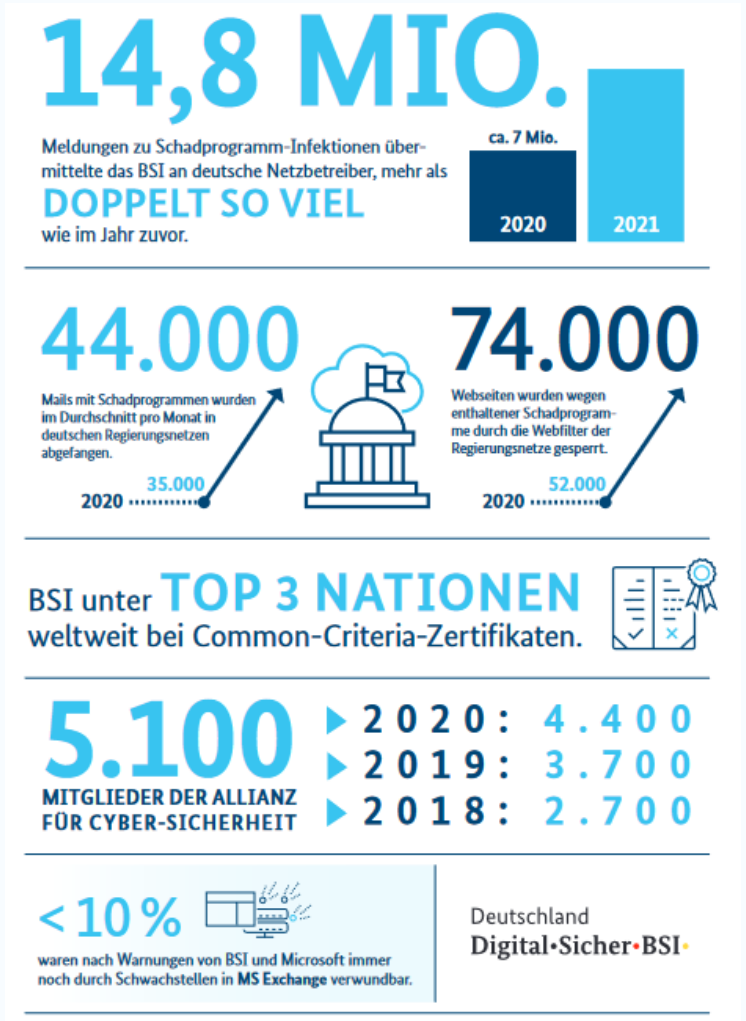
- 30 Jahre Erfahrung als Berater in der IT-Sicherheit
- Leitende Tätigkeiten in Projekten für Firmen wie HP, IBM, Siemens, ICL und Bull in Belgien, Deutschland, Frankreich, Italien, Österreich, Schweiz und USA
- Als unabhängiger Evaluator und Berater der Europäischen Union vor allem im Bereich der ECMA und ISO-Standards für die IT-Sicherheit tätig
- Seit 2002 Geschäftsführer der itWatch GmbH
- Aktive Mitarbeit in 40+ zum Teil vertraulichen Arbeits- und Gesprächskreisen wesentlicher Fach- und Interessens-Verbände

Adressierte Themen

- Cyber-Sicherheit in Deutschland – Status Quo
- Folgen der steigenden Cyber-Bedrohung
- Digitalisierung im Gesundheitswesen
- Gesetzeslage
- Wie kommt Ransomware ins Krankenhaus?
- Digitalisierung im Krankenhaus
- Was schützt gegen Ransomware?
- Die Problematik – Gut und Böse zu unterscheiden
- Datenschleuse und Datenwäsche
- Sichere Handlungsräume im Cyber Space schaffen
- Sichere digitale Transformation
- Medizinprodukte: Ein Blick auf Lieferketten
- Digitale Souveränität und Business Continuity – Ein Managementprozess

Cyber-Sicherheit in Deutschland – Status Quo

- aus BSI Lagebericht 2021



Quelle: BSI – Die Lage der It-Sicherheit in Deutschland 2021

Cyber-Sicherheit in Deutschland – Status Quo

- Ransomware ist aktuell die größte operative Bedrohung der Cyber-Sicherheit
- Angriffe mit steigender Qualität und hoher Agilität
- Es kann jeden treffen!!! Es geht nur um Geld auf dem Konto
- Ransomware als Wirtschaftsmodell: CaaS (Cybercrime-as-a-Service)
- Erpressungsdruck durch
  - Verschlüsselung
  - Daten-Leaks
  - DDoS (Distributed Denial-of-Service)
  - Kontaktaufnahme zu Patienten und Partnerfirmen

Folgen der steigenden Cyber-Bedrohung

- schwerwiegende IT-Ausfälle in Kommunen, **Krankenhäusern** und Unternehmen

https://www.spiegel.de/netzwelt/it-ausfall-in-duesseldorfer-uniklinik-a-fe3d228f-0621-4609-81a1-120b572cd61b

- nicht nur erhebliche wirtschaftliche Schäden
  - temporärer Ausfall der Notfallversorgung
  - Stilllegung von Dienstleistungsangeboten
  - Datenverschlüsselung
  - ...

Zur Gesetzeslage

Bundesverfassungsgericht

Leitsätze zum Beschluss des Ersten Senats
vom 08. Juni 2021
- 1 BvR 2772/18 –
- (IT-Sicherheitslücken)

2. a) Die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verpflichtet den Staat, zum Schutz der Systeme vor Angriffen durch Dritte beizutragen.

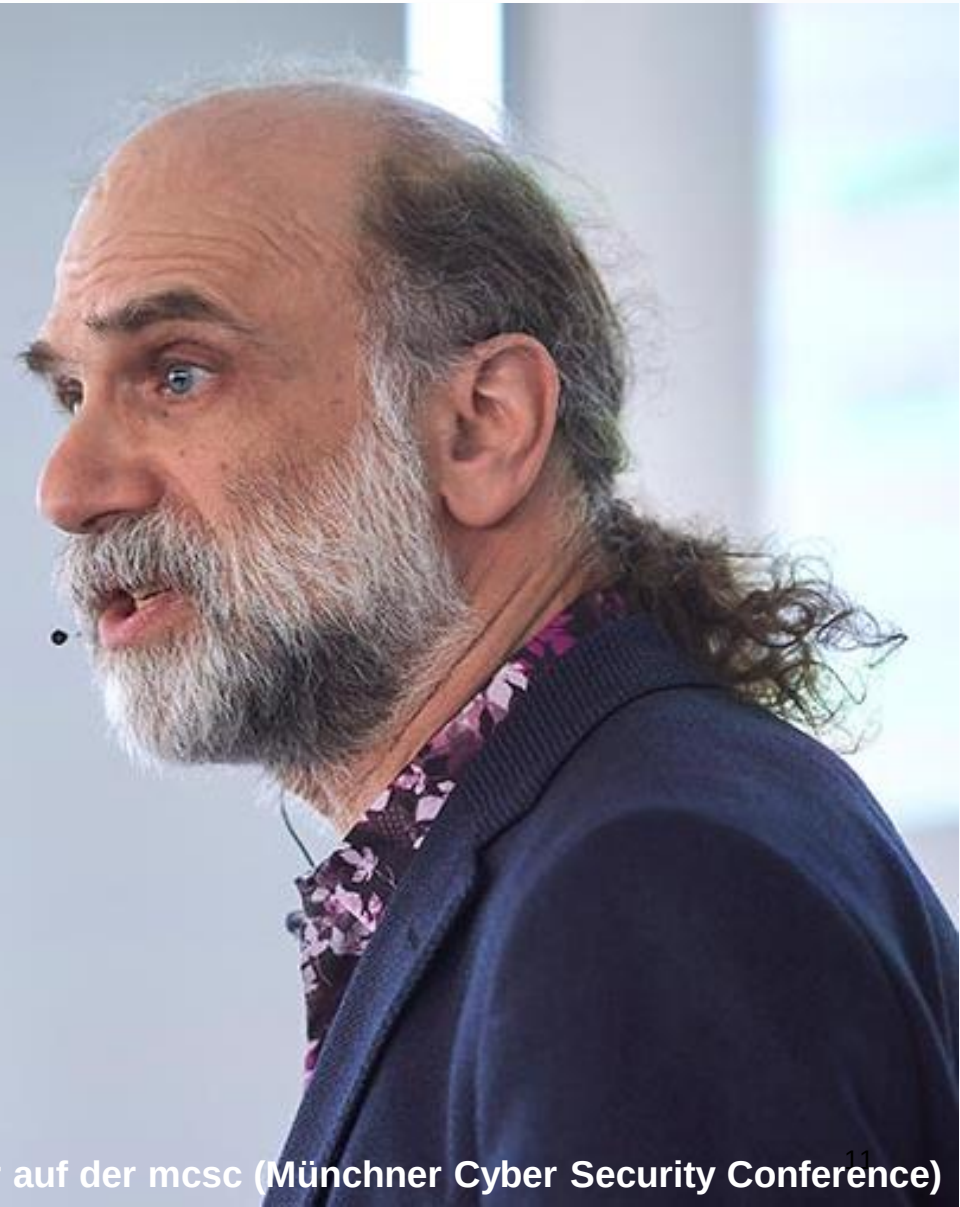
Quelle: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/06/rs20210608_1bvr277118.html;jsessionid=9312273303BF02AF2F6BABEF09C71D56.2_cid507

Wie kommt Ransomware ins Krankenhaus?

Wozu sind Downloads im Internet … da?
… um den Anwendern zu sagen:
NICHT Klicken – gefährlich

Wozu sind USB Sticks da?
… um den Anwendern zu sagen:
NICHT Einstecken – gefährlich

Wozu sind Mail-Attachments da?
… um den Anwendern zu sagen:
NICHT Öffnen – gefährlich



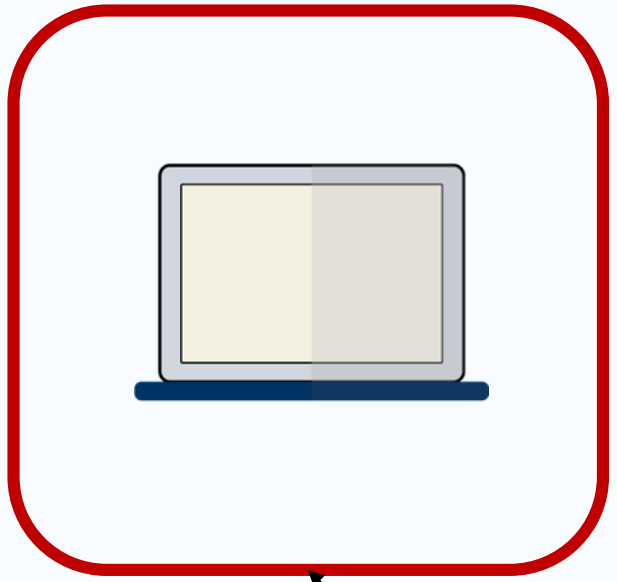
Bruce Schneier auf der mcsc (Münchner Cyber Security Conference)

Design against Crime

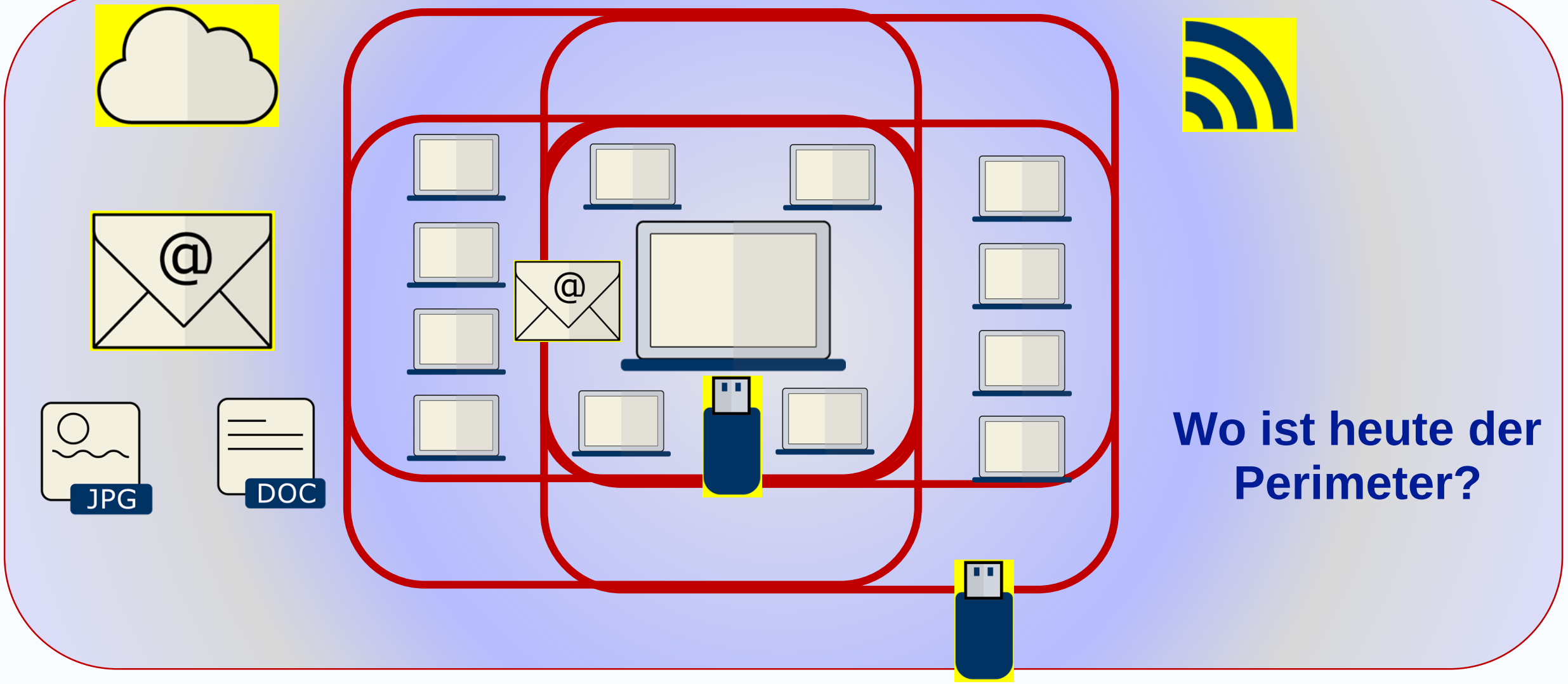
Design against Crime

Sichere Handlungsräume schaffen

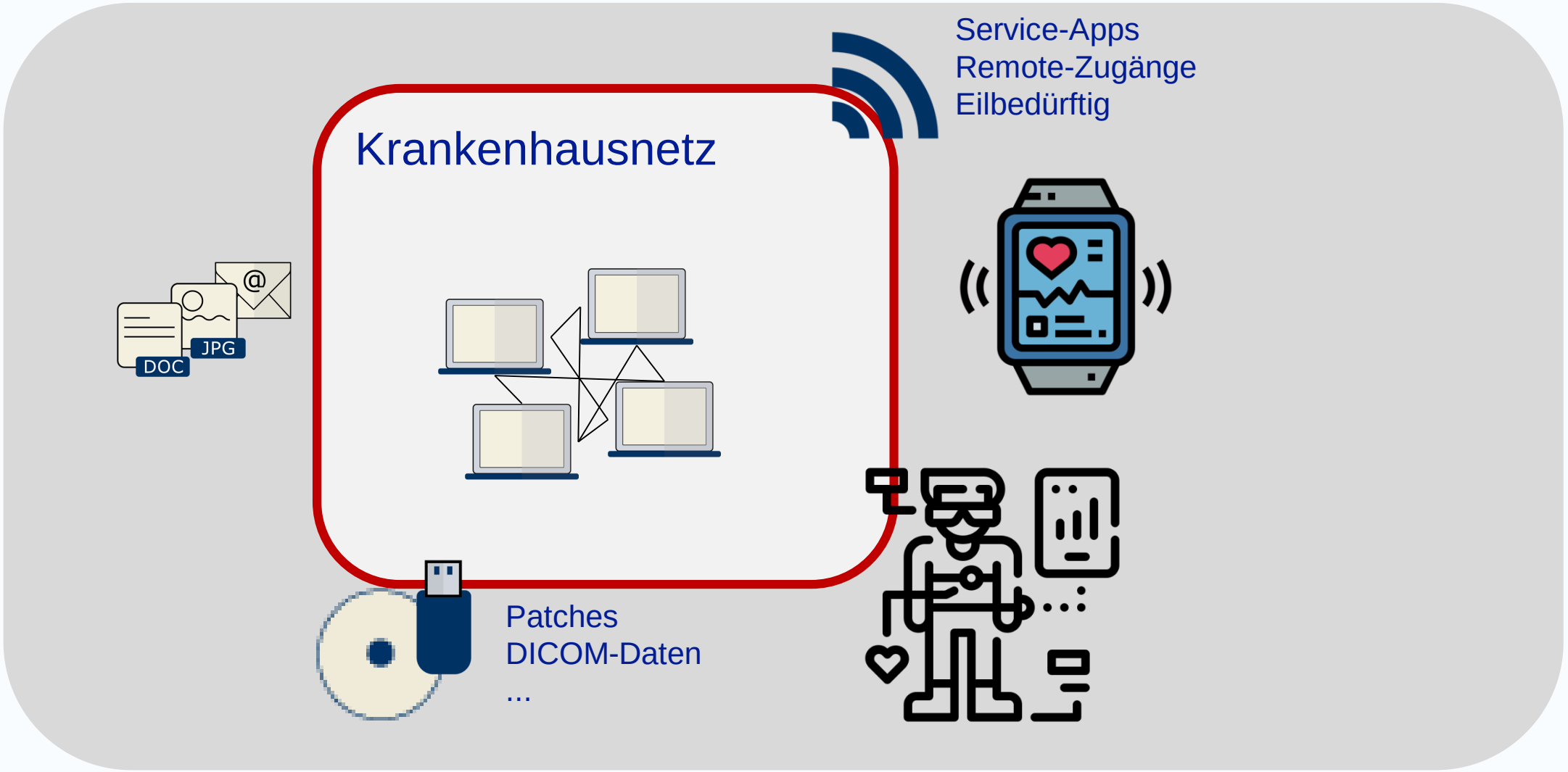
Früher, als alles noch gut war ... ;-)



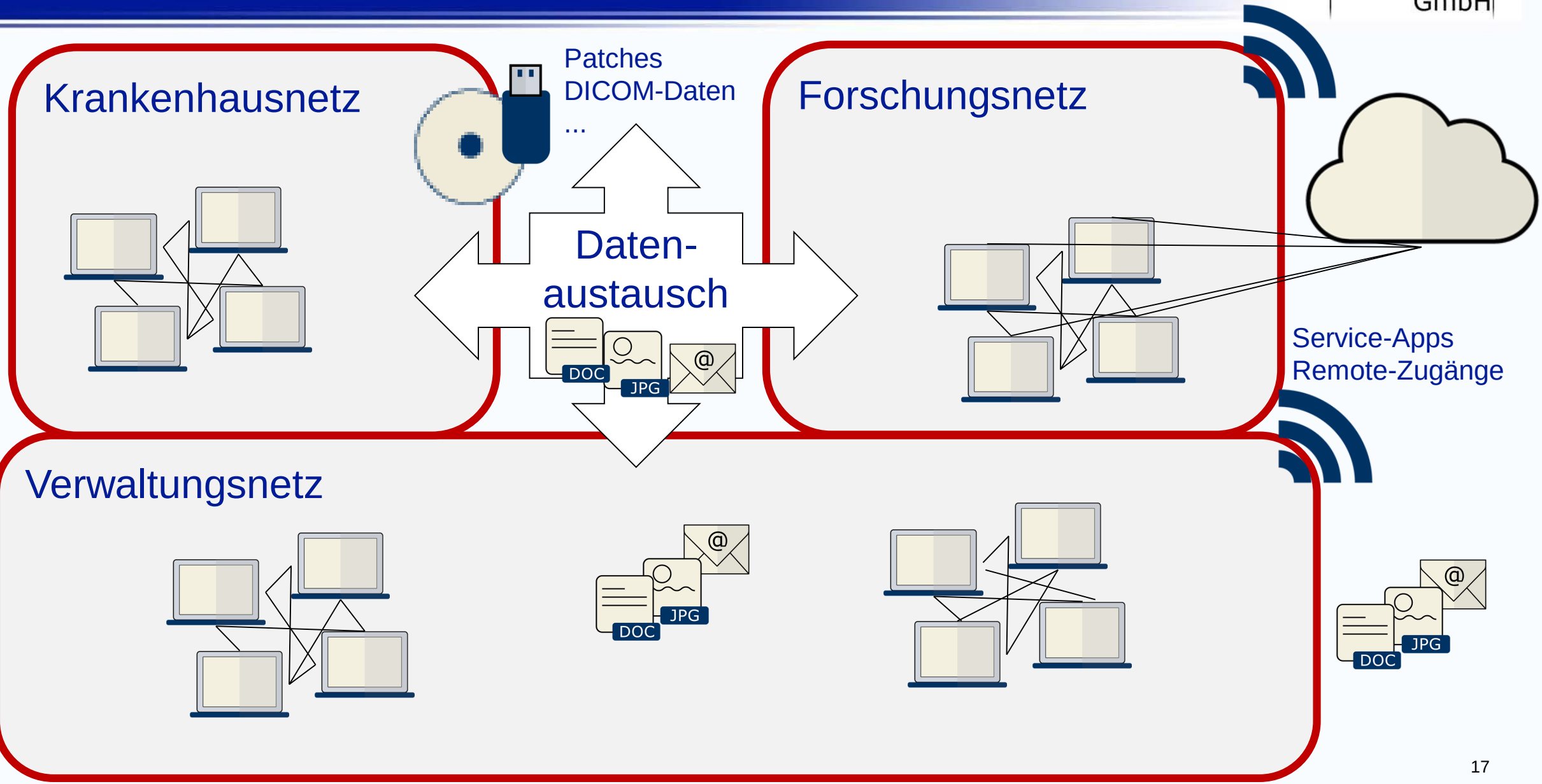
Heute ist es etwas komplexer ...



Digitalisierung im Krankenhaus



Digitalisierung im Krankenhaus



Sichere digitale Transformation

Lifecycle von Sicherheitseigenschaften digitaler Produkte

Entwickler

Schutz der Entwicklungsumgebung

Security by Design
Privacy by Design

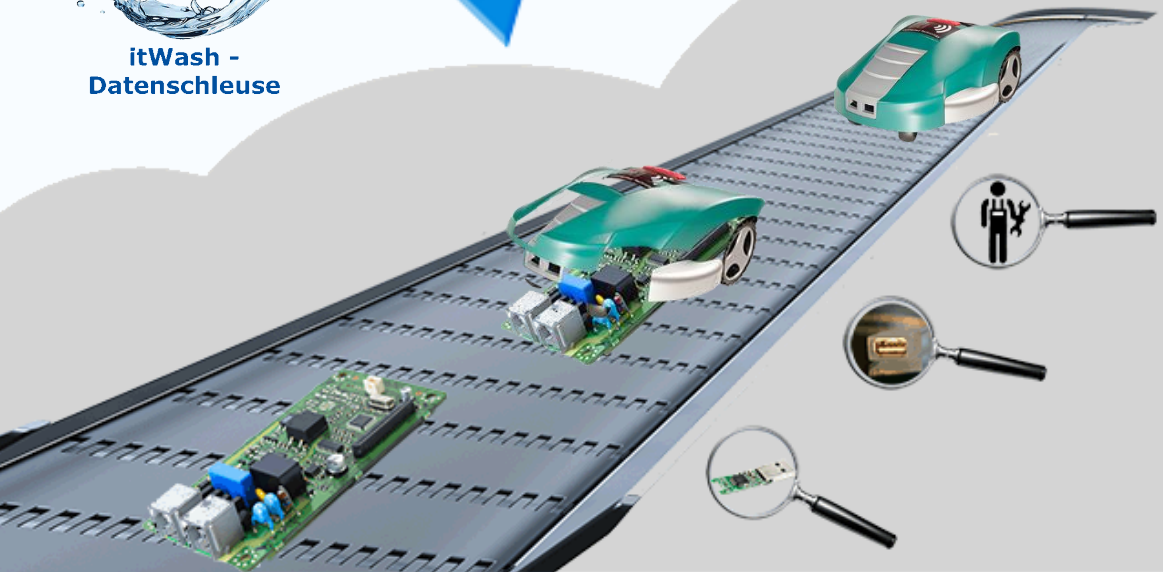
itWatch GmbH

Sichere digitale Transformation

PD Watch - Verschlüsselung

Sicherheit der Produktionsumgebung

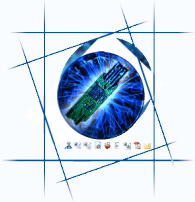
itWash - Datenschleuse



Sicherheitszone Produktion

Security as Infrastructure

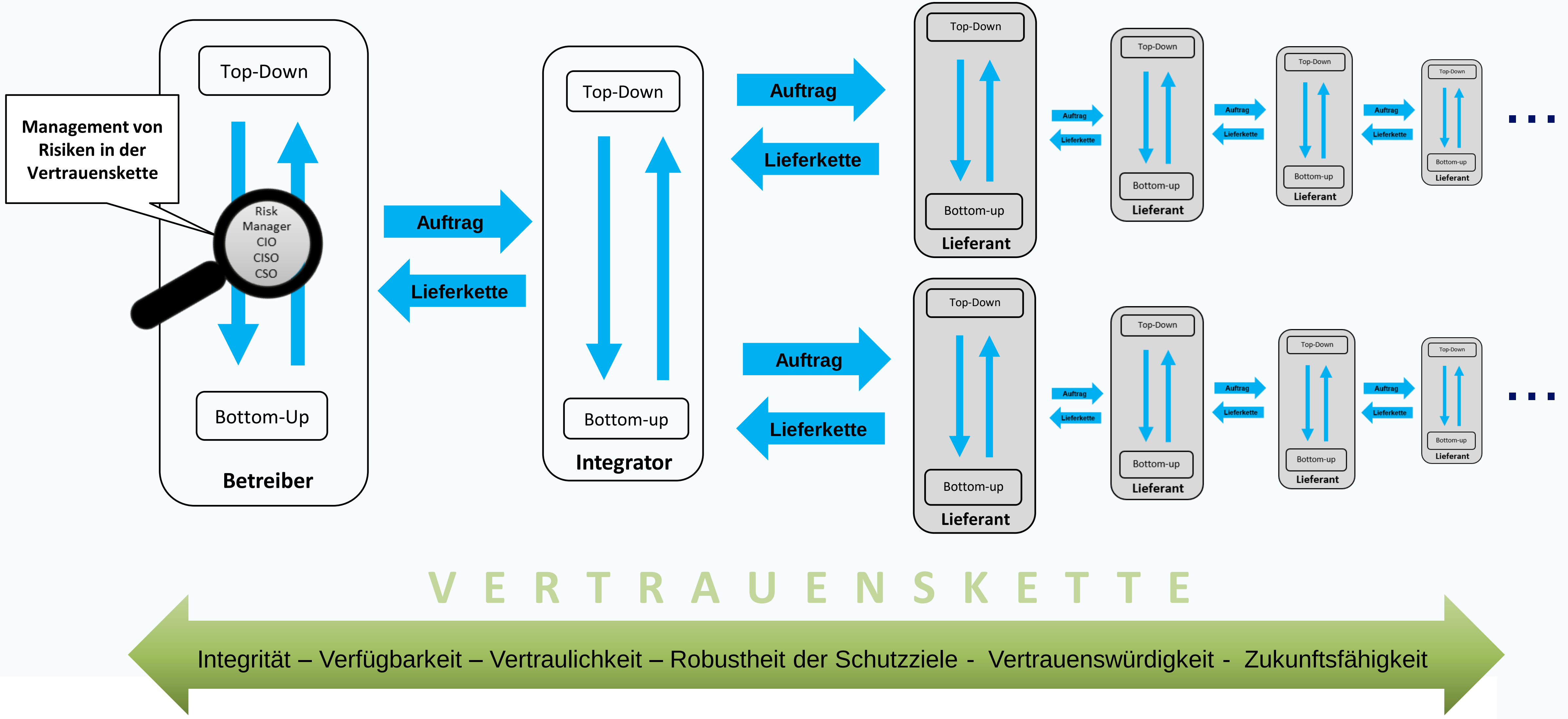
ApplicationWatch - Applikationskontrolle



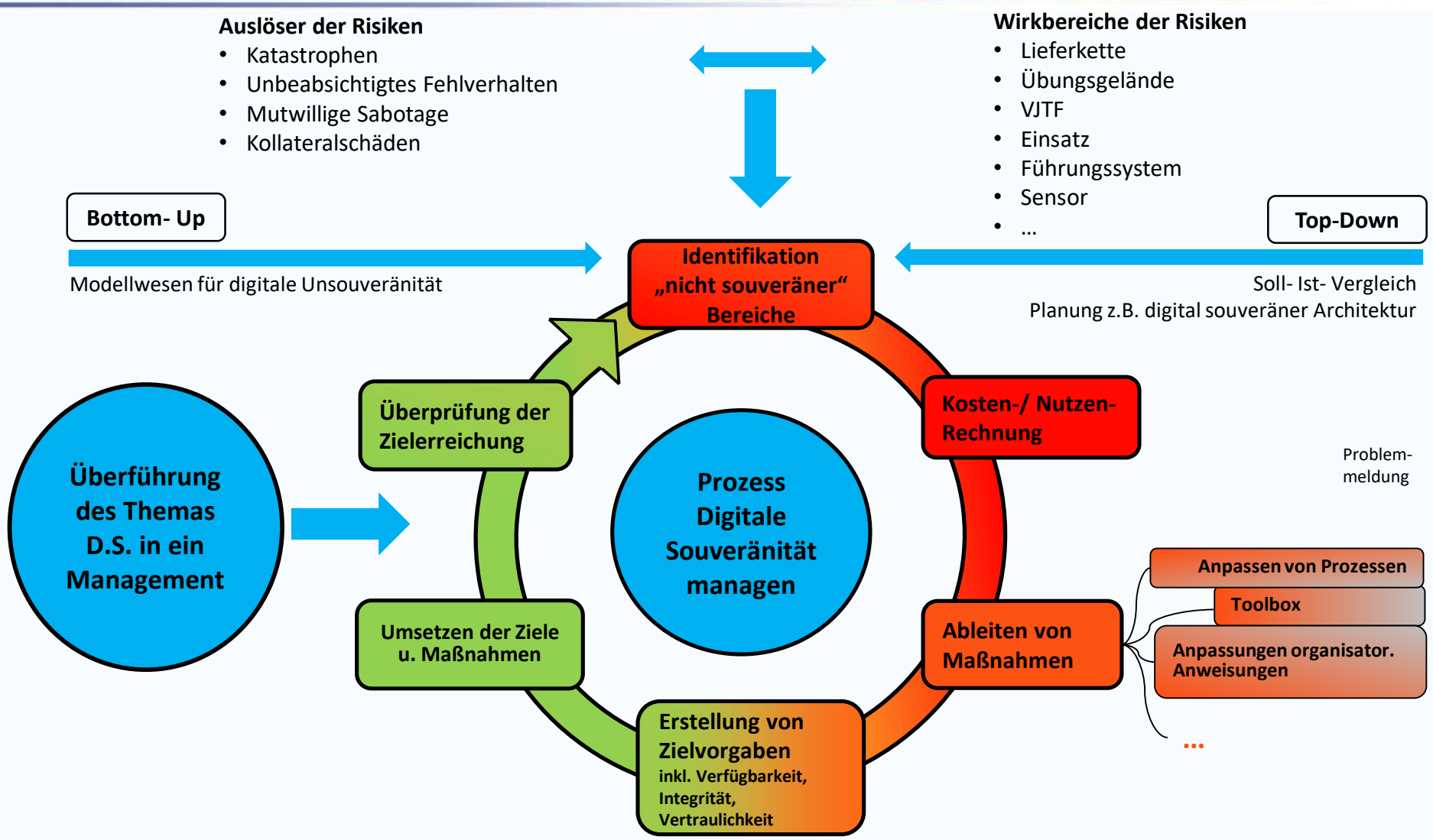
XRayWatch - Contentkontrolle

Sicherheitszone Produkt im Betrieb

Dig. Medizinprodukte: Ein Blick auf Lieferketten



Digitale Souveränität – Business Continuity



Digitale Souveränität ist kein definierter, erreichbarer Endzustand sondern beschreibt den Wunsch nach einem selbstbestimmteren Handeln im Cyber- und Informationsraum.

Die praktischen Notwendigkeiten

Das Arbeiten soll nicht eingestellt werden, nur weil zugelieferte Information möglicherweise infiziert ist.

Aktuelle Situation verlangt nach

- mehr Detail-Information in kürzerer Zeit
- schnellerer und vor allem filigranerer Reaktionsmöglichkeit
- nicht nur Sperren, sondern „das sichere Arbeiten ermöglichen“

Immer mehr Flexibilität und Mobilität wird in den Prozessen benötigt – das Einbinden

- neuer Geräte der Informationslieferanten
- Gesundheits-Apps
- unbekannter Informationen
- spontaner Kommunikationsbeziehungen
- von Workflows, um der Menge an Information Herr zu werden

Digitalisierung im Krankenhaus

Herausforderungen

- Gefahr von möglichem Schadcode
- Notwendigkeit der Vertraulichkeit der medizinischen Daten – sobald sie in Ihre Hände übergehen –

Security als Infrastruktur kann längere „Security-by-Design-Phasen“ ersetzen, Legacy-Produkte einbinden und Ergebnisse verbessern

Die Problematik

Man weiß nie, wo sich Angreifer verstecken!

Kann der Anwender gut und böse erkennen?

Schadcode z.B. in Bildern

RSA Security 2015 in San Francisco:
Marcus Murray zeigt eine einfache Methode, um Schadcode in Bilddateien zu verstecken –und einen Webserver zu übernehmen

- Murray verbirgt Schadcode als Kommentar in der EXIF-Information von Bilddateien
- Der Schadcode wird im Rechteraum des Anwenders ausgeführt, ohne dass ein Nutzer das merkt.
- Ähnliche Verstecke für Schadcodegibt es in allen Dateiformaten, DICOM, Office-Dokumente etc.
- Risiken sind in allen ausführbaren Elementen –Makros etc. enthalten

- **Wie können potentiell risikobehaftete Dateien importiert, bearbeitet, archiviert und auf jedem Rechner weiter bearbeitet werden?**

Datenwäsche am Bsp. JPG

Im Kommentarfeld kann eine exe-Datei enthalten sein!

Canon EOS

2020:05:20 14:26:22

…..

…

.

Was ist Datenwäsche

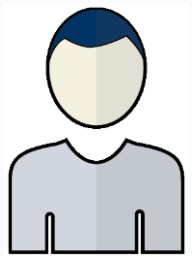
- Potentiell **schädliche Daten** von extern (Web, E-Mail, USB-Stick, iPhone / Mobiles, eigene Anwendungen …) sollen sauber und **sicher** in das **innere Netz geschleust**, in einem standardisierten Prozess mit weiteren Daten (z.B. **Metadaten**) angereichert und im inneren (sicheren) Netz weiter verarbeitet werden.
- Die Daten werden hierzu in einem isolierten, als **Opfersystem** ausgeprägten **Schleusensystem** erfasst. Die Integrität des Systems wird nach jedem Boot wieder hergestellt und das System selbst wird durch eine Sicherheitspolicy gehärtet.
- Potentiell schädliche Daten werden an das „Reinigungssystem“ weitergereicht und gereinigt. Die Originaldaten bei Bedarf archiviert.

Wo braucht man Datenwäsche?

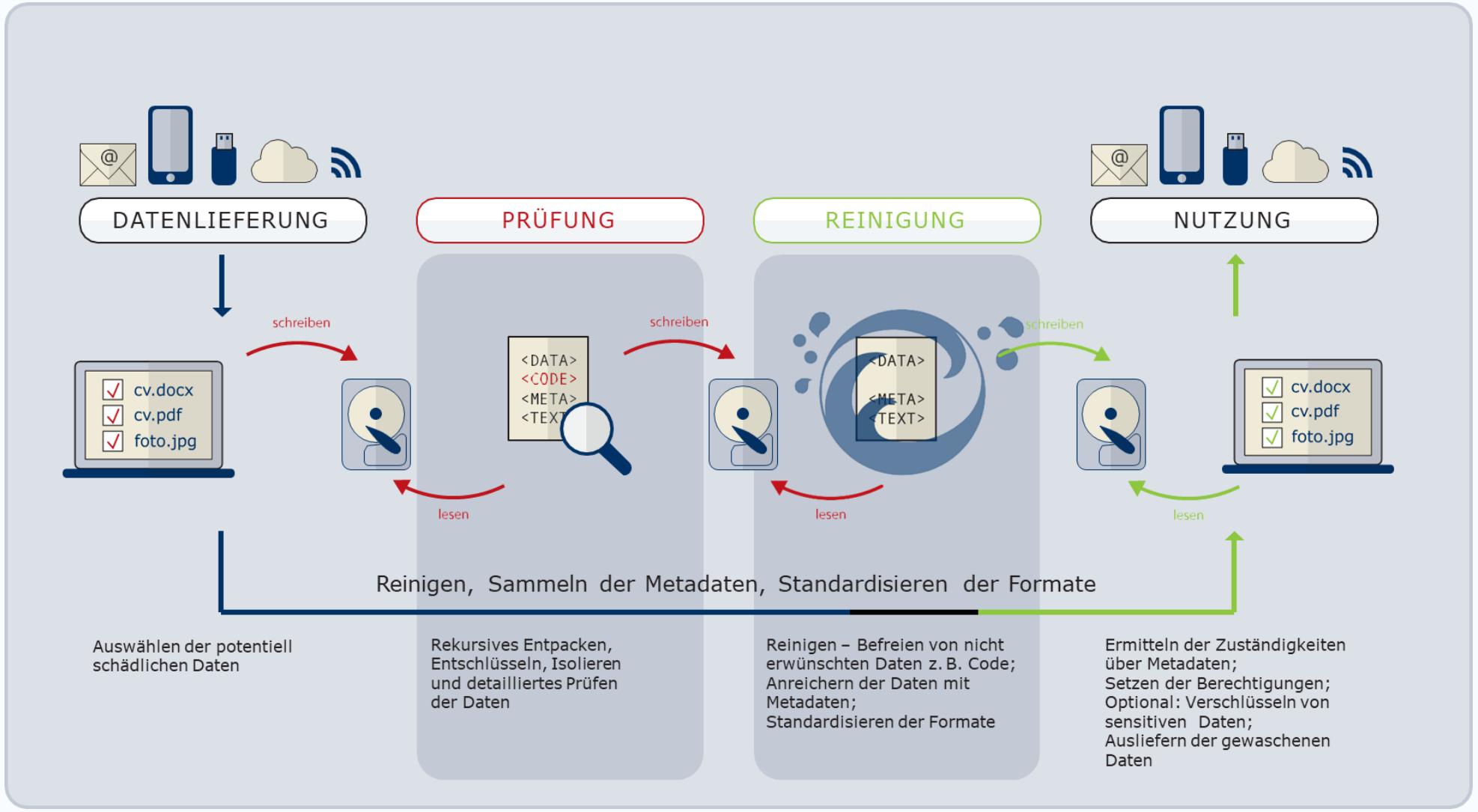
Daten (potentiell) unsicherer Herkunft gibt es im Krankenhaus an vielen Stellen

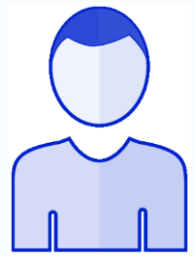
- Personalabteilung, Pressestelle, ...
- Patientendaten
  - CD / DVD mit bildgebenden Verfahren – DICOM
  - Wearables
  - Mobile Geräte mit medizinisch relevanten Daten
- Allgemein vernetzte IoT Devices
  - Überwachungskameras
  - Smart Building
  - …
- Unsichere mobile Devices (BadUSB)
- Fernwartung, Patchverfahren
- Ersetzen einer manuellen Datenübergabe durch konkrete Regelwerke mit Monitoring und Datenkonversion in Standardformate…

Sicherheitsarchitektur mit Netztrennung



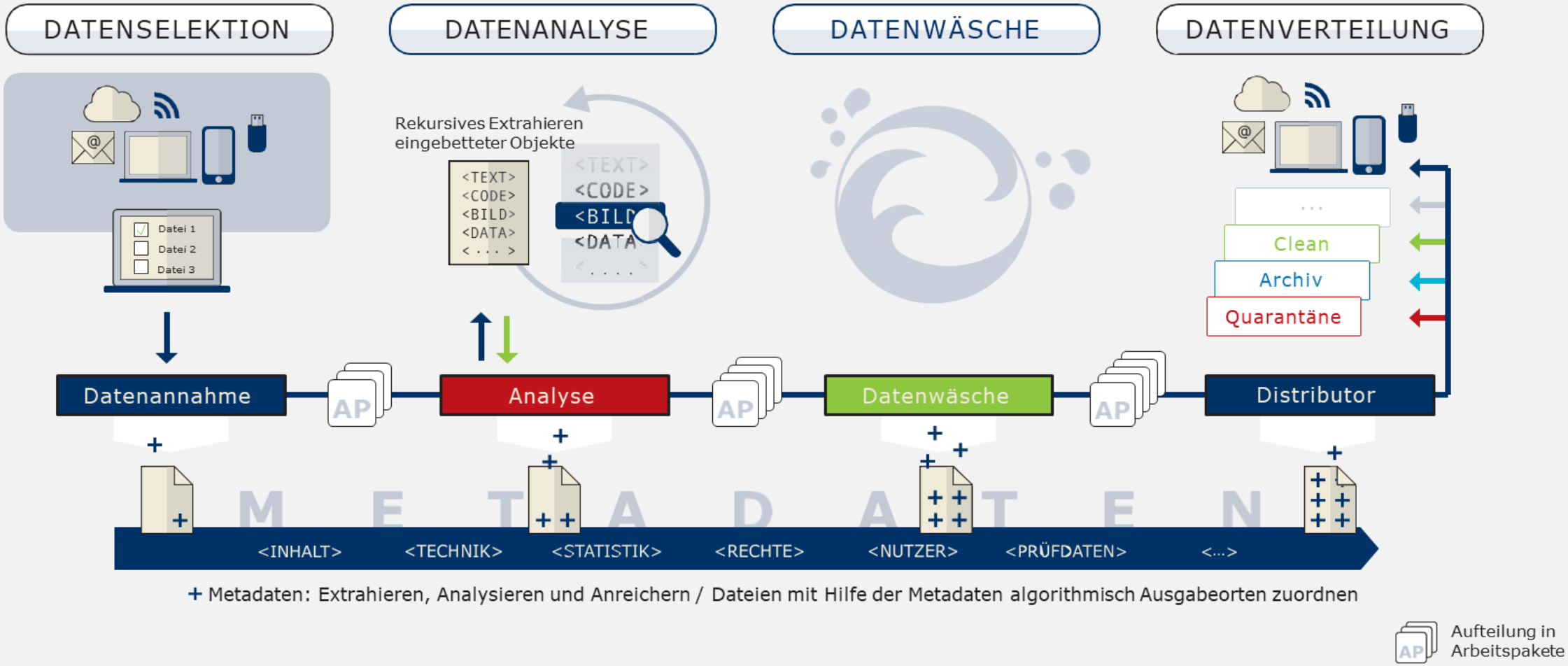
Lieferant





Nutzung

Sinnvolle Schleusen-Architektur



Denn: AntiVirus genügt nicht

Unterschied zwischen Anti Virus Lösungen und itWash:

	itWash	Anti Virus	AV basierte Schleuse
Reinigung – Veränderung des Dokuments	✓	✗	✗
Herauswaschen aller ausführbaren eingebetteten Objekte	✓	✗	✗
Blocken von identifizierbaren bereits bekannten Pattern von Schadcode	✓	✓	✓
Archivbomben entdecken und davor schützen	✓	✗	?
Rollenbasierte Verarbeitungstemplates	✓	✗	✗
Erkennung und Entschlüsselung von verschlüsselten Inhalten vor Prüfung	✓	✗	✗
BadUSB verhindern	✓	✗	✗
Virenbefallene Informationen lesbar verändern	✓	✗	✗
Workflow Rollen- und Inhalts-basiert	✓	✗	✗
Archiv vor Verarbeitung rekursiv entpacken	✓	✗	?
Metadaten extrahieren und archivieren	✓	✗	✗
(Zwangs)Verschlüsselung/Signatur nach Verarbeitung	✓	✗	?

itWatch Produkte

DeviceWatch	Gerätekontrolle
ApplicationWatch	Applikationskontrolle
XRayWatch	Dateien, Inhalte blockieren & auditieren
PDWatch	Verschlüsselung mobil, lokal und zentral
CDWatch	Medienbasierter Schutz
DEvCon	Kaskadierende Device Event Konsole
ReCAppS	Virtuelle Schleuse
DataEx	Sicher löschen und formatieren

PrintWatch	DLP Kontrolle über gedruckte Dokumente
AwareWatch	Security Awareness in Echtzeit
ReplicationWatch	Sichere Datenreplikation
RiskWatch	Risikoidentifikation auf Knopfdruck
LogOnWatch	Sicheres Microsoft Login – geschützt gegen Ausspähen
MalWareTrap	APT erkennen & isolieren

die **itWESS** - ein einziger Cyber Defense-Agent!

Datenschleuse mit Datenwäsche und Workflow

www.itwash.de

CryptWatch	HW-Verschlüsselung
Sichere Tastatur	Vollständige Lösung BadUSB
Private Data Room	Geschützter Datenraum
itWESS2Go	Mobilitätslösung für alle Sicherheitsklassen

Produktübersicht zum Download

Übersicht weiterführender Vorträge

- **„Digitale Souveränität und die Einschätzung der Sicherheit von Lieferketten – eine Managementdisziplin“** Problembeschreibung und Lösungsansätze“, Vortrag von Ramon Mörl am 01.02.2022 auf dem 18. Deutschen IT-Sicherheitskongress des BSI

- Vortrag von Ramon Mörl "Alle ausführbaren Objekte/Anwendungen überall erkennen, qualifizieren und sicher nutzen: wie geht das?"
  Vortrag von Ramon Mörl "Ohne ausführbares Objekt kein Angriff: alle Anwendungen sicher nutzen – was braucht man dazu?"
  Interview mit Ramon Mörl: Wie nutzt man fremde Daten in den eigenen Daten ohne Risiko? Schadcode, Makros, embedded Apps ... ob in Büro, Industrie, Leitstelle. (Alle Themen von der it-sa 365 2021).

- Unter dem Motto "Cyber Security - Rethinking Cyber Strategies in Tumultuous Times" fand im April 2021 die siebte mcsc des Sicherheitsnetzwerkes München e.V. statt. Ramon Mörl diskutierte in einem Panel mit dem Titel **„Corporate Cyber Risk Management – What Makes the Difference?“** (Munich Cyber Security Conference (mcsc) 2021)

- **„Data Centric Cyber Security – denn eigentlich geht es doch um Daten“**
  Vortrag von Ramon Mörl (it-sa 365 2020)

itWatch Kontaktdaten

Bitte kontaktieren Sie uns für weitere Informationen:

itWatch GmbH
Aschauer Str. 30
81549 München
Tel.: +49 (0)89 6203 010 0
eMail: Vertrieb@itWatch.de
www.itWatch.de
www.itWash.de

Fragen…

Ramon.Moerl@itWatch.de