HEALTH TECH CLUSTER SWITZERLAND

ISSS Information Security Society Switzerland

FH

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Digitalisierung im Gesundheitswesen: Risiken und Chancen

Prof. Dr. Eric Dubuis
Berner Fachhochschule

Information Security in Healthcare 2019

Wer bin ich?

Prof. Dr. Eric Dubuis

Leiter des «Research Institute for Security in the Information Society» RISIS

*… «Man betrachte "die **Zentralisierung persönlicher Informationen als eine Bedrohung**", unabhängig davon, ob diese in Apples Hand oder in Besitz einer anderen Firma sind. … Auf lange Sicht könne "**Sicherheit in der Server-Welt allein keinen adäquaten Schutz für die Privatsphäre bieten**".»*

Craig Federighi, Apple Inc.

Quelle: heise.de

Gliederung des Referats

I. «Klassische» Risiken

II. Schutzziele

III. Daten in der Cloud

IV. Elektronisches Patientendossier EPD

V. Fazit

I. «Klassische» Risiken

«Klassische» Angriffe auf die Gesundheitsinfrastruktur

- DDoS (distributed denial of service) -Angriffe

- Erpressungssoftware (Ransomware)

- Angriff «vor Ort»

DDoS (distributed denial of service) -Angriffe

Quelle: computerworld.ch

DDoS-Angriffe: Vorbeugende Massnahmen

Quelle: MELANI

Auszug

- Kenntnis der eigenen Infrastruktur
- Kenntnis des «Normalzustandes»
    - Intrusion Detection System
    - Zentralisierte Logauswertung
- Gehärte Systeme
- Firewall + Web-Application Firewall
- Ev. separater Internetzugang
- Ev. GeoIP-Blocking

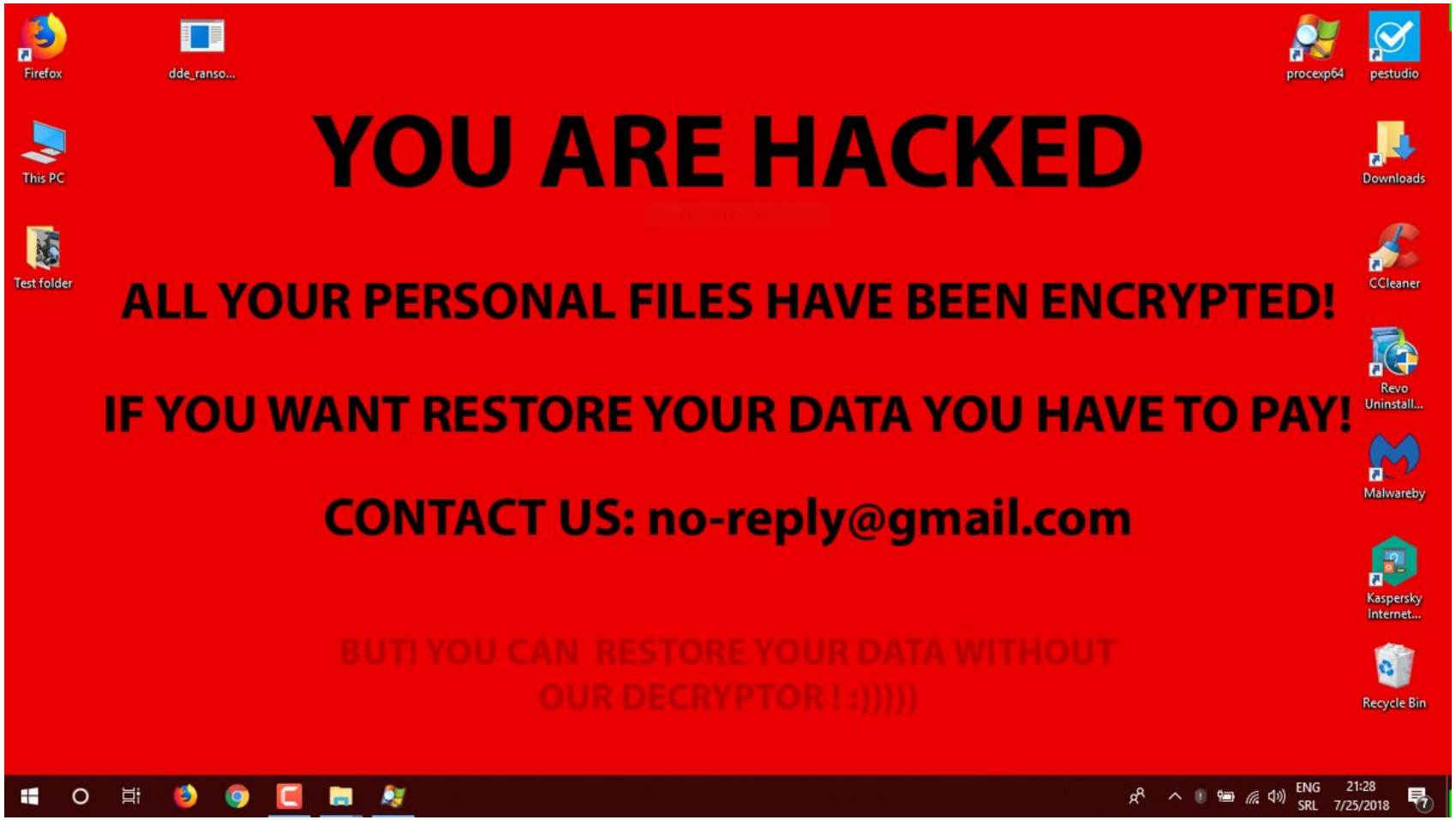
DDoS-Angriffe: Gegenmassnahmen

Quelle: MELANI

Auszug

- Protokollieren
- Angriff analysieren
- Abwehrstrategie festlegen
- Vorfall dem MELANI melden

Erpressungstrojaner (Ransomware)



Quelle:
bleepingcomputer.com

Erpressungstrojaner am Beispiel Lukaskrankenhaus in Neuss (D)

Quelle: sueddeutsch.de

Erpressungstrojaner: Präventive Massnahmen

Quelle: MELANI

- Regelmässige Sicherungskopien
- Software auf dem aktuellen Stand halten
- Aktueller Virenschutz
- Gerätspezifische Firewall

- Vorsicht bei E-Mails (Links, Anhänge)

Erpressungstrojaner: Massnahmen nach erfolgtem Angriff

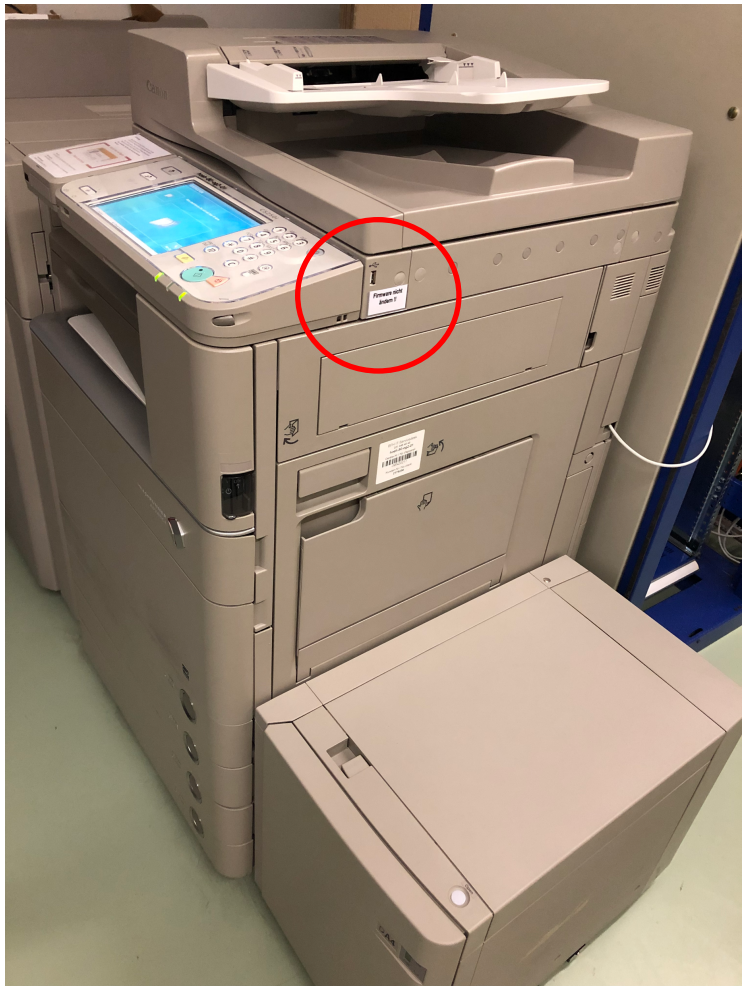
Quelle: MELANI

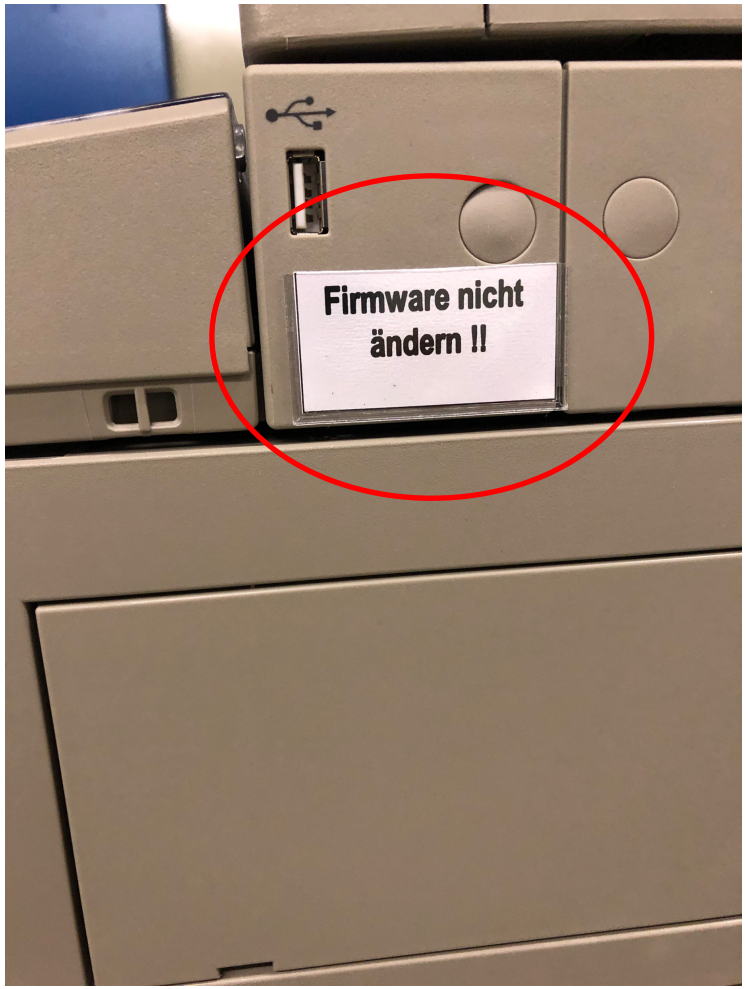
- Computer vom Netz trennen
- Computer säubern
- Daten von Sicherungskopie (falls vorhanden) zurückspielen

- Meldung an MELANI

- Kein Lösegeld bezahlen

Angriff «vor Ort»





Quelle: bfh.ch

Angriff «vor Ort»: Z.B. Bildschirm, der nicht gesperrt ist

The Wolf: Die Jagd geht weiter

Quelle: hp.com

Minderung der Risiken: Grundlegende Schutzmassnahmen

- Technische
  - **Updates**
  - **Firewall, Virenschutz**
  - Zugriffschutz
  - Zugangsschutz aller Geräte mit **starken Passworten**

- Verhaltensregeln
  - Sicheres Passwort
  - Mail: Vorsicht bei **unbekannten Absendern**
  - Mail: Vorsicht bei **Anhängen**
  - Web: Vorsicht beim Surfen, keine unbekannten Programme herunterladen

- Organisatorische Massnahmen
  - Vorgaben, Weisungen, Schulung
  - Awareness von Mitarbeitenden fördern

II. Schutzziele

«Klassische» Schutzziele

C I A

- C: Confidentiality (Vertraulichkeit)
- I: Integrity (Integrität)
- A: Availability (Verfügbarkeit)

Schutzziele

Schutzziele	
Haftung (accountability)	
Nachvollziehbarkeit (auditability)	
Authentizität (authenticity)	
Verfügbarkeit (availability)	
Vertraulichkeit (confidentiality)	
Integrität (integrity)	
Nichtabstreitbarkeit (non-repudiation)	
Privatsphäre (privacy)	

Beispiel «Aktenversand per E-Mail»

- Normale E-Mail

Schutzziele	
Haftung (accountability)	
Nachvollziehbarkeit (auditability)	
Authentizität (authenticity)	
Verfügbarkeit (availability)	
Vertraulichkeit (confidentiality)	
Integrität (integrity)	
Nichtabstreitbarkeit (non-repudiation)	
Privatsphäre (privacy)	-

Beispiel «Aktenversand per E-Mail»

- Digital signiertes E-Mail

Schutzziele	
Haftung (accountability)	
Nachvollziehbarkeit (auditability)	
Authentizität (authenticity)	
Verfügbarkeit (availability)	
Vertraulichkeit (confidentiality)	
Integrität (integrity)	
Nichtabstreitbarkeit (non-repudiation)	
Privatsphäre (privacy)	-

Beispiel «Aktenversand per E-Mail»

- Digital signierte und verschlüsselte E-Mail

Schutzziele	
Haftung (accountability)	
Nachvollziehbarkeit (auditability)	
Authentizität (authenticity)	✓
Verfügbarkeit (availability)	
Vertraulichkeit (confidentiality)	✓
Integrität (integrity)	✓
Nichtabstreitbarkeit (non-repudiation)	
Privatsphäre (privacy)	-

Fazit «Aktenversand per E-Mail»

III. Daten in der Cloud

Was sind Gesundheitsdaten?

«Als Gesundheitsdaten werden alle Daten bezeichnet, die den Gesundheitszustand des Patienten betreffen, also solche Daten, die häufig auch in einer Patientenakte zu finden sind.»

Quelle: Vitabook

Beispiele Gesundheitsdaten

- Stammdaten (Name, Adresse …)
- Krankengeschichte (Anamnese)
- Informationen über aktuelle Erkrankungen, Diagnosen, …
- Informationen zu chronischen Erkrankungen, Vorerkrankungen, Allergien, Unverträglichkeite
- Informationen zum Imp tatu
- Andere gesund eit zoge Informatio n (zu B ispiel Gewicht, Körperfettwe e, Blutzuckerwerte, Ernährungstagebuch)
- Medikamentierung
- Laborerge nisse
- Röntgenbilde
- Pat daten
- Patientenverfügung
- Im weitesten Sinne auch: Informationen zum Versichertenstatus, Arztrechnungen, Arzttermine etc.

Fast alles...

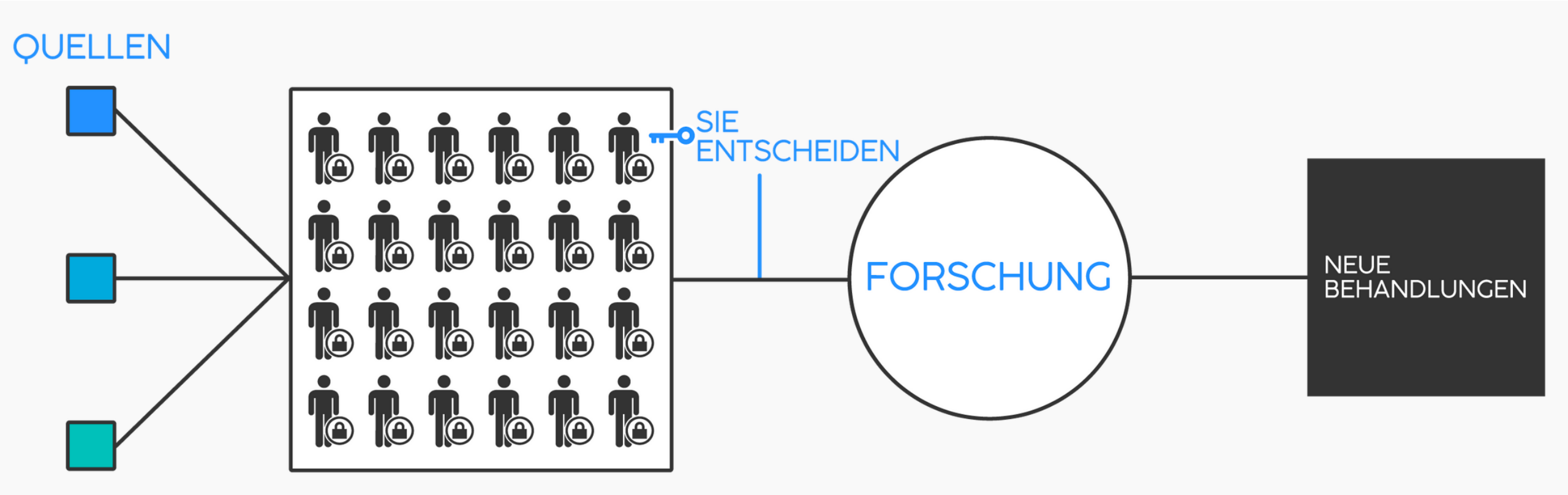
Daten in der Cloud

- Nicht personenbezogene Daten
  - Unfallschwerpunkte auf Strassen
  - Nebenwirkungen eines Medikaments
  - Zeitreihen, um Veränderungen festzustellen

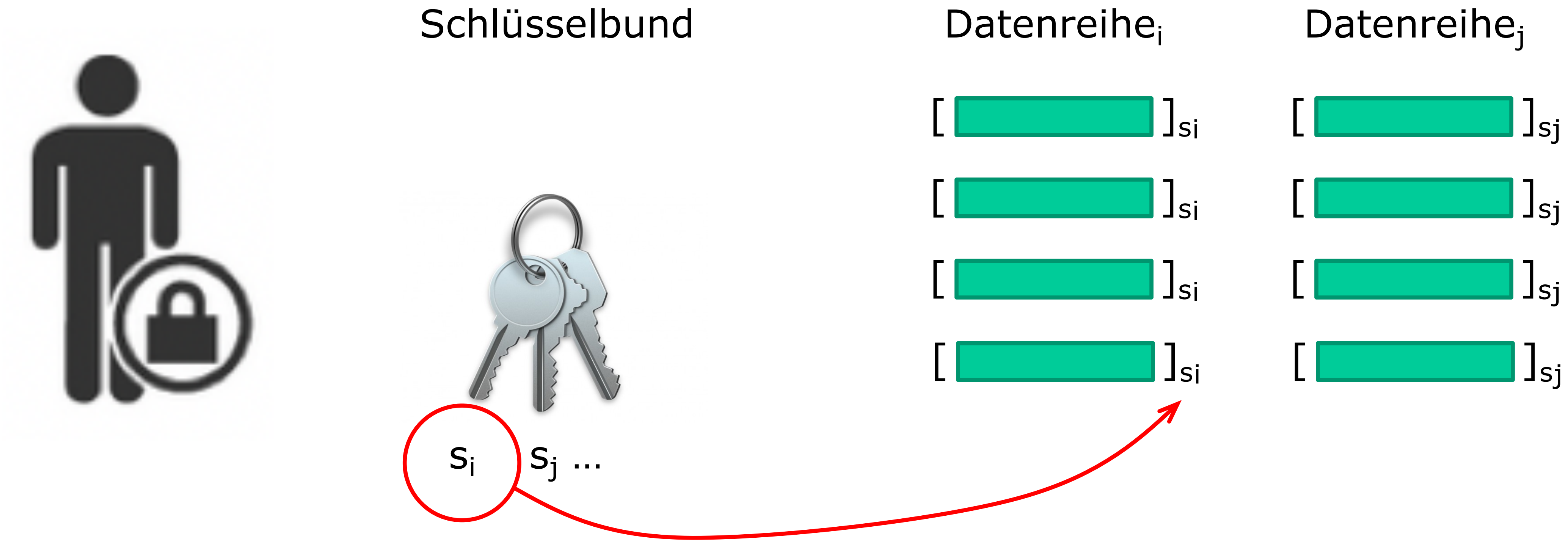
- **Personenbezogene Daten**
  Daten, welche sich auf eine bestimmte oder bestimmbare natürliche Person beziehen

- Der Angreifer ist in der Regel einfach «neugierig»…

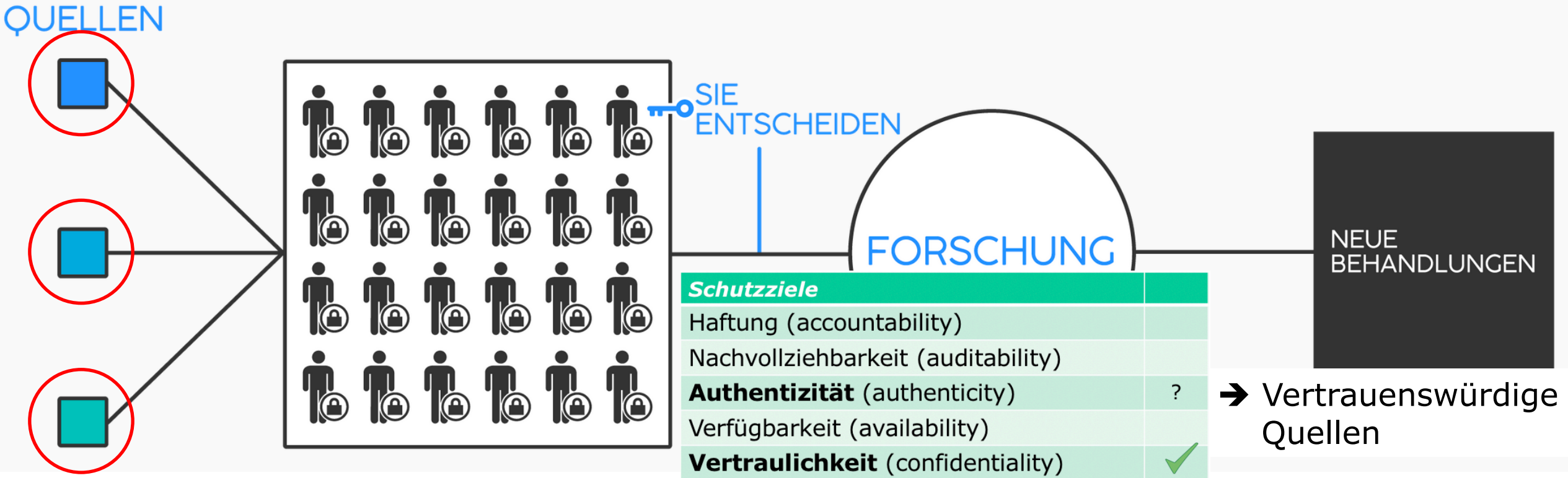
Beispiel «Datenkooperative»: Freischalten von Daten



Beispiel «Datenkooperative»: Selektives Freischalten



Beispiel «Datenkooperative»: Authentizität der Quellen?

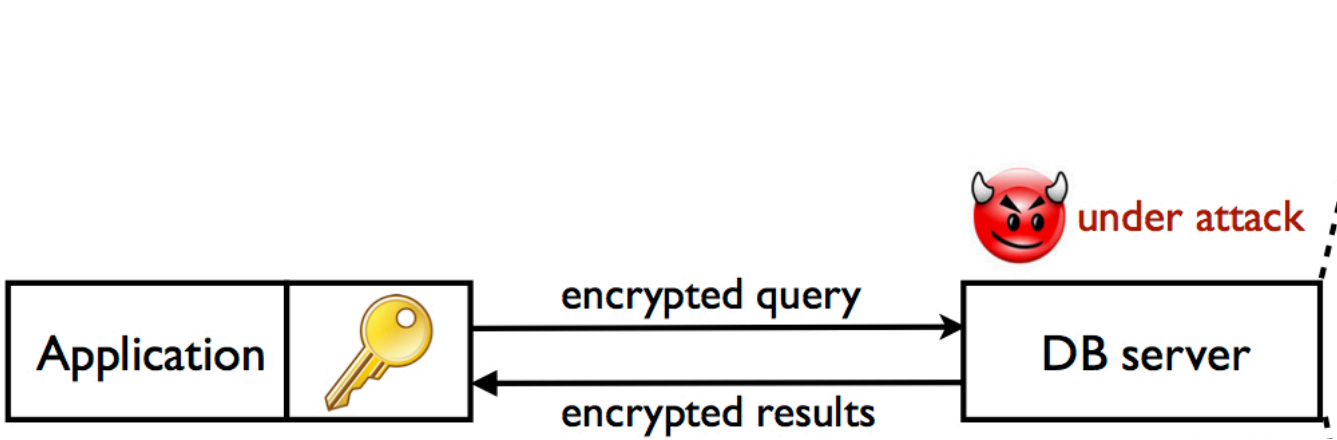


Schutzziele	
Haftung (accountability)	
Nachvollziehbarkeit (auditability)	
Authentizität (authenticity)	?
Verfügbarkeit (availability)	
Vertraulichkeit (confidentiality)	✓
Integrität (integrity)	✓
Nichtabstreitbarkeit (non-repudiation)	
Privatsphäre (privacy)	?

➔ Vertrauenswürdige Quellen

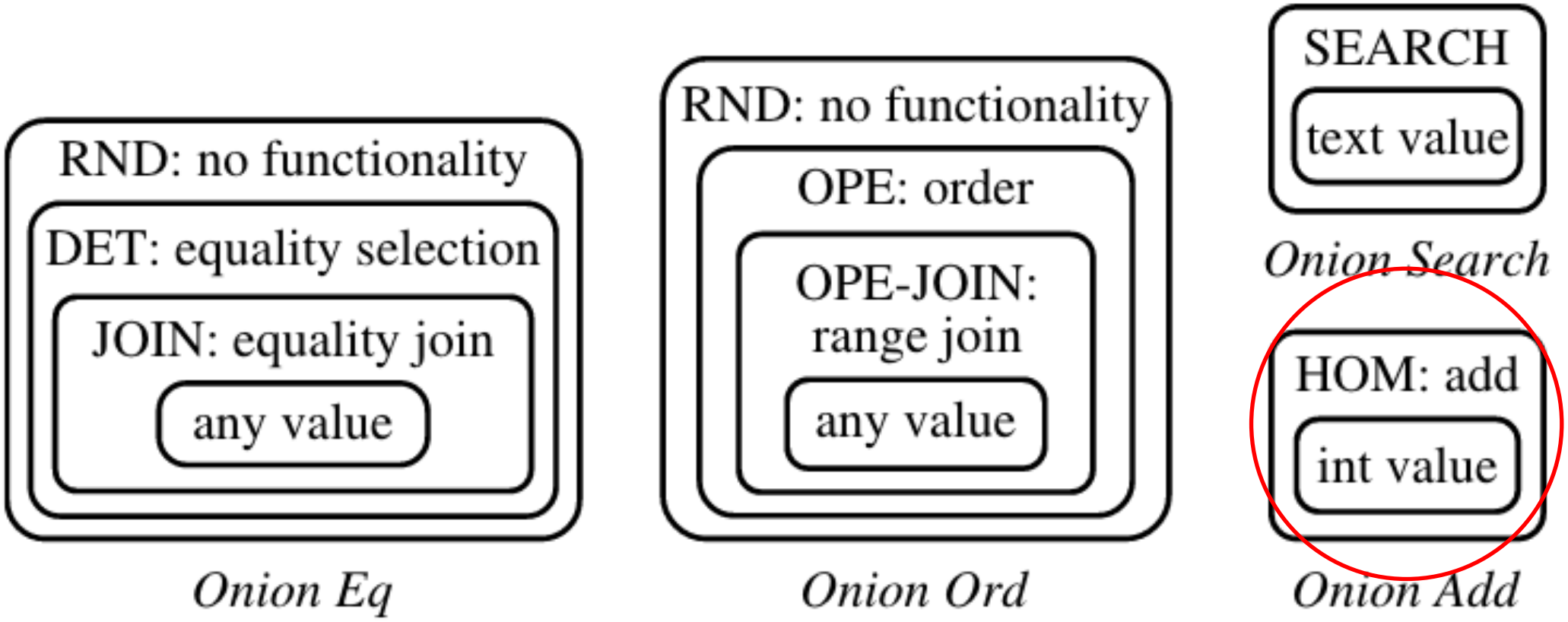
Stimmen diese Werte?

Beispiel «CryptDB»: End-to-end-Verschlüsselung



Schutzziele	
Haftung (accountability)	
Nachvollziehbarkeit (auditability)	
Authentizität (authenticity)	?
Verfügbarkeit (availability)	
Vertraulichkeit (confidentiality)	✓
Integrität (integrity)	?
Nichtabstreitbarkeit (non-repudiation)	
Privatsphäre (privacy)	✓

Beispiel «CryptDB»: Mehrstufige / homomorphe Verschlüsselung



Einschub: Additive homomorphe Verschlüsselung

- Werte m_1, m_2

- Verschlüsselte Werte: $Enc(m_1)$, $Enc(m_2)$

- «Addition» der verschlüsselten Werte: $Enc(m_1) \oplus Enc(m_2) = Enc(m_1 + m_2)$

Die Summe wird über die verschlüsselten Werte gebildet. Das Resultat ist eine Verschlüsselung. Wird sie entschlüsselt, so entspricht die Entschlüsselung der Summe der ursprünglichen Werte.

IV. Elektronisches Patientendossier EPD

EPD
elektronisches
Patientendossier

Quelle: patientendossier.ch

EPD: Grundsätze

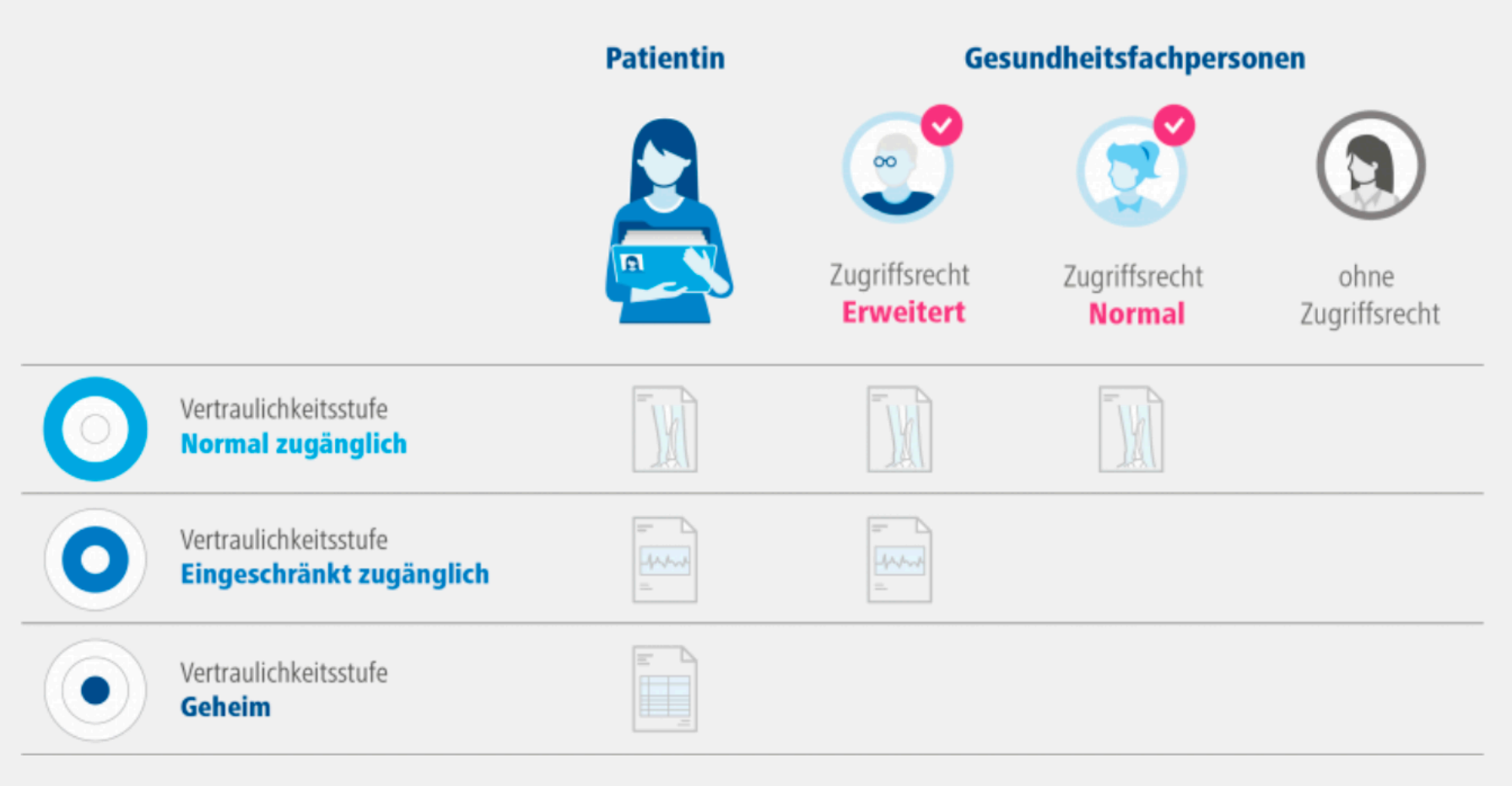
- Keine zentrale Speicherung
- Zertifizierung der EPD-Anbieter
- Neue Patienten-Identifikationsnummer
- Sichere Identifizierung
- Zwei-Faktor-Authentisierung (2FS)

- Zentraler Grundsatz: «**informationelle Selbstbestimmung der Patienten**»: Jeder Patient soll zu jeder Zeit das Recht erhalten, Gesundheitsfachpersonen das Zugriffsrecht zu seinen Gesundheitsdaten zu gewähren oder zu entziehen

EPD: Verteilte Datenhaltung

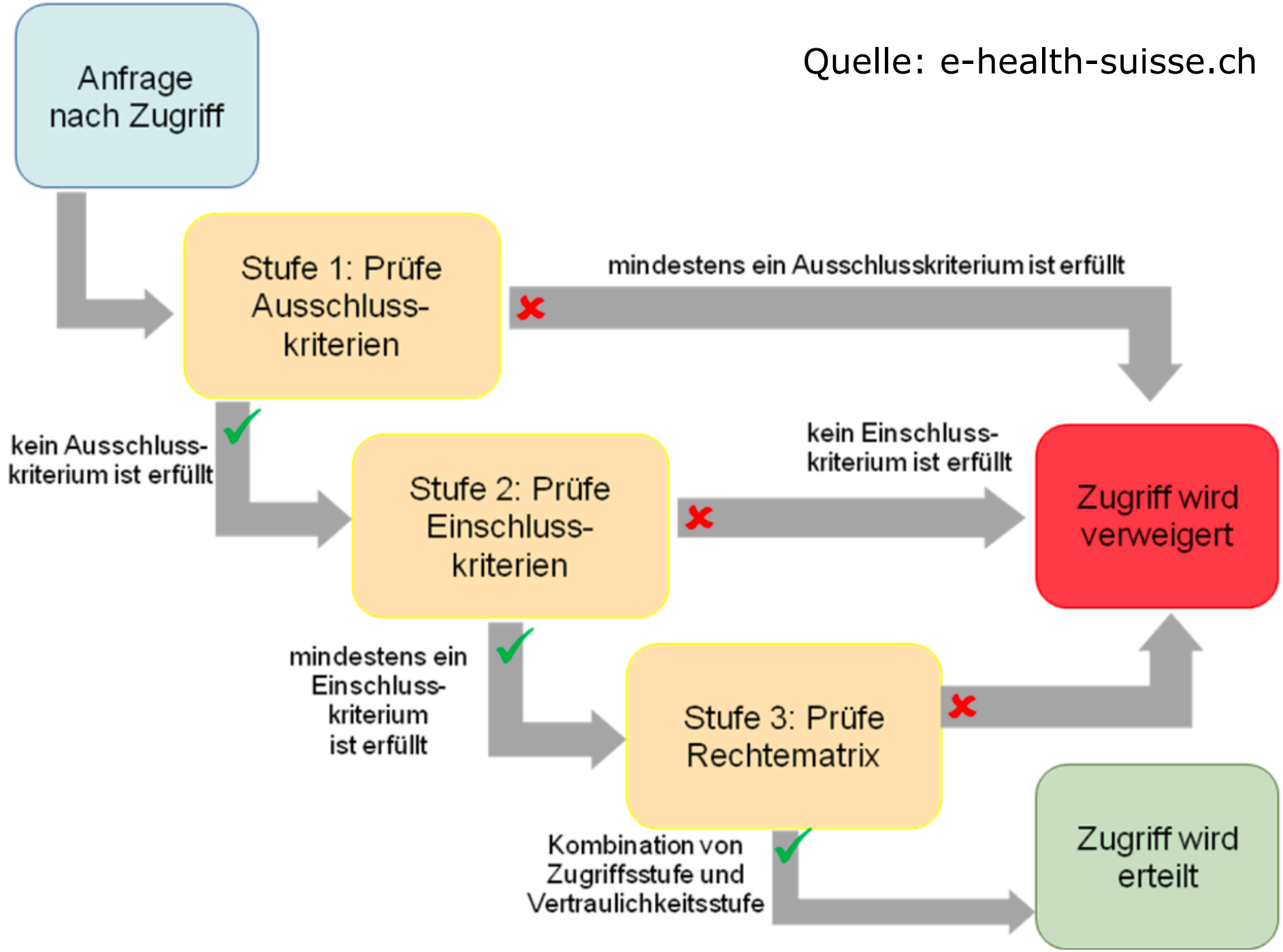
Quelle: patientendossier.ch

EPD: Drei Vertraulichkeitsstufen



Quelle: patientendossier.ch

Quelle: e-health-suisse.ch



Wie steht’s mit den Schutzzielen?

Schutzziele	
Haftung (accountability)	
Nachvollziehbarkeit (auditability)	✓
Authentizität (authenticity)	✓
Verfügbarkeit (availability)	
Vertraulichkeit (confidentiality)	✓
Integrität (integrity)	✓
Nichtabstreitbarkeit (non-repudiation)	
Privatsphäre (privacy)	✗

➔ Vertrauen zu den Beteiligten

EPD: Strenge Zertifizierung

«Jeder Anbieter des EPD wird umfassend geprüft, zertifiziert und regelmässig kontrolliert. …»

Quelle: patientendossier.ch

EPD: Aber…

«Aufgrund des Aufwands bei der Umsetzung gibt es nun leider keine End-To-End-Verschlüsselung der Daten. Zwar liegen die Daten verschlüsselt bei den diversen Teilnehmern, ***aber den Schlüssel hat immer jemand Drittes*** […]. Jedoch muss das Ziel sein, dass der Patient zu jedem Zeitpunkt die Datenhoheit hat.»

Dr. Reinhold Sojer, Abteilungsleiter der Abteilung Digitalisierung / eHealth an der FMH

Quelle: healthcare-in-europe.com

V. Fazit

Fazit «Allgemeine Infrastruktur»

Chancen	Risiken
– Verbesserung der Behandlungsqualität – Verbesserung der Behandlungsprozesse – Verbesserung der administrativen Prozesse	– Unautorisierter Zugang wegen Lücken – Unautorisierter Zugang durch «social engineering» – Verlust der Daten – …

Fazit «Daten in der Cloud»

Chancen	Risiken
– Viele Daten nützlich für die Forschung	– Unautorisierter Zugang wegen Lücken – Verlust des Master-Schlüssels – Datenquellen nicht vertrauenswürdig

Fazit «Elektronisches Patientendossier»

Zielkonflikt

Chancen	Risiken
– Verbesserung der Behandlungsqualität – Einfacher Zugriff auf Gesundheitsdaten im Notfall – Optimierung der Medikation – Vermeidung von Doppelspurigkeiten – …	– Unautorisierter Zugang zu den Gesundheitsdaten durch Dritte – Schutz der Privatsphäre

Vielen Dank

Prof. Dr. Eric Dubuis
Berner Fachhochschule
Biel