HERZLICH WILLKOMMEN!

SIMPLY SAFE CONNECTED?

DATENSICHERHEIT IN DER SMARTEN WELT

EINE DER GRÖSSTEN HERAUSFORDERUNGEN FÜR WIRTSCHAFT UND GESELLSCHAFT

Alle 39 Sekunden findet weltweit ein Cyberangriff statt.

Alle 14 Sekunden erfolgt weltweit ein Ransomware-Angriff

40% der weltweiten Cyberangriffe sind Datendiebstähle von z.B. Benutzernamen und Passwörtern.

Bei 80% der Hacker-Angriffe werden persönliche Daten gestohlen.

Rund 30% der deutschen Unternehmen haben in den letzten drei Jahren durch den schwerwiegendsten Datendiebstahl jeweils einen Schaden von mehr als 1 Mio. Dollar erlitten. Das sind 3% mehr als bei ähnlichen Vorfällen in anderen Länder.

ZUNEHMENDER VERNETZUNGSGRAD BIRGT CHANCEN BEI GLEICHZEITIG STEIGENDENDEM RISIKOPOTENZIAL

- **Alle** verbundenen intelligenten Geräte und der Zugriff auf diese werden zu Zielen.
- **Jeder vernetzte Knotenpunkt** erhöht das Sicherheitsrisiko eines Netzwerks exponentiell.
- Wenn ein einzelner Endpunkt in einem intelligenten System ungeschützt ist, **ist das gesamte System gefährdet.**

HACKER LIEBEN ANMELDEINFORMATIONEN!

DIE HÄUFIGSTE MOTIVATION FÜR DIEBSTAHL VON ANMELDEINFORMATIONEN IST RANSOMWARE

Anmeldeinformationen ermöglichen Angreifer ohne großen Aufwand vollen Zugriff auf Netzwerke und Anwendungen.

Bei Datenschutzverletzungen sind Anmeldeinformationen, die Nummer 1 über alle Angriffs-Vektoren hinweg.

System-Intrusion-Angriffe erfolgen z.B. zu 42 % über Anmeldedaten. Social-Engineering-Angriffe zu 63 %.

Webanwendungsangriffe werden zu 80 % gestohlenen Anmeldeinformationen zugeschrieben. Business E-Mail Kompromittierung zu 43 %.

DER GESUNDHEITSSEKTOR EIN BELIEBTES ZIEL

Positives Kosten-/Nutzenverhältnis aus Sicht der Angreifer:

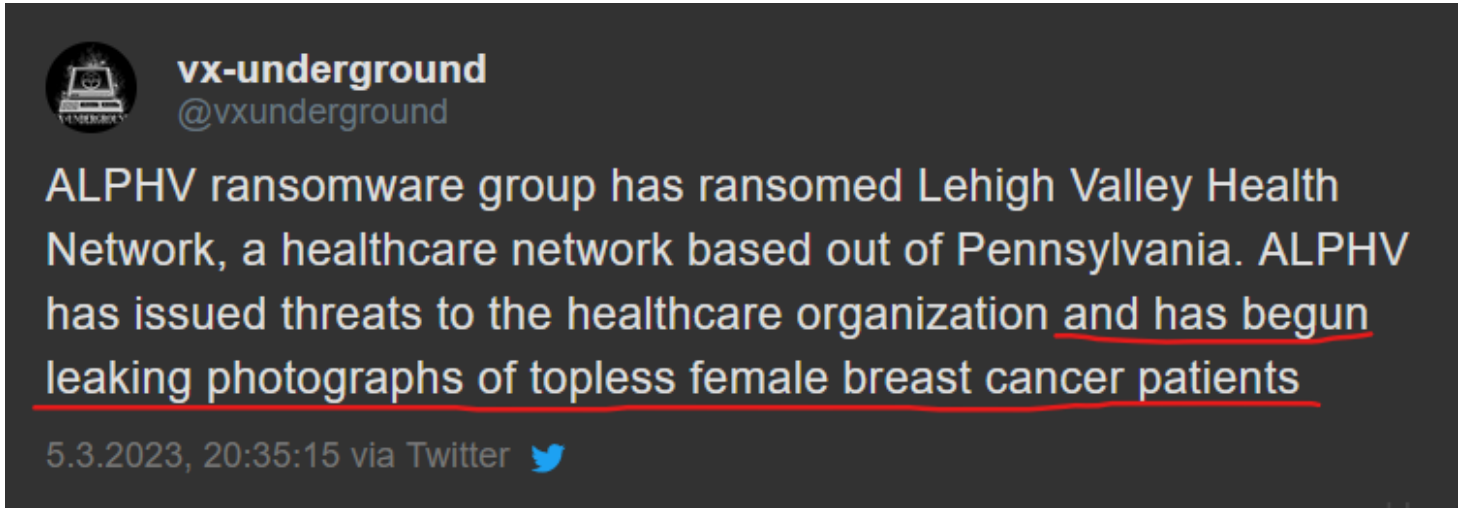
- Medizinische Einrichtungen sind häufig unzureichend geschützt.
- **Daten aus dem Gesundheitswesen sind besonders wertvoll.**
- Die Schwere potenzieller Folgen die bei einem Angriff auf Gesundheits-daten drohen erhöhen die Chancen auf Lösegeld.

Personenbezogene Faktoren:

- Mitarbeiter haben durchschnittlich Zugriff auf 11 Millionen Dateien. Dies entspricht knapp 20% des gesamten Datenbestandes.
- Im Durchschnitt sind 12% der sensiblen Daten, wie Forschungsergebnisse, geistiges Eigentum und Gesundheitsdaten, für jeden Mitarbeiter zugänglich.
- In kleineren Krankenhäusern und Unternehmen (bis 500 Mitarbeitern) beträgt dieser Wert sogar 22%.
- Der Mensch ist und bleibt die größte Schwachstelle.

POTENZIELLE FOLGEN FÜR PATIENT_INNEN

DAS BEISPIEL EINES ANBIETERS AUS PENNSYLVANIA



Die Cybergang habe unter anderem sensiblen Daten aus der **Patientendatenbank, Ausweis- und persönliche Daten und Nacktbilder**. "Eure Zeit läuft ab. Wir sind bereit, unsere volle Macht gegen euch zu entfesseln!", schließen die Cyberkriminellen ihre Nachricht ab.

https://www.heise.de/news/Skrupellos-Cybergang-Alphv-veroeffentlicht-Patientenbilder-nach-Einbruch-7536239.html

RANSOMWARE-ANGRIFFE

DIE KOMPONENTEN FINANZIELLER AUSWIRKUNGEN

Offensichtliche Kosten

- Lösegeld:
  Cyberkriminelle verlangen i.d.R. zwischen 0,7 – 5% vom Jahresumsatz des Opfers.

Versteckte Kosten

mit steigender Tendenz seit 2020, aufgrund des Anstiegs von Doppelerpressung und Großwildjagd, **unabhängig erfolgter Lösegeldzahlung**

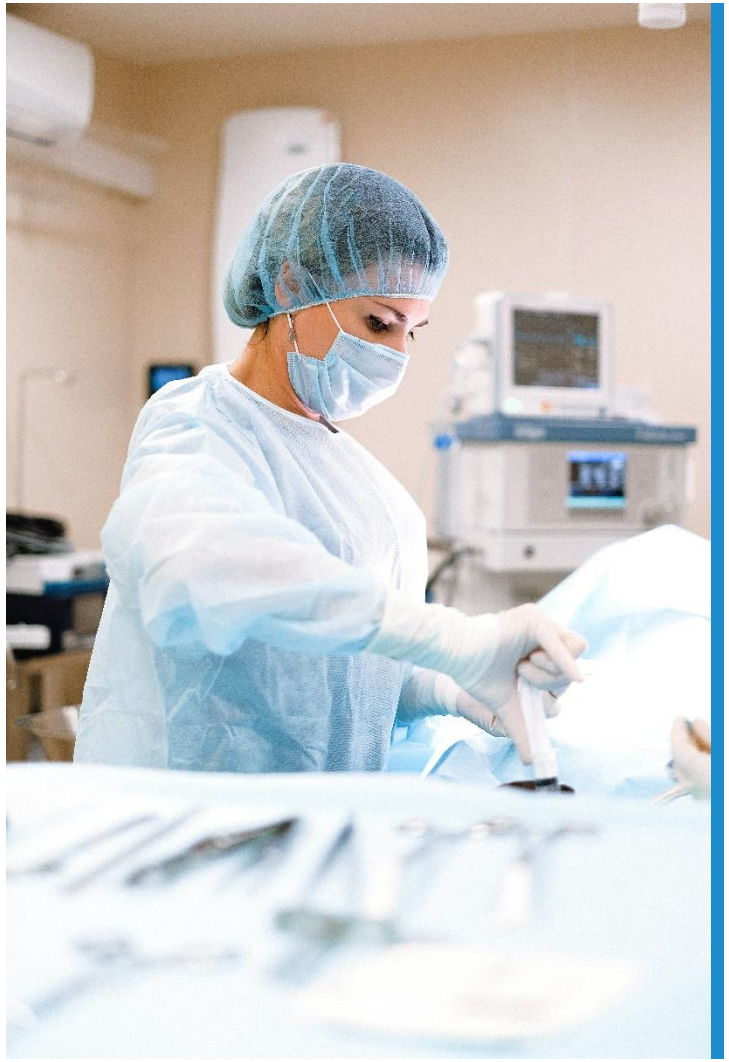
- Reaktions- und Wiederherstellungskosten
- Anwaltskosten
- IT-Forensik, Überwachung
- Ggf. Schadensersatzansprüche Dritter
- **Strafzahlungen durch Verletzung datenschutzrechtlicher Aspekte**
- Kosten durch Reputationsschäden und damit verbundene Umsatzverluste

Die Gesamtkosten sind 7x höher als das Lösegeld*

*Quellen: Check Point Research/KOVRR

RISIKOMINIMIERUNG!

FAKTOREN EFFIZIENTER ZUGRIFFSKONZEPTE



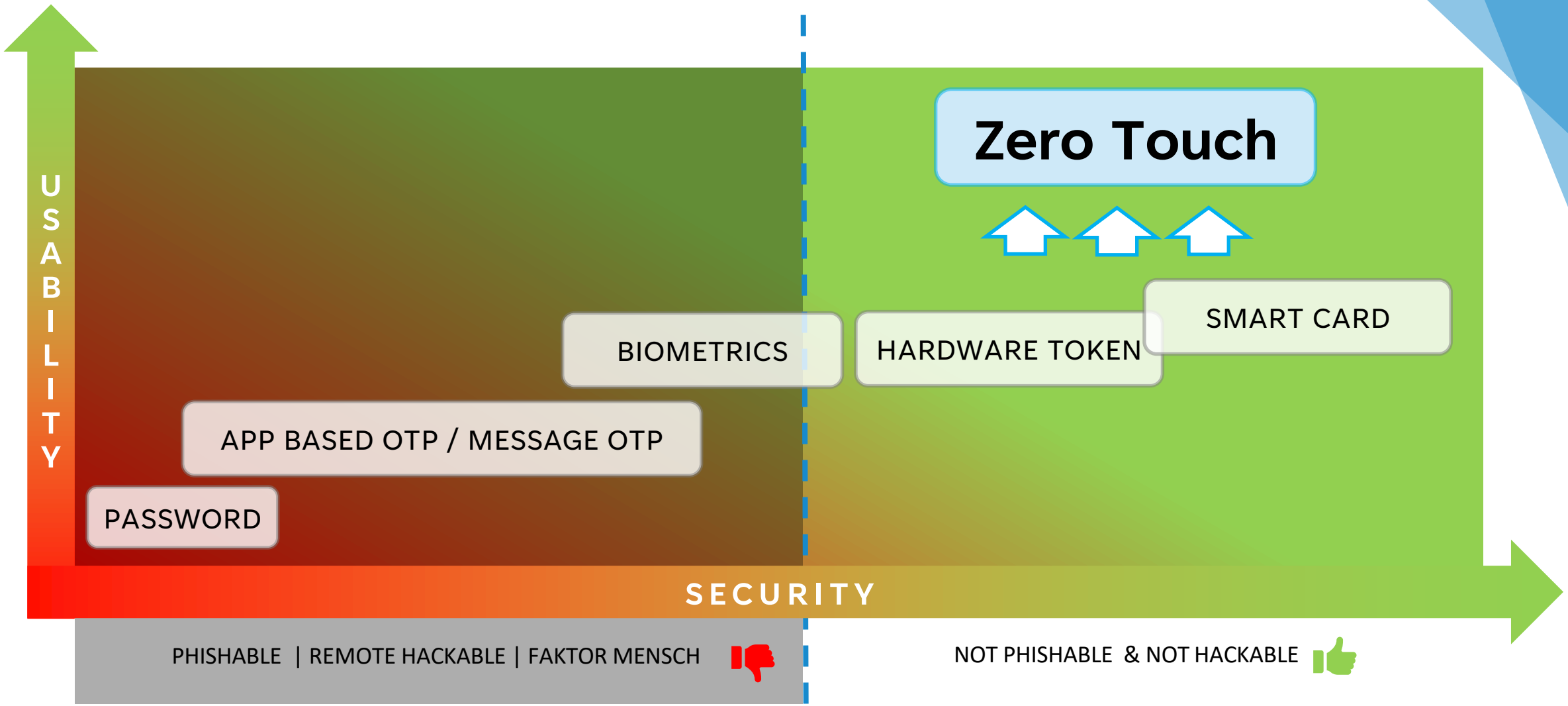
Daten müssen nicht nur auf dem PC, sondern auch auf mobilen Geräten sowie im Kontext von Health 4.0 und Cloud Sicherheit **verschlüsselt** werden.

Alle notwendigen Sicherheitsprozesse laufen automatisch „im Hintergrund" ab. Und das auch dann, wenn Sie **beide Hände voll zu tun** haben.

Geräte müssen **zentral** konfiguriert werden können im Hinblick auf **unkomplizierte Nutzerverwaltung**, **Skalierbarkeit der Sicherheitslösung** und **Datenhoheit**.

BENUTZERFREUNDLICHKEIT = HOHE SICHERHEIT

NUTZERZENTRIERTE AUTHENTISIERUNG



Sicherheit auf drei Ebene

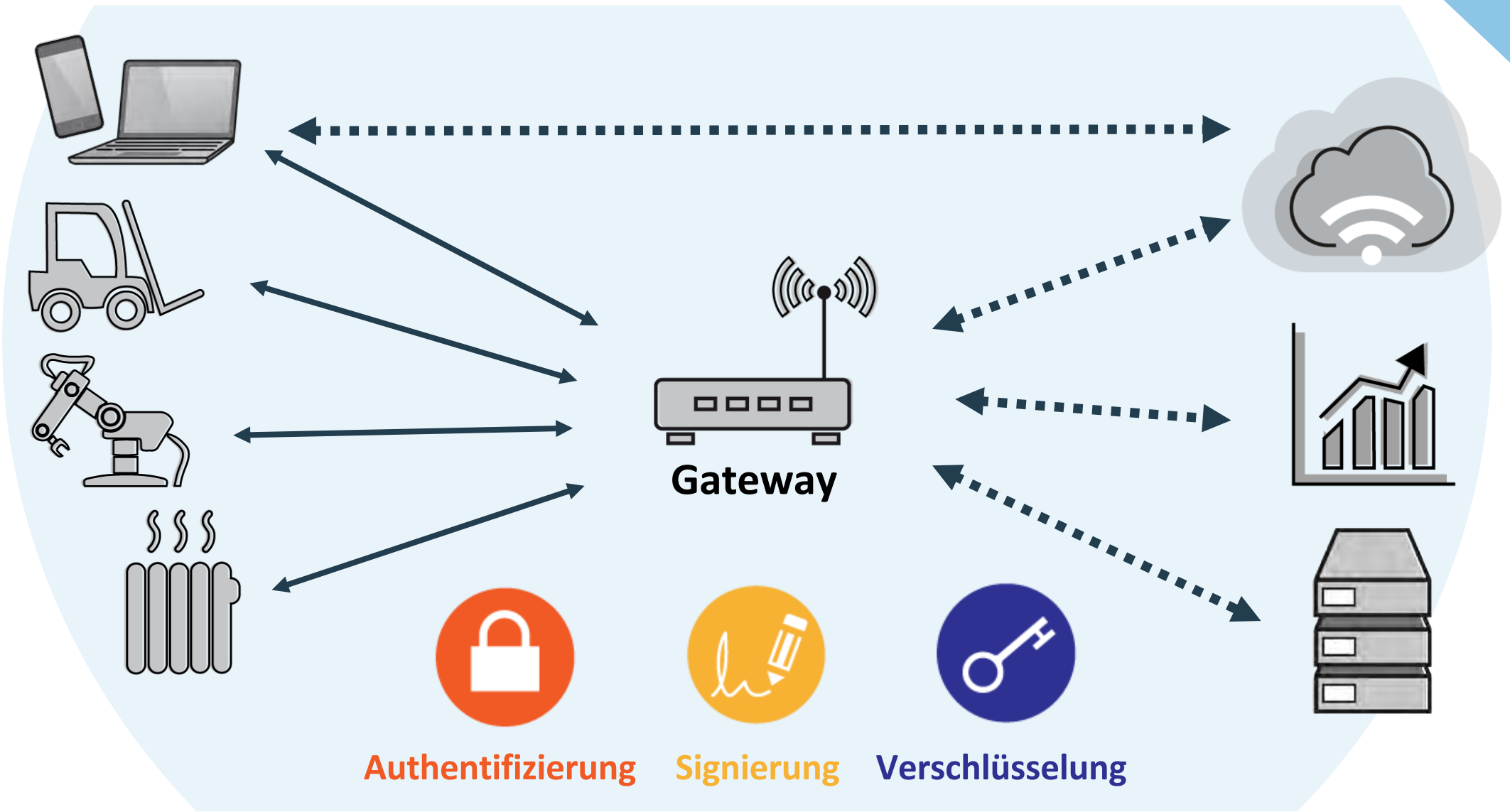
SCHUTZZIELE: VERTRAULICHKEIT – INTEGRITÄT - VERFÜGBARKEIT

Authentifizieren: Identitätsprüfung von Benutzern, Maschinen oder Geräten für komplexe Netzwerke

Signieren: Schutz gegen Daten- und Softwaremanipulation

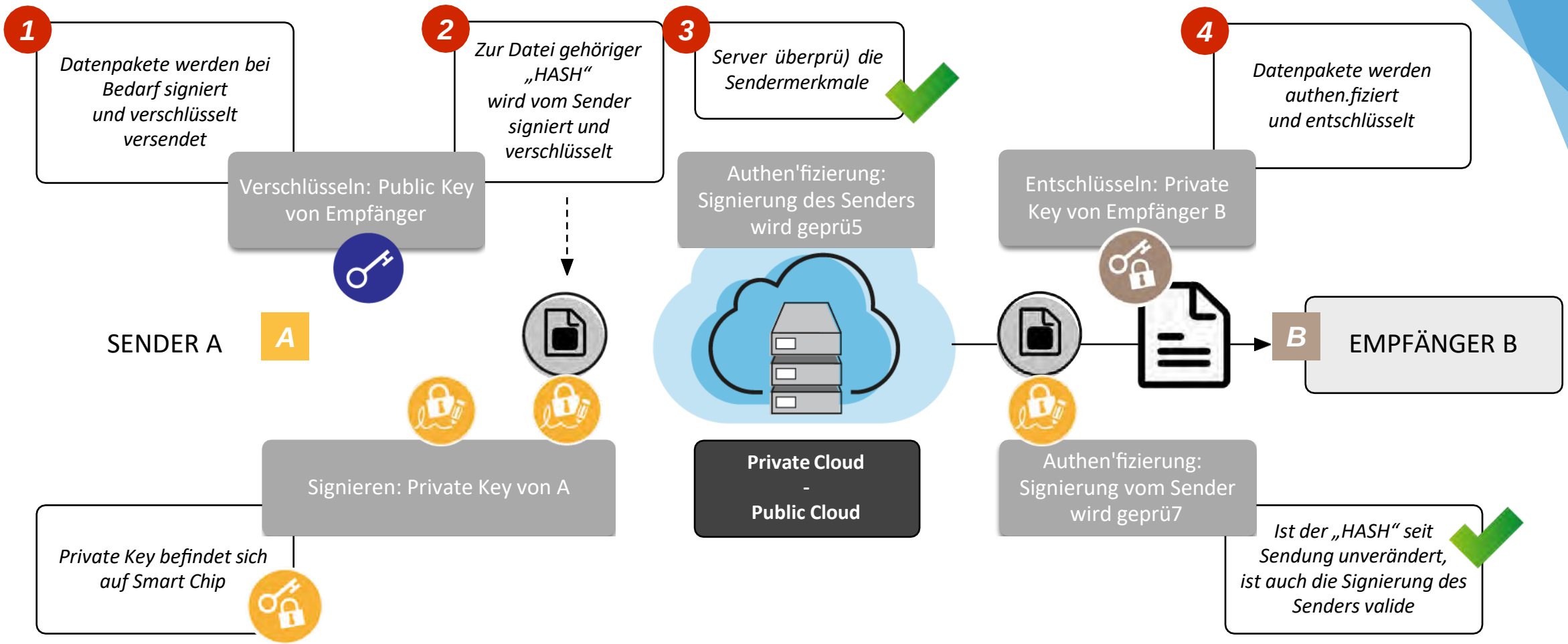
Verschlüsseln: Kryptologische Sicherung vertraulicher Daten auf Hardware-Ebene

ABSICHERUNG DES DATENVERLAUFS



SICHERHEITSKONZEPT

KOMPONENTEN EINES VERTRAUENWÜRDIGER KOMMUNIKATION



SIMPLY SAFE CONNECTED!

Vielen Dank!