strategy& 25. April 2018

Kritische Infrastrukturen im Gesundheitswesen

Auswirkungen der zunehmenden Digitalisierung

Prof. Dr. Rainer Bernnat

pwc

Strategy& ist die führende Beratung bei der Digitalisierung des deutschen Gesundheitswesens

AUSWAHL

Normativ

1. **Weiterentwicklung der eHealth-Strategie** eine Studie im Auftrag BMG
2. **KRITIS-Sektorstudie Gesundheit** eine Studie im Auftrag BSI
3. **Ökonomische Bestandsaufnahme und Potenzial-analyse der digitalen Gesundheitswirtschaft** eine Studie im Auftrag BMWi

Strategisch

4. **Effizienzpotentiale durch eHealth** eine Studie im Auftrag bvitg und CGM
5. **eCare-Anwendungen in der ambulanten Pflege** eine Studie im Auftrag CGM
6. **Pain Detect** Studie im Auftrag von Pfizer

Patientenfokus

Organisationsfokus

Operativ

7. **Konzeptionelle** & **strategische** Beratung im Rahmen der **Einführung eGK** im Auftrag gematik
8. Studie **Gesundheitspolitische Herausforderungen von eHealth** im Auftrag für die PKV
9. Diverse Digitalisierungs-Projekte bei führenden **GKVen**

Agenda

1 **Kritische Infrastrukturen und deren Bedeutung für das Gesundheitswesen**

2 **Informationstechnologien im Gesundheitssektor und deren zunehmende Anwendung**

3 **Potentielle Zielkonflikte im Spannungsfeld von IT-Schutzmaßnahmen und ethischen Fragestellungen**

Digitalisierung im Gesundheitswesen trägt zur Dämpfung des Kostenanstiegs bei

Zentrale Studienergebnisse: Effizienzpotenziale eHealth, 2017

I. **Potentiale von eHealth noch weitgehend ungenutzt,** wenn auch schon im Versorgungsalltag messbar

II. Gesamthaft umgesetzte **eHealth-Lösungen führen zu signifikanten Verbesserung** der medizinischen und operativen Exzellenz

III. **Effizienzpotential durch eHealth in Deutschland beträgt ca. 39 Mrd. Euro,** ca. 12,2 % der gesamten Krankheitskosten im Jahre 2014

IV. **eHealth erleichtert sektorübergreifende & multidisziplinäre Versor-gungsmodelle,** ist jedoch kein Substitut zum Arzt-Patienten-Dialog

V. **Zur Realisierung** des Effizienzpotentials ist **Telematik-Infrastruktur** zu etablieren und die **elektronische Patientenakte** einzuführen

Das E-Health-Gesetz schafft Grundlagen – Konsequenz in der Umsetzung bislang noch nicht erzielt

- **Modernes Stammdatenmanagement** (bis Mitte 2018 flächendeckend eingeführt) 
- **Medizinische Notfalldaten** ab 2018 auf eGK gespeichert (auf Wunsch des Versicherten) 
- **Elektronische Arztbriefe**, bereits vor Einführung der Telematik-Infrastruktur gefördert ✓
- Förderung des Einstiegs in die **elektronische Patientenakte** – Schaffung der Voraussetzungen bis Ende 2018 durch die gematik 
- Patientennutzen und Patientenselbstbestimmung – auch mittels **Patientenfach** (Schaffung der Voraussetzungen bis Ende 2018 durch die gematik) 
- Förderung der Telemedizin durch **telekonsiliarische Befundung** von Röntgenaufnahmen (ab April 2017) und Online-Videosprechstunde (ab Juli 2017) 
- Erstellung eines **Interoperabilitätsverzeichnisses** (bis Juni 2017) (✓)
- Weiterentwicklung Zugang über **Smartphones / mobile Endgeräte** ?

„Mit dem E-Health-Gesetz treiben wir den Fortschritt im Gesundheitswesen voran. Dabei stehen Patientennutzen und Datenschutz im Mittelpunkt. Eine sichere digitale Infrastruktur verbessert die Gesundheitsversorgung und stärkt die Selbstbestimmung der Patienten – das bring echten Nutzen für die Versicherten. Ärzte, Kassen und Industrie stehen jetzt gleichermaßen in der Pflicht, die gesetzlichen Vorgaben im Sinne der Patienten zügig umzusetzen.“

Bundesminister Hermann Gröhe, Dezember 2015

Quelle BMG 2015

Kritische Infrastrukturen sind ein wesentlicher Bestandteil zur Aufrechterhaltung der öffentlichen Versorgung

Kritische Infrastrukturen (KRITIS) sind **Organisationen** oder **Einrichtungen mit wesentlicher Bedeutung** für das **staatliche Gemeinwesen.**

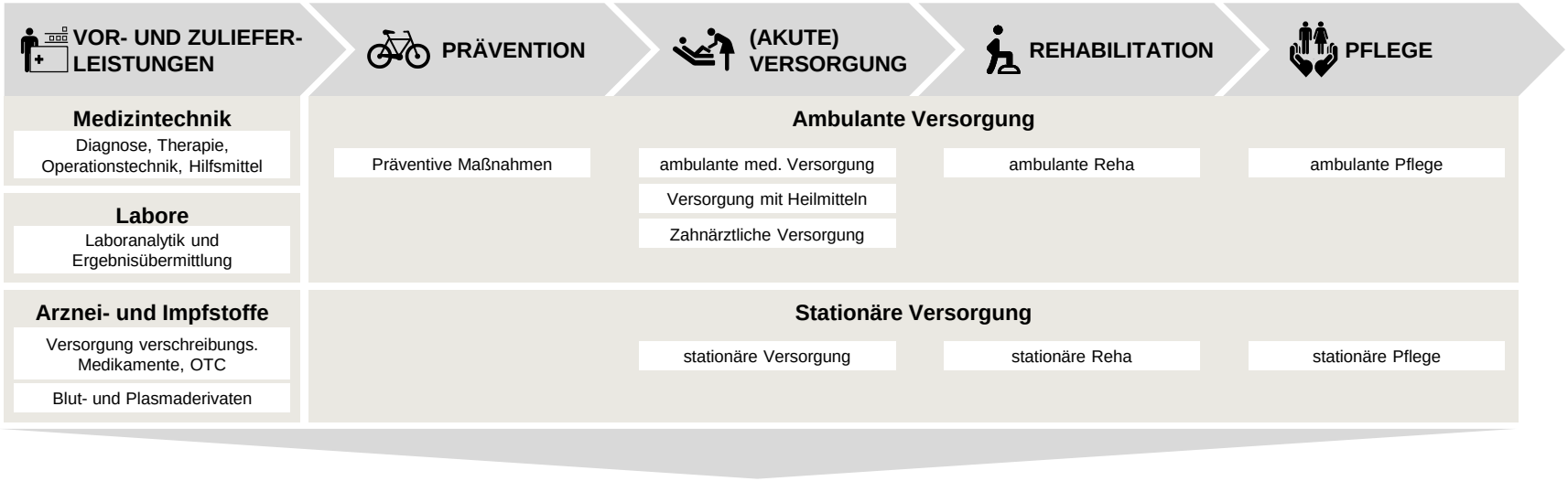
§ GESETZLICHER RAHMEN

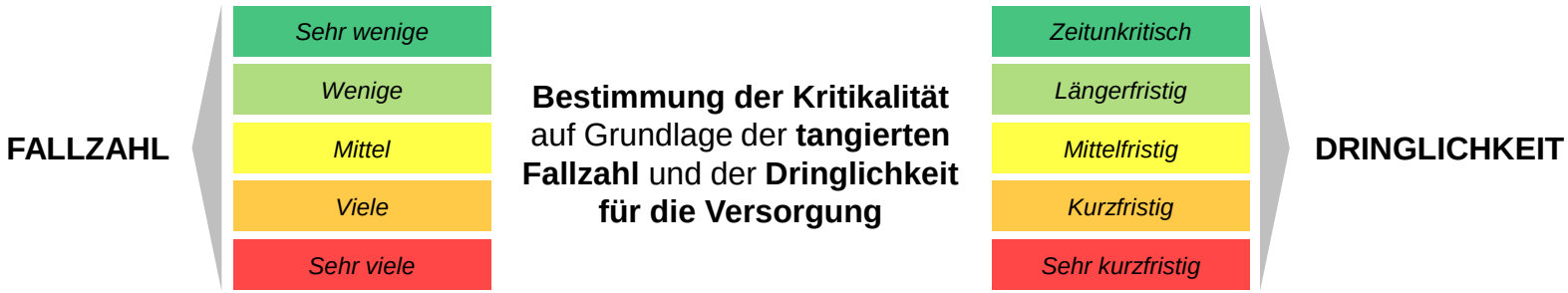
Definition von Kritischen Infrastrukturen auf Grundlage von **EU-Richtlinie 2008/114/EG**

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz**) seit Juli 2015

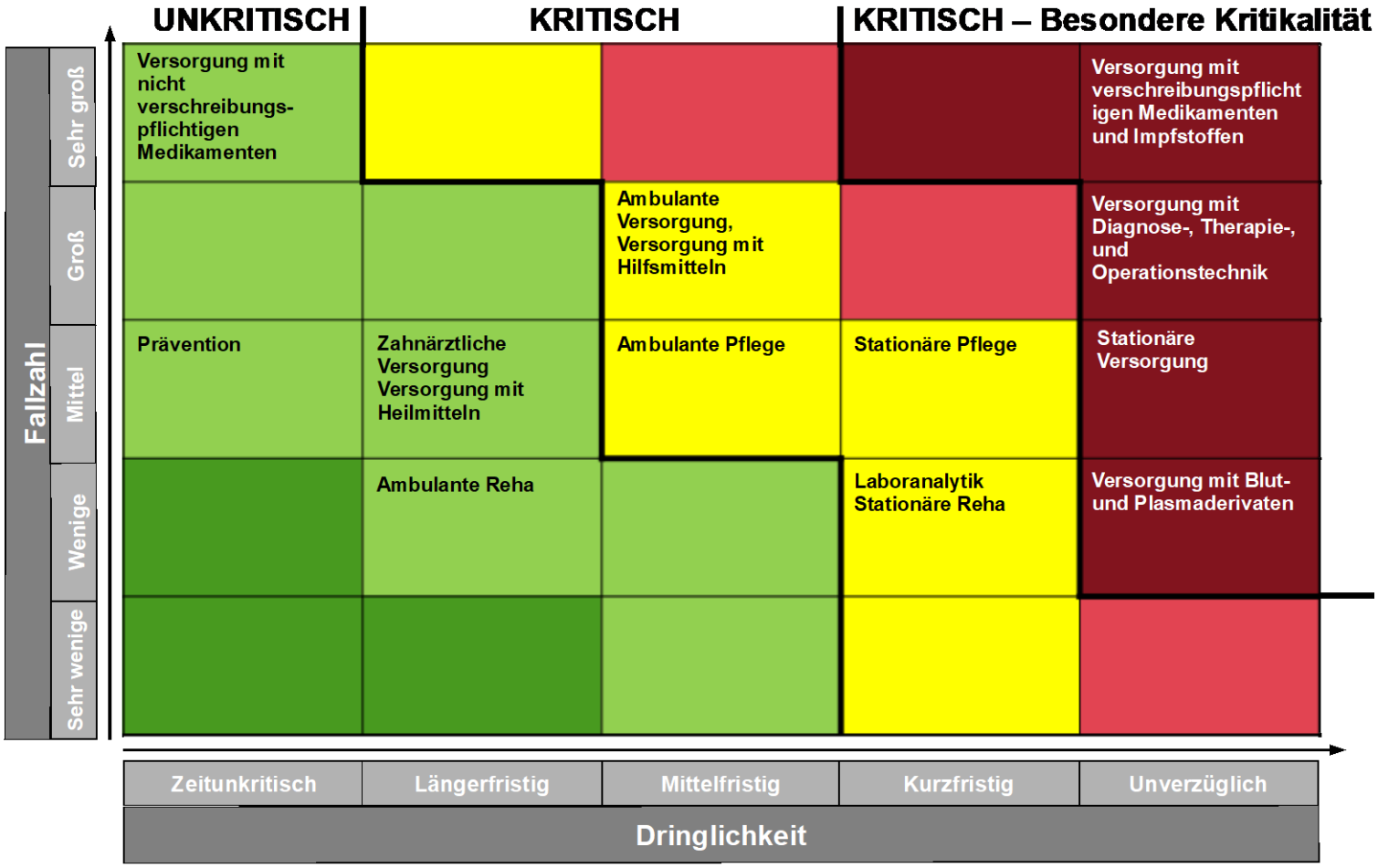
- **Digitale Anbindung** und digitale **Vernetzung** der Infrastrukturen **steigt stetig**
- **Abhängigkeit von** der Verfügbarkeit und **Sicherheit der IT-Systeme nimmt** kontinuierlich **zu**
- **Cybersicherheit** ist einer der sehr gut verfügbaren und damit **bedeutenden Angriffsvektoren**

Erster Schritt: Identifikation kritischer Versorgungs-dienstleistungen entlang der med. Wertschöpfungskette





Medizinische Bereiche mit hohen Fallzahlen und hoher Dringlichkeit werden als besonders kritisch eingestuft



1 Kritische Infrastrukturen und deren Bedeutung für das Gesundheitswesen

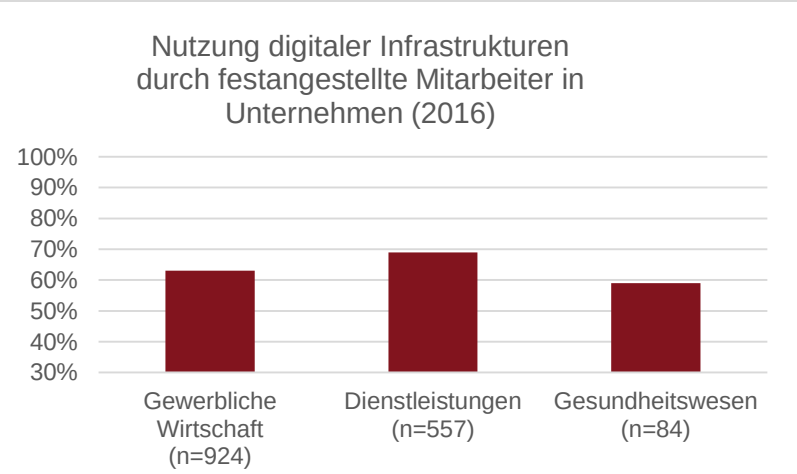
2 Informationstechnologien im Gesundheitssektor und deren zunehmende Anwendung

3 Potentielle Zielkonflikte im Spannungsfeld von IT-Schutzmaßnahmen und ethischen Fragestellungen

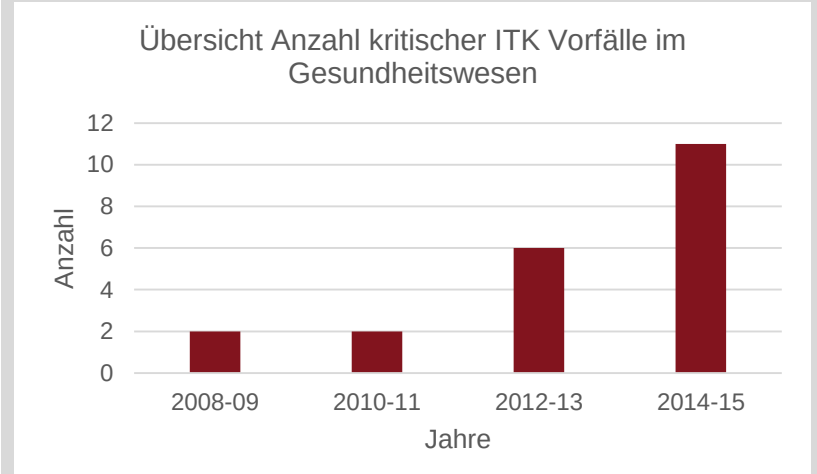
Der zunehmende Einsatz von Informationstechnologien ist ein wesentlicher kritische Faktor für das Gesundheitswesen

Die **Einrichtungen** des **Gesundheitswesens** sind im **ITK-Umfeld nur** in **begrenztem Maße auf Krisensituationen eingestellt**, obwohl sie gerade in diesen Situationen gefordert sein könnten.

Die zunehmende Nutzung von ITK Technologie erhöht auch das Risiko für Angriff aus diesem Bereich.



Quelle: Monitoring Report Wirtschaft Digital – Zentrum für europäische Wirtschafsforschung



Quelle: KRITIS-Sektorstudie Gesundheit 2016

Fallbeispiel: **Internet-Attacke gegen das elektronisches Gesundheitssystem in Lettland – Januar 2018**
Die Webseite des elektronischen Gesundheitssystem in Lettland wurde durch eine DDoS-Attacke aus mehr als 20 Ländern lahmgelegt (Ausstellung elektronischer Rezepte). Nach Angaben des Ministerium gab es dabei keinen Zugriff auf Patientendaten.

Der Einsatz von IKT ist in den einzelnen Branchen des Gesundheitssektors sehr unterschiedlich ausgeprägt

	STATIONÄRE VERSORGUNG	AMBULANTE VERSORGUNG
	 **Detaillierte Betrachtung** der **Versorgungprozesse** und der eingesetzten **ITK Anwendungen**	
DURCHDRINGUNG	• **hohes Maß** an ITK Abhängigkeit • IT-Durchdringung in einzelnen Krankenhäusern sehr unterschiedlich • Adaption digitaler Anwendungen wie der digitalen Patientenakte ist ausbaufähig	• **geringer Grad** der ITK Durchdringung • Wesentliche digitale Einsatzbereiche beschränken sich häufig auf lokale Anwendungen
PROZESSE	• **Krankenhausinterne Prozesse** (Diagnose- und Therapie) **umfangreich digital abgebildet** • **Adaption digitaler Anwendungen** wie der elektronischen Patientenakte oder Einführung eines Entlassmanagement **ist ausbaufähig**	• Diagnose- und Therapieprozesse mit **geringer digitaler Unterstützung**
ENTWICKLUNG	• Steigender Kostendruck und demographischer Wandel werden **Einsatz digitaler Techniken weiter steigern**	• Weiterentwicklung der Telematikinfrastruktur wird die **ITK Abhängigkeit und deren Einsatz weiter steigern**
ROBUSTHEIT	• flächendeckende Verteilung von Einrichtungen trägt zur **Robustheit der Versorgung** bei • Für **Spezialbereiche** wie Isolationsstationen **kann** eine **erhöhte Kritikalität festgestellt werden**	• Fragmentierte Versorgungsdienstleisterlandschaft erhöht die **Robustheit des Systems** • Ausfall einzelner Praxen hat keinen Einfluss im Sinne einer kritischen Infrastruktur

Die Etablierung spezifischer IT-Sicherheitsmaßnahmen ist auch bei aktuell geringen Angriffszahlen notwendig

Schutzmaßnahmen können einer Vielzahl von **Angriffsszenarien entgegenwirken** oder das **Ausmaß** möglicher Schadenfälle **reduzieren**. Darüber hinaus kann sowohl die **Regulierung** als auch die Einführung eines **Krisenmanagements** die **IT-Sicherheit unterstützen**.

ANWENDUNGSBEREICHE

Medizintechnik

- **Diagnostik** (Bildgebung, Messsysteme, stoffliche Analysesysteme)
- **Überwachung** (stationäre Intensivmedizin, mobile ambulante IoT-Systeme)
- **Robotik** (Chirurgie)
- **Implantate** (Herzschrittmacher)

Software

- **Krankenhausinformationssysteme**
- **Arztinformationssysteme**
- **Gesundheits-/Patientenakten**
- **Spezialanwendungen** (PACS)

Infrastruktur

- **Telematikinfrastruktur**
- **lokale Vernetzung** (Krankenhaus und Arztpraxis)

MASSNAHMEN (KRITIS)

IT-Sicherheitsgesetz
Umgang mit und Maßnahmen für die Sicherheit kritischer Infrastrukturen

Etablierung eines IT-Sicherheitsmanagements
z. B. auf Basis von ISO/IEC 27001:2013

WEITERE MASSNAHMEN

IT-Sicherheit im Rahmen der Zulassung von Medizinprodukten (Erweiterung Medizinproduktegesetz)

Einführung konkreter Verordnungen für den operativen Gesundheitssektor (auf Basis des IT-Sicherheitsgesetzes)

Einführung konkreter Verordnungen für den forschenden und entwickelnden Gesundheitssektor (Arzneimittel und Impfstoffe, neue medizintechnische Technologien wie IoT)

Das IT-Sicherheitsgesetz regelt den Umgang mit und Maßnahmen für die Sicherheit kritischer Infrastrukturen

Wesentliche Verpflichtungen im IT-Sicherheitsgesetzes für Betreiber kritischer Infrastrukturen

Betreiber Kritischer Infrastrukturen sind **verpflichtet**, …, **angemessene** organisatorische und technische **Vorkehrungen zur Vermeidung von Störungen** der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse **zu treffen**, …

Betreiber Kritischer Infrastrukturen **können branchenspezifische Sicherheitsstandards** zur Gewährleistung der Anforderungen **vorschlagen**.

Die **Betreiber** Kritischer Infrastrukturen **haben mindestens alle zwei Jahre** die **Erfüllung der Anforderungen** … auf geeignete Weise **nachzuweisen**.

Die **Betreiber** Kritischer Infrastrukturen **haben** dem **BSI** … eine **Kontaktstelle** für Kommunikationsstrukturen … **zu benennen**.

Die **Betreiber** Kritischer Infrastrukturen **haben Störungen … unverzüglich** an das Bundesamt **zu melden**.

Soweit im Rahmen dieser Vorschrift **personenbezogene Daten** erhoben, verarbeitet oder genutzt werden, **ist eine** über die vorstehenden Absätze **hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig**.
Im Übrigen sind die **Regelungen des Bundesdatenschutzgesetzes anzuwenden**.

BSI-KritisV regelt, wer Betreiber von Kritischen Infrastrukturen sind

Verantwortlich für Inhalte, Vorgaben und Regelungen

- **Zentrale Meldestelle** für Betreiber Kritischer Infrastrukturen
- **Wesentliche Informationen zur Abwehr von Gefahren** für die IT-Sicherheit zu **sammeln und auszuwerten**
- Auswirkungen auf **Verfügbarkeit kritischer Infrastrukturen zu analysieren**
- **Lagebild kontinuierlich** zu **aktualisieren**
- **Unverzüglich** mit aktuellen Information **betroffene Einrichtungen zu unterrichten**

Gesetzliche Verankerung zur Auswahl der kritischen Versorgungsdienstleister durch **Erste Verordnung zur Änderung der BSI-Kritis Verordnung**

- **Krankenhäuser mit jährlich mindestens 30.000 vollstationären Fällen** (etwa 110 Kliniken bundesweit),
- **Hersteller lebenswichtiger Medizinprodukte** etwa zur Beatmung, für die parenterale Ernährung, enterale Ernährung, ableitende Inkontinenz und Diabetes Typ 1 ab einem Jahresumsatz von 90,68 Millionen Euro,
- **Arzneimittelhersteller** ab einer **Jahresproduktion von 4,65 Millionen Packungen**,
- **Apotheken ab** einer Abgabe von **4,65 Millionen Packungen im Jahr**
- und medizinische **Laboratorien** ab **1,5 Millionen Aufträgen pro Jahr**

1 Kritische Infrastrukturen und deren Bedeutung für das Gesundheitswesen

2 Informationstechnologien im Gesundheitssektor und deren zunehmende Anwendung

3 Potentielle Zielkonflikte im Spannungsfeld von IT-Schutzmaßnahmen und ethischen Fragestellungen

Mit der steigenden Digitalisierung im Gesundheitswesen kommt der IT-Sicherheit eine zunehmend wichtige Rolle zu

POTENTIELLE DIGITALISIERUNGSBEREICHE	IST-SITUATION	ZUKÜNFTIGE SITUATION	GEFAHRENPOTENTIAL
	Überwiegend **papierorientierter Informationsaustausch**, insbesondere bei einrichtungsübergreifendem Austausch.	**Digitaler Austausch von medizinischen Informationen**, z. B. Telematik Infrastruktur	**Erhöhung der Gefahr des unerlaubten Zugriffs und erweiterten Umfangs auf Patientendaten**
	Die **Verfügbarkeit von patientenbezogenen medizinischen Informationen** ist **gering** und meist auf eine Einrichtung begrenzt.	**Zentrale Speicherung von medizinischen Informationen,** z. B. elektronische Patientenakte	
	Die **Diagnose und Behandlung** des Patienten erfolgt häufig **analog** und ausschließlich **durch den Mensch**.	**Digitale Unterstützung der medizinische Prozesse**, z. B. Expertensysteme, Robotik	**Erhöhung der Gefahr einer Manipulation des Versorgung- und Behandlungsprozesses**
	Bei der medizinischen **Behandlung und Therapie** sind **Patienten auf Ärzte** und **medizinisches Personal angewiesen**.	**Digitale Lösungen zur Steigerung der Eigenständigkeit des Patienten**, z. B. medizinische IoT-Anwendungen	

Angriffsvektoren zu erkennen und geeignete Präventionsmaßnahmen zu ergreifen, ist eine wesentliche Aufgabe für medizinische Einrichtungen, die als kritische Infrastruktur eingestuft sind.

Für potentielle Angriffsvektoren gilt es, geeignete präventive IT-Sicherheitsmaßnahmen zu bestimmen

IT-Sicherheitsmaßnahmen im Gesundheitswesen stehen im Konfliktfeld einerseits effektiv vor Angriffen zu schützen, anderseits gesetzliche und ethische Werte der Patienten zu gewährleisten.

POTENTIELLE ANGRIFFSVEKTOREN

- **Spear-Phishing**
  betrügerische E-Mails
- **Distributed Denial-of-Service (DDoS) Angriffe**
  verteilte Überlastangriffe
- **Ausnutzen von Softwareschwachstellen**
- **Schadsoftware/-programm**
  z.B. Viren, Trojaner etc., die Daten zerstören oder stehlen
- **Ransomeware**
  Erpressungssoftware
- **Missbrauch von Vorrechten**
  z.B. unrechtmäßiges Einholen von Admin-Rechten
- **Datenmanipulierung**
  Veränderung von Daten

MÖGLICHE SCHUTZMASSNAHMEN

Daten- und Informationssicherheit

- Datenverschlüsselung
- Dezentralisierte IT-Infrastruktur
- Backup

Netzwerksicherheit

- Firewall
- Deep Packet Insepection
- Physische/logische Entkopplung vom Internet
- Netzwerkszugangskontrolle
- Port-Management
- Verschlüsselte Übertragung

Gerätesicherheit

- Mobile Device Management
- Personal Firewall
- Antivirus und Malware

Identitäts- und Zugriffverwaltung

- User-Identifizierung (z. B. 2-Faktor, Qualifizierte elektronische Signatur)
- Berechtigungskonzept

GESETZLICHER RAHMEN

- a **Sozialgesetzbuch**
- b **Bundesdatenschutzgesetz**
- c **EuDSGV**
- d **Gesetz zur Verbesserung der Patientenrechte**

ETHISCHE WERTE

1. **Selbstbestimmung**
2. **Schadensvermeidung**
3. **Patientenwohl**
4. **Gerechtigkeit**

Übergreifend betrachtet, unterstützen viele IT-Sicherheits-maßnahmen sowohl rechtliche als auch ethische Werte

Zielkonflikte ergeben sich insbesondere dann, wenn ethische Werte des Individuum dem Gemeinwohl und der gesellschaftlichen Entwicklung entgegen stehen.

	Abwehr von Angriffen auf medizinischen IT-Systeme	**Verfügbarkeit medizinischer Daten im Notfall**
PROBLEM / ZIELSETZUNG	Überwachung und Analyse des Netzwerk-Datenverkehrs mit dem Ziel schädigende Aktivitäten und Daten frühzeitig zu erkennen und präventive Maßnahmen einzuleiten.	Insbesondere in Notfallsituationen ist die Verfügbarkeit von medizinischen Daten entscheidend. Begrenzende Zugriffsrechte verhindern aber einen uneingeschränkten Zugriff durch Ärzte.
MASSNAHME	**Angewendete IT-Sicherheitsmaßnahme** Deep Packet Insepection	**Angewendete IT-Sicherheitsmaßnahme** Identitäts- und Zugriffverwaltung
ZIELKONFLIKT	**Bundesdatenschutzgesetz** **EuDSGV** **Gerechtigkeit**	**Gesetz zur Verbesserung der Patientenrechte** **Selbstbestimmung** **Patientenwohl**

Es ist zu erkennen, dass insbesondere der Datenschutz Zielkonflikte verursacht und damit die ethischen Werte Selbstbestimmung und Gerechtigkeit beeinflusst. Maßnahmen die dem entgegenstehen, wirken aber konträr zu gesellschaftlichen Werten oder dem individuellen Patientenwohl.

Zur Lösung von Zielkonflikten werden neue Ansätze im Umgang mit medizinischen Daten benötigt

Die Herausforderung, zukünftig sowohl das Gemeinwohl als auch das individuelle Patientenwohl sicherzustellen, bedarf neuer technologischer Ansätze.

EXEMPLARISCHE THEMEN UND ANSÄTZE

Umgang mit Patientendaten

Notwendigkeit zur Entwicklung neuer Technologien, die einerseits die Selbstbestimmung und die Anforderungen an den Datenschutz des Patienten gewährleisten, anderseits diese für die medizinische Forschung, Entwicklung und Validierung von Therapien zur Verfügung stellen. Gleichzeitig könnten diese Verfahren auch dem Einschleusen von Schadcode vorbeugen und damit den sicheren Betrieb kritischer Infrastrukturen gewährleisten.

Technologische Ansätze

- Anonymisierung der Daten
- Konsolidieren von Daten
- Datenfreigabe durch Patienten
- Trennung medizinischer und persönlicher Daten

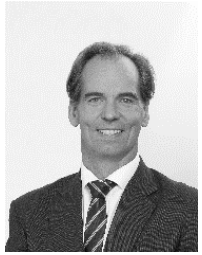
Umgang mit Zugriffsverfahren

Als elementarer Bestandteil zur Verhinderung eines unbefugten Zugriffes auf Patientendaten sind Zugriffsverfahren zu entwickeln, die sowohl einfach als auch übergreifend und sicher sind. Im Zuge einer heterogenen Anbieterlandschaft für digitale Gesundheitsanwendungen ist ein einheitliches und verständliches Zugriffsverfahren zu entwickeln. Darüber hinaus ist zu analysieren, welche Technologien den Zugriff auf wichtige medizinische Daten in Notfallsituationen im Sinne des Patientenwohls garantieren können.

Technologische Ansätze

- Neue Formen der Identitätsfeststellung
- Datenfreigabe im Falle einer Bewusstlosigkeit
- Einfache und verständliche Zugriffsverwaltung durch den Patienten

Vielen Dank für Ihre Aufmerksamkeit.



strategy&

Prof. Dr. Rainer Bernnat
Partner PwC Strategy&
Frankfurt

Rainer.Bernnat@strategyand.de.pwc.com