Neues zum IT-Sicherheitsgesetz 2.0

Was können wir erwarten, was ist bisher bekannt?

23. September 2019 - Wiesbaden

Markus Holzbrecher-Morys
Stellv. Geschäftsführer (IT, Datenaustausch, eHealth)

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Agenda

DEUTSCHE KRANKENHAUS GESELLSCHAFT

- Aktueller Stand zur Umsetzung des ITSiG 1.0
  - 4 Jahre IT-Sicherheitsgesetz – eine Bestandsaufnahme
  - Prüfung nach § 8a BSIG zum 30.6.2019
- Referentenentwurf – Inhalte, Kritik, Ausblick
  - Leak von netzpolitik.org - die Hersteller im Blick
  - wesentliche Änderungen
  - Kritik im Entwurf („Internetsicherheitsgesetz“)
  - weiterer Zeitverlauf
- Novellierung der BSI-Kritis-Verordnung
  - Anlagenkategorien, Bemessungskriteren, Schwellenwerte
  - erwarteter Zeitverlauf

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Weltweit ungesicherte Bildarchivsysteme (PACS) im Netz – auch Deutsche Patienten betroffen

Deutschland & Welt

Millionenfach Patientendaten ungeschützt im Netz

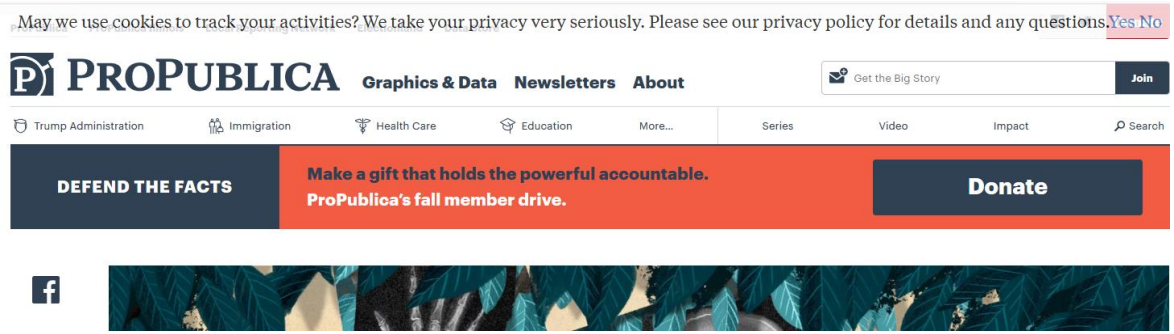
Hochsensible medizinische Daten, unter anderem von Patienten aus Deutschland und den USA, sind nach Recherchen des BR und der US-Investigativplattform ProPublica auf ungesicherten Internetservern gelandet. Jeder hätte darauf zugreifen können. [mehr]

www.br-online.de, Abruf am 17.9.2019

© Deutsche Krankenhausgesellschaft e. V.

Kurzer Einschub zum aktuellen Thema

medizinische Daten im Internet



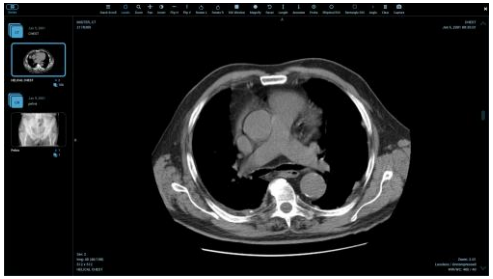
Millions of Americans' Medical Images and Data Are Available on the Internet. Anyone Can Take a Peek.

Hundreds of computer servers worldwide that store patient X-rays and MRIs are so insecure

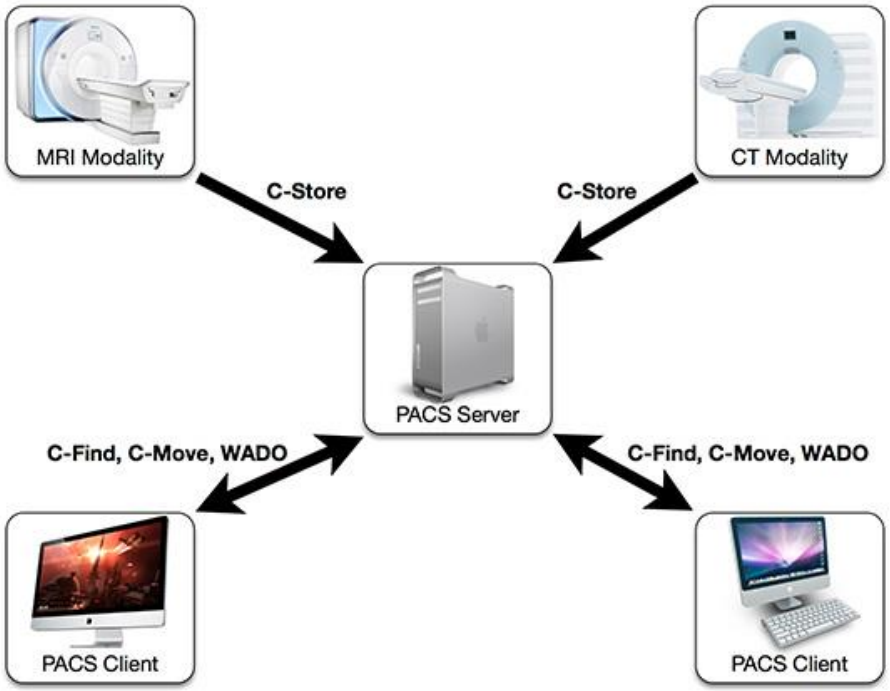
Gibt es einen systemrelevanten Vorfall?

Ein paar (technische) Fakten:

DICOM



PACS-Server



Quelle: www.osirix-viewer.com

Ein paar (technische) Fakten:

vs.

System-Suchmaschine Shodan

Shodan | Developers | Monitor | View All...

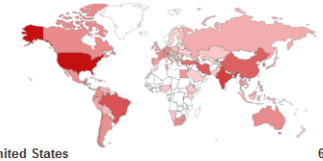
SHODAN | dicom | Explore | Pricing | Enterprise Access | New to Shodan? | Login or Register

Exploits | Maps | Images

TOTAL RESULTS

2,173

TOP COUNTRIES



United States	638
India	264
Brazil	163
Iran, Islamic Republic of	132
China	115

TOP SERVICES

104	1,481
11112	635
33338	7
RDP	7
8081	5

TOP ORGANIZATIONS

Comcast Business	76
Amazon.com	43
Microsoft Azure	42
Turk Telekom	36
Vivo	15

TOP OPERATING SYSTEMS

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

12.70.252.33
Konica Minolta Healthcare Americas
Added on 2019-09-22 07:15:44 GMT
United States, Durham

medical

```
DICOM Server Response
\x02\x00\x00\x00\x00\xb8\x00\x01\x00\x00ANY-SCP         FINDSCU         \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10\x00\x00\x00\x151.2.840.10008.3.1.1.1!\x00\x00\x19\x01\x00\x03\x00@\x00\x00...
```

196.15.240.83
Telkom Internet
Added on 2019-09-22 07:33:32 GMT
South Africa, Boksburg

medical

```
DICOM Server Response
\x02\x00\x00\x00\x00\xb3\x00\x01\x00\x00ANY-SCP         FINDSCU         \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10\x00\x00\x00\x151.2.840.10008.3.1.1.1!\x00\x00\x19\x01\x00\x03\x00@\x00\x00...
```

50.224.29.222
50-224-29-222-static.hfc.comcastbusiness.net
Comcast Business
Added on 2019-09-22 07:20:51 GMT
United States, Denver

medical

```
DICOM Server Response
```

2 Varianten

+ „normal“ konfiguriert = Systemproblem

+ falsch konfiguriert = Daten-GAU

2 Varianten

Systemproblem

- PACS-Server sind grundsätzlich über das Internet ansprechbar
- Ein direkter Zurgiff auf Daten ist aber nicht möglich
- Systeme sind aber bezüglich potentieller Sicherheitslücken hackbar
- In Deutschland 35-70 Systeme betroffen
    - Unklar ob Echtdaten, Testdaten, Daten von Menschen

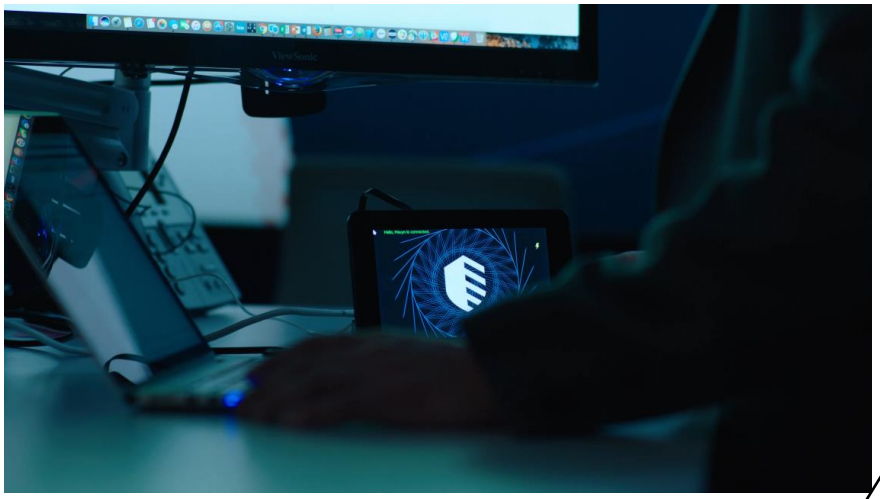
Daten-GAU

- PACS-Server sind grundsätzlich über das Internet ansprechbar
- Ein direkter Zurgiff auf Daten ist aufgrund einer falschen Konfiguration mittels netzbasierter DICOM-Befehle (z.B. C-FIND, C-MOVE) möglich
- In Deutschland waren nach veröffentlichen Daten 2 Systeme betroffen
    - Raum Ingolstadt 7200 Patienten
    - Raum Kempen wohl ca. 4000 Patienten (Zahl hier ohne Gewähr)

IT-Sicherheit im Gesundheitswesen

DEUTSCHE KRANKENHAUS GESELLSCHAFT

„IT-Sicherheit? Wir haben ganz andere Probleme!“



- Krankenhäuser immer wieder durch Cyberangriffe beeinträchtigt
- Grad der Digitalisierung in der medizinischen Versorgung steigt
- Patientensicherheit bedeutet auch IT-Sicherheit
- IT-Sicherheit erfordert qualifiziertes Personal

- Koalitionsvertrag bleibt in Bezug auf Digitalisierung weit hinter den Erwartungen zurück
- Ausgliederung der Pflege bedeutet „Meteoriteneinschlag“ im DRG-System
- Investitionsfinanzierung dürfte noch prekärer ausfallen
- Personalbedarf kann an vielen Stellen nicht adäquat gedeckt werden

© Deutsche Krankenhausgesellschaft e. V.

Aktuelle Gesetzgebungsverfahren

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Aktuelle G

Ps

Geset

Digitale

MDK-R

Reha-
Stärku

Gese
zur/z

Ge

Deutscher Bundestag — Drucksache 19/12809

19. Wahlperiode — 29.08.2019

Kleine Anfrage

der Abgeordneten Harald Weinberg, Susanne Ferschl, Matthias W. Birkwald, Sylvia Gabelmann, Dr. Achim Kessler, Katja Kipping, Jutta Krellmann, Pascal Meiser, Cornelia Möhring, Sören Pellmann, Jessica Tatti, Pia Zimmermann, Sabine Zimmermann und der Fraktion DIE LINKE.

Arbeitsbelastung im Bundesgesundheitsministerium

Als „Minister Fleißig“ wurde Bundesgesundheitsminister Jens Spahn betitelt. 16 Gesetze in 16 Monaten habe er vorgelegt und sei „Alleinunterhalter“ bei der letzten Kabinettsitzungvor der Sommerpause gewesen (www.aerzteblatt.de/nachrichten/104703/Minister-Fleissig-16-Gesetze-in-16-Monaten). Aus keinem anderen Ressort sind seit der letzten Bundestagswahl mehr Initiativen gekommen als aus dem Bundesministerium für Gesundheit (BMG) (ebenda). Der Ärztetag 2019 verlegte sich darauf, den „Turbo-Spahn“ zu entschleunigen (www.aerztezeitung.de/kongresse/aerztetag/article/989198/eroeffnung-aerztetag-will-turbo-spahn-entschleunigen.html9).

gesetz

eken

esetz

esetz

U

on

Bildnachweis: pictu

© Deutsche Krankenhausgesellschaft e. V.

Aktueller Stand zur Umsetzung ITSiG 1.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

2005

Nationaler Plan
zum Schutz der Informationsinfrastrukturen

© Deutsche Krankenhausgesellschaft e. V.

Aktueller Stand zur Umsetzung ITSiG 1.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

2005

Nationaler Plan
zum Schutz der Informationsinfrastrukturen

2007

Nationaler Plan
zum Schutz der Informationsinfrastrukturen
Umsetzungsplan KRITIS

Nationaler Plan
zum Schutz der Informationsinfrastrukturen
Umsetzungsplan Bund

© Deutsche Krankenhausgesellschaft e. V.

Aktueller Stand zur Umsetzung ITSiG 1.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

2005

2007

2009

© Deutsche Krankenhausgesellschaft e. V.

Aktueller Stand zur Umsetzung ITSiG 1.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

2005

Nationaler Plan
zum Schutz der Informationsinfrastrukturen

2007

Nationaler Plan
zum Schutz der Informationsinfrastrukturen
Umsetzungsplan KRITIS

Nationaler Plan
zum Schutz der Informationsinfrastrukturen
Umsetzungsplan Bund

2009

2011

© Deutsche Krankenhausgesellschaft e. V.

Aktueller Stand zur Umsetzung ITSiG 1.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

2005

Nationaler Plan
zum Schutz der Informationsinfrastrukturen

2007

Nationaler Plan
zum Schutz der Informationsinfrastrukturen
Umsetzungsplan KRITIS

Nationaler Plan
zum Schutz der Informationsinfrastrukturen
Umsetzungsplan Bund

2009

2011

2014

© Deutsche Krankenhausgesellschaft e. V.

Aktueller Stand zur Umsetzung ITSiG 1.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

2005

Nationaler Plan zum Schutz der Informationsinfrastrukturen

2007

Nationaler Plan zum Schutz der Informationsinfrastrukturen – Umsetzungsplan KRITIS

Nationaler Plan zum Schutz der Informationsinfrastrukturen – Umsetzungsplan Bund

2009

2011

2014

2015

© Deutsche Krankenhausgesellschaft e. V.

Aktueller Stand zur Umsetzung ITSiG 1.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

2009

2007

2011

2014

2015

2016

© Deutsche Krankenhausgesellschaft e. V.

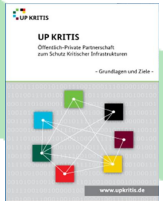
Aktueller Stand zur Umsetzung ITSiG 1.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

2009

2011

2014



2015

2016

2017

© Deutsche Krankenhausgesellschaft e. V.

Aktueller Stand zur Umsetzung ITSiG 1.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

2014

2011

2015

2016

2017

2019

© Deutsche Krankenhausgesellschaft e. V.

Stand der Prüfungen nach § 8a BSIG

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Aus Sicht des BSI

- Flut von Meldungen zum Ende Juni führte zu hoher Belastung des BSI
- noch nicht alle Meldungen eingetroffen, Mahnschreiben des BSI an „säumige Betreiber“
- BSI derzeit noch mit „moderater Aufsichtsfunktion“, d.h. zunächst Unterstützung bei der Erfüllung der Nachweispflicht anstelle von Bußgeldbescheiden
- Geltungsbereich (Scope) häufig sehr eng begrenzt
- Auswertung auf Vollständigkeit noch nicht abgeschlossen, inhaltliche Meldung noch nicht begonnen, Lagebild nicht vor Ende des Jahres möglich

© Deutsche Krankenhausgesellschaft e. V.

Stand der Prüfungen nach § 8a BSIG

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Aus Sicht der Betreiber

- „Prüfende Stellen“ als limitierender Faktor:
  - Verfügbarkeit ↘
  - Kosten ↗
  - Branchenkompetenz (Definition hierfür ist offen)
  - Unabhängigkeit
  - Zuverlässigkeit
- Nutzung interner Audits könnte möglicherweise Prüfaufwand reduzieren
- Grundsatz der Gleichbehandlung
- künftig bessere Abbildung der Branchenkompetenz gefordert („Prüfer-Pool“)

© Deutsche Krankenhausgesellschaft e. V.

Stand der Prüfungen nach § 8a BSIG

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Branchenspezifischer Sicherheitsstandard („B3S“)

- mögliche Grundlage für Prüfungen nach § 8a BSIG
- B3S = Katalog an Maßnahme-Empfehlungen
- Ziel: sichere und resiliente IT-Infrastruktur
- Abstraktionsgrad der Anforderungen variiert
- individuelle Ausgestaltung notwendig, kein „Checklisten-Charakter“
- gestuftes Realisierungskonzept über mehrere Iterationen notwendig
- risikoorientierte Priorisierung bei stufenweiser Umsetzung
- ISMS ist ein wesentlicher Aspekt der Umsetzung, jedoch allein nicht ausreichend

© Deutsche Krankenhausgesellschaft e. V.

Stand der Prüfungen nach § 8a BSIG

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Nutzbarkeit des Branchenspezifischen Sicherheitsstandards („B3S“)

- aus Sicht von Betreibern, Prüfern und prüfenden Stellen als Prüfgrundlage geeignet
- Eignungsfeststellung des BSI steht noch aus (in Kürze erwartet)
- unterschiedliche Kompetenzniveaus der Prüfer durch kurze Vorlaufzeit des B3S (BSI: jede Version seit 0.86 vom 18.12.2018 wurde in den Prüfungen zugelassen)
- Weiterentwicklung auf Basis der Erfahrungen aus den aktuellen Prüfungen geplant
- Scope-Definition führt häufig zu Nachfragen
- Umfang der Prüfung könnte durch weiteres Dokument („Prüfnachweisplaner“) ergänzt werden

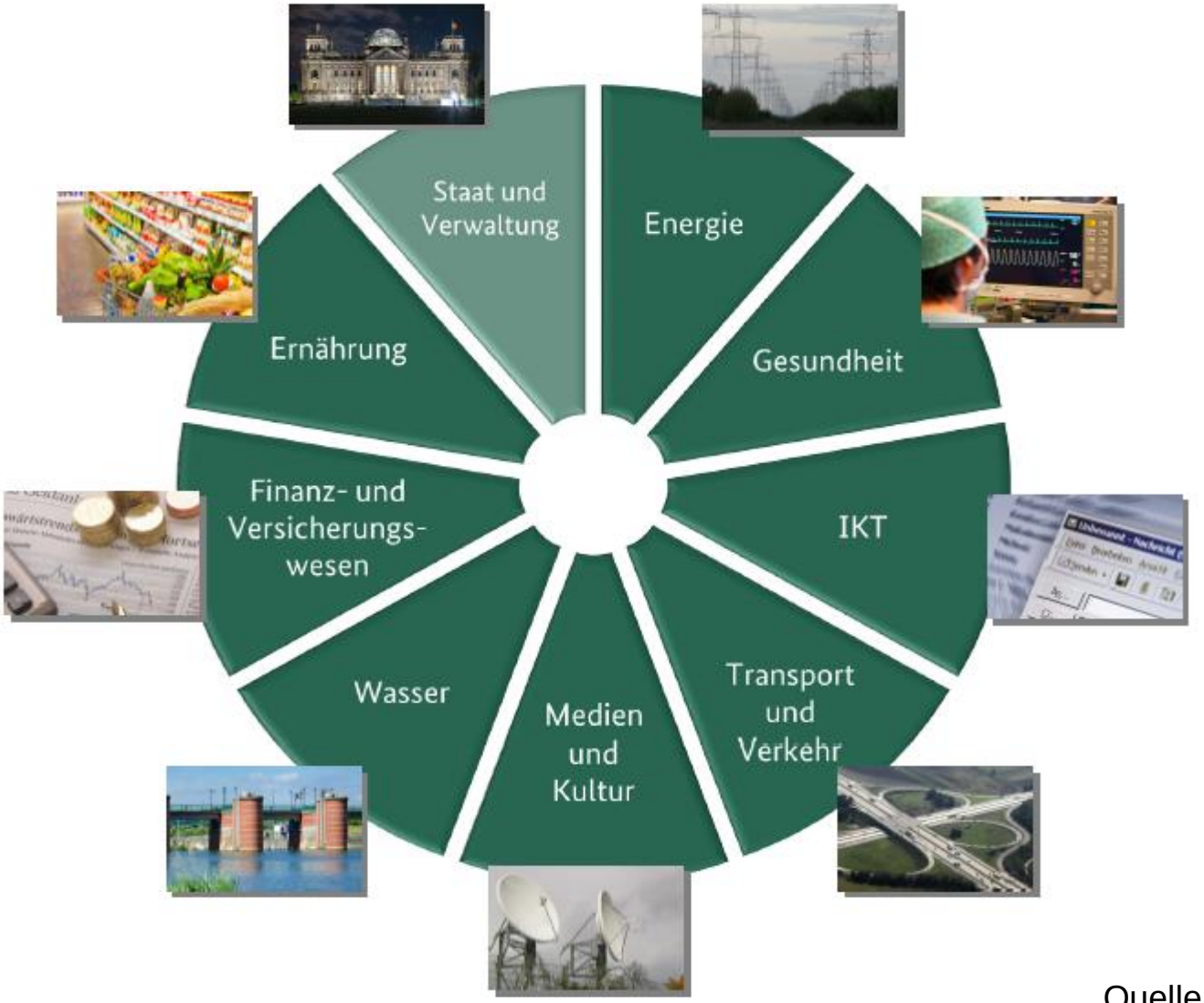
© Deutsche Krankenhausgesellschaft e. V.

Agenda

DEUTSCHE KRANKENHAUS GESELLSCHAFT

- Aktueller Stand zur Umsetzung des ITSiG 1.0
  - 4 Jahre IT-Sicherheitsgesetz – eine Bestandsaufnahme
  - Prüfung nach § 8a BSIG zum 30.6.2019
- Referentenentwurf – Inhalte, Kritik, Ausblick
  - Leak von netzpolitik.org - die Hersteller im Blick
  - wesentliche Änderungen
  - Kritik im Entwurf („Internetsicherheitsgesetz“)
  - weiterer Zeitverlauf
- Novellierung der BSI-Kritis-Verordnung
  - Anlagenkategorien, Bemessungskriteren, Schwellenwerte
  - erwarteter Zeitverlauf

Die Kritischen Infrastrukturen Deutschlands



Quelle: kritis.bund.de

© Deutsche Krankenhausgesellschaft e. V.

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Veröffentlichung eines internen Referentenentwurfs

- Dezember 2018: „Politiker- und Promihack“ –BSI: „Müssen digital Streife fahren“
- Veröffentlichung eines internen Gesetzentwurfs am 3.4.3019 durch Plattform „Netzpolitik.org“
- scharfe Kritik an geplanter Ausweitung der „Überwachung des Internets“
- Änderung der IT-Sicherheitspolitik von defensiv zu offensiv befürchtet:
  - „Angriff als beste Verteidigung“
  - „hack back“ als Option
- Ansätze zum Verbraucherschutz positiv bewertet

© Deutsche Krankenhausgesellschaft e. V.

IT-Sicherheitsgesetz 2.0

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Schwerpunkte des geplanten Gesetzentwurfs

- Einbeziehung weiterer Wirtschaftsbereiche im besonderen öffentlichen Interesse unter den Schutzmantel des IT-Sicherheitsgesetzes
- Einführung eines IT-Sicherheitskennzeichens
- Verbraucherschutz als Aufgabe des BSI
- Erweiterung der operativen Befugnisse des BSI
- Meldepflichten / Sensorik für Kritische Infrastrukturen
- Anforderungen an die Vertrauenswürdigkeit für Zulieferer Kritischer Infrastrukturen
- Meldepflichten / Sensorik für Telekommunikationsanbieter
- Illegale Handelsplattformen – Darknet – Anpassung des StGB / der StPO

© Deutsche Krankenhausgesellschaft e. V.

DEUTSCHE KRANKENHAUS GESELLSCHAFT

neue Wirtschaftsbereiche

- Wirtschaftsbereiche im besonderen öffentlichen Interesse:
  - Rüstungsindustrie
  - Unternehmen von erheblicher volkswirtschaftlicher Bedeutung aufgrund inländischer Wertschöpfung oder Größe
  - Unternehmen, die mit Gefahrstoffen (ABC) und aufgrund dessen bereits einer speziellen Regulierung z.B. nach Gefahrstoffgesetzgebungen unterliegen
- neuer Kritis-Sektor „Entsorgung“

© Deutsche Krankenhausgesellschaft e. V.

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Die Wirtschaft im Blick: Anforderungen an Zulieferer

- „KRITIS-Kernkomponenten“
- Vertrauenswürdigkeitserklärung des Herstellers
- Mindestanforderungen für Vertrauenswürdigkeitserklärung durch BMI
- Meldepflichten für Hersteller von KRITIS-Kernkomponenten
- Kritische Kernkomponente für Krankenhäuser:

  „Krankenhausinformationssysteme“

© Deutsche Krankenhausgesellschaft e. V.

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Weitere Schwerpunkte des BMI für den Gesetzentwurf

- Evaluierung der BSI-KritisV
- Nationaler Pakt für Cybersicherheit
- Krisenkommunikationssystem
- Angleichung der Sanktionen bei Verstößen an die nach DSGVO bekannten Strafrahmen:

  bis zu 20 Mio. EUR bzw. 4 % des gesamten weltweit erzielten Jahresumsatzes

© Deutsche Krankenhausgesellschaft e. V.

Agenda

DEUTSCHE KRANKENHAUS GESELLSCHAFT

- Aktueller Stand zur Umsetzung des ITSiG 1.0
  - 4 Jahre IT-Sicherheitsgesetz – eine Bestandsaufnahme
  - Prüfung nach § 8a BSIG zum 30.6.2019
- Referentenentwurf – Inhalte, Kritik, Ausblick
  - Leak von netzpolitik.org - die Hersteller im Blick
  - wesentliche Änderungen
  - Kritik im Entwurf („Internetsicherheitsgesetz“)
  - weiterer Zeitverlauf
- Novellierung der BSI-Kritis-Verordnung
  - Anlagenkategorien, Bemessungskriteren, Schwellenwerte
  - erwarteter Zeitverlauf

DEUTSCHE KRANKENHAUS GESELLSCHAFT

geplante Anpassungen BSI-KritisVO (Gesundheit)

- neue Anlagenkategorie „Krankenhaus-IT-Verbund“ geplant
- Beibehaltung des Bemessungskriteriums „vollstationäre Fallzahl“ absehbar
- Absenkung des Schwellenwertes geplant (Zielwert offen)

Bereits Absenkung um 2.000 Fälle /Jahr würde eine Zunahme um 50 % der betroffenen Einrichtungen bedeuten

© Deutsche Krankenhausgesellschaft e. V.

Ausblick - Veränderte Bedrohungslage

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Ransomware

Cyberkriminalität

Datendiebstahl

Cyberterrorismus

Offenbarung von Patientendaten

Notfallversorgung bei Großschadenslagen (MANV)

Trojaner

Zero-Day-Exploits

Social Engineering

DoS (Denial of Service)

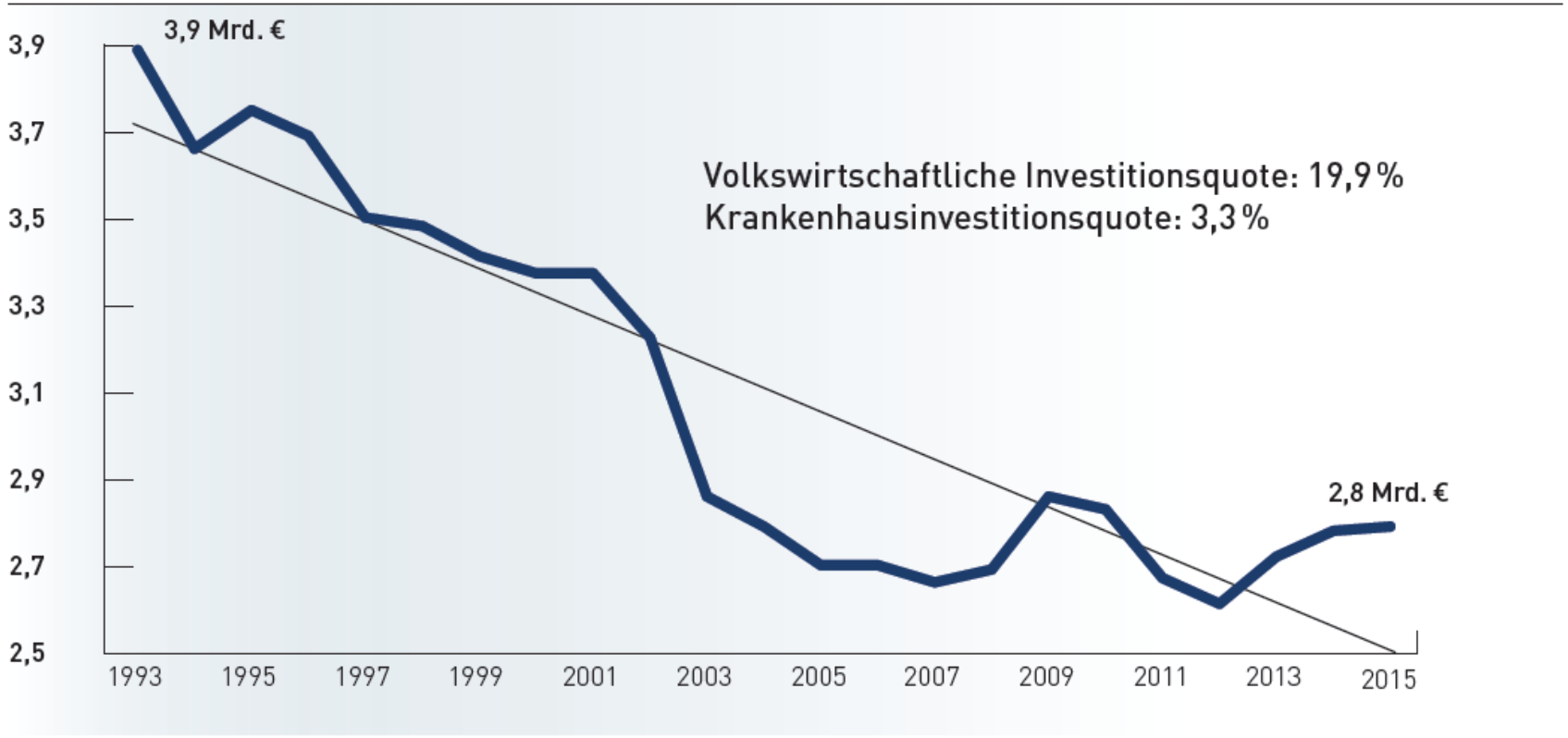
Advanced Persistent Threats

der Nutzer selbst

© Deutsche Krankenhausgesellschaft e. V.

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Entwicklung der Investitionsförderung seit 1993



Quelle: AOLG

Krankenhäuser sind in vielen Regionen der größte Arbeitgeber und ein zuverlässiger Beschäftigungsmotor!

© Deutsche Krankenhausgesellschaft e. V.

Finanzierung entstehender Aufwände

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Erwartete Mehrkosten für Umsetzung von Anforderungen an Informationssicherheit

Investitionskosten

in Verantwortung der Bundesländer

Betriebskosten

ggf. im Rahmen der Budgetplanung zu berücksichtigen

Personalkosten

heterogenes Anforderungsprofil

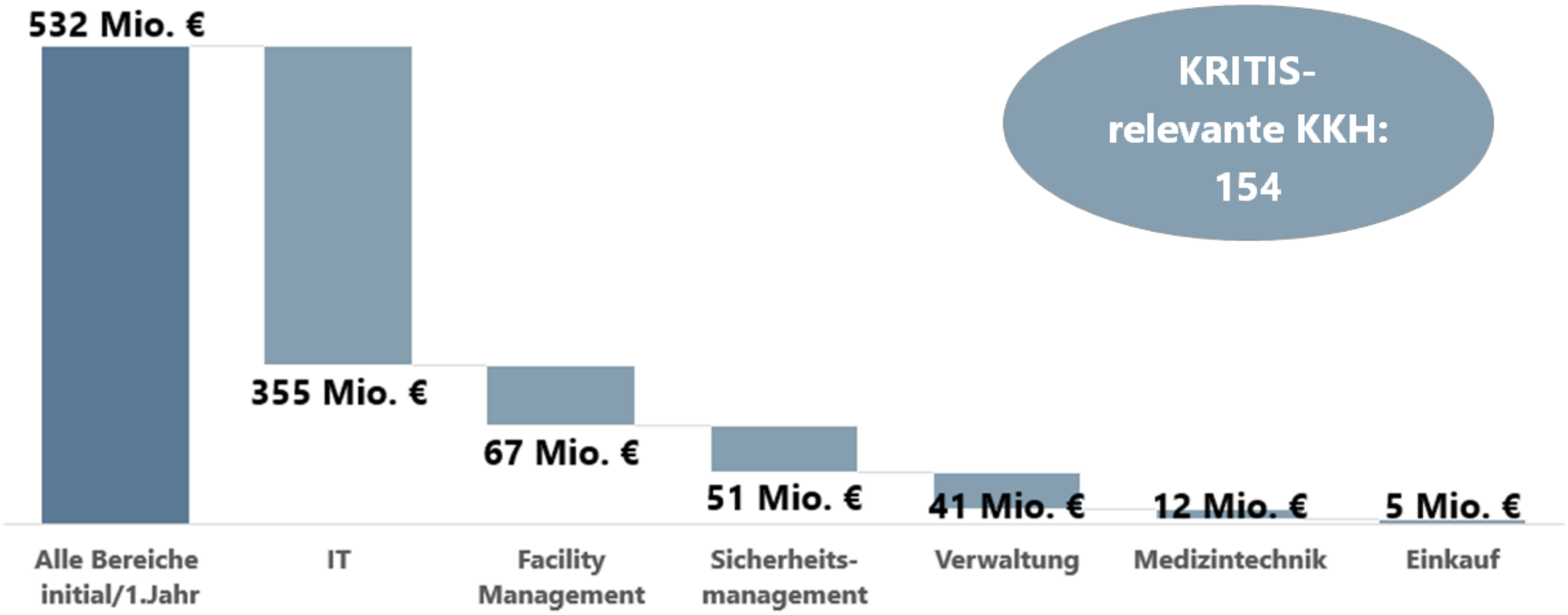
allgemeine Marktsituation schwierig

© Deutsche Krankenhausgesellschaft e. V.

Kostenerhebung DKG (noch nicht veröffentlicht)

DEUTSCHE KRANKENHAUS GESELLSCHAFT

3.2 Initiale Kosten im 1. Jahr für 154 KritisV-relevante Krankenhäuser*, in Mio. EUR

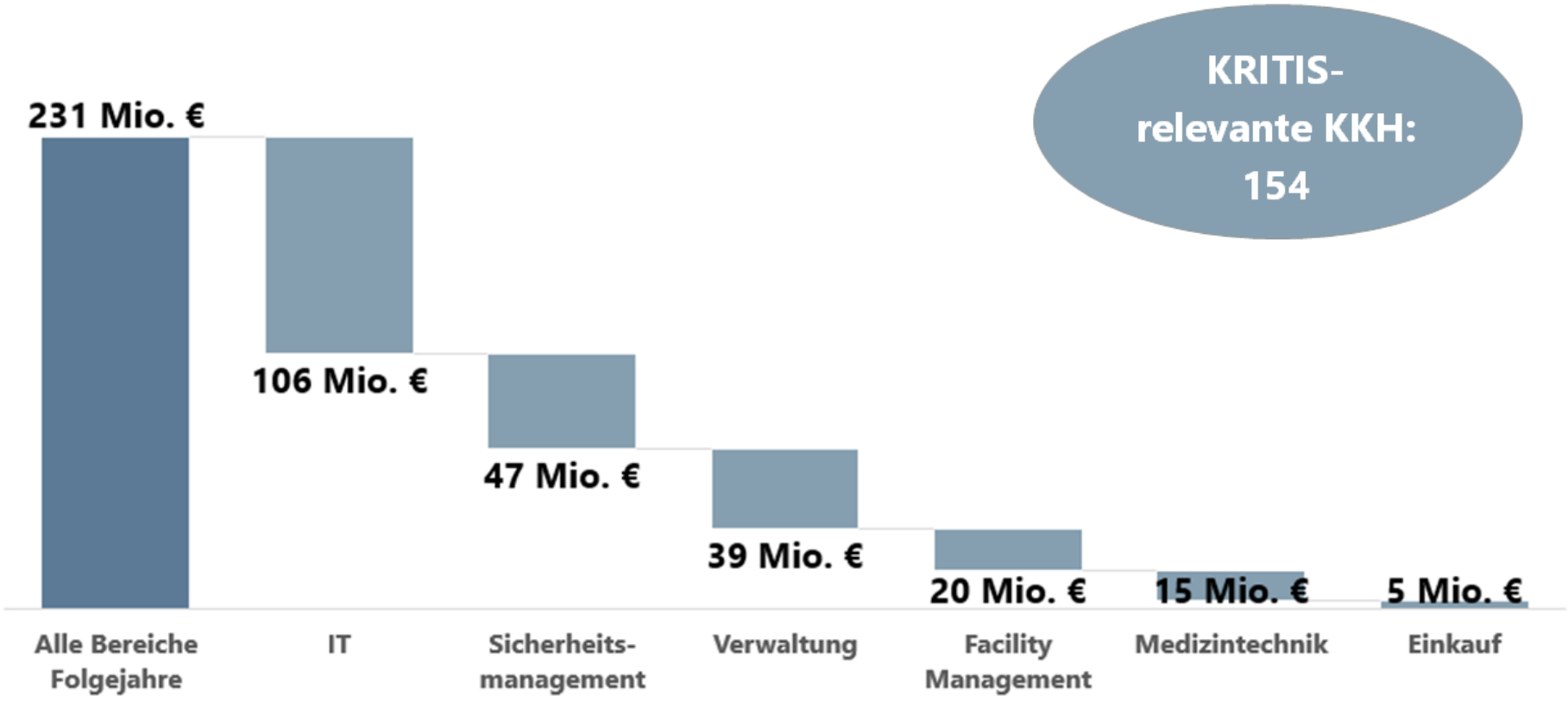


© Deutsche Krankenhausgesellschaft e. V.

Kostenerhebung DKG (noch nicht veröffentlicht)

DEUTSCHE KRANKENHAUS GESELLSCHAFT

3.3 Wiederkehrende Kosten für 154 KritisV-relevante Krankenhäuser*, in Mio. EUR/Jahr

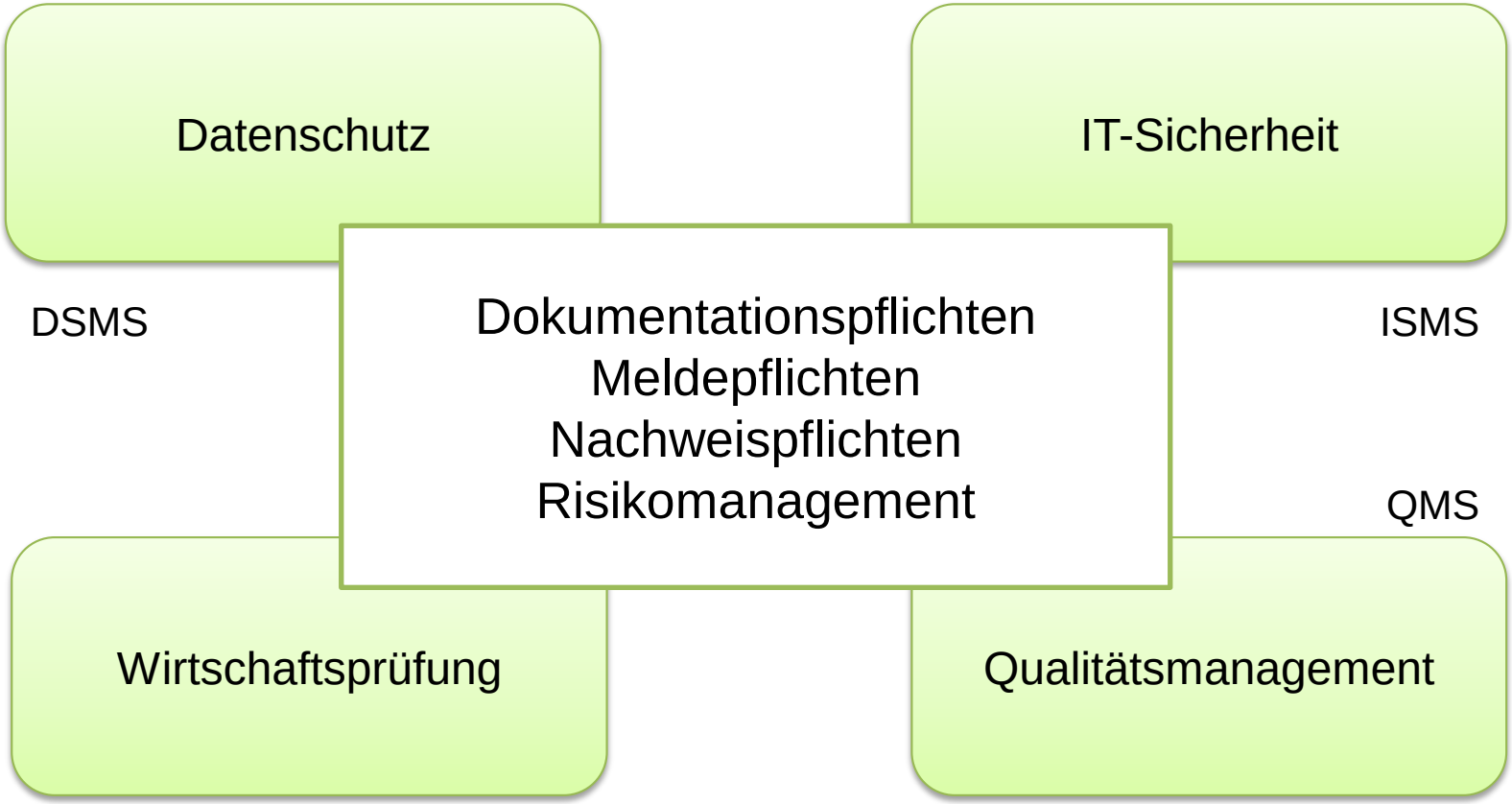


© Deutsche Krankenhausgesellschaft e. V.

Empfehlung an Krankenhäuser: IT-Strategie

DEUTSCHE KRANKENHAUS GESELLSCHAFT

*Krankenhäuser **benötigen eine IT-Strategie**, die übergreifende Compliance-Anforderungen adressiert*



© Deutsche Krankenhausgesellschaft e. V.

Vielen Dank für Ihre Aufmerksamkeit!

DEUTSCHE
KRANKENHAUS
GESELLSCHAFT