KRITIS – Grundlagen, Geltungsbereich und Nutzen für alle Kliniken

Markus Holzbrecher-Morys, DKG e.V.

21. März 2018

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

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Agenda

- **KRITIS - Grundlagen**
  - Kritische Infrastrukturen in Deutschland – UP KRITIS
  - der Branchenarbeitskreis „Medizinische Versorgung“
- **IT-Sicherheitsgesetz**
  - Krankenhaus-IT im Kontext von WannCry & Co.
  - Das IT-Sicherheitsgesetz im Fokus
- **Chancen und Risiken**
  - IT-Sicherheit = Patientensicherheit
  - Branchenspezifischer Sicherheitsstandard „B3S“
  - Anforderungen für Nicht-KRITIS-Betreiber

Ihr Referent

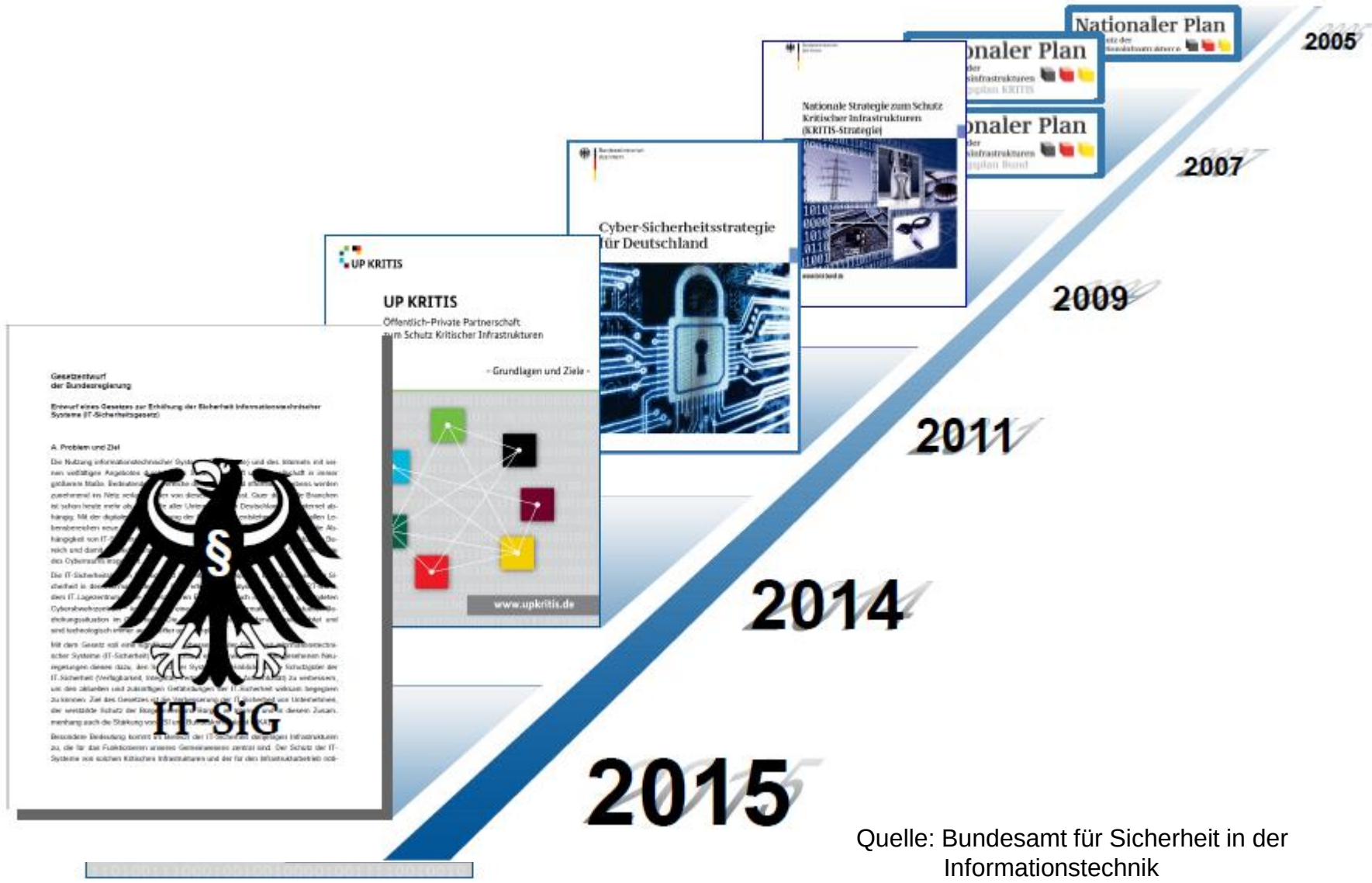
DEUTSCHE KRANKENHAUS GESELLSCHAFT

Dipl. Inform. (FH) Markus Holzbrecher-Morys

Stellvertretender Geschäftsführer („IT, Datenaustausch, eHealth“)

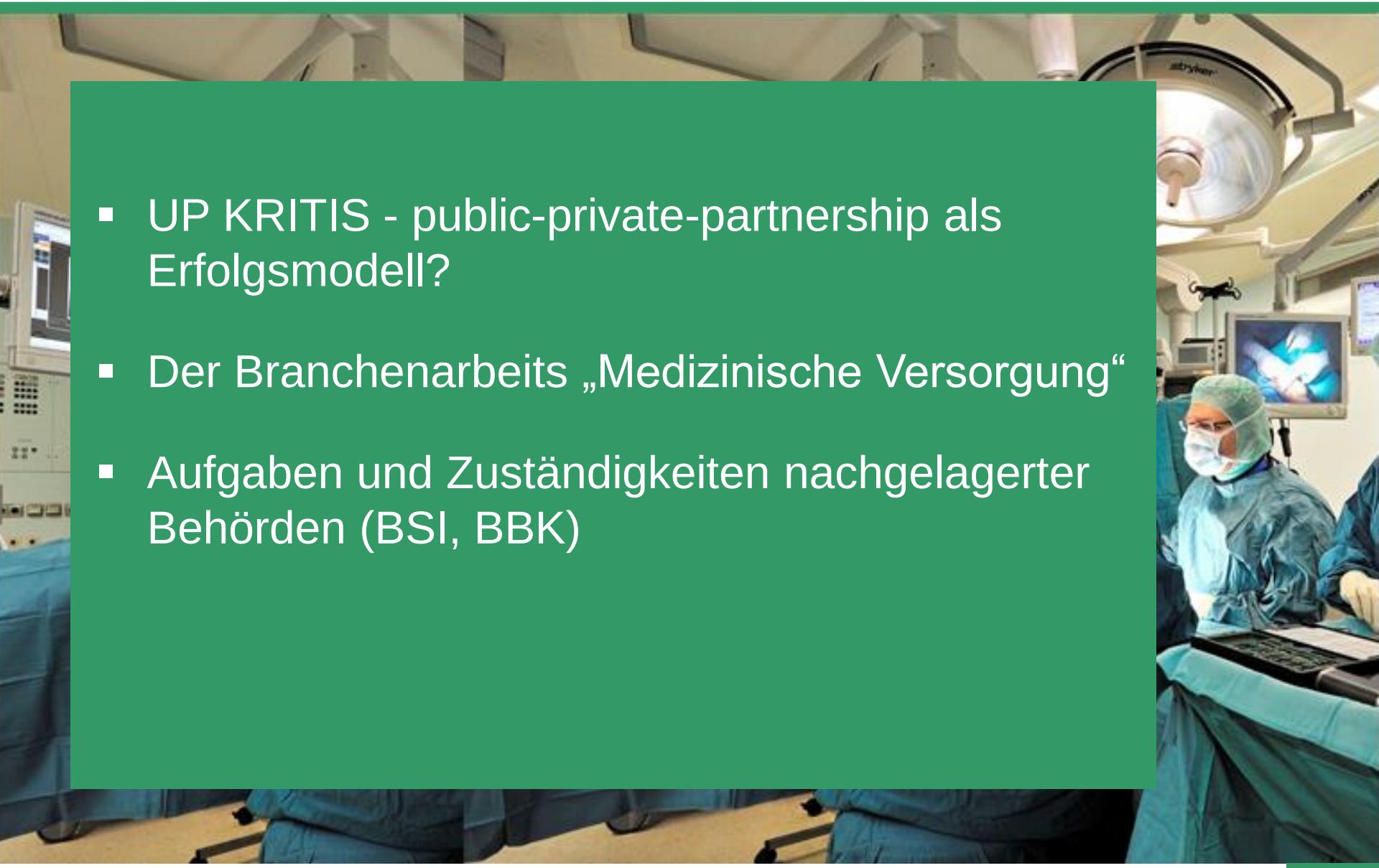
- Elektronische Datenaustauschverfahren
  - § 301 Verfahren im Bereich GKV, PKV, DGUV
  - § 21 Datenübermittlung
- Krankenhausinformationstechnik
  - Technischer Datenschutz im Krankenhaus
  - IT-Risikomanagement
  - Kritische Infrastrukturen (IT-Sicherheitsgesetz)
- Leiter der Arbeitsgruppe „Krankenhaus-Informationstechnik“ der DKG
- Sprecher des Branchenarbeitskreises „Medizinische Versorgung“ im „Umsetzungsplan Kritische Infrastrukturen (UP KRITIS)“

Kritische Infrastrukturen in Deutschland



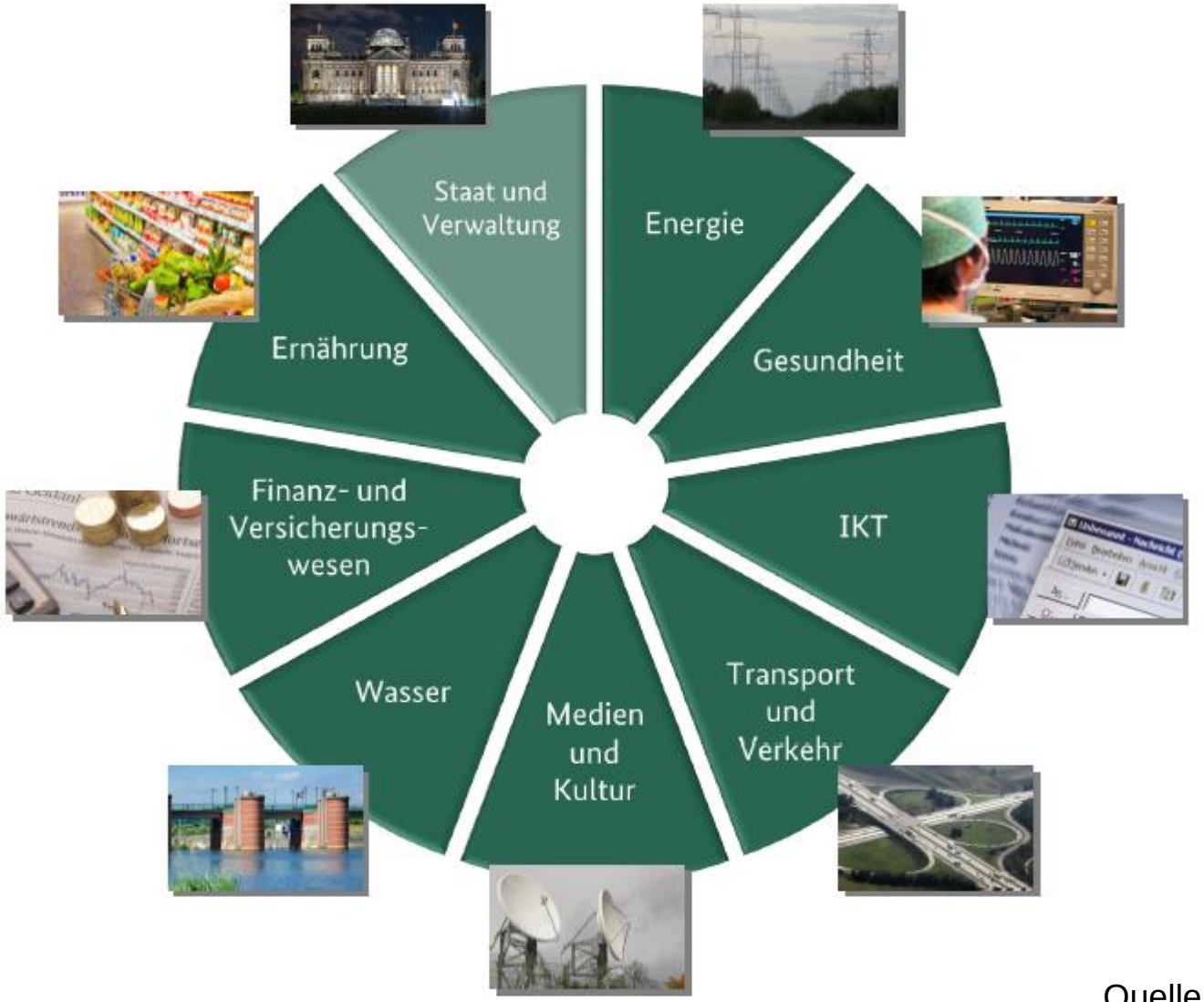
Quelle: Bundesamt für Sicherheit in der Informationstechnik

Kritische Infrastrukturen – der UP KRITIS



- UP KRITIS - public-private-partnership als Erfolgsmodell?
- Der Branchenarbeits „Medizinische Versorgung“
- Aufgaben und Zuständigkeiten nachgelagerter Behörden (BSI, BBK)

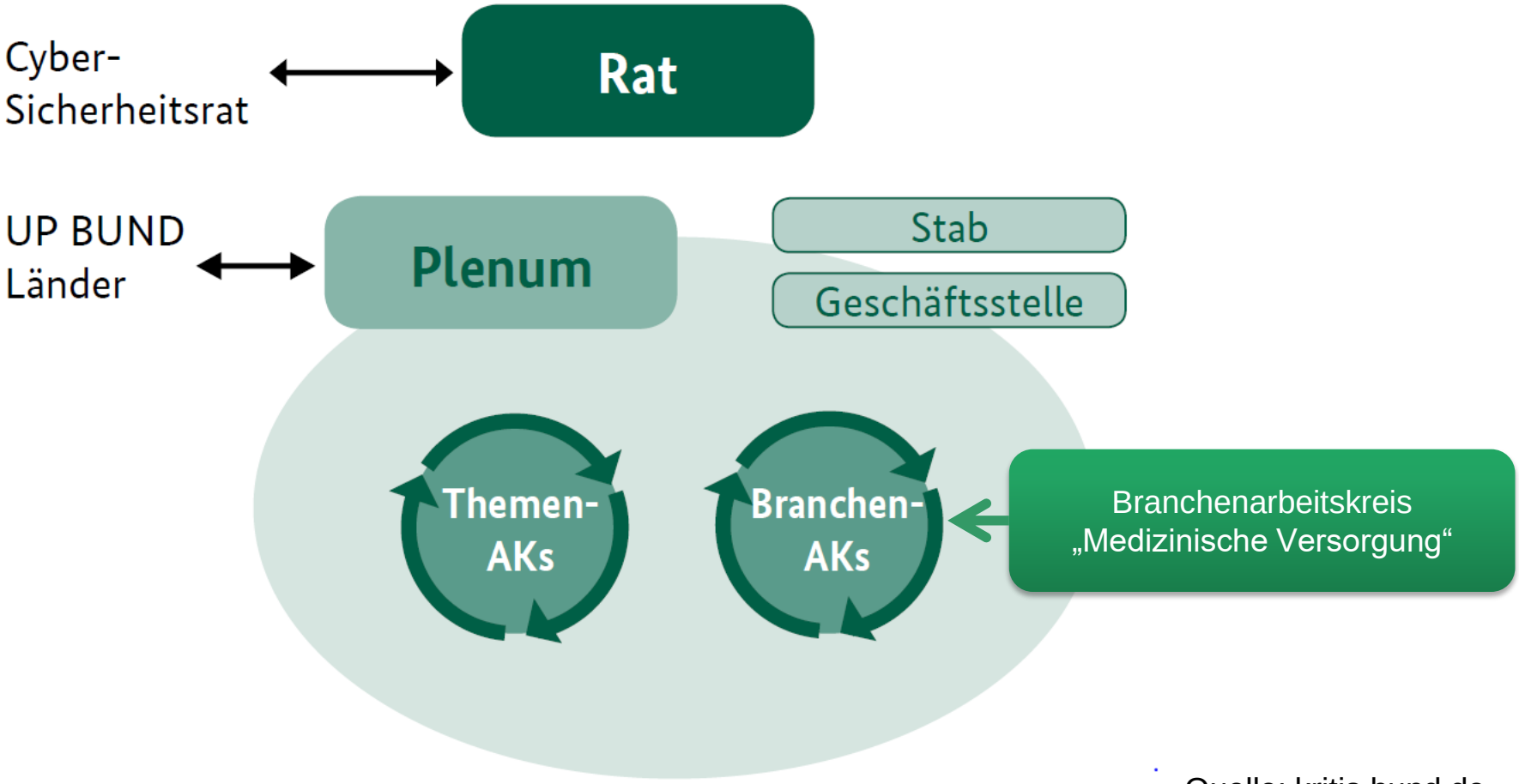
Die Kritischen Infrastrukturen Deutschlands



Quelle: kritis.bund.de

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Organisationsstruktur des UP KRITIS



Quelle: kritis.bund.de

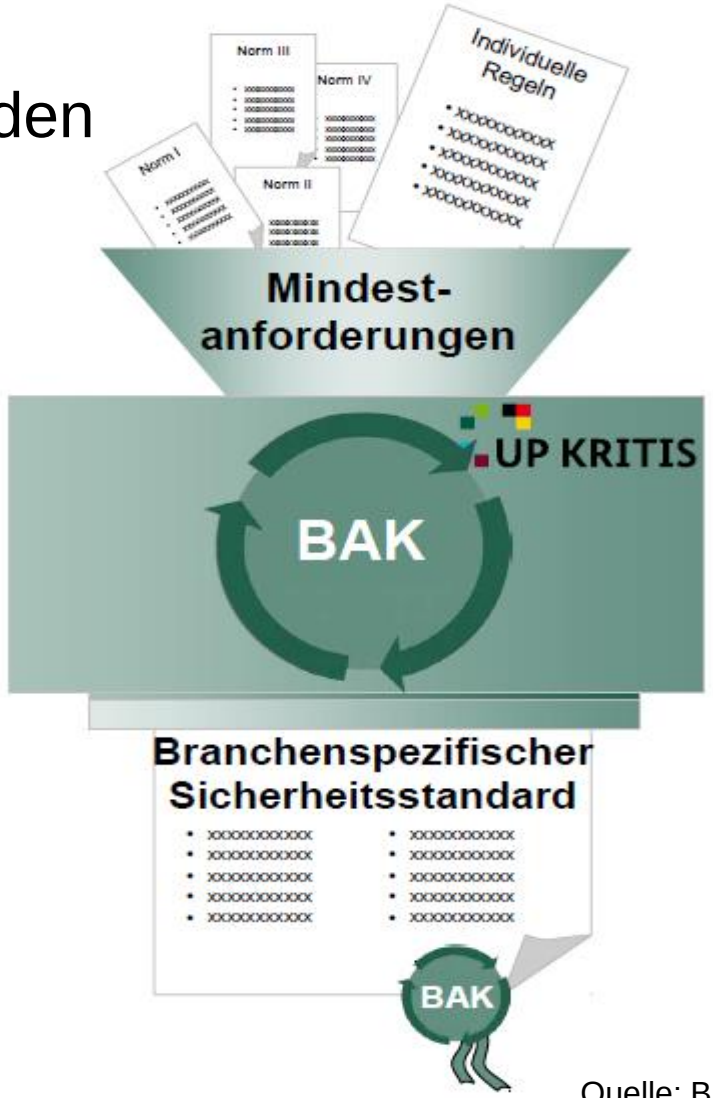
Der BAK „Medizinische Versorgung“

Wer ist Mitglied im BAK?

- Krankenhäuser, Verbände, Behörden

„Ziele und Aufgaben“ des BAK:

- Ermittlung des „Status quo“ der IT
- Analyse einschlägiger Normen und Standards
- Erstellung B3S
- „Best Practice“-Empfehlungen
- Mitarbeit im UP KRITIS zur Weiterentwicklung allgemeiner sektorenübergreifender Festlegungen



Quelle: BSI

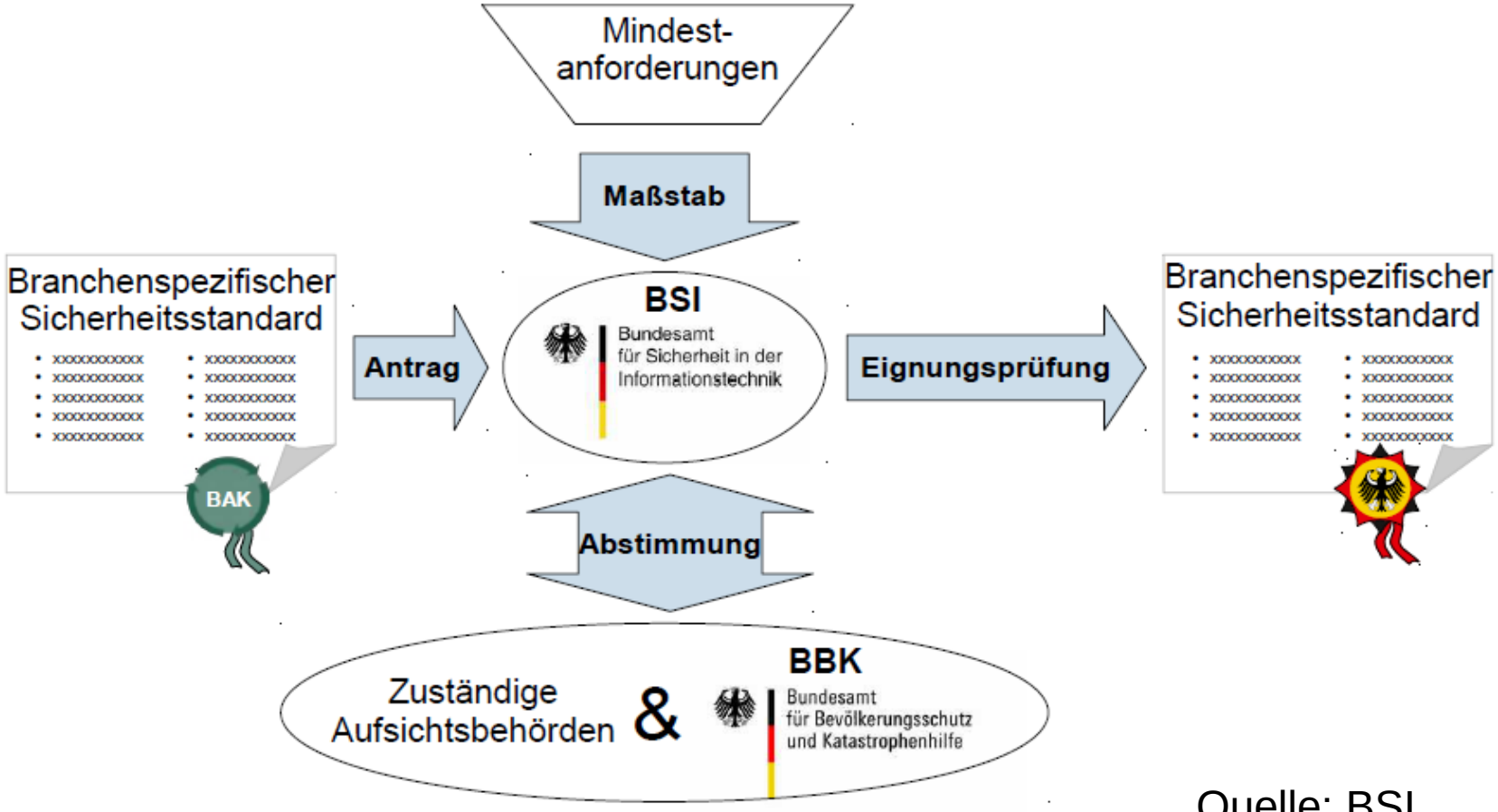
Mitglieder des BAK „Medizinische Versorgung

AKH Celle
ALB FILS Kliniken
BSI
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Bundesverband der Krankenhaus IT-Leiterinnen/Leiter e.V.
Deutsche Krankenhausgesellschaft e.V.
edia.con gGmbH
Helios Kliniken GmbH
Katholische Hospitalvereinigung
Katholische Kliniken Emscher-Lippe GmbH
kbo Kliniken des Bezirks Oberbayern
Kliniken Nordoberpfalz AG
Klinikum Itzehoe
Klinikum Nürnberg
Klinikum Schloß Winnenden
Klinikum Stuttgart
Städtisches Klinikum München
Medizinische Einrichtungen des Bezirks Oberpfalz
Saarland Heilstätten GmbH
Sana Management GmbH
Städtisches Klinikum Braunschweig gGmbH
Städtisches Klinikum Lüneburg
Unfallkrankenhaus Berlin
Universitätsklinikum Bonn
Universitätsklinikum Carl Gustav Carus Dresden
Universitätsklinikum des Saarlandes
Universitätsklinikum Erlangen
Universitätsklinikum Göttingen
Universitätsklinikum Köln
Universitätsklinikum Münster
Universitätsklinikum Schleswig-Holstein (UKSH)
Universitätsklinikum Tübingen
Universitätsklinikum Rostock
Universitätsklinikum Jena
Universitätsklinikum Fulda
Vinzentius-Krankenhaus Landau GmbH
Vinzenz von Paul Kliniken gGmbH
Westpfalz-Klinikum

Aufgaben und Zuständigkeiten nachgelagerter Behörden

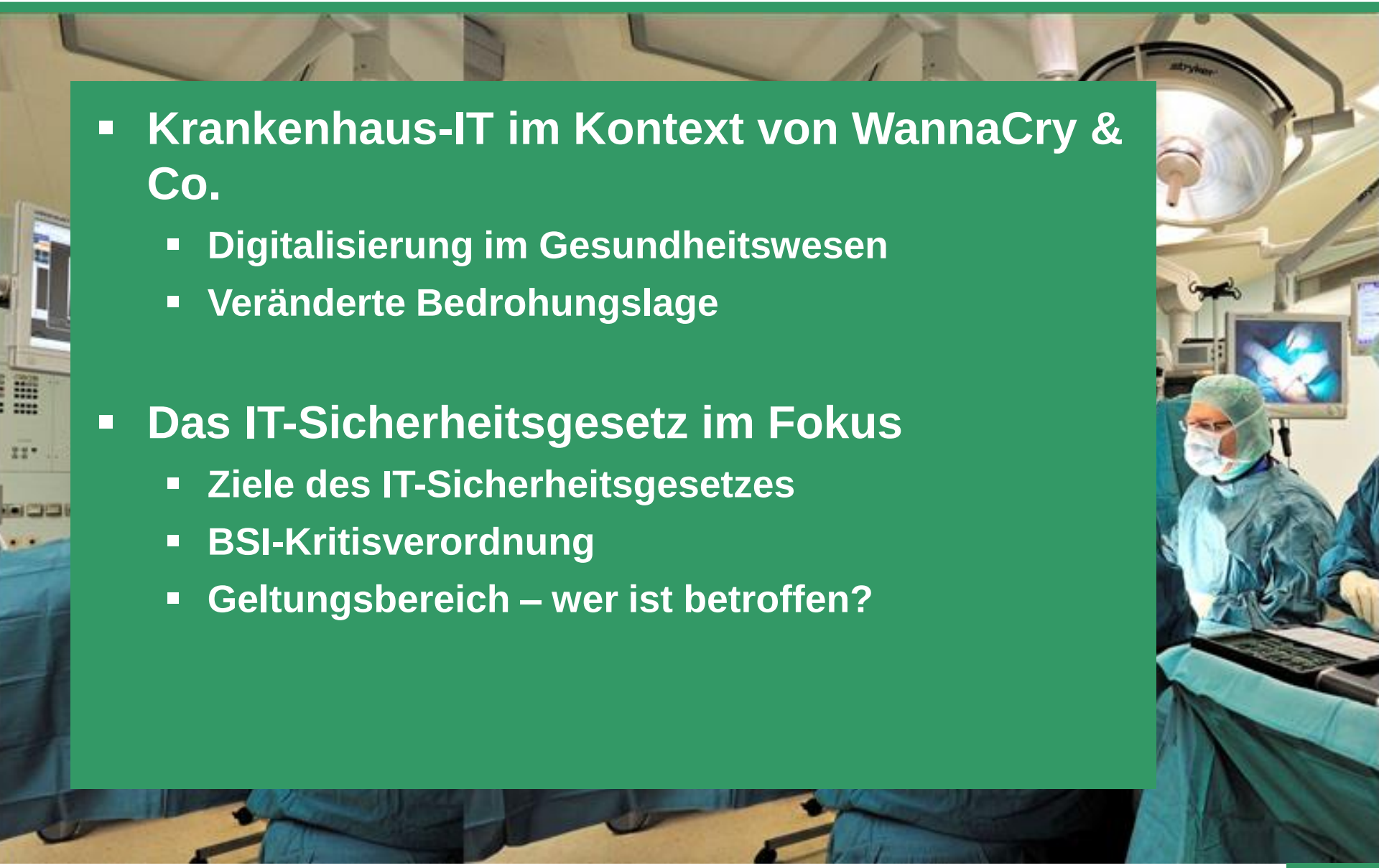
DEUTSCHE KRANKENHAUS GESELLSCHAFT

Branchenverbände können branchenspezifische Sicherheitsstandards vorschlagen (§ 8a Abs. 2 BSI-Gesetz)



Quelle: BSI

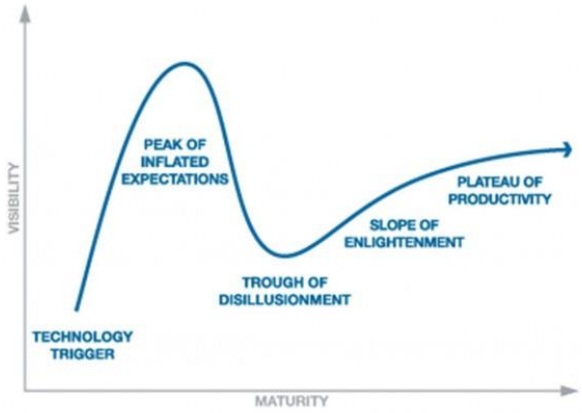
IT-Sicherheitsgesetz



- **Krankenhaus-IT im Kontext von WannaCry & Co.**
  - **Digitalisierung im Gesundheitswesen**
  - **Veränderte Bedrohungslage**
- **Das IT-Sicherheitsgesetz im Fokus**
  - **Ziele des IT-Sicherheitsgesetzes**
  - **BSI-Kritisverordnung**
  - **Geltungsbereich – wer ist betroffen?**

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Die IT-Landschaft im Gesundheitsbereich verändert sich rapide

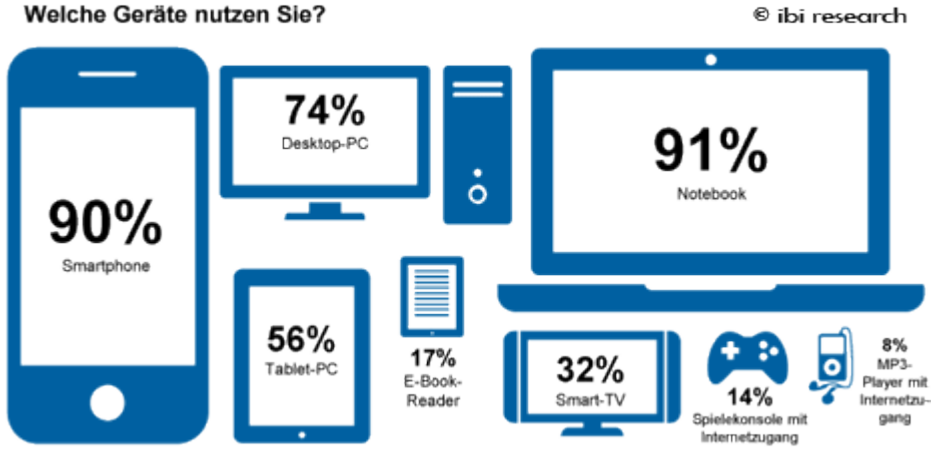


Kurze Hype-Zyklen:

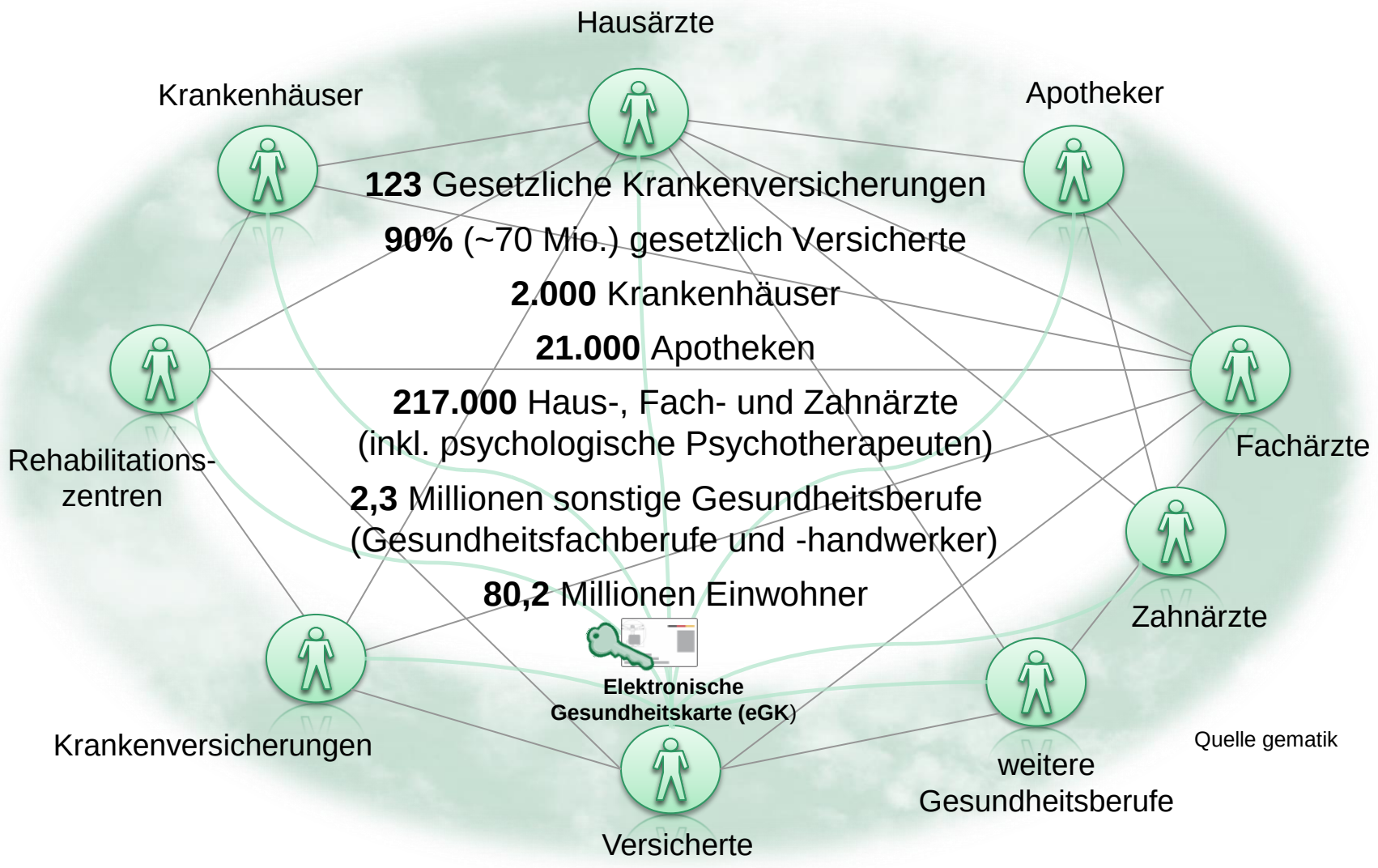
- Unternehmen setzen auf die *Cloud*
- *Big-Data*-Analytics ist die Zukunft
- *Social Media* treiben die IT voran
- Bring your own device *(BYOD)*
- Internet of Things *(IoT)* wird die Technik revolutionieren – Industrie 4.0
- *Elektromobilität* ist die Zukunft des Automobils
- *Digitalisierung* ist die neue industrielle Revolution

Aktueller Trend: Digitalisierung

- Derzeit die wichtigste Entwicklung, da auf einer höheren Abstraktionsebene
- Sehr hoher Veränderungsdruck seitens der Consumer, aber auch extremer Druck von großen Unternehmen der Consumer-IT-Branche
- Dadurch auch Veränderungen in der Krankenhaus-IT zu erwarten



Vernetzung im Gesundheitswesen



Quelle gematik

Digitalisierung – Risiken und Nebenwirkungen

„Ich weiß, was Du letzten Sommer getan hast…“

Hollywood, 1997

„Ich weiß, was Du letzte Nacht getan hast…“

San Francisco, 2015

„Ich weiß, wen Du nächsten Dienstag wählen wirst…“

New York City, 2016

Veränderte Bedrohungslage

DEUTSCHE KRANKENHAUS GESELLSCHAFT

„Größter Erpresser-Software Angriff der Geschichte“

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Anmelden

NETZWELT Schlagzeilen | Wetter | DAX 12.770,41 | TV-Programm | Abo

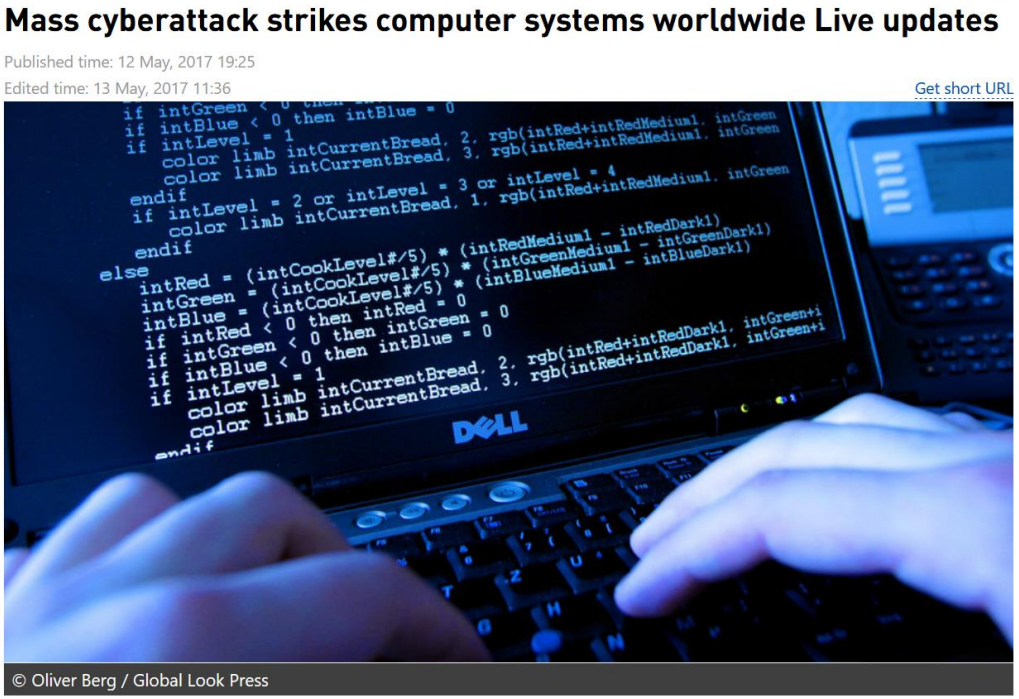
Nachrichten > Netzwelt > Web > Computersicherheit > "WannaCry"-Attacke - Fakten zum globalen Cyber-Angriff

Erpresser-Software

"WannaCry"-Attacke - Fakten zum globalen Cyberangriff

Der größte Erpressersoftware-Angriff der Geschichte hat weltweit Zigtausende Computer lahmgelegt, auch die Bahn und Krankenhäuser waren betroffen. Antworten auf die wichtigsten Fragen.

Quelle: www.spiegel.de vom 13.5.2017



Mass cyberattack strikes computer systems worldwide Live updates

Published time: 12 May, 2017 19:25

Edited time: 13 May, 2017 11:36

Get short URL

© Oliver Berg / Global Look Press

Tens of thousands of computers in 99 countries have been infected by a ransomware virus which extorts users by blocking Windows files and demanding payment to restore access.

Quelle: www.rt.com vom 13.5.2017

Veränderte Bedrohungslage

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

Social Engineering

Ansatz

Es ist teilweise sehr viel einfacher, einen Menschen dazu zu verleiten, etwas unvorsichtiges zu tun, als die z.T. sehr komplexen IT-Sicherheitssystemen zu überwinden…

Phishing, Malware-Attachments, CEO-Fraud

*Der Autozulieferer **Leoni** ist nach eigenen Angaben Opfer eines millionenschweren Betrugs geworden. Unter Verwendung gefälschter Dokumente und Identitäten sowie unter Nutzung elektronischer Kommunikationswege seien Gelder des Unternehmens auf Zielkonten im Ausland transferiert worden, teilte das im MDax notierte Unternehmen am Dienstag mit.*

Der Schaden belaufe sich auf einen Abfluss an liquiden Mitteln von insgesamt rund 40 Millionen Euro.

(Quelle: 16.08.2016)
http://www.managermagazin.de/unternehmen/autoindustrie/autozuliefererleoni-um-40-millionen-betrogen-a-1107998.html

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Zero-Day-Exploits & Geheimdienste

Ansatz

Lücken in IT-Systemen, die nicht offengelegt oder von Dritten erkannt werden und so Zugriffe auf IT-Systeme ermöglichen.

u.a. „Drive-By-Attacken“ im „WWW“

Staatliche Cyberwaffen wie Stuxnet nutzten gleich mehrere davon.

US- Geheimdienste zahlen angeblich bis zu eine Million US-Dollar dafür, um heimlich an fremde Daten zu gelangen. Das BKA hätte für seine Staats-Trojaner auch gerne welche. Die Rede ist von den geheimnisvollen Zero-Day-Exploits. Eine aktuelle Studie gibt erstmals Einblick in deren Ökosystem und könnte so zu einer Versachlichung der Diskussion um die staatliche Nutzung beitragen

(Quelle: 31.03.2017)
https://www.heise.de/ct/ausgabe/2017-8-Gefaehrliche-Sicherheitsluecken-ueber-viele-Jahre-ausnutzbar-3666934.html

DEUTSCHE KRANKENHAUS GESELLSCHAFT

(D)DoS-Attacken

Ansatz

Überlastungsangriff auf IT-Infrastruktur.

Ausfall von Webservices inkl. Cloud-Diensten …

*Wegen einer massiven DDoS-Attacke sind die **Services großer US-Internet-dienste wie Twitter, Paypal, Netflix und Spotify am Freitagabend in Teilen der USA und Europas immer wieder zeitweise nicht zu erreichen**. Das US-Unternehmen Dyn teilte am Freitag mit, es untersuche eine Reihe von Angriffen auf seine DNS-Infrastruktur. Dyn betreibt nicht nur den Service DynDNS zur dynamischen Aktualisierung von Domain-Einträgen, sondern ist auch Provider für die klassischen DNS-Systeme vieler großer US-Konzerne.*

(Quelle: 31.03.2017)
https://www.heise.de/newsticker/meldung/DDoSAttacke-legt-Twitter-Netflix-Paypal-Spotify-und-andere-Dienste-lahm-3357289.html

Erpressungstrojaner (Typ: Locky)

Ansatz

Verschlüsselungs-Trojaner – Geld gegen Entschlüsselung.

Beeinträchtigung / Ausfall ganzer Geschäftsprozesse …

Aus Sicherheitsgründen verschoben die Mediziner Operationen, die engmaschig mit Laboruntersuchungen hätten begleitet werden müssen. Vorübergehend meldete sich die Klinik auch von der Notallversorgung ab und nahm keine Schwerverletzten mehr auf. Die Cyberattacke habe die Versorgung der Patienten nicht gefährdet, so Kremer. Dennoch seien die Konsequenzen enorm:

„Wir werden unsere IT neu aufstellen müssen und rechnen derzeit mit einem Schaden von etwa 750.000 Euro.“

Quelle (30.3.16):
http://www.spiegel.de/netzwelt/web/locky-teslacryptcryptolocker-co-zahlen-sie-nicht-a-1082315.html

Erpressungstrojaner (Typ: WannaCry)

Ansatz

Verschlüsselungs-Trojaner – Geld gegen Entschlüsselung.

Verbreitet sich aktiv weiter.

Beeinträchtigung / Ausfall ganzer Geschäftsprozesse …

Großbritannien schwer getroffen

… Es sind vor allem ältere Windows-Versionen betroffen, die nicht mehr mit Sicherheits-Updates versorgt werden. Besonders schwere Folgen hatte das in Großbritannien, wo WannaCry zahlreiche Rechner des National Health Service (NHS) befallen hat.

Patienten berichteten von chaotischen Zuständen. Viele Kranke mussten in andere Kliniken umgeleitet werden. Auch Krebs- und Herzpatienten, deren Daten nicht zur Verfügung standen, wurden nach Hause geschickt.

Quelle (13.05.17):
https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.htmll

Erpressungstrojaner (Typ: NotPetya)

Ansatz

„Wiper“-Trojaner

- **keine** Entschlüsselung gegen Geld
- Angriffsvektor: Software-Update-Mechanismen
- Verbreitet sich aktiv weiter
- **blockiert IT-Systeme vollständig**

Beeinträchtigung / Ausfall ganzer Geschäftsprozesse …

… legte der Trojaner bei Maersk Systeme auf Bohrinseln lahm und brachte das Beladen und Löschen von Containerschiffen zum Stocken. Auch die Herstellung von Nivea bei Beiersdorf in Hamburg-Billbrook war demnach betroffen. TNT meldet nach wie vor eine Störung der IT-Systeme und weist darauf hin, dass deswegen das Paket-Tracking verzögerte Informationen anzeige. **Auch Auslieferungen und das Abholen von Lieferungen verzögern sich seit dem Trojaner-Angriff immer mal wieder.**

Quelle (25.7.17):
https://www.heise.de/security/meldung/Cyber-Attacke-NotPetya-Unternehmen-haben-immer-noch-viel-Arbeitmit-dem-Fallout-des-Angriffs-3782794.html

Advanced-Persistent-Threats (APT)

Ansatz

… Stromausfälle in der Ukraine. Die Täter nutzten dabei offenbar ein Schadprogramm namens BlackEnergy, um Zugang zu den Netzwerken von Stromversorgern zu erhalten …

Beeinträchtigung / Ausfall ganzer Geschäftsprozesse …

Ein Advanced Persistent Threat (APT)-Angriff zeichnet sich im Gegensatz zu anderen Cyber-Angriffen dadurch aus, dass der Angreifer seine Ziele sorgfältig auswählt. … Stattdessen versuchen die Täter, sich im internen Netzwerk der angegriffenen Organisation auszubreiten und sich langfristig Zugang zu sichern. Dies erfordert in der Regel, dass sich die Täter manuell auf kompromittierte Rechner verbinden und über lange Zeit mit dem System interagieren.

(Quelle: Die Lage der IT-Sicherheit in Deutschland, BSI) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=3

Das IT-Sicherheitsgesetz

DEUTSCHE KRANKENHAUS GESELLSCHAFT

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

Vom 17. Juli 2015

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des BSI-Gesetzes

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 7 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

„§ 1

Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern."

2. Dem § 2 wird folgender Absatz 10 angefügt:

„(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erheblich wirkende Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt."

3. § 3 wird wie folgt geändert:

a) Absatz 1 Satz 2 wird wie folgt geändert:

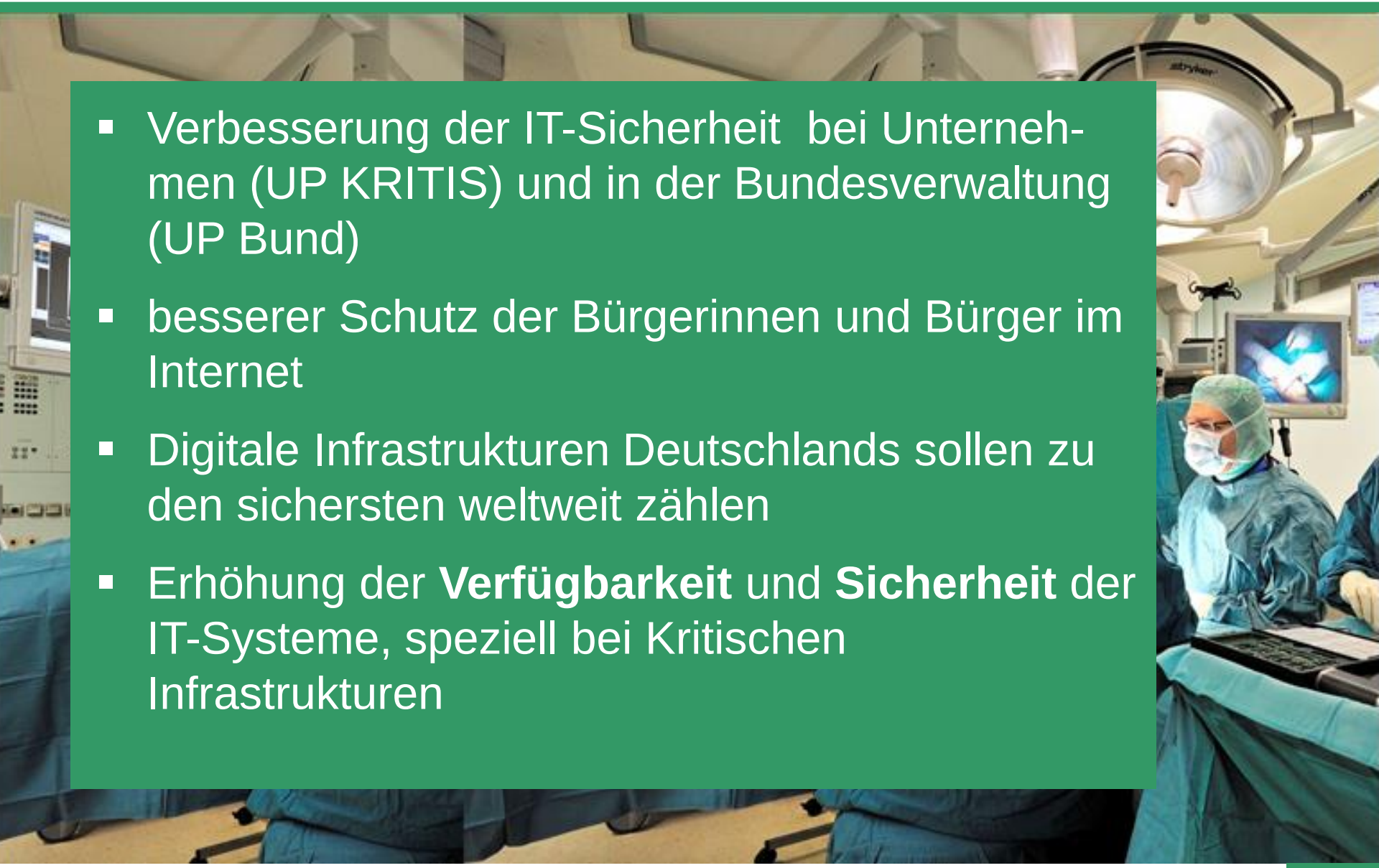
aa) In Nummer 2 werden die Wörter „zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" durch die Wörter „erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" ersetzt.

bb) In Nummer 15 werden die Wörter „kritischen Informationsinfrastrukturen" durch die Wörter „Sicherheit in der Informationstechnik Kritischer Infrastrukturen" und der Punkt am Ende durch ein Semikolon ersetzt.

cc) Die folgenden Nummern 16 und 17 werden angefügt:

„16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;

Ziele des IT-Sicherheitsgesetzes



- Verbesserung der IT-Sicherheit bei Unternehmen (UP KRITIS) und in der Bundesverwaltung (UP Bund)
- besserer Schutz der Bürgerinnen und Bürger im Internet
- Digitale Infrastrukturen Deutschlands sollen zu den sichersten weltweit zählen
- Erhöhung der **Verfügbarkeit** und **Sicherheit** der IT-Systeme, speziell bei Kritischen Infrastrukturen

ITSiG – wesentliche Neuregelungen

- Betreiber sind nach § 8a Abs. 1 BSIG zur **Umsetzung von angemessenen Sicherheitsmaßnahmen** verpflichtet („Stand der Technik“)
- Betreiber müssen nach § 8a Abs. 3 BSIG die **Umsetzung** entsprechender Maßnahmen **regelmäßig** (spätestens alle 2 Jahre) **nachweisen**
- das **BSI** nimmt nach § 8b BSIG die Aufgabe einer **zentralen Meldestelle** für sicherheitsrelevante Informationen wahr
- **Betreiber** haben nach § 8b Abs. 2 BSIG ein **Informationsrecht** gegenüber dem BSI
- **Betreiber müssen** nach § 8b Abs. 4 BSIG IT-Störungen an das BSI **melden**

Stand der Technik

„Auf Grund der weitreichenden gesellschaftlichen Auswirkungen ist bei den technischen und organisatorischen Vorkehrungen der „Stand der Technik“ zu berücksichtigen [BSIG: „einzuhalten“].
„Stand der Technik“ in diesem Sinne ist der **Entwicklungsstand fortschrittlicher**

- Verfahren,
- Einrichtungen oder
- Betriebsweisen,

der die **praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit** von informationstechnischen

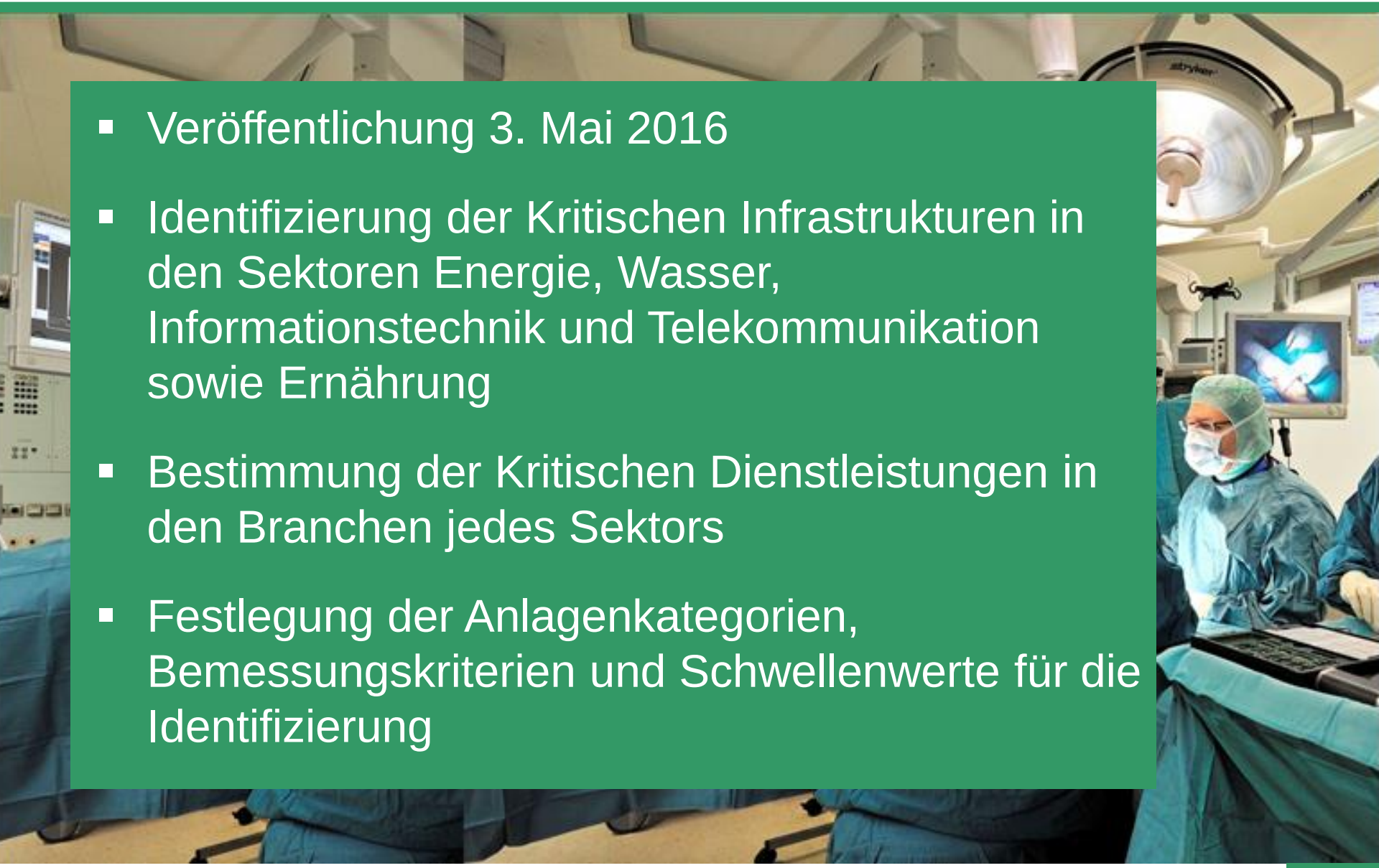
- Systemen,
- Komponenten oder
- Prozessen

gegen Beeinträchtigungen der

- Verfügbarkeit, Authentizität
- Integrität und
- Vertraulichkeit gesichert erscheinen lässt.“

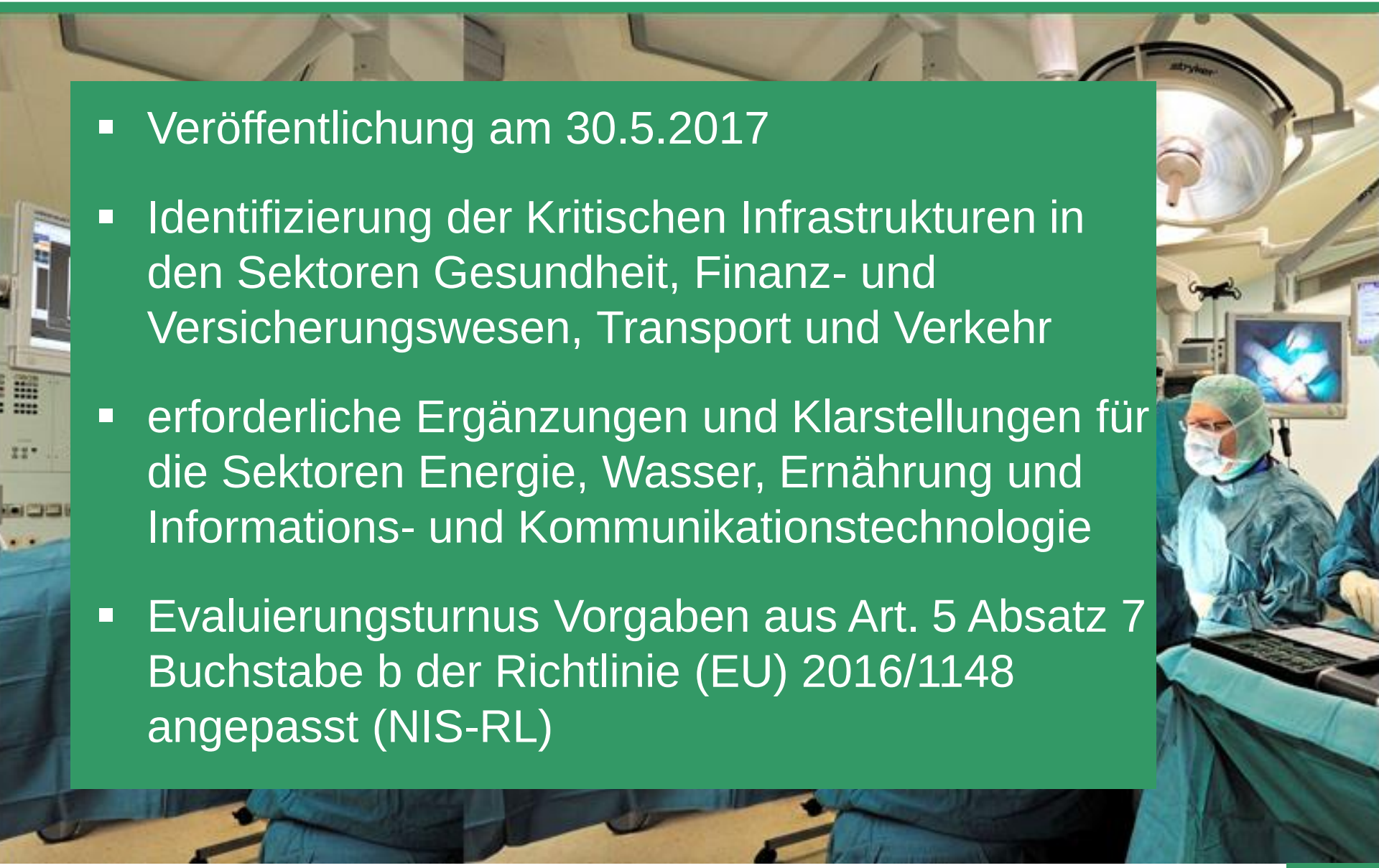
Quelle: BSI-Schulungsmodule Prüfnachweis § 8a

BSI-KritisV („Korb 1“)



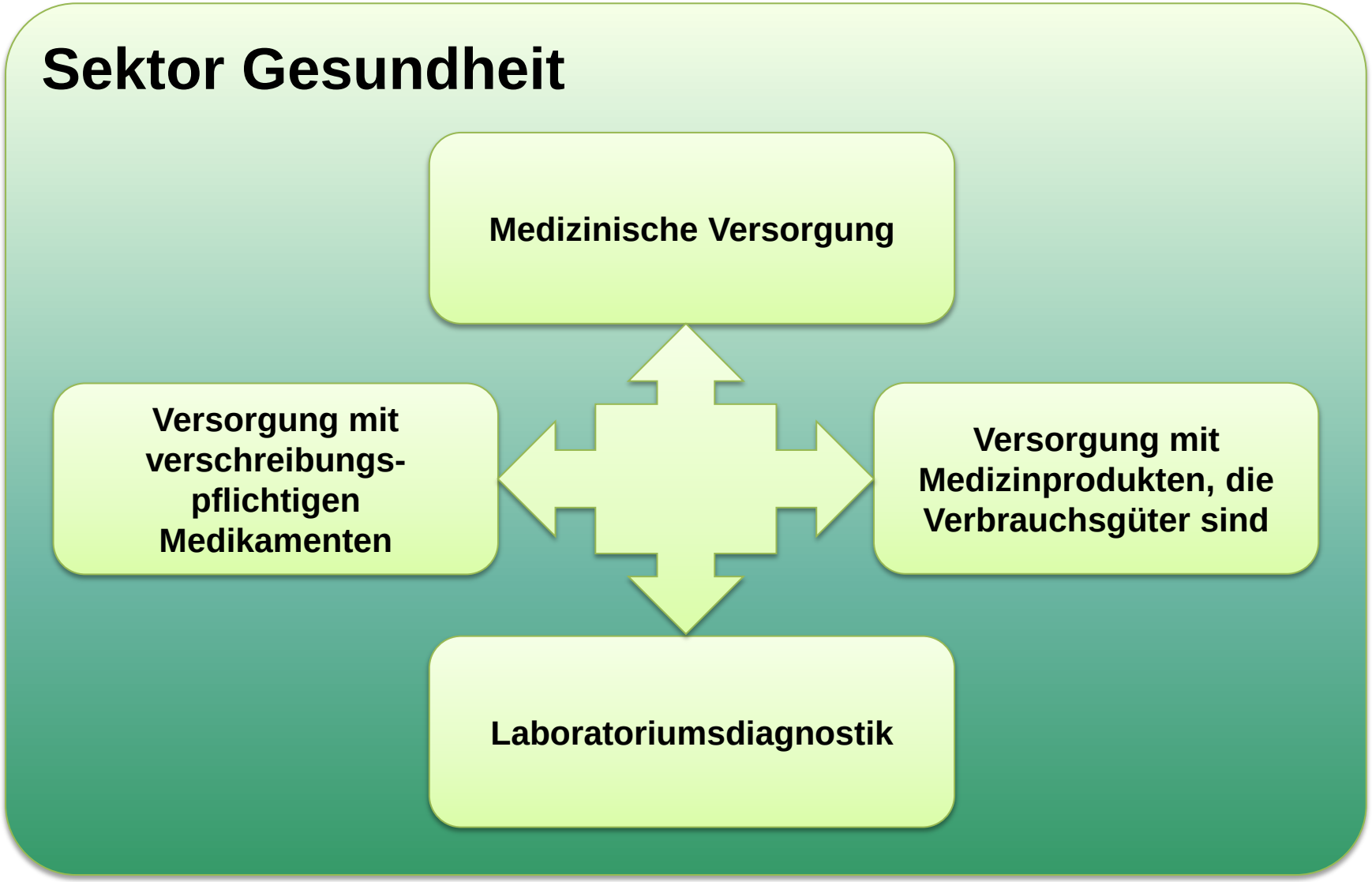
- Veröffentlichung 3. Mai 2016
- Identifizierung der Kritischen Infrastrukturen in den Sektoren Energie, Wasser, Informationstechnik und Telekommunikation sowie Ernährung
- Bestimmung der Kritischen Dienstleistungen in den Branchen jedes Sektors
- Festlegung der Anlagenkategorien, Bemessungskriterien und Schwellenwerte für die Identifizierung

BSI-KritisV („Korb 2“)



- Veröffentlichung am 30.5.2017
- Identifizierung der Kritischen Infrastrukturen in den Sektoren Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr
- erforderliche Ergänzungen und Klarstellungen für die Sektoren Energie, Wasser, Ernährung und Informations- und Kommunikationstechnologie
- Evaluierungsturnus Vorgaben aus Art. 5 Absatz 7 Buchstabe b der Richtlinie (EU) 2016/1148 angepasst (NIS-RL)

Festlegungen für den Sektor „Gesundheit“



DEUTSCHE KRANKENHAUS GESELLSCHAFT

Festlegungen für die Branche „medizinische Versorgung“

- Anlagenkategorie: Krankenhäuser
- Bemessungskriterium: Anzahl vollstationärer Behandlungen
- Schwellenwert: 30.000 / Jahr
- ambulante Versorgung derzeit nicht betrachtet (keine relevante Größenordnung einzelner Betreiber)
- Föderalismus: Standort eines Krankenhauses nicht einheitlich (Verzeichnis nach § 293 Abs. 6 SGB V?)
- ca. 5 – 10 % aller Kliniken betroffen

Definition des Anlagenbegriffs

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Anlagenbegriff aufgrund föderaler Bestimmungen nicht einheitlich (Landeskrankenhausplanung)

Krankenhaus (Anlagenkategorie)

„Standort oder Betriebsstätten eines nach § 108 des fünften Buches Sozialgesetzbuch in der jeweils geltenden Fassung zugelassenen Krankenhauses, die für die Erbringung stationärer Versorgungsleistungen notwendig sind.“

Begründung

„Der Krankenhausbegriff ist im Sinne der Landeskrankenhauspläne zu verstehen, welche die zugelassenen Krankenhäuser, teilweise differenziert nach Betriebsstätten oder Standorten, ausweisen. Dabei sind räumlich getrennte Standorte oder Betriebsstätten eines Krankenhauses als eine Anlage anzusehen, wenn sie aus planungsrechtlicher Sicht, etwa aus organisatorischen, technischen, medizinischen oder sicherheitsbezogenen Aspekten als Einheit betrachtet werden.“

Definition des Anlagenbegriffs

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Klarstellung des Bundesministeriums des Innern (BMI) vom 18.9.2017

„Die BSI-Kristisverordnung verweist im Hinblick auf die Anlagenkategorie "Krankenhaus" auf § 108 SGB V. Anknüpfungspunkt für die Identifikation des Standorts und der Betriebsstätten eines Krankenhauses im Sinne der Verordnung ist damit die (Landes-)Krankenhausplanung. Die BSI-Kritisverordnung definiert die Anlagenkategorie „Krankenhaus“ als „Standort oder Betriebsstätten eines nach § 108 des Fünften Sozialgesetzbuches […] zugelassenen Krankenhauses [...]“ (s. Anhang 5, Teil 1 Nr. 1a BSI-KritisV).

Die Definition beinhaltet also zwei alternative Tatbestände:

1. *„Ein Krankenhaus ist der Standort eines nach § 108 […] zugelassenen Krankenhauses.“*

   und

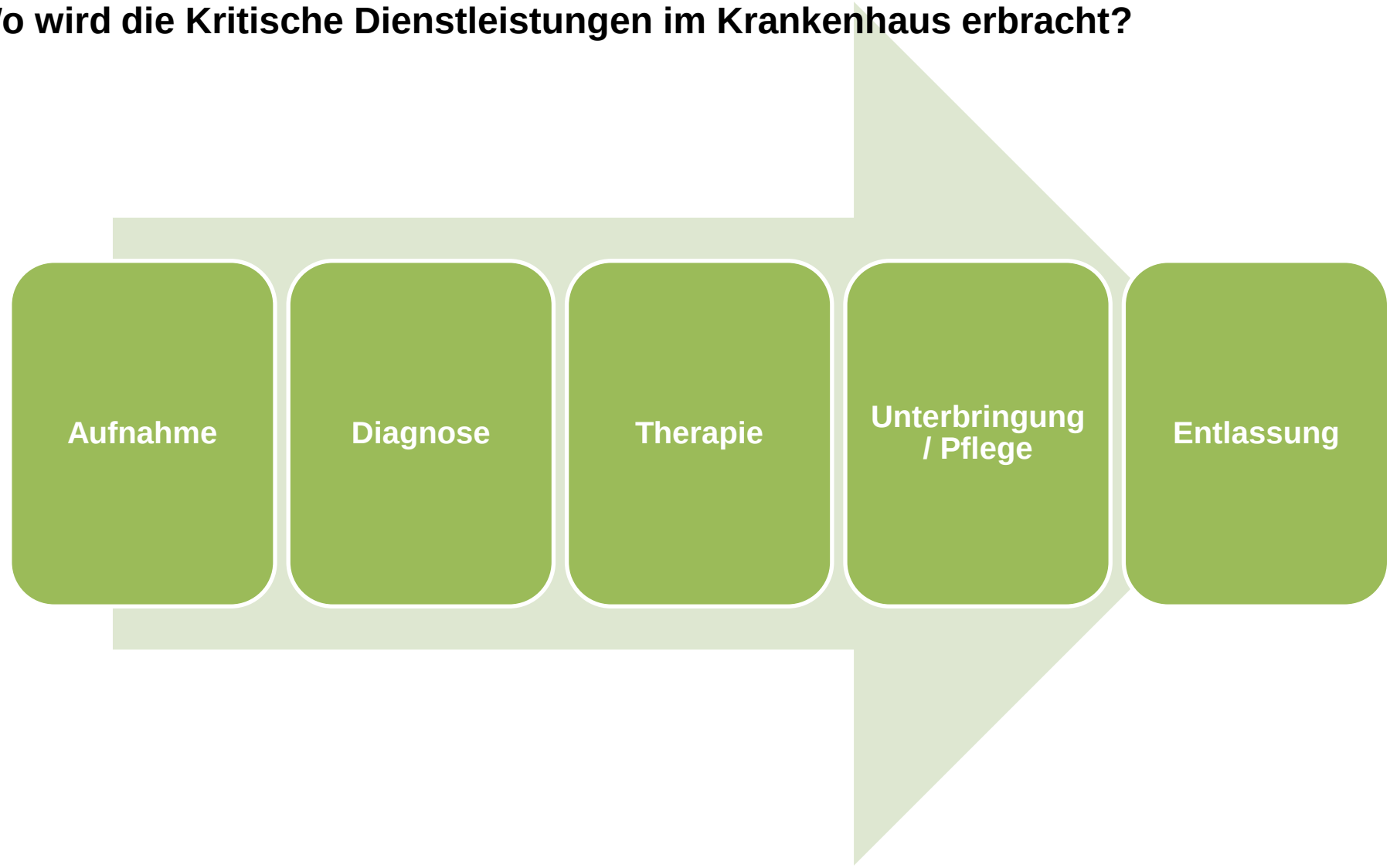
2. *„Ein Krankenhaus sind die Betriebsstätten (und zwar alle) eines nach § 108 […] zugelassenen Krankenhauses.“.*

*Im Falle von Nummer 2 sind alle Betriebsstätten, die im Sinne des (jeweiligen) Landeskrankenhausplans als **ein Krankenhaus** behandelt werden (**Feststellungsbescheid**), in Anwendung der Verordnung **als eine Anlage** zu betrachten.*

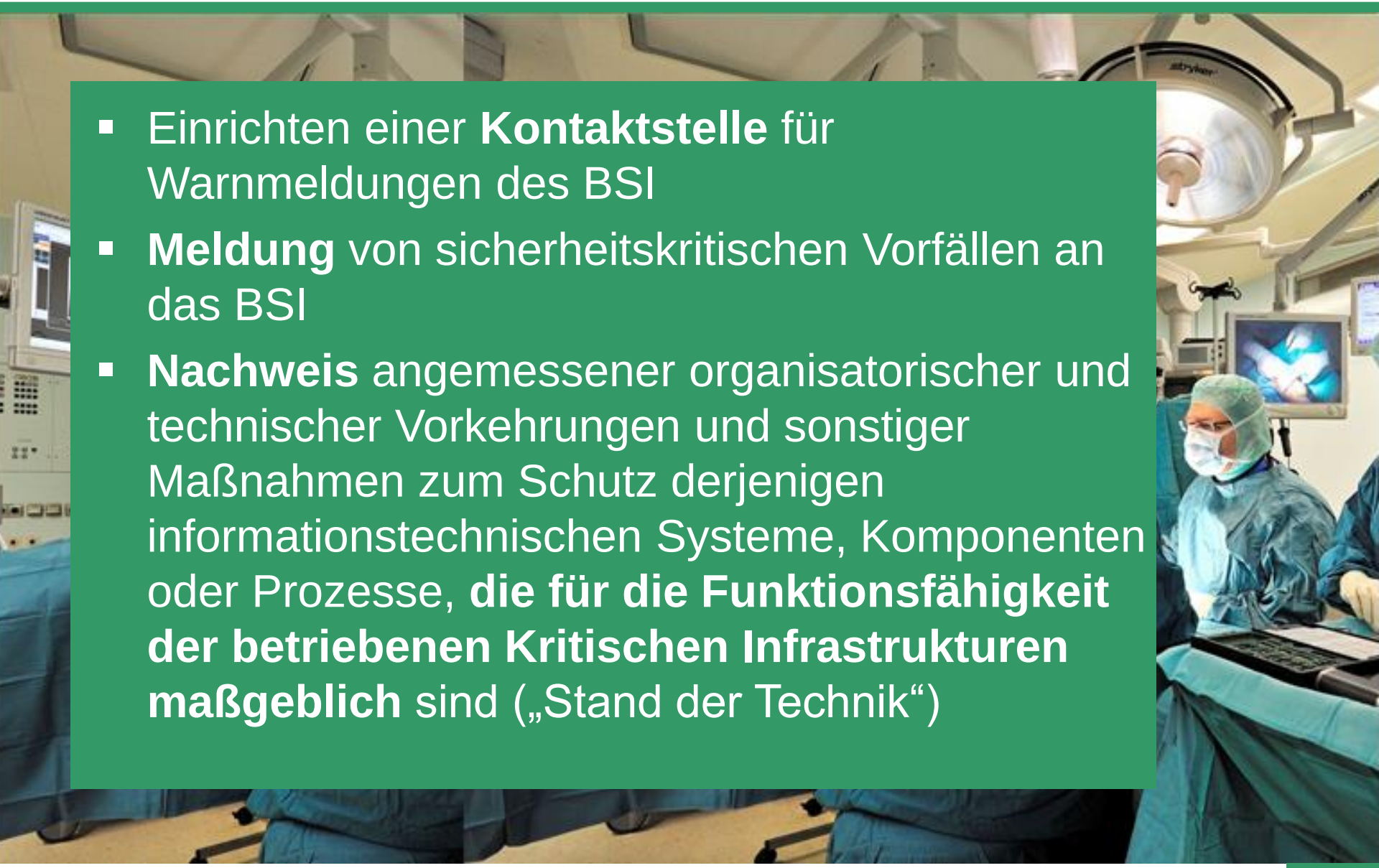
***In diesem Fall** sind die vollstationären Fälle der einzelnen Betriebsstätten zu summieren."*

Bereiche „Medizinischer Versorgung“

Wo wird die Kritische Dienstleistungen im Krankenhaus erbracht?

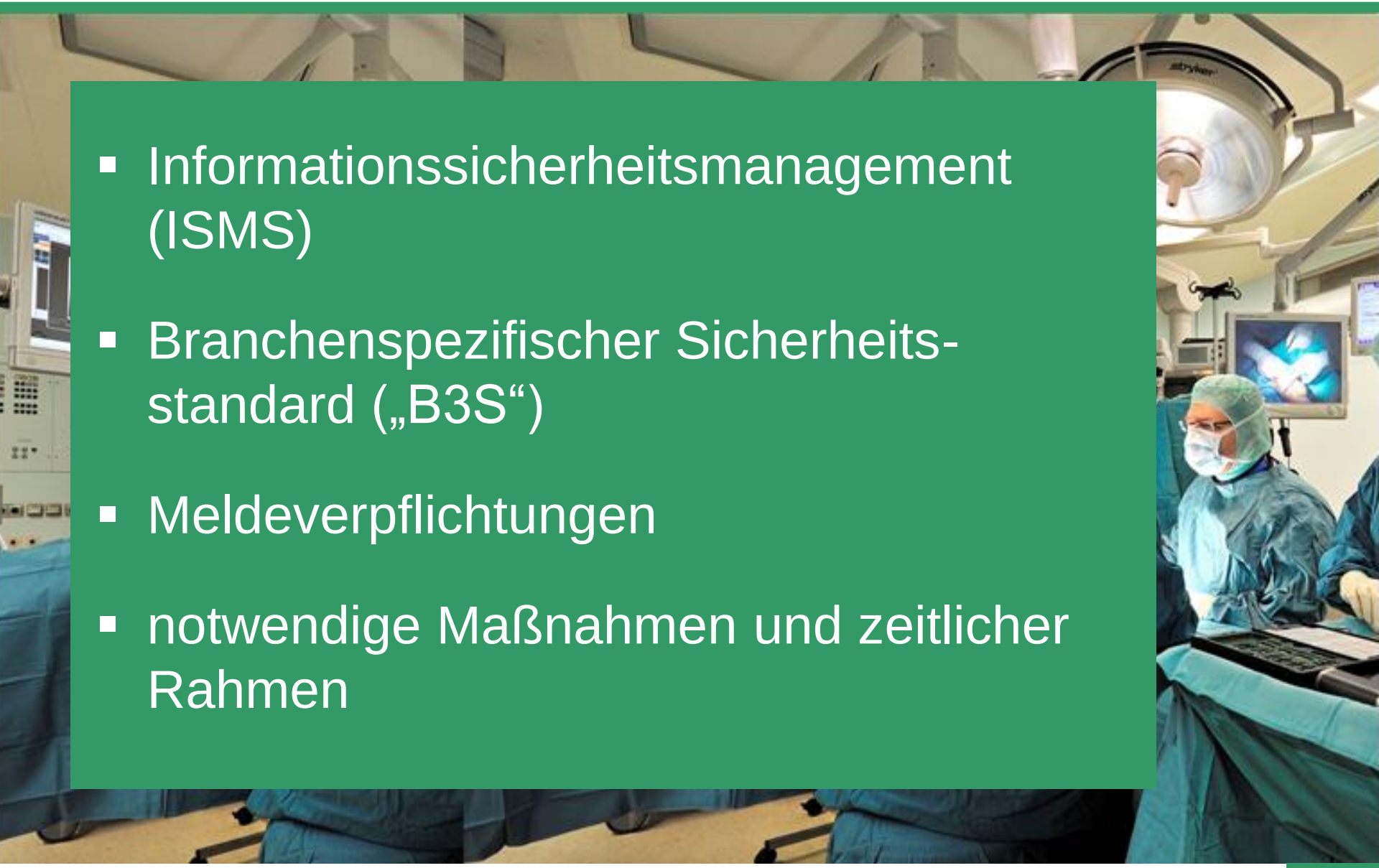


Welche Maßnahmen sind umzusetzen?



- Einrichten einer **Kontaktstelle** für Warnmeldungen des BSI
- **Meldung** von sicherheitskritischen Vorfällen an das BSI
- **Nachweis** angemessener organisatorischer und technischer Vorkehrungen und sonstiger Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse, **die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich** sind („Stand der Technik“)

Chancen und Risiken für alle Kliniken



- Informationssicherheitsmanagement (ISMS)
- Branchenspezifischer Sicherheits-standard („B3S“)
- Meldeverpflichtungen
- notwendige Maßnahmen und zeitlicher Rahmen

Geltungsbereich – Wer ist betroffen?

- **IT-Sicherheitsgesetz richtet sich ausschließlich an Betreiber kritischer Infrastrukturen**

ABER

- **IT-Sicherheit = Patientensicherheit**
- **Grad der IT-Durchdringung im Gesundheitswesen steigt**
- **ein IT-Sicherheitsvorfall kann schnell zu einem Datenschutzverstoß führen (EU-DSGVO)**
- **Maßnahmen zur Verbesserung der IT-Sicherheit künftig auch in für Wirtschaftsprüfung und Versicherungen relevant**

Verbesserung der IT-Sicherheit ist ein Thema für alle Krankenhäuser

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Anforderungen des IT-Sicherheitsgesetzes (BSI-Gesetz)

„§ 8a

Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

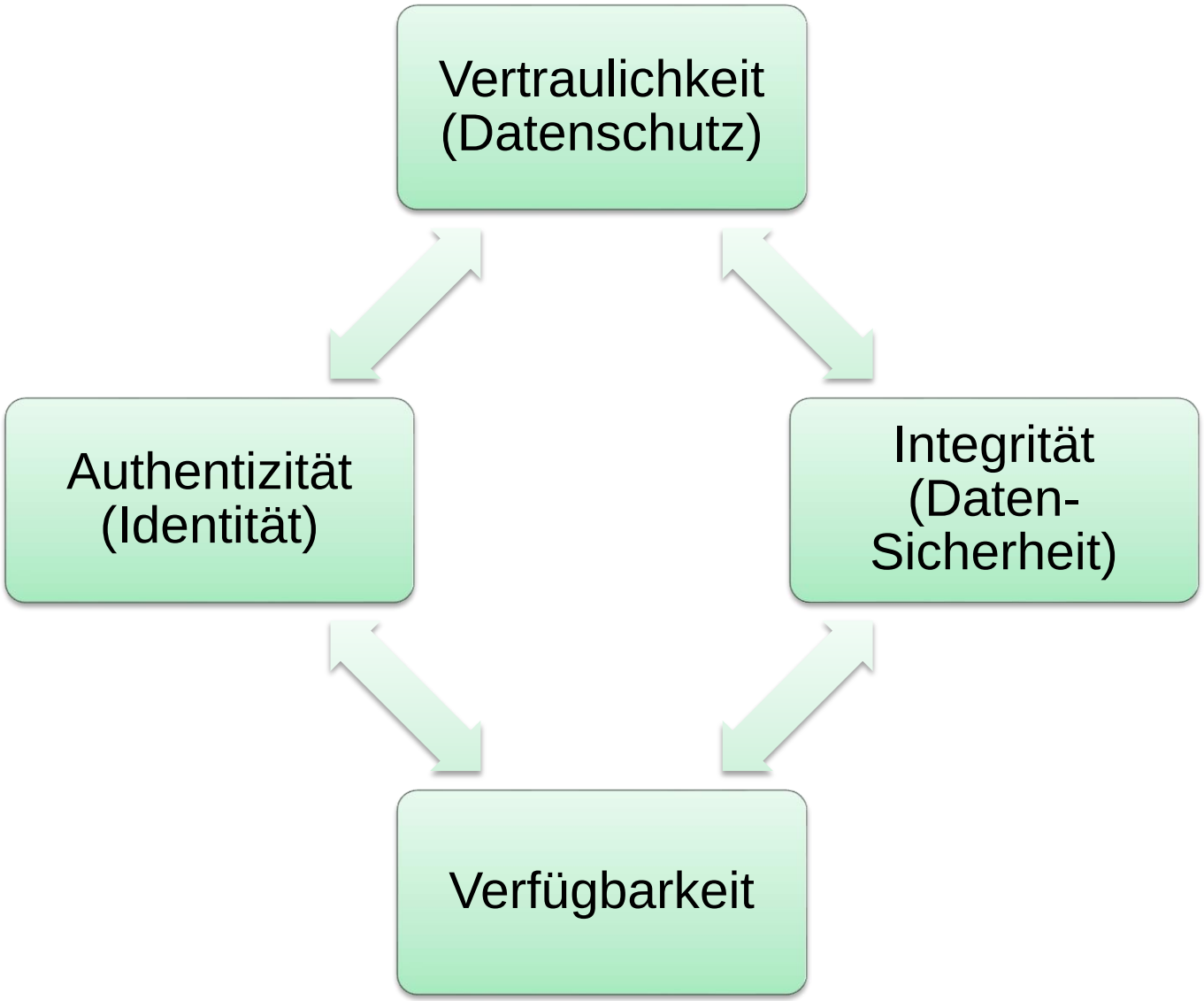
expressis verbis ist kein ISMS gefordert

Nachweis geeigneter Maßnahmen in Abstimmung mit dem BSI

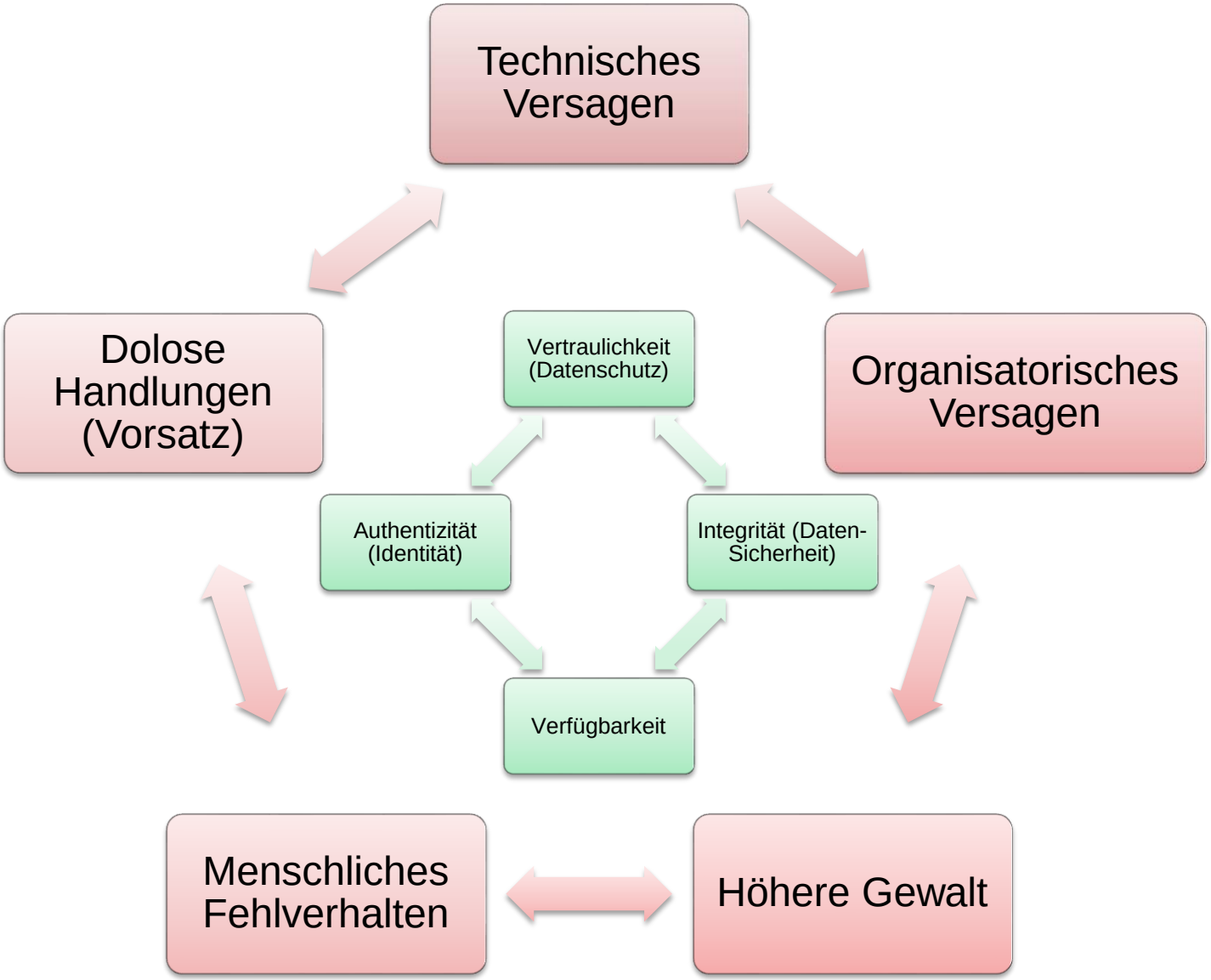
(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln verlangen:

1. die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel.

Schutzziele gem. § 8a Abs. 1 BSI-Gesetz



5 Hauptrisiken der Informationssicherheit

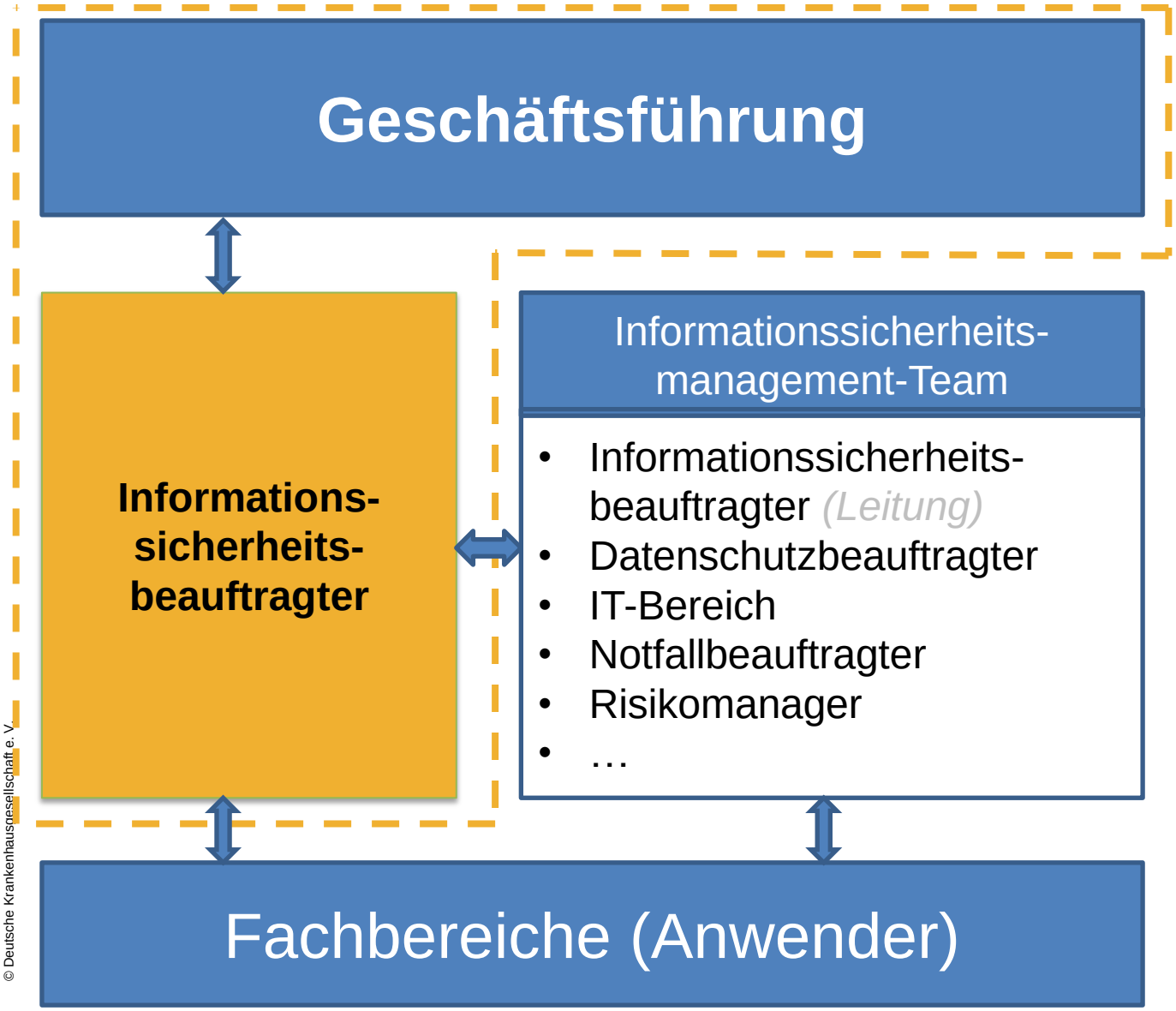


Grundsätze der Informationssicherheit

- Einhaltung unternehmensinterner Anforderungen
- Einhaltung gesetzlicher Anforderungen, Standards und Regeln
- Sicherheit als integraler Bestandteil
- Schutz von Daten und Ressourcen
- Gewährleistung der Nachvollziehbarkeit
- Einhaltung Maßnahmen zum Schutz vor Angriffen und bei Notfällen
- Gewährleistung vertraglicher Beziehungen
- Gewährleistung des Geschäftsbetriebs

Ziele des Sicherheitsmanagements

Sicherheitsorganisation

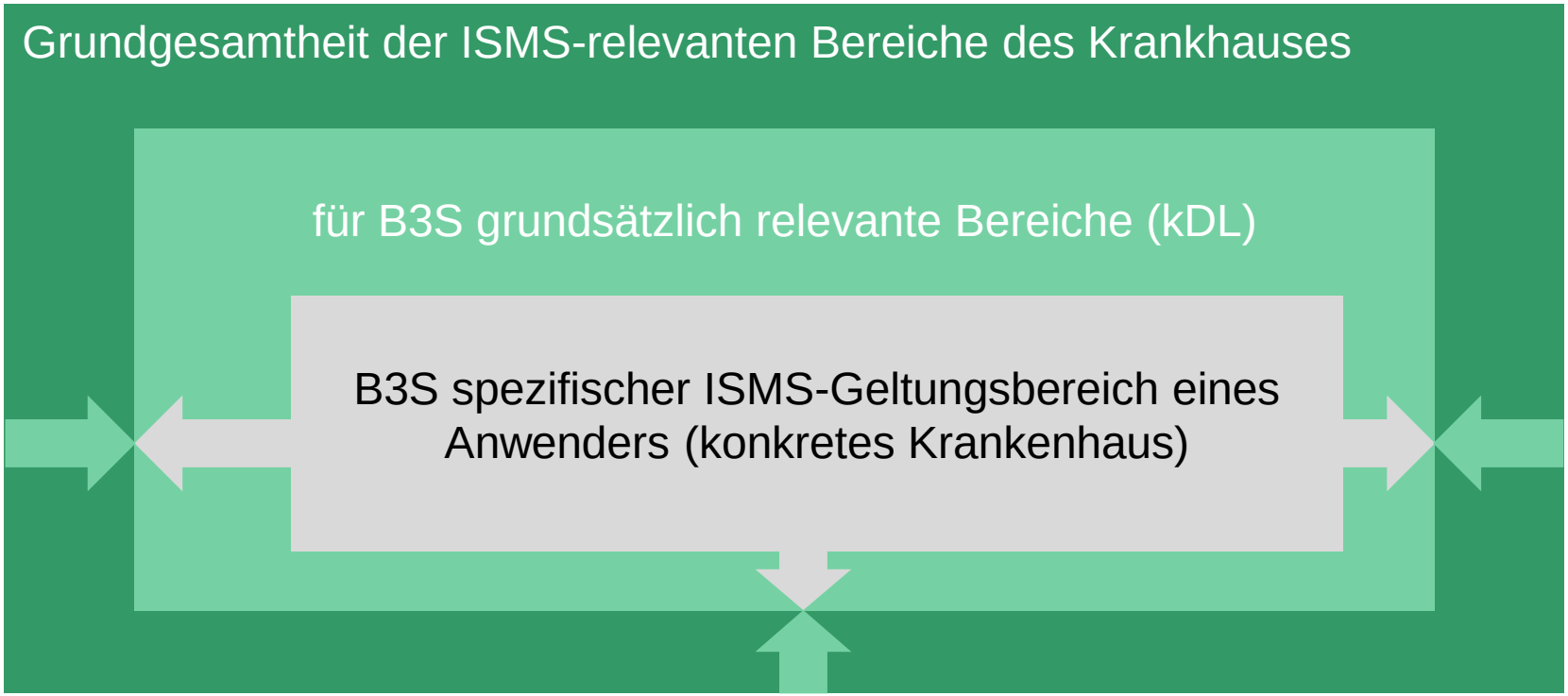


Vorgabe von Leitlinien zur Informations-sicherheit

Vorgabe von Leitlinien zur Informationssich erheit

Vorgabe von Leitlinien zur Informationssich erheit

Informationssicherheitsmanagementsystem (ISMS)



Branchenspezifischer Sicherheitsstandard (geplant)

- Rahmendokumentation
- Geltungsbereich und Schutzziele
- Gefährdungslage
- Risikobehandlung
- Maßnahmenkatalog
- Nachweis der Umsetzung
- Anlagen

DIN 13080:2016

Funktionsbereiche und Funktionsstellen im Krankenhaus

Meldeverpflichtungen

DEUTSCHE KRANKENHAUS GESELLSCHAFT

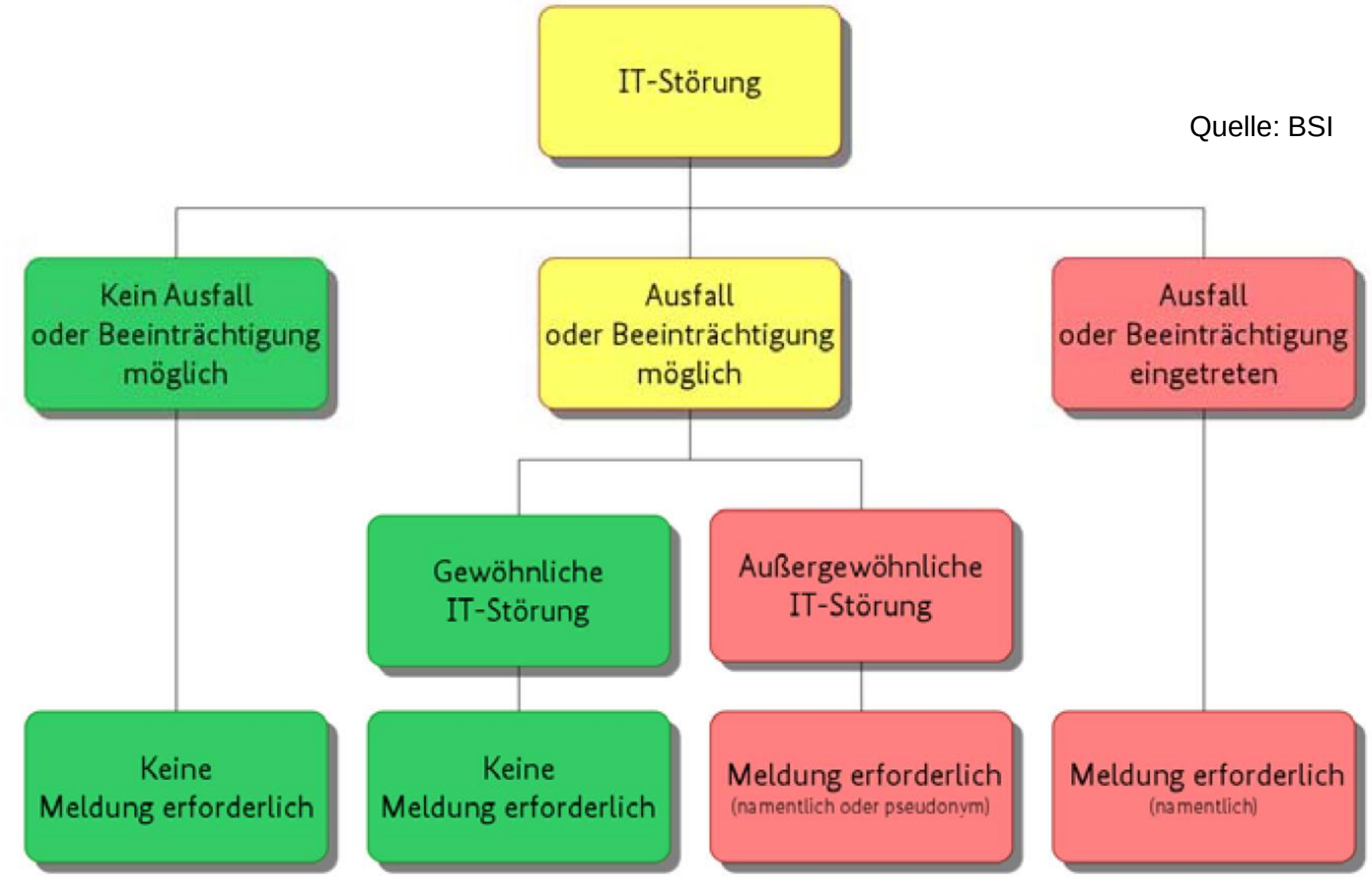
Mit der Meldung als kritische Infrastruktur entstehen Meldeverpflichtungen:

- die Verpflichtung zur Übermittlung meldepflichtiger Vorfälle an das BSI, sowie
- die Einrichtung / Benennung einer Kontaktstelle für Meldungen des BSI an kritische Infrastrukturen

Was muss gemeldet werden?

IT-Störungen, wenn sie einen Ausfall oder eine Beeinträchtigungen des Regelbetriebs nach sich gezogen haben (dann namentliche Nennung) oder potentiell hätten haben können (dann anonyme Meldung möglich)

Meldeverpflichtungen



Quelle: BSI

Wann sind die Maßnahmen umzusetzen?

Mai 2016: BSI-Kritisverordnung („Korb 1“)

Mai 2017: 1. Änderungsverordnung BSI-KritisV – „Korb 2“ [1)]

November 2017: Kontaktstelle einrichten (§ 8b Abs. 3 BSIG) Meldung erheblicher Störungen an BSI [1)]

Nachweis geeigneter Maßnahmen (§ 8a Abs. 3 BSIG): **Mai 2019**

Stichtag für die Prüfung des Schwellenwerts: **31. März**

Kritische Infrastruktur bei Überschreiten des Schwellenwerts ab: **1. April**

Nachweispflichten bei Überschreitung des Schwellenwerts in **2 aufeinander folgenden Jahren**

[1)] gültig für Schwellenwertüberschreitung in 2016

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Informationssicherheit

Schutz von Daten und Informationen jeglicher Art

IT-Sicherheit

Primärer Schutz elektronisch gespeicherter Informationen und deren Verarbeitung

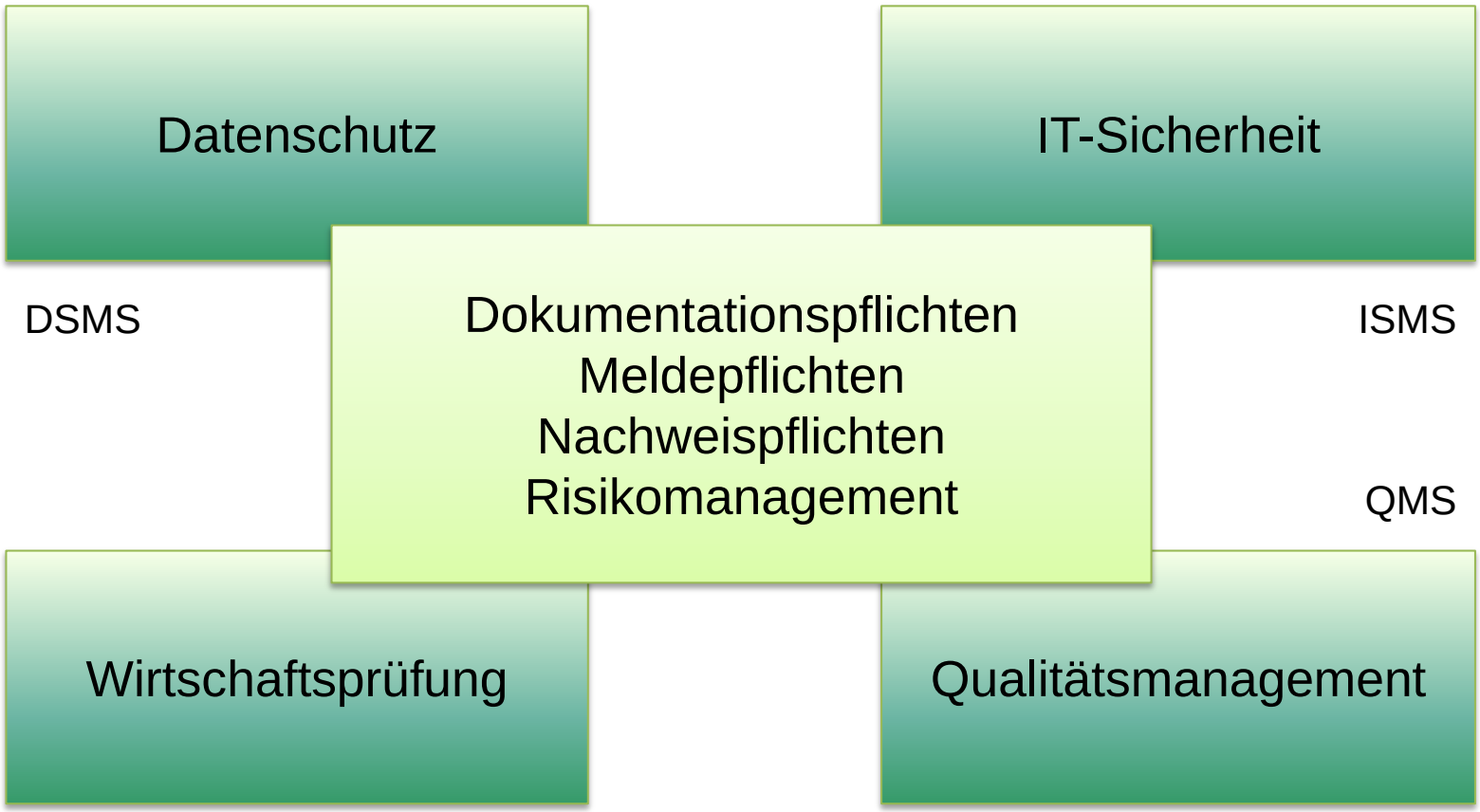
Datenschutz

Schutz personenbezogener Daten

Verfahrensverzeichnis

Empfehlung an Krankenhäuser: IT-Strategie

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



ITSiG - Finanzierung entstehender Aufwände

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Erwartete Mehrkosten für Umsetzung von Anforderungen an IT-Sicherheit

Investitionskosten

in Verantwortung der Bundesländer

Betriebskosten

ggf. im Rahmen der Budgetplanung zu berücksichtigen

Personalkosten

heterogenes Anforderungsprofil

allgemeine Marktsituation schwierig

Kostenschätzung IT-Sicherheitsgesetz

Ergebnisse

- Krankenhäuser erwarten Mehrbelastungen in der Größenordnung von **2 bis 3 Mio. EUR jährlich**
- hiervon entfallen ca**. 60 %** auf **Investitionskosten** sowie **jeweils 20 %** auf **Betriebs-** und **Personalkosten**
- zusätzlicher Personalmehrbedarf (IT-Fachkräfte) liegt zwischen **1,9** (Grundversorgung) bis **16** (Universitätsklinikum) FTE (Maximalversorger und Universitätsklinika im Mittel mit stärkeren Belastungen – überproportionales Ansteigen der Belastungen ab ca. 1.000 Betten)
- Krankenhäuser erwarten insbesondere auch Umsetzung baulicher Anforderungen (Perimeterschutz) – Mehrbelastungen gerade am Anfang

ITSiG und EU-DSGVO

- gegenüber BSIG kürzere Meldefristen und wesentlich höhere Strafzahlungen im Falle eines Datenschutzverstoßes (2% bzw. 4% des Jahresumsatzes)
- Umgang mit Datenschutz-Folgeabschätzung noch offen (auch für bestehende Verfahren?)
- Muster-AV-Verträge: Arbeitsgruppe der Verbände (BvD, bvitg, DKG, GMDS, GDD) hat orientiert an DS-GVO Muster erstellt
- spezifische Ausgestaltung aufgrund konkreter Anforderungen notwendig, Beschreibung typischer Merkmale einer AV
- inhaltliche Anforderungen an einen AV-Vertrag, insbesondere:
  - Wartung / Fernwartung
  - Sozialdatenschutz
  - Forschung
  - Anonymisierung
  - Schweigepflicht vs. Datenschutz

ITSiG und EU-DSGVO (2)

- künftig nur noch Regelungen der EU-DS-GVO hinsichtlich der Auftragsverarbeitung (AV) gültig
- Überarbeitung betroffener Normen und Gesetze notwendig (z.B. Landeskrankenhaus- und Landesdatenschutzgesetze)
- weiterhin offene Punkte:
  - Umgang mit Zurückbehaltungsrecht
  - Schadensersatz- und Haftungsfragen
  - Umgang mit den Informationspflichten
  - Wünsche bzgl. einer Zweckänderung durch den Auftragnehmer, z. B. Weitergabe der Daten nach Pseudonymisierung/Anonymisierung
  - Fragen zu Sozialdaten
  - Datenschutz-Folgeabschätzun
  - Umgang mit Datenverarbeitung außerhalb EU/EWR, d. h. auch Umgang mit EU-Standardvertragsklausen

Vielen Dank für Ihre Aufmerksamkeit!

DEUTSCHE
KRANKENHAUS
GESELLSCHAFT