Digitalisierung im Fadenkreuz

DIGITALISIERUNG IM SOZIAL- UND GESUNDHEITSWESEN
VKD-LANDESGRUPPE MITTELDEUTSCHLAND, MERSEBURG, 12.04.2018

DR. GREGOR HÜLSKEN

Sicherheitslage 2017-2018 in Deutschen Krankenhäusern

- Aktuelle Situation
- Technische Herausforderungen
- Gesetzliche Veränderungen
- Praktische Ratschläge

- **Computervirus:** aktive Übertragung durch Nutzer, wurde abgelöst von Computerwürmern.
- **Computerwurm:** aktives eindringen in neue Systeme, liest Passwörter oder andere Daten aus.
- **Trojaner:** getarnt als nützliches Programm oder Informationen, Ausführung von Funktionen ohne Wissen des Nutzers, lädt andere Schadprogramme runter - > Verschlüsselung

Übertragungsarten: Download über Websites, Memory-Sticks, Lücken in Firewalls ….

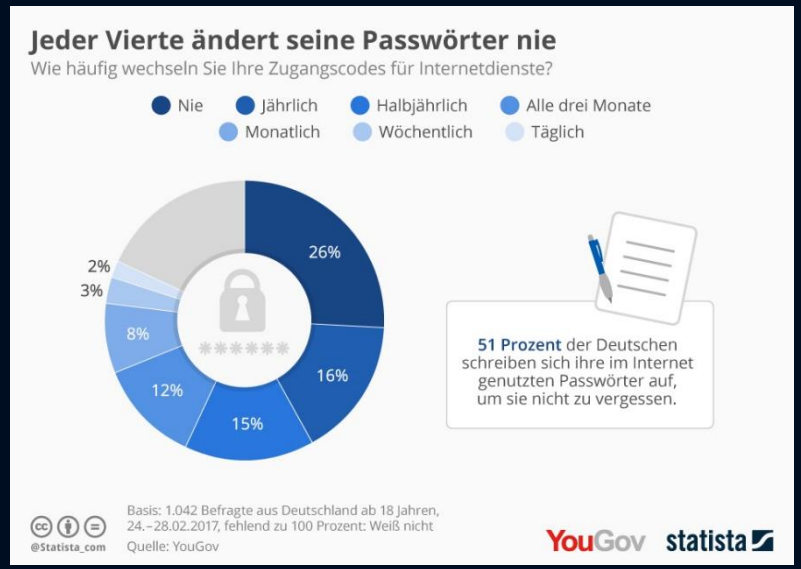
Aktuell: **IoT und Industrie 4.0 torpedieren die IT-Sicherheit auch in Krankenhäusern:**

Intelligente Steuerungen drängen nun in: isoliert betriebene Maschinen und Roboter, Dinge des täglichen Gebrauchs in Büro, Station, Labor, OP, und in allem, was sich elektrisch betreiben lässt.

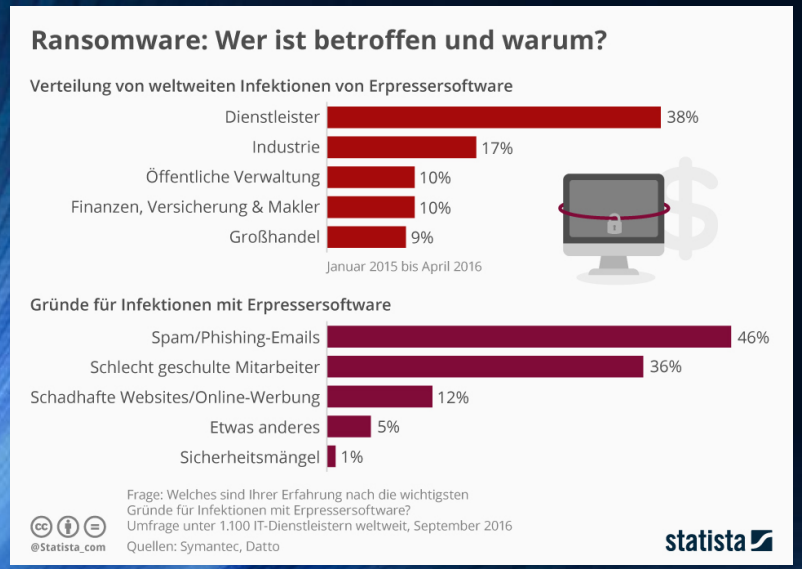
Aber: für diese kleinen Module gibt es oft keine Updates. Betriebssysteme für IoT-Geräte sind stark reduziert.

Eugene Kaspersky, Chef des russischen IT-Sicherheitsspezialisten Kaspersky Lab, definiert „IoT", die englische Übersetzung fürs Internet der Dinge, inzwischen neu: Das „Internet of Things" sei nun ein „Internet of Threats" – das „Internet der Gefahren".

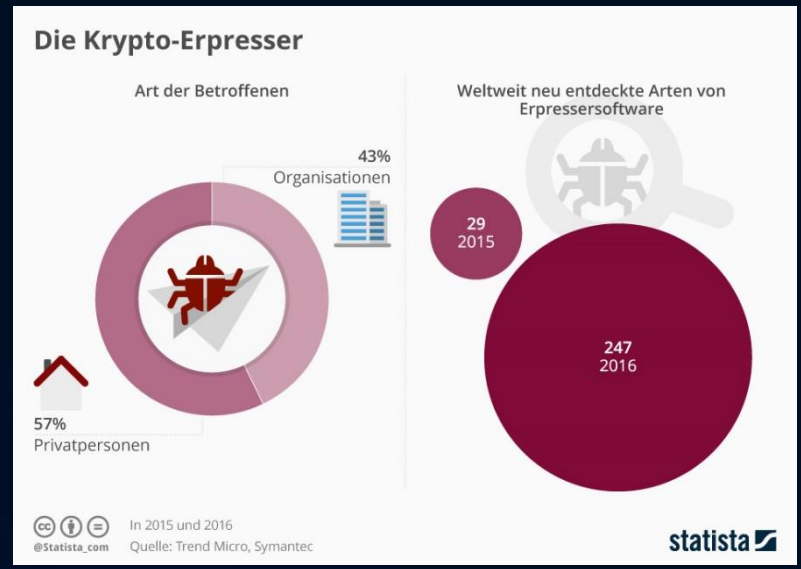
Mai 2017: "WannaCry" hat laut Europol innerhalb weniger Stunden über 200.000 Rechnersysteme, darunter auch die NHS, die Bahn und Autohersteller etc. lahmgelegt.



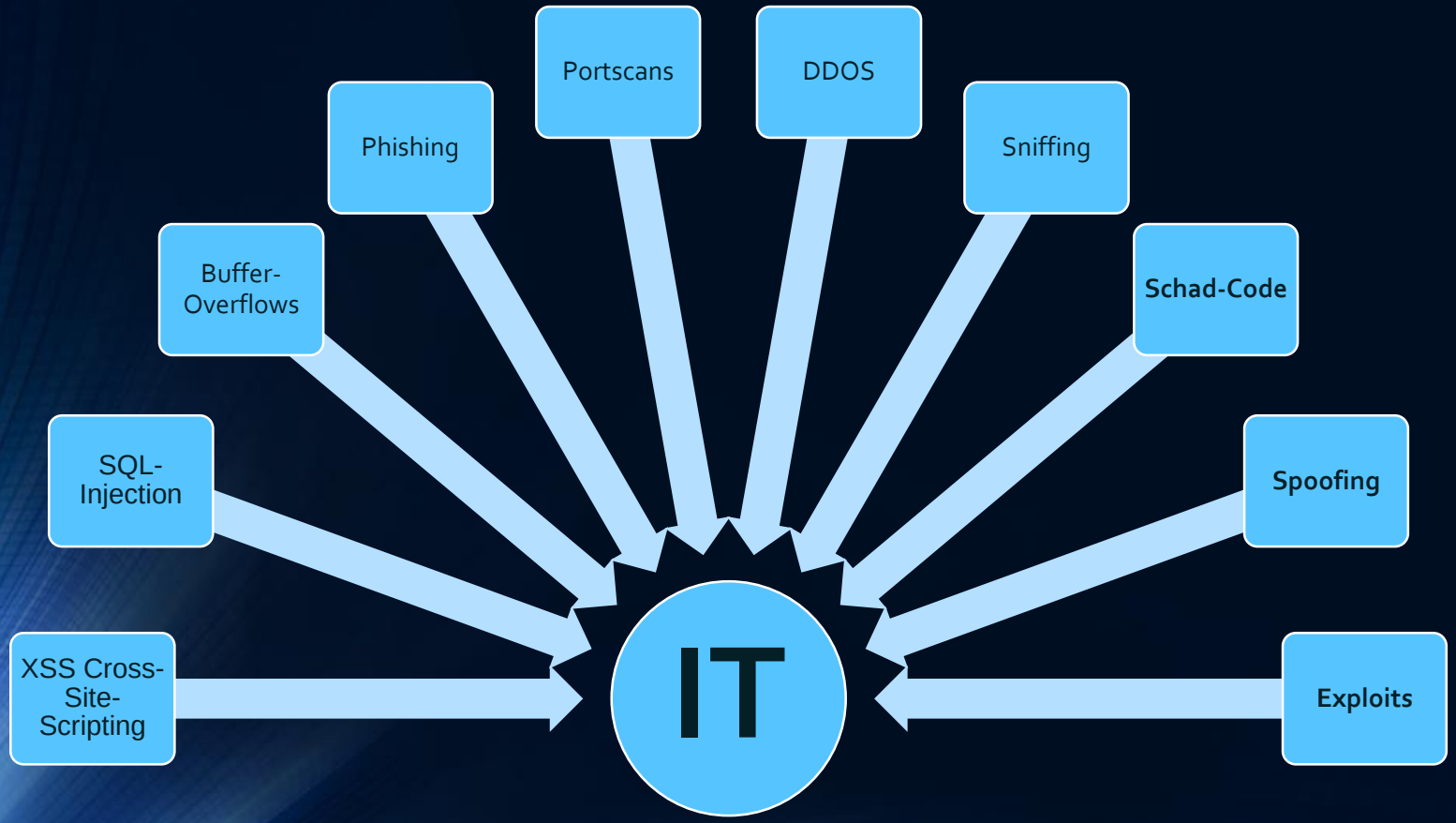
YouGov/Statista-Umfrage: 26 Prozent der Deutschen wechseln ihre Passwörter für Internetdienste nie. 16 Prozent der Befragten gaben an, einmal im Jahr ihre Zugangscodes zu ändern, 15 Prozent machen das jedes halbe Jahr, wie die Grafik von Statista zeigt.



Februar 2016: Verschlüsselungs-Trojaner legt IT der Krankenhäuser in Neuss, Kleve, Arnsberg, Kalkar lahm. Geschätzer Schaden: rd. 1 Mio Euro. (Quelle: https://heise.de/-3617880)



Angriffstechniken



Ziele:

- PCs
- Server
- Router
- Firewalls
- mDevices
- IoT-Devices

Welche Angriffsvektoren gibt es?

- E-Mail Anhänge
- Datenträger mit Viren, Würmern und Trojanern
- Webseiten über Phishing, Spamming
- Instant-Messenger-Nachrichten
- Pop-up-Fenster
- Direkt auf offene Ports oder Firewalls (Sniffing, Injections, Buffer-Overflows und Portscans)
- Social Engineering
- Lücken im Betriebssystem,
  → besonders bei IoT
- **→Neu: Schwächen in der Chip-Architektur**

Neu: Schwächen in der Chip-Architektur
Meltdown- und Spectre-Exploits

- Architekturschwäche in Intel und AMD-Prozessoren:
  d.h. so gut wie jedes Gerät ist betroffen
- Auslesen von Sicherheitsinformationen möglich
- Patches werden erarbeitet, Sicherheitslücken werden bedingt geschlossen. Erst die kommenden CPU-Generationen schaffen Abhilfe.
- Aber: Performanceeinbussen von 20%
- Wahrscheinlichkeit, betroffen zu sein, ist jedoch nicht so hoch, da der Exploit sehr aufwendig ist.

Quelle: https://www.computerwoche.de/a/hacker-inside,3332375

Mittwoch, 12:30 **Andrea Barthélémy, dpa** 32

Sicherheitslücken: Medizinische Geräte können gehackt werden

Bild: Pixabay / CC0

Medizinische Geräte wie Herzschrittmacher oder Insulinpumpen können gehackt werden – auch wenn die Gefahr gering ist. Anfälliger ist eher die IT in Krankenhäusern, die ein Einfallstor für Hacker zu medizinischen Überwachungsgeräten sein kann.

Ein Herzschrittmacher, der einen zu starken Stromstoß verabreicht. Eine Insulinpumpe, die plötzlich zu viel Insulin pumpt. Für Menschen, die mit einem medizinischen Hilfsmittel leben, ist die Vorstellung, dass das Gerät gehackt und manipuliert werden könnte, ein Horror. Wie angreifbar ist Medizintechnik? Und wie groß ist die Gefahr für Betroffene?

„Muddy Waters Capital und MedSec haben vorige Woche einen Untersuchungsbericht vorgelegt, laut dem die Ferndiagnosesysteme der Herzschrittmacher anfällig für Attacken von außen sein und gestört werden könnten, die Herzhelfer könnten gar außer Betrieb gesetzt werden. Konkret geht es dabei um den Transmitter Merlin@home, über den Daten aus den Implantaten ausgelesen werden können."

"Bei Tests konnten Angreifer in Einzelfällen zum Beispiel den nur ungenügend abgesicherten WLAN Schlüssel auf dem Gerät im Klartext auslesen und infolge dessen die Produkte bis hin zur falschen Abgabe von Medikamenten manipulieren."

30.08.2016 11:42 **Andreas Wilkens** 74

Sicherheit implantierbarer Medizintechnik: Herzschrittmacher von St. Jude Medical sollen hackbar sein

Defibrillatoren

Bild: St. Jude Medical

Streit mit harten Bandagen: Der US-amerikanische Medizingerätehersteller St. Jude Medical zofft sich mit dem Sicherheitsspezialisten MedSec und der Investmentfirma Muddy Waters Capital über die Sicherheit von lebenswichtigen Geräten.

05.08.2017 13:59 **Alexander Neumann** 90

Zwei Jahre alte Sicherheitslücken in Tomografen von Siemens UPDATE

Bild: Siemens

Die für die Sicherheit von Industrieanlagen zuständige US-Behörde ICS-CERT weist auf gravierende Sicherheitslücken hin, die die Sicherheit von Siemens' medizinischen Diagnosegräten zur Tomographie gefährden.

Das US-amerikanische Cyber Emergency Response Team für Industrial Control Systems (ICS-CERT) warnt vor mehreren, zwei Jahre alten Lücken, die die Sicherheit von Siemens' Tomografen für PET/CT (Positron Emission Tomography/Computed Tomography) und SPECT (Single-Photon-Emissions-Tomographie) gefährden. Mit diesen Geräten zur molekularen Bildgebung lassen sich Tumore, aber auch Anzeichen von Hirnkrankheit erkennen.

„Die anfälligen Systeme laufen unter Windows 7; und es gibt bereits Patches von Microsoft und HP/Persistent Systems, den Herstellern der betroffenen Software, aber bisher offenbar nicht für die medizinischen Geräte. Über diese Lücken können Angreifer ein System übers Netz hinweg übernehmen. Das für die Sicherheit von Industrieanlagen zuständige ICS-CERT stuft sie in die oberste Gefahrenkategorie ein (CVSS 9,8 von 10) und empfiehlt deshalb unter anderem, die Geräte als Sicherheitsmaßnahme vom Netz zu trennen und möglichst im Standalone-Modus zu betreiben."

https://m.heise.de/newsticker/meldung/Sicherheit-implantierbarer-Medizintechnik-Herzschrittmacher-von-St-Jude-Medical-sollen-hackbar-sein-3307510.html
https://m.heise.de/newsticker/meldung/Sicherheitsluecken-Medizinische-Geraete-koennen-gehackt-werden-4007227.html
https://m.heise.de/security/meldung/Zwei-Jahre-alte-Sicherheitsluecken-in-Tomografen-von-Siemens-3793673.html

Risiko: „drahtlose Vernetzung von Geräten“ im Krankenhaus

Beispiele:

- Geräte-Hersteller Johnson & Johnson musste 2016 mehr als 11.000 Besitzer von vernetzten Insulinpumpen anschreiben, weil es Software-Sicherheitslücken gab
- Smith Medical musste 2017 bei ihren Insulinpumpen die Software nachbessern.
- St. Jude Medical rief 2017 fast eine halbe Million Träger von Herzschrittmachern oder Defibrillatoren in die Kliniken, um ihre Geräte dort mit sicheren Updates zu versorgen

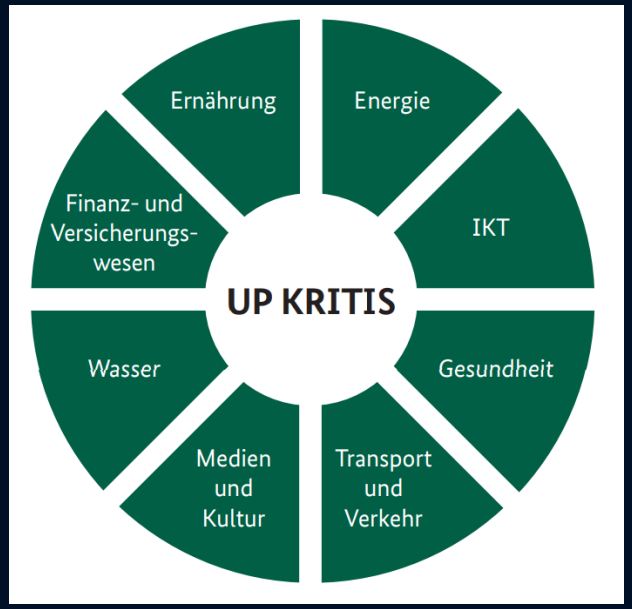
Medizingeräte sind teuer, oft viele Jahre lang im Einsatz und deshalb nicht zwingend auf dem neuesten - oder einem nachrüstbaren - Stand. Die drahtlose Vernetzung von Geräten und die Möglichkeit, berührungsfrei auf sie einzuwirken, bringt therapeutisch viele Vorteile.
Aber auch neue Angriffsmöglichkeiten für Hacker!

https://www.aerztezeitung.de/praxis_wirtschaft/e-health/telemedizin/article/960786/cybercrime-echte-life-hack.html?sh=1&h=461545393

Was wird getan?

IT-Sicherheitsgesetz & UP KRITIS

Der Umsetzungsplan (UP) KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen, insbesondere dem BSI



- Förderung der Robustheit der kritischen Prozesse, insbesondere der IKT-Anteile
- Austausch über aktuelle Vorkommnisse
- Bewertung von Risiken, Abhängigkeiten und der Cyber-Sicherheitslage
- Erarbeitung gemeinsamer Dokumente und Positionen
- Auf- und Ausbau von Krisenmanagementstrukturen
- Koordinierte Krisenreaktion und -bewältigung
- Durchführung von Notfall- und Krisenübungen
- Gemeinsames Handeln gegenüber Dritten

https://www.planet-wissen.de/video-blackout--ploetzlich-ohne-strom-100.html

- 2005: Umsetzungsplan KRITIS beschlossen, in der Folge sind Arbeitsgruppen aus Verwaltung und Wirtschaft zusammen getreten.
- 18. Februar 2014: **Kooperation erneuert** und Dokument **Umsetzungsplan Kritis beschlossen**.
- 12.06.2015: „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" vom Bundestag verabschiedet (**IT-Sicherheitsgesetz**)
- 3. Mai 2016: der erste Teil der BSI-Kritis - Verordnung **tritt in Kraft**
- 02.06.2017: Bundestag beschließt: ab 30.000 Krankenhausfällen "**kritische Infrastruktur**"
- 19.12.2017: Identifikation betroffener Einrichtungen, Anforderungen im Gesundheitswesen.* → Einhaltung der Mindeststandards
- 03.05.2018: Energieversorger, die Wasserwirtschaft, Unternehmen des Informations- und Kommunikationssektors und dem Nahrungsmittelbereich müssen ITSiG umgesetzt haben
- Mai 2019: Kritis-KH müssen Nachweis geeigneter Maßnahmen (ISO 27001) erbringen

- 4.3 Hinweise zum Schwellenwert Mit der Festlegung von 30.000 vollstationären Behandlungsfällen als Schwellenwert werden voraussichtlich 5 - 10% aller Krankenhäuser in Deutschland betroffen sein. Mit der absehbaren Weiterentwicklung der gesetzlichen Grundlage und dem allgemeinen Ziel, bei zunehmender Digitalisierung die IT-Sicherheit in allen Bereichen des gesellschaftlichen Lebens zu verbessern, wird eine künftige Absenkung des Schwellenwertes erwartet.
- Grundsätzlich sind IT-Störungen zu melden, die zu einem Ausfall oder der Beeinträchtigung der Versorgungsdienstleistung geführt haben oder hätten führen können.
- Die Meldung an das BSI hat „ohne schuldhaftes Verzögern" zu erfolgen.

IT-Sicherheitsgesetz: Sektor Gesundheit – Bereich Krankenhäuser

IT-Sicherheitsgesetz: Schutz Kritischer Infrastrukturen - Umsetzungshinweise der DKG: Krankenhäuser als kritische Infrastrukturen - Umsetzungshinweise der Deutschen Krankenhausgesellschaft.

Ab 30.000 stationären Fällen müssen bereits ab 2018 Verpflichtungen zum Meldeverfahren umsetzen

Roland Berger Studie

Aber: Die „Krankenhausstudie 2017" von Roland Berger zeigt, knapp 60 Prozent der Kliniken erzielen zu wenig Überschuss, um diesen in moderne Infrastrukturen und IT-Sicherheit investieren zu können.*

*https://www.kma-online.de/aktuelles/it-digital-health/detail/mittel-zur-digitalisierung-und-it-sicherheit-in-kliniken-fehlen-a-35214

Zentrale Meldestelle für IT-Sicherheitsvorfälle im IT-Lagezentrum im BSI.

Die Welt, 28.03.2018

Kein Geld für IT-Sicherheit

Der Medizin-Wirtschaftsinformatiker Prof. Thomas Jäschke vom Institut für Sicherheit und Datenschutz im Gesundheitswesen ergänzt, in vielen Kliniken gebe es **Geldmangel** im IT-Bereich. Teils seien noch veraltete Betriebssysteme im Einsatz, für die es gar keine Patches oder Updates mehr gibt. Erhöhte Sicherheits-anforderungen müssen laut Gesetz (KRITIS) nur rund **90** von **2.000** Krankenhäusern erfüllen – weil sie mehr als 30.000 vollstationäre Fälle haben. Dabei könne der Ausfall eines kleineren Krankenhauses in **ländlicher Umgebung** – ohne Alternativen im näheren Umkreis – schwerwiegender sein als der eines großen in einem Ballungsgebiet, argumentiert Jäschke.

https://www.welt.de/gesundheit/article174960479/Digitale-Medizin-Koennen-Hacker-den-Herzschrittmacher-stoppen.html

Kurzfristige Handlungsempfehlungen

1. Überprüfen der Patch-Stände Router, Server, PCs, AV-Systeme, Backup
2. Überprüfen, ob White-Listing / Black-Listing realisiert werden kann
3. **Identifikation aller IT-kritischen Patientenversorgungsprozesse der stationären Versorgung.**
4. **Organisatorische Konzepte für einen IT-Sicherheitsvorfall → Leitfaden für IT-Notfälle**
5. **Technische Konzepte für einen IT-Sicherheitsvorfall → Ausfallsystem**
6. Dort wo medizinische Daten verarbeitet werden, darf kein Zugriff auf das Internet möglich sein.
7. Netztrennung: medizinische Geräte haben keine Internetverbindung! Sie werden in eigenen Netzen betrieben.
8. Private Internetnutzung nur an ausgewiesenen Geräten in speziellen Netzen!
9. Veraltete Betriebssysteme haben nichts im Netz zu suchen.

Plan - B

Mittelfristige Handlungsempfehlungen

1. Aufbau Information Security Management Systems (ISMS)
2. Einbindung des IT-Risikomanagements in das Unternehmensrisikomanagement
3. Zertifizierung nach ISO 27001 – unabhängig von der Fallzahl!

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Gregor Hülsken

Arzt ◆Medizinische Informatik

FOM Hochschule für Oekonomie und Management

IT-Managementberatung im Gesundheitswesen

Gregor.Huelsken@Dr-Huelsken.de