Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Cyber Attacken im Gesundheitswesen

Interne Netzwerke - löchrig wie Schweizer Käse

Information Security in Health Conference

Rotkreuz – 22. Juni 2017

Martin Darms
Darms Engineering
www.darms.ch

FH Zentralschweiz

EFQM
Recognised for excellence
5 star - 2015

Agenda

- Einleitung
- Geschichtliches / Übersicht über aktuelle Bedrohungen
- Neueste Forschung und ausgewählte Studien
- Gefährdung Schweizer Spitäler gegenüber Cyberangriffen
- Reales Beispiel
- Wertvolle Tipps, Empfehlungen und Gegenmassnahmen

Interne Netzwerke - löchrig wie Schweizer Käse

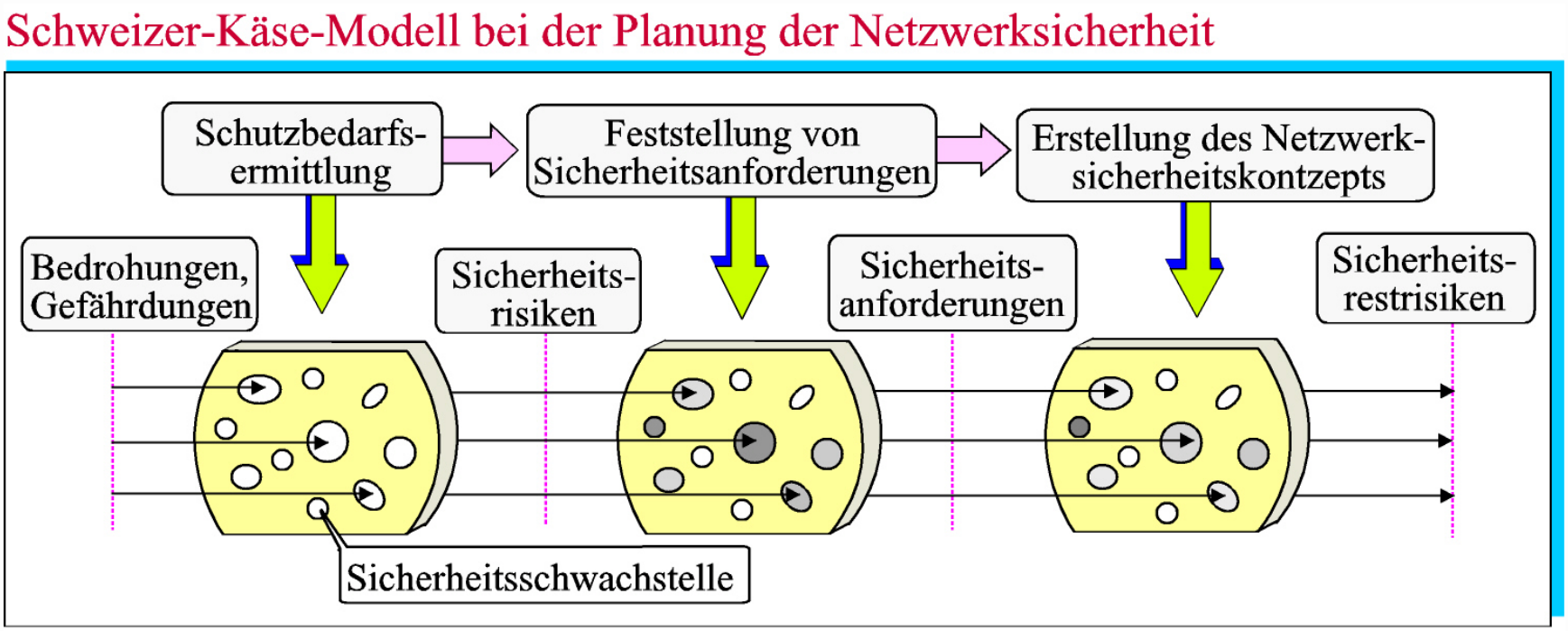


Abb. 6.2-6 im Fachbuch - Badach, A., Rieger, S.: Netzwerkprojekte, HANSER

Source [P6]

Wenn man versucht Probleme zu beheben…

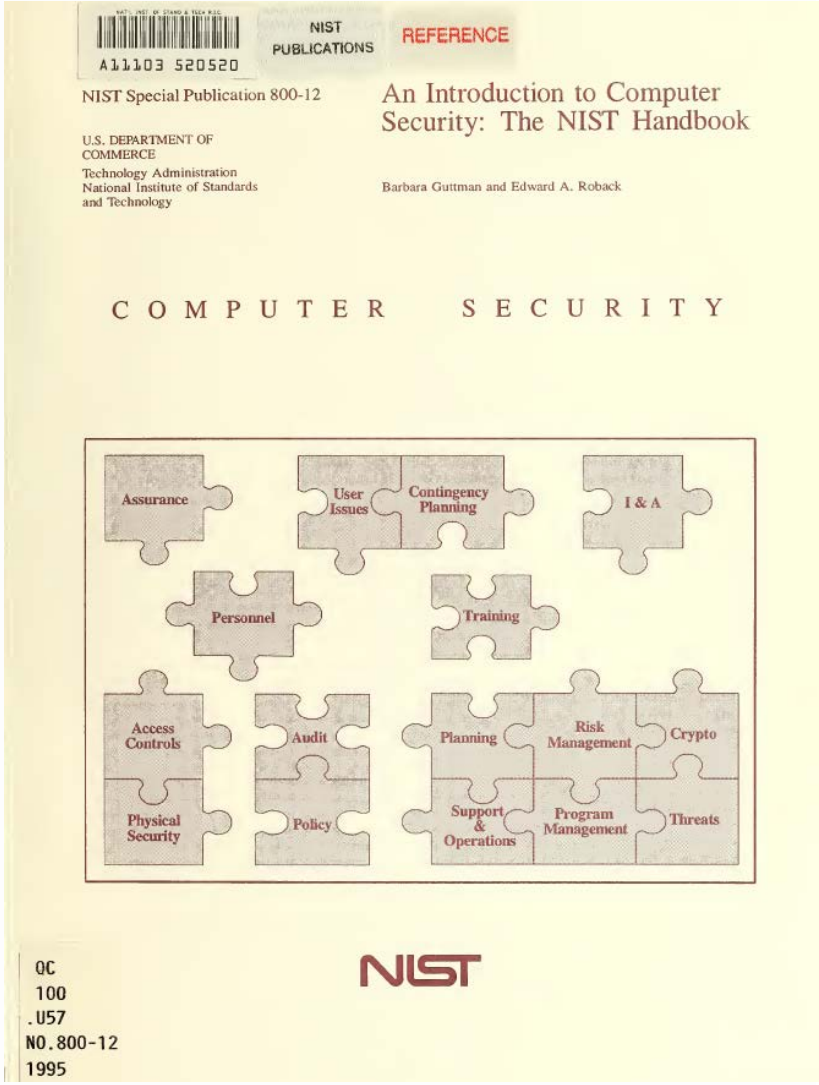
Or Security

Source: https://youtu.be/75wa8Lx4yc4

Einleitung

- Wie viele von Ihnen wurden noch NIE gehackt? (Geschäftlich oder Privat)

- Ist die IT Sicherheit ein neues Gebiet?



Ref[9]

Einleitung

Ist WannaCry neu?

Technisch: ja.

Kombination:
Wurm und Ransomware

WannaCry ein Déjà-vu-Erlebnis?

Veröffentlicht: 18.05.2017

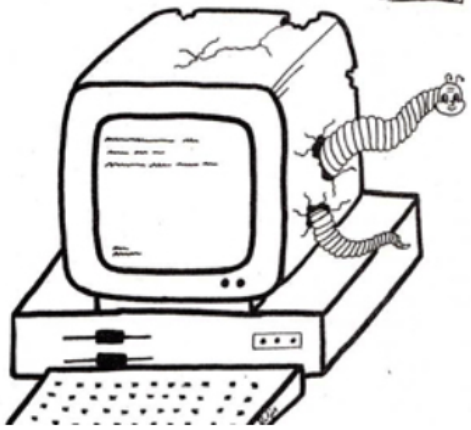
WannaCry ein Déjà-vu-Erlebnis?

Computer-Sabotageprogramme

Weltweite Erpressung mit AIDS-Informationsdiskette

Fr. 13.

Ein bislang einzigartiger Fall von Computer-Kriminalität beschäftigte Ende 1989 Scotland Yard und das FBI. Das Medium: Eine 5,25-Zoll-Diskette mit einem Sabotageprogramm — einem sogenannten Trojanischen Pferd. Das Ende der Geschichte: Die Verhaftung des Initiators und eine große Anzahl geschädigter Computeranwender, die Daten nicht mehr auffinden und Programme nicht mehr bearbeiten konnten.



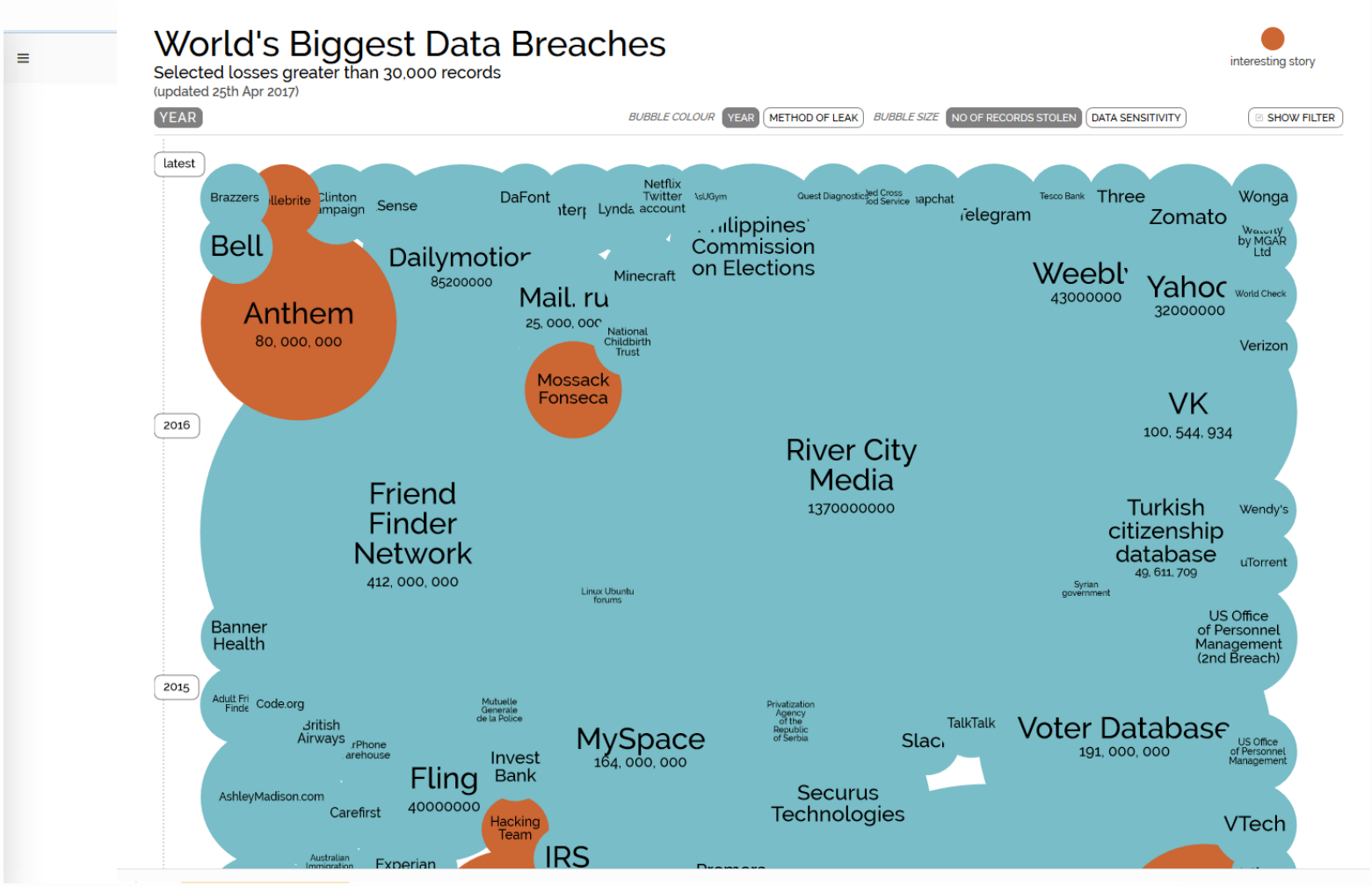
Ein spektakulärer Rasomware-Fall ereignete sich bereits 1989

In der letzten Woche ereigneten sich bekanntermaßen die weltweiten Angriffe durch "WannaCry". Zahlreiche Krankenhäuser in England waren betroffen und mussten teilweise den Betrieb einstellen oder reduzieren.

Dieses Phänomen ist jedoch nicht neu. Bereits 1989 ereignete sich ein spektakulärer Cyberangriff mit einem Trojaner in Europa, Afrika und Australien. Was heute eher belustigend klingt, war damals die gängige Methode: Die Verbreitung erfolgte über Disketten (in diesem Fall von 20.000!) . Das eingeschleuste Programm sollte angeblich über das persönliche AIDS-Risiko informieren, entpuppte sich aber als Erpressungssoftware.

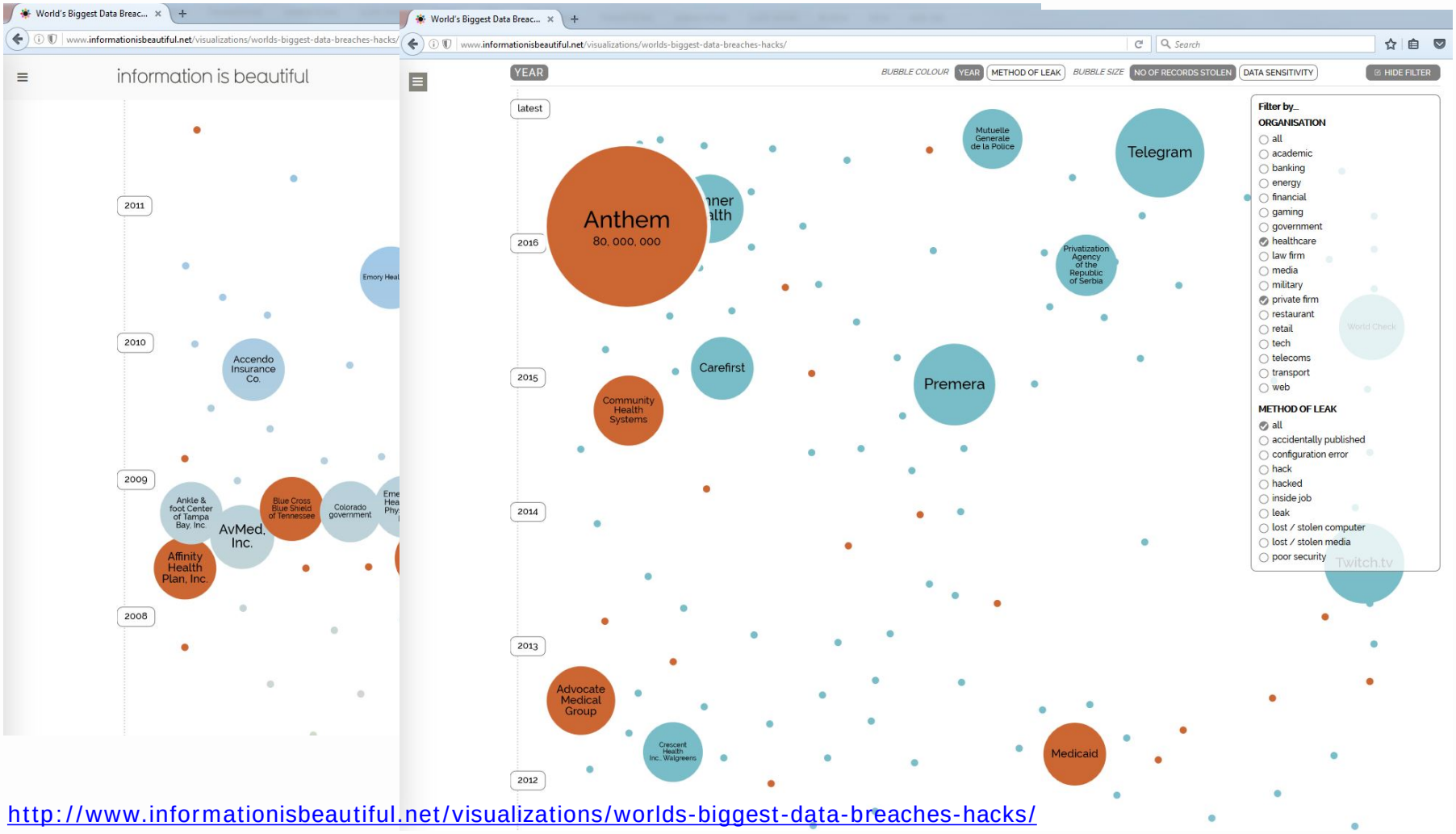
Ref[13]

Cyberattacken Generell: 2005 – 2017



Ref[10]

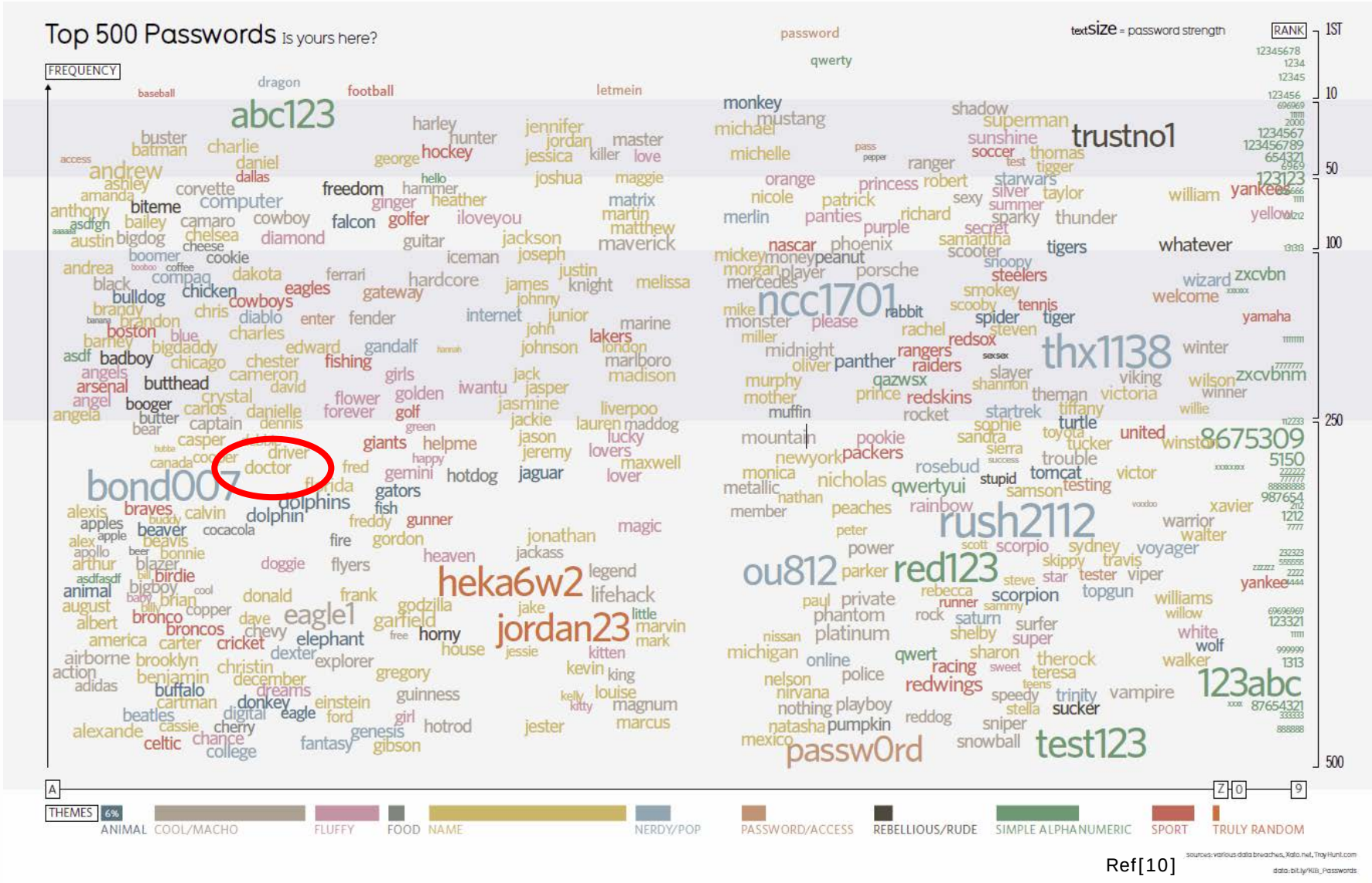
Cyberattacken im Gesundheitswesen: 2008 – 2017



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

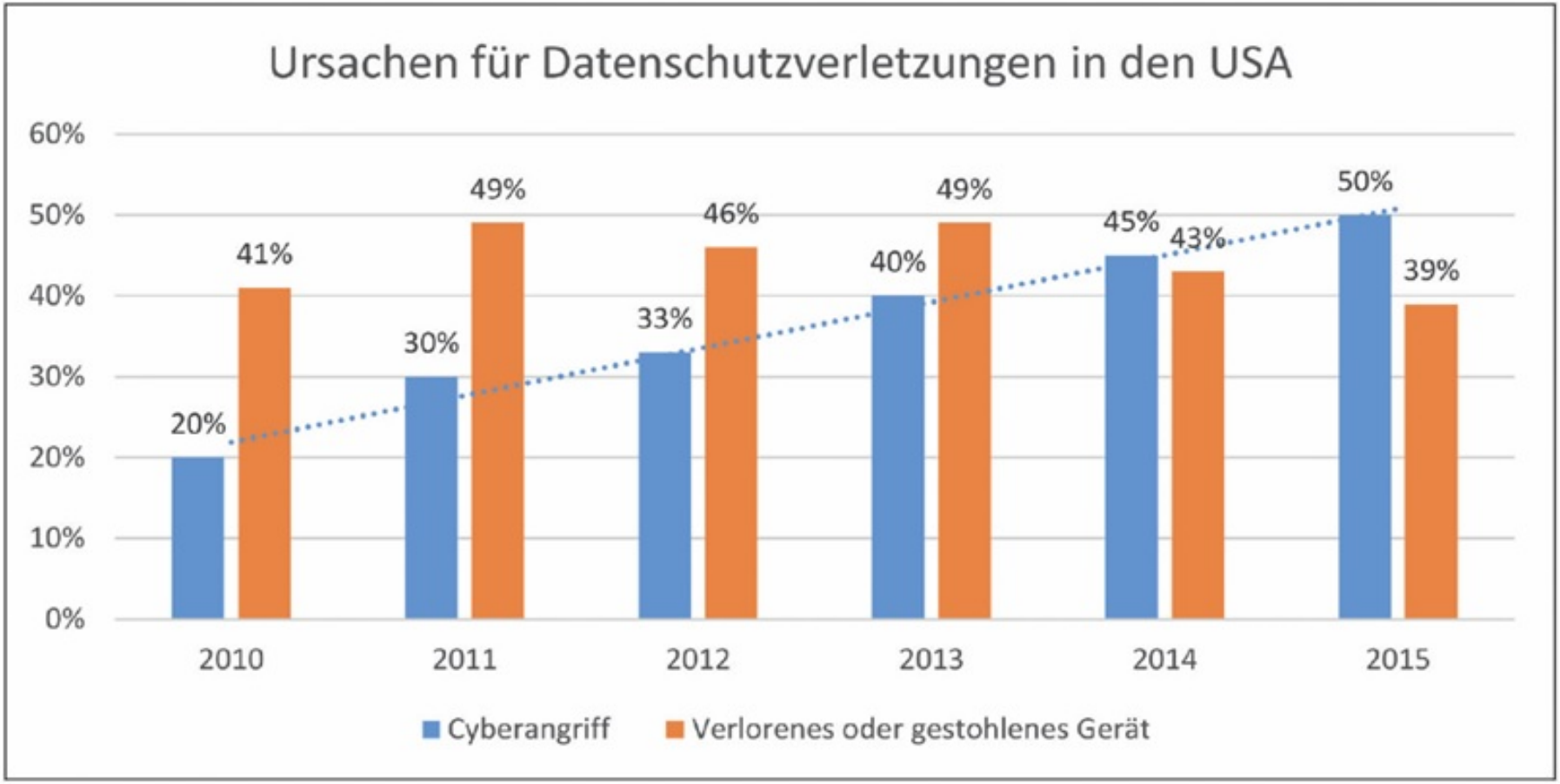
Ref[10]

Unsichere Passwörter



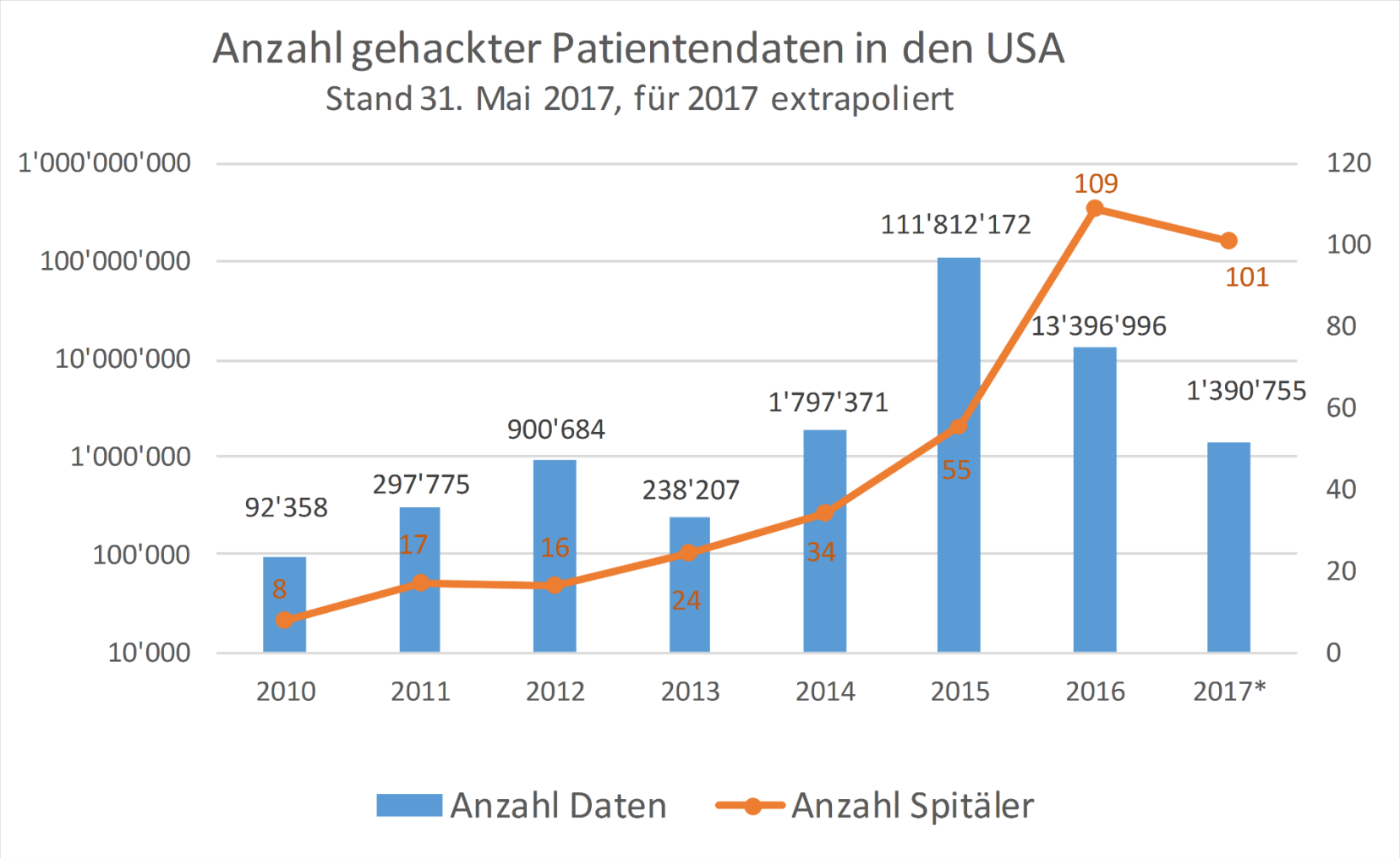
Ref[10]

Datenschutzverletzungen



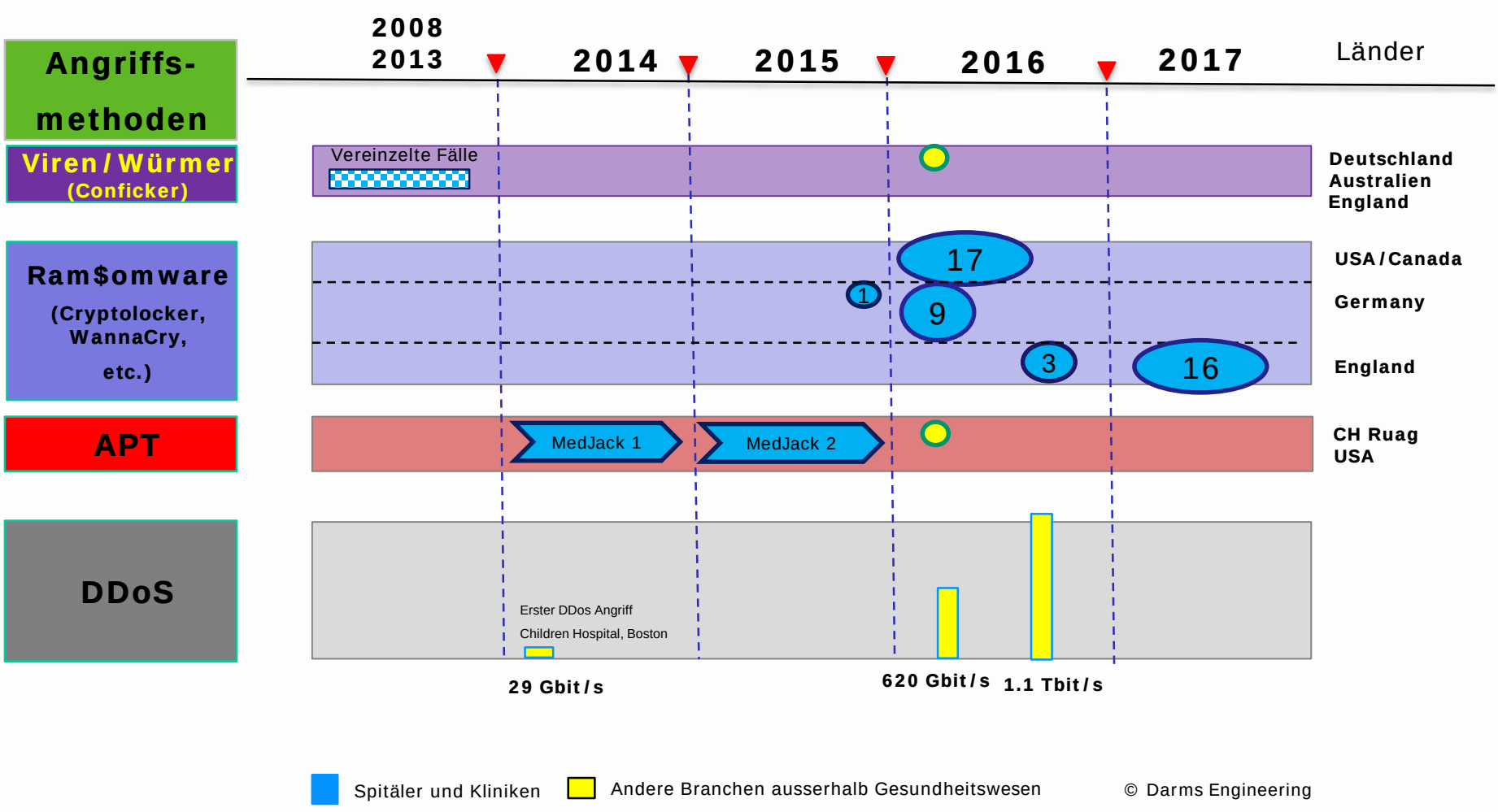
Ref[1]

Cyberangriffe nehmen weltweit stetig zu



Ref[1]

Geschichte von Cyberattacken aufs Gesundheitswesen



Geschichte von Cyberattacken aufs Gesundheitswesen (Spitäler)

- Bis 2008: Wenig bis keine Vorfälle
  - Virus / Malware
- Keine (öffentlich bekannten) erfolgreichen Angriffe in der Schweiz aufs Gesundheitswesen
- 2014: Hacktivist 29 GBit/s
- 2016:
  - Februar USA, Hollyword Presbyterian Medical Center, Los Angeles, zahlten 17k$ Lösegeld
  - Februar D, Neuss Krankenhaus und 5-6 weitere Krankenhäuser
  - September «Krebs On Security» war Ziel mit 620 Gbit/s
    1.1 Tbit/s mit Hilfe der IoT (u.a mit Hilfe von gekapperten Sicherheitskameras)
  - Oktober GB: Ost-England (mehr als 100 Operationen) wurden verschoben – Virus
- 2017:
  - Mai: WannaCry, GB, 16 Gesundheits-Institutionen der NHS waren betroffen, weltweit in den Medien, verschiedene Branchen (Transport, Industrie) waren ebenfalls betroffen

Beispiel: 30. Okt - 2. Nov 2016 / Diana Princess of Wales Hospital

BBC Sign in | News | Sport | Weather | Shop | Earth | Travel | M

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts

England | Regions | Humberside

Lincolnshire operations cancelled after network attack

31 October 2016 | Humberside

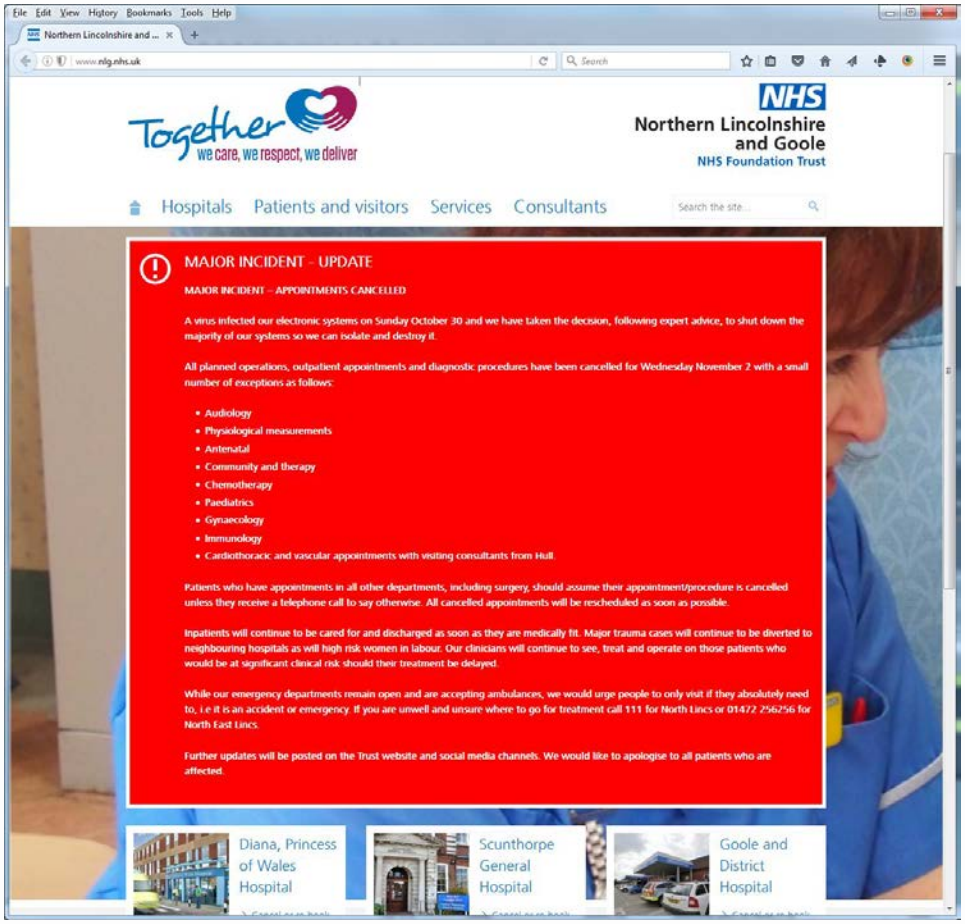
Share

Hospitals in Grimsby, Scunthorpe and Goole, Boston and Lincoln among those hit by the virus

Hundreds of planned operations and outpatient appointments have been cancelled across Lincolnshire after an NHS computer network was attacked.

Northern Lincolnshire and Goole NHS Foundation Trust (NLAG) said systems were infected with a virus on Sunday, with it treated as a "major incident".

The trust, which runs hospitals in Goole, Grimsby and Scunthorpe, said the measures would remain into Tuesday.



Source Ref[14]

National Hospital Service (NHS) England
Gründe für den «Erfolg» von WannaCry in England

"For example, East Sussex Healthcare has 413 XP machines, Sheffield Children's Hospital has 1,290, and Guy's and St Thomas' NHS Trust in London has an incredible 10,800 computers running Windows XP, all of which are not receiving security updates."
Ref [17]

New England Journal of Medicine Ref. [16]
Cancellation of his open-heart surgery:
"I'd been waiting for 18 months for this surgery, I was shaved ready for the operation but then the consultant said there had been a hack and there was nothing they could do. He was worried that if I needed a lot of blood for the operation, they wouldn't be able to access the right kind on their systems."

The British press discovered that the NHS IT system was particularly vulnerable to the WannaCry infection since, despite cybersecurity warnings, former Prime Minister David Cameron had elected to cut costs by scrapping a £5.5 million ($7.07 million) annual deal with Microsoft to provide ongoing security support for the 14-year-old Windows XP system that's still running on several hundred thousand NHS hospital computers.

Was ist eigentlich möglich?

- Fast alles ist möglich!
  - USB Stick / oder das E-Zigarette Beispiel
  - Drohne fällt runter
  - Lungenaspirator
  - Jeep Cherokee ferngesteuert
  - Eindringen via Gebäudesteuerung (Klinik Gut, Ref[15])
  - ...
  - MedJack ... (später)
  - HW Sensoren werden manipuliert → Fehlverhalten eines Systems

→ Bis heute, gab es zum Glück, keine Hackerangriffe die zur Folge hatte, dass Patienten daran gestorben sind.

→ Paul Vixie, Internet Innovator, hat ebenfalls bestätigt, dass seines Wissen nach, bisher noch keine Todesfälle in Spitälern aufgrund von Hackern gegeben hat (http://internethalloffame.org/inductees/paul-vixie)

Security und Safety - Standards

- Keine Safety kann garantiert werden ohne Security
- Wieso ist IT Security wichtig für MedTech Firmen und Spitäler?
  - Spitäler brauchen den Zugriff auf ihre Systeme
  - Als Betreiber der MedTech System sind Sie verantwortlich für die Sicherheit der Systeme
  - Reputation und Image Schaden
- FDA Post market Management of Cybersecurity in Medical Devices (Ref [7])
- Cybersecurity for Medical Imaging (Ref [8])
- ISO 80001-1:2010-10 Application of risk management for IT-networks incorporating medical devices
- ISO 2700x, ISO/IEC 27799:2008
- SIGS: Security Technical Implementation Guide (z. B. USAF)

Studien

- Gefährdung Schweizer Spitäler gegenüber Cyberangriffen, Ref [1]
  Einige Spitäler sind 10 Mal schlechter geschützt als andere.
  Die meisten Schwachstellen (Vulnerabilitäten) wurden bei medizinischen Geräten gefunden!

- MedJack 1 and 2. Medical Device Hijacked, Ref [2], [3]
  Alte medizinische Systeme mit Windows XP wurden ohne das Wissen des Spitals infiziert.
  Vulnerabilities MS08-067.

- Space, the Final Frontier for Cybersecurity? Ref [4]
  Gefahr vom Weltraum, Satelliten

MedJack - APT's in Spitälern

MedJack 1 and 2

- APT in Krankenhäusern!

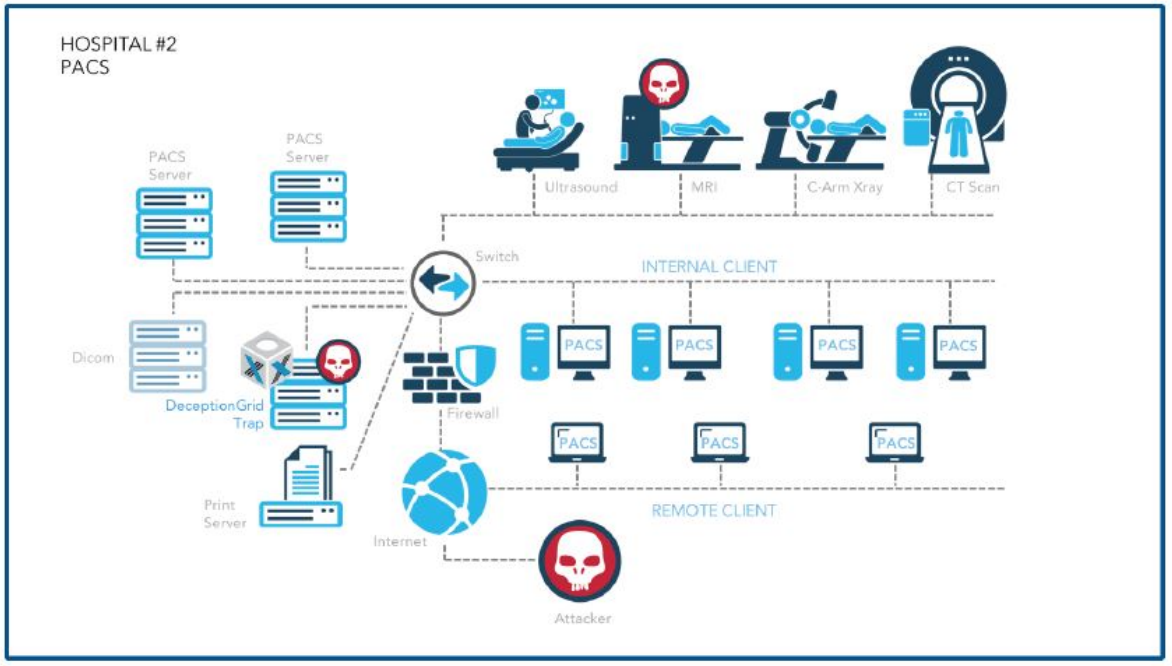
"MEDJACK.2 adds a new layer of camouflage to the attacker's strategy. New and highly capable attacker tools are cleverly hidden within very old and obsolete malware. It is a most clever wolf in very old sheep's clothing. They have planned this attack and know that within healthcare institutions they can launch these attacks, with impunity or detection, and easily establish backdoors within the hospital or physician network in which they can remain undetected, and exfiltrate data for long periods of time."
– Moshe Ben Simon , TrapX

Ref [3]

Am dem Beispiel PACS

Fast jedes Krankenhaus verfügt über mindestens ein zentrales PACS-System. Wenn ein Angreifer innerhalb des PACS Fuß fassen kann, haben sie Netzwerkpfade zu jedem anderen möglichen System im Krankenhaus sowie viele der externen aber vernetzten Einheiten.

Angreifer haben Backdoors eingebaut.



Ref [3]

Motivation

Welche Gründe oder Motivationen gibt es um medizinische Geräte und Spitäler zu hacken?

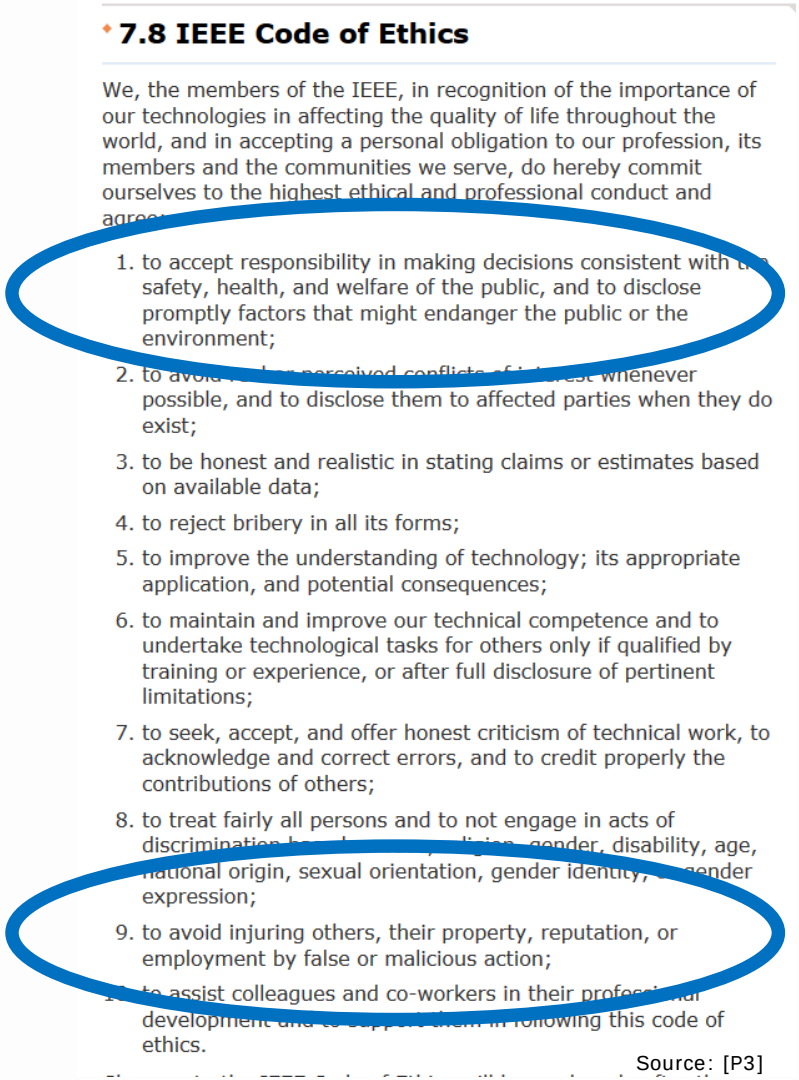
[P5]

- 3 Gründe: Money, Money, Money
- Ansehen / Ruhm / Prestige
- Sie sind einfach zu hacken (Ref [2] and [3])
- Aktienmanipulationen, St. Jude Medical Case (Ref [5])
- Mangel an Verständnis
- Nicht bewusst über die möglichen Konsequenzen sein (möglicher Tod von Personen)

Motivation

Welche Gründe gibt es, medizinische Geräte und Spitäler NICHT zu hacken?

- Ethische Gründe
- IEEE Code of Ethics
- Man möchte niemanden verletzen
- Ich könnte eines Tages das Gerät selbst brauchen?
- Und hoffentlich bald, medizinische Geräte und Spitäler im Allg. sind schwierig (oder fast nicht möglich) zu hacken



7.8 IEEE Code of Ethics

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree

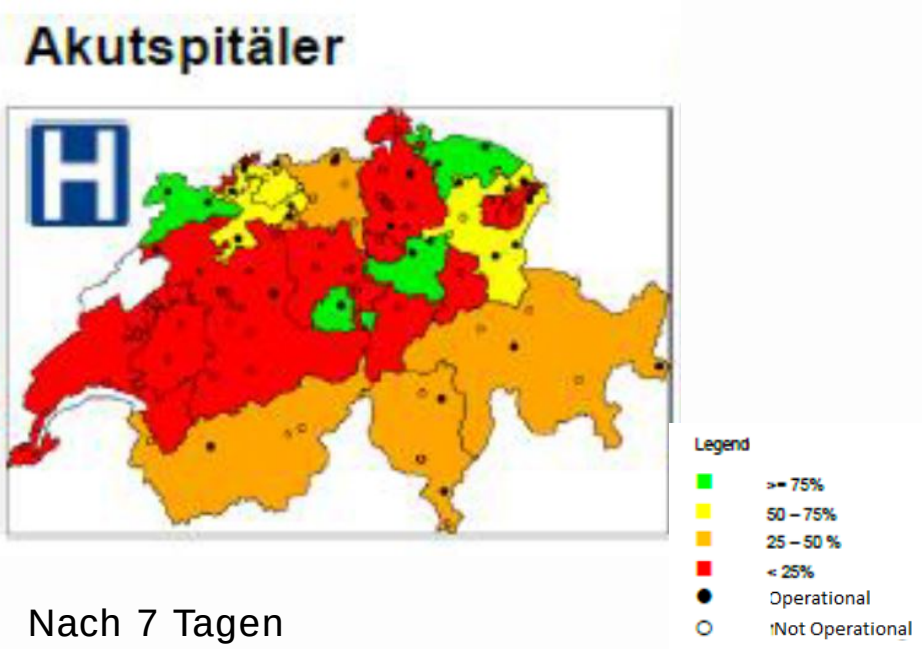
1. to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology; its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

Source: [P3]

Strom-Mangellage / Blackout

Was geschieht wenn Krankenhäuser für mehrere Tage keine externe Stromversorgung mehr haben (aufgrund von Hackerattacken)?

Nach 4 Tagen



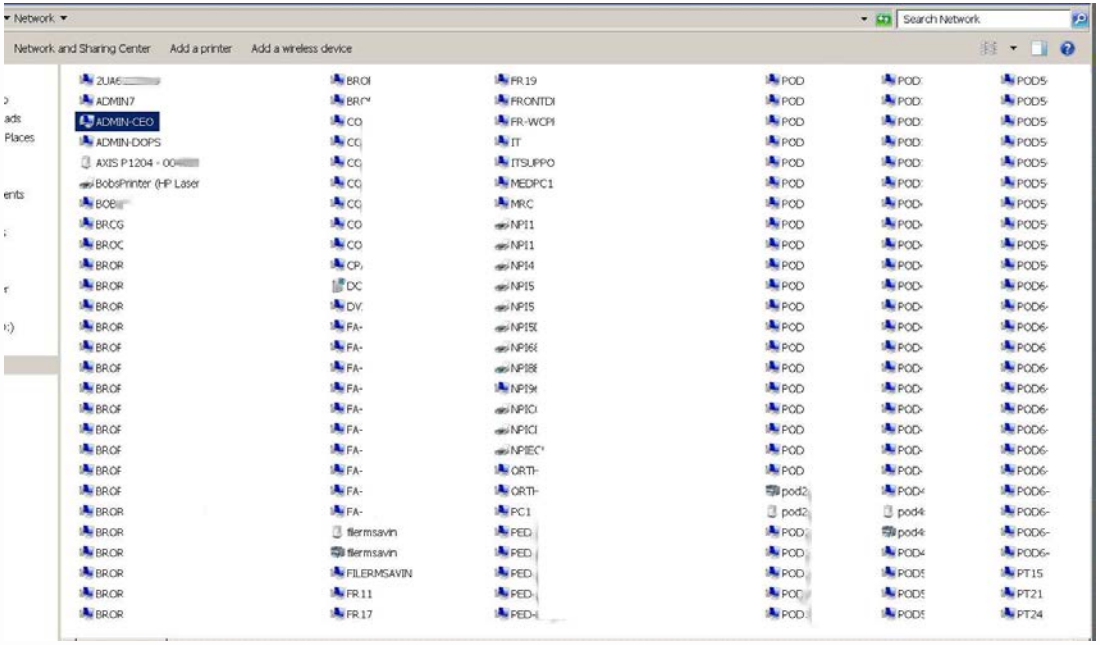
Nach 7 Tagen

Source: [P1]

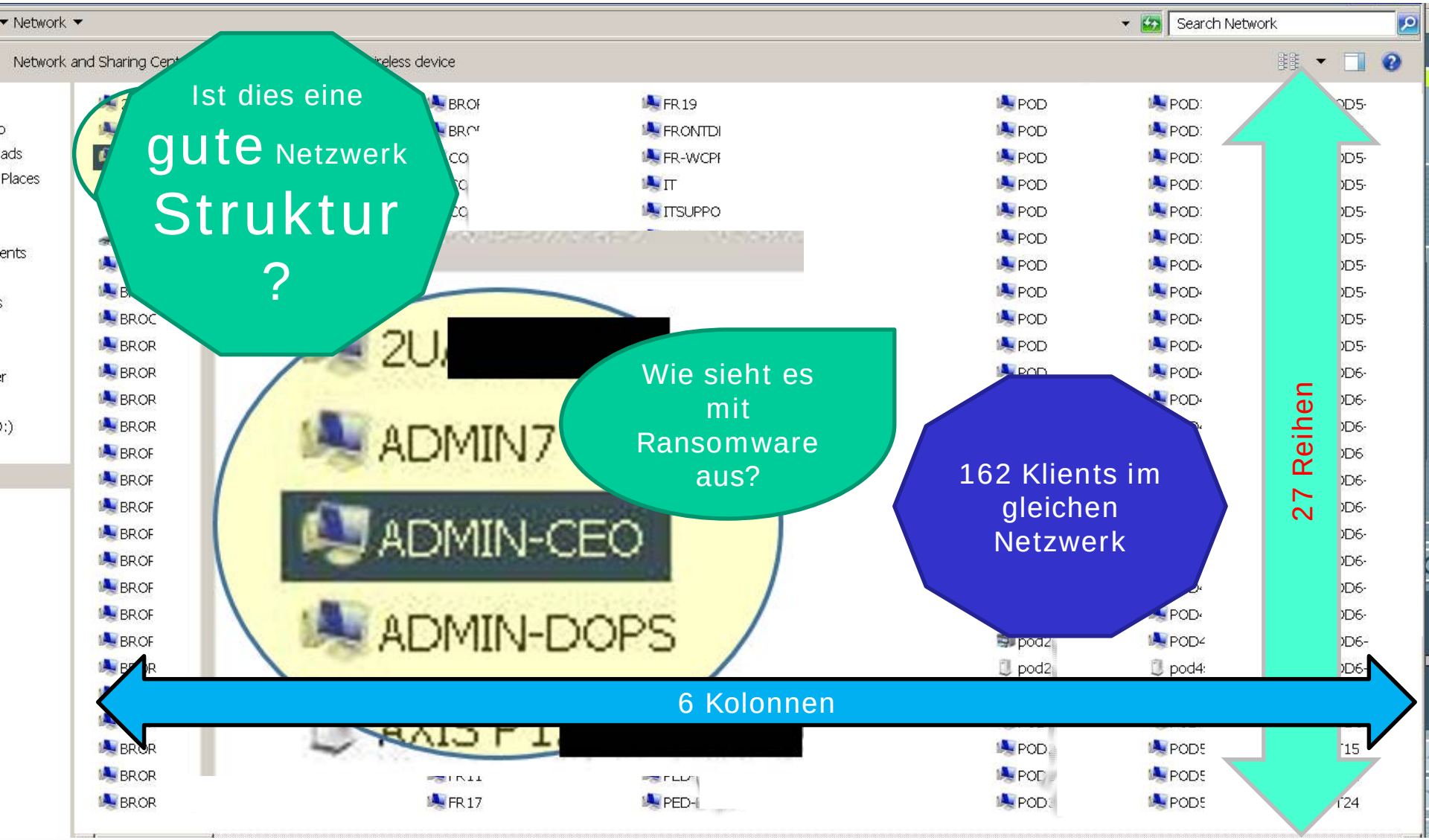
Lese-Empfehlung: Blackout, morgen ist es zu spät, Ref [9]

Reales Netzwerk-Beispiel

Starten wir mit einem realen Beispiel eines Spitalnetzwerks



Reales Netzwerk-Beispiel



Ausgewählte Resultate der Studie (I)

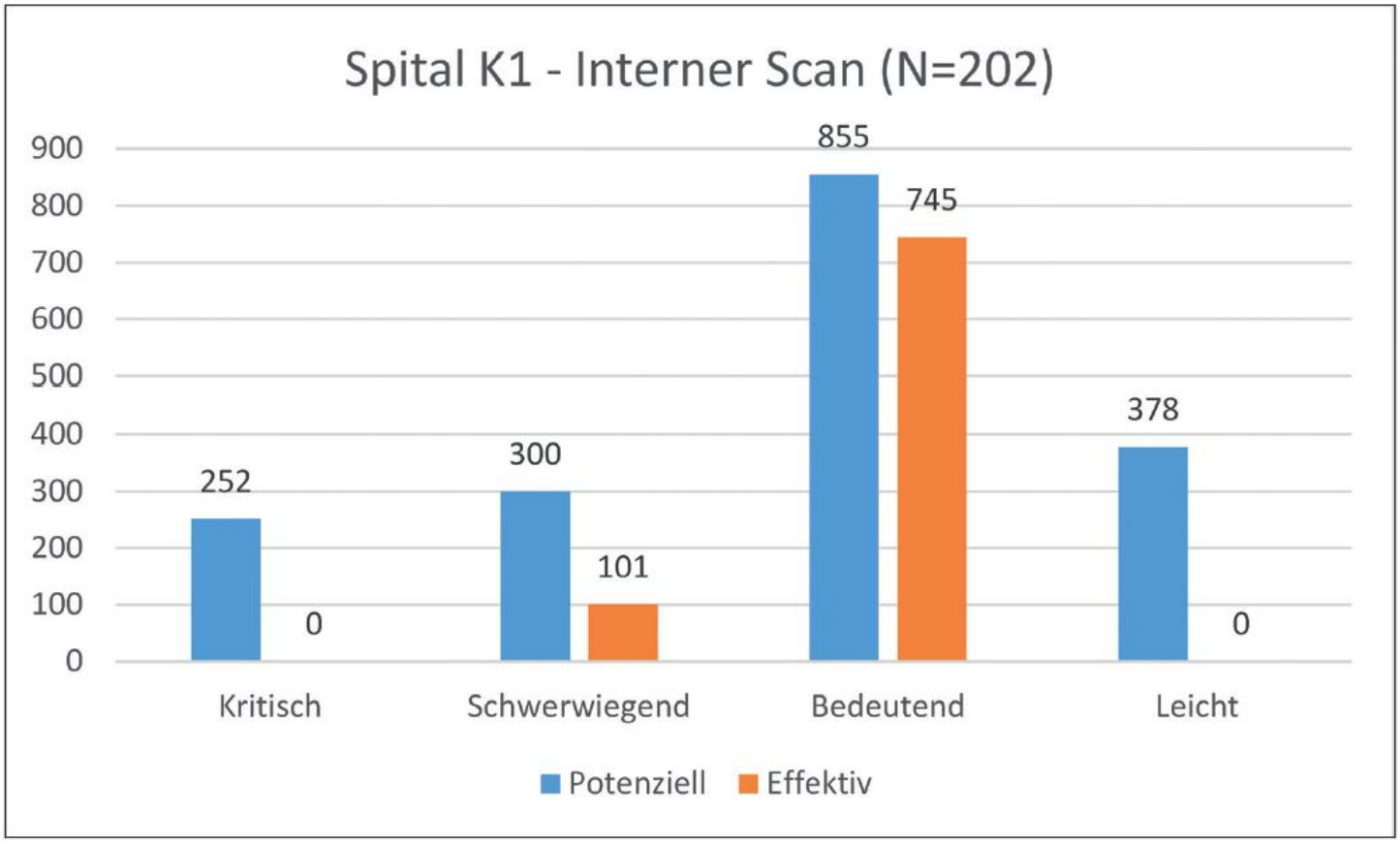


Abbildung 39: Spital K1 – Interner Scan.

Ref. [1]

Ausgewählte Resultate der Studie (II)

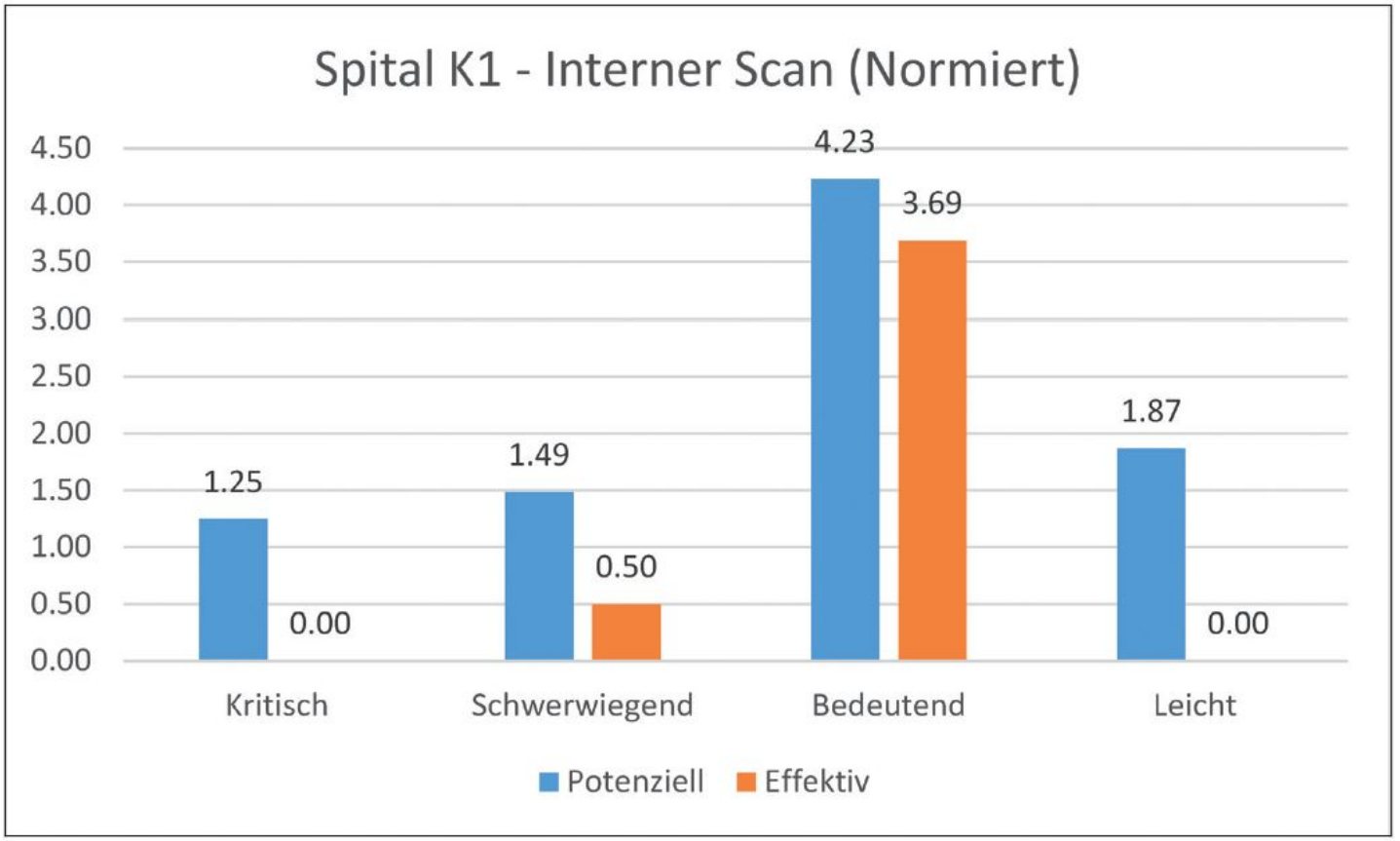


Abbildung 40: Spital K1 – Interner Scan – Normiert pro Host.

Ref. [1]

Ausgewählte Resultate der Studie (III)

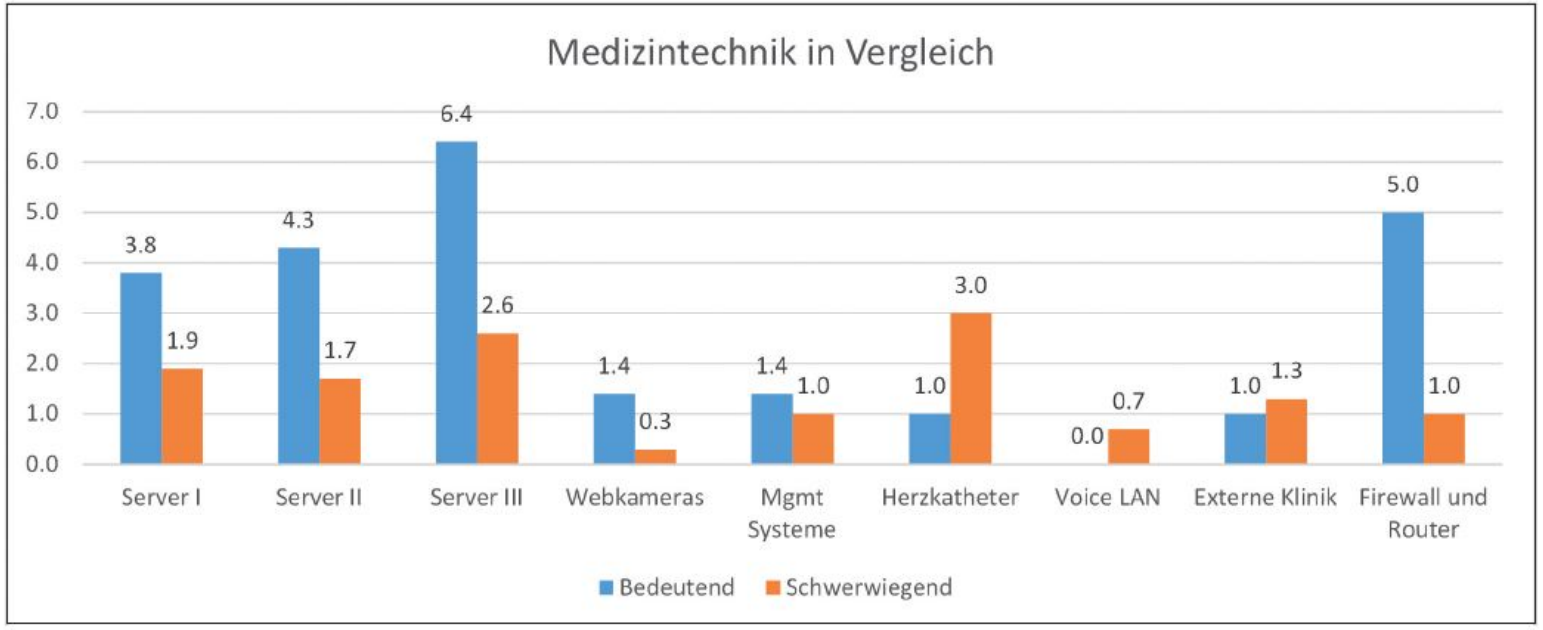


Abbildung 54: Interner Scan in der Referenzklinik.

Ref. [1]

Ausgewählte Resultate der Studie (IV)

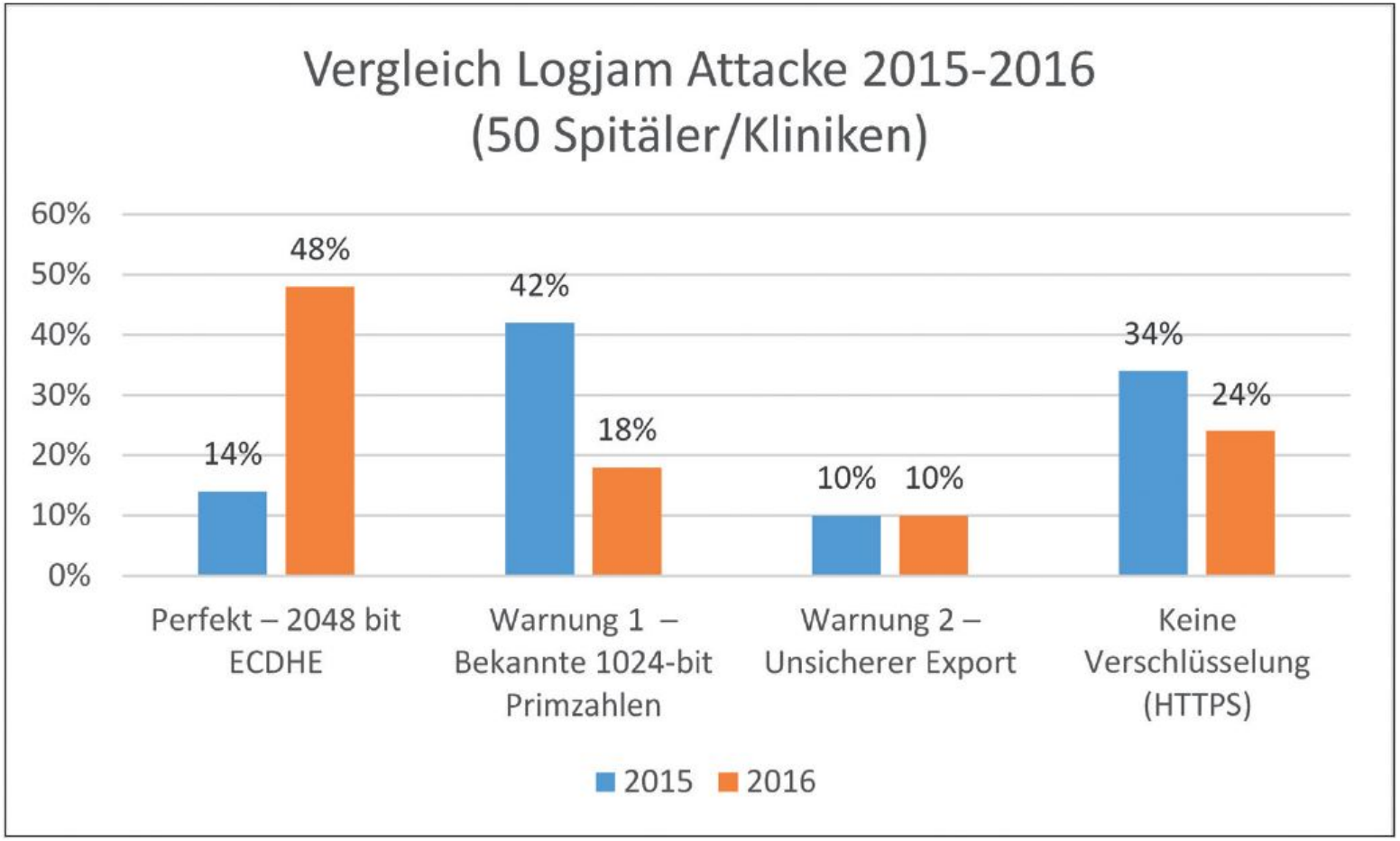


Abbildung 18: Diffie-Hellman-Logjam-Attack Vergleich 2015–2016.

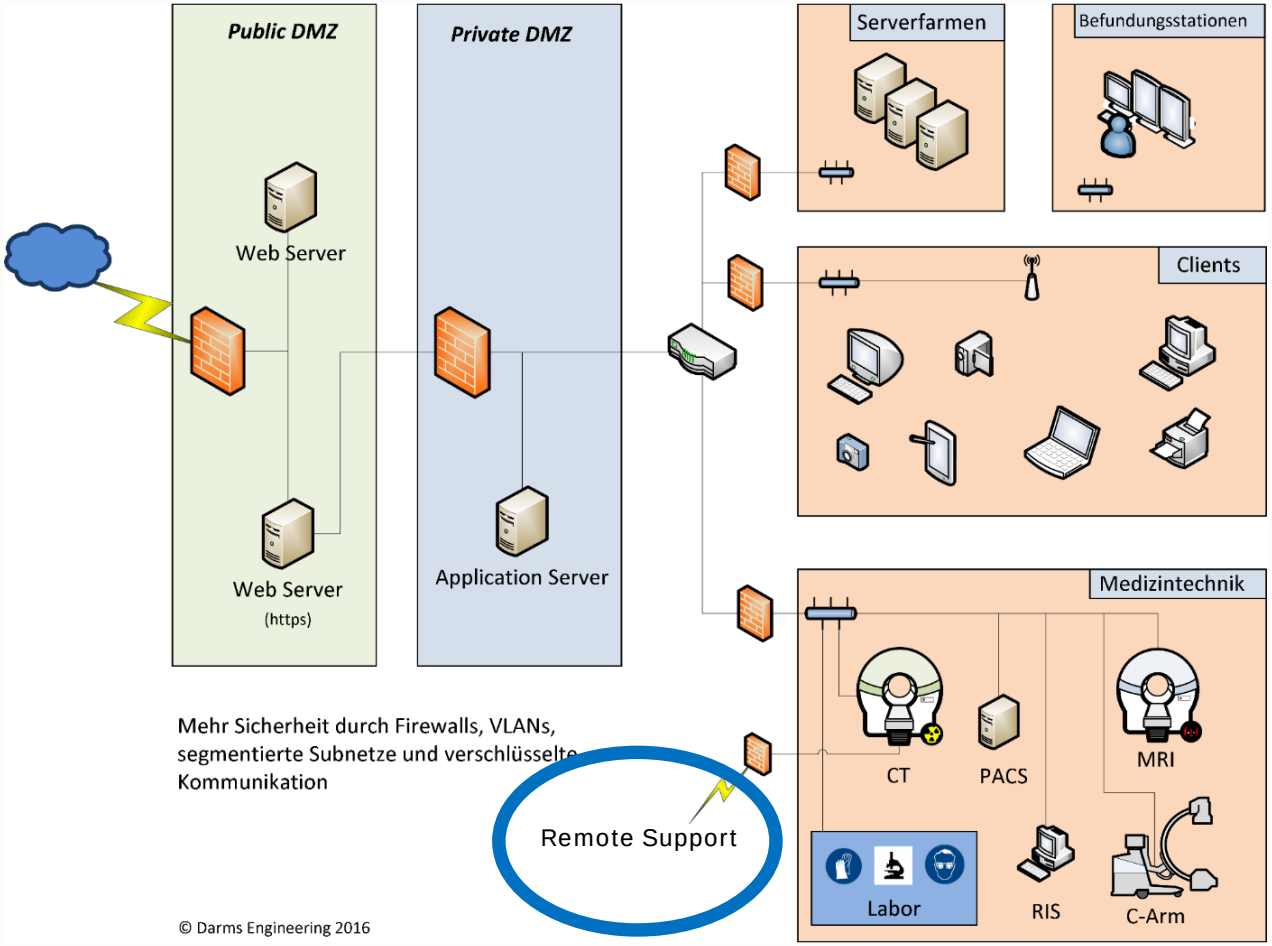
Ref. [1]

Was kann für Medizintechnik Firmen und Spitäler gemacht werden?

- Geeignete Massnahmen für sichere Spitalnetzwerke sind in der Studie «Gefährdung Schweizer Spitäler gegenüber Cyberangriffen» beschrieben (Ref. [1])
- Sichere Zonen / Firewalls
- Segmentierung und strikte Kommunikationskanäle
- Regelmässige Schwachstellen-Scans

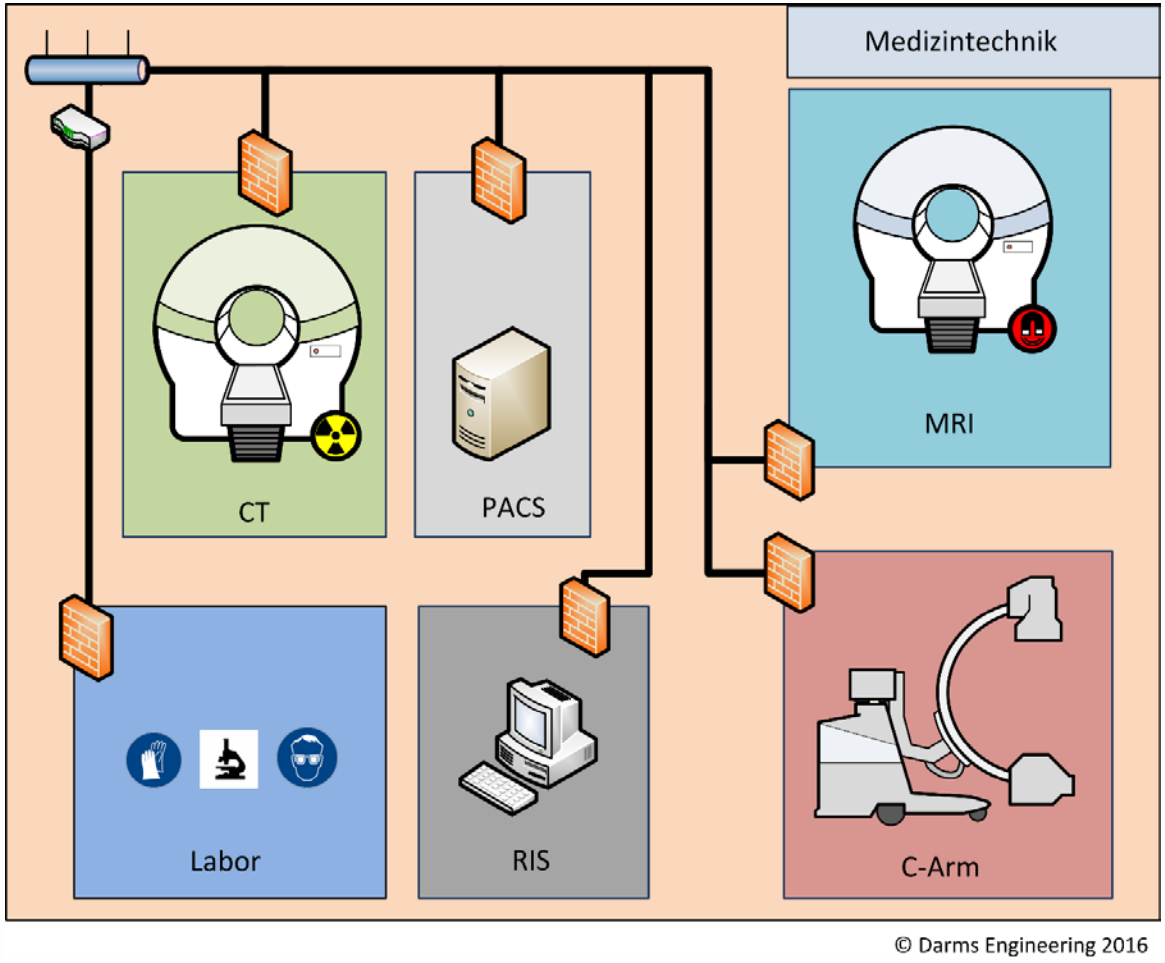
Sicheres Spital Netzwerk

Wo ist die Schwachstelle?



Source: Ref [1]

Ein noch sicheres Medizintechnik-Netzwerk



- Sicherung jedes MedTech Device mittels Firewall
- Verwendung von VLAN
- Einschränkung der Kommunikation
- Whitelisting lohnt sich
- Vulnerability - Scans

Source: Ref [1]

Lessons Learned

Was ist falsch?

Source: [P1]

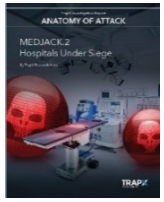
Source: [P4]

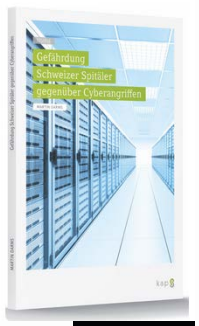
- Folgen Sie die Regeln (Standards)!
- Interpretieren Sie die Regeln richtig
- Setzen Sie auf das richtige Pferd (Partnerfirma – Berater)

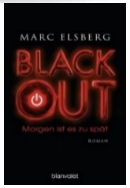
Referenzen

Referenzen:

(alle letztmals besucht: 08.06.2017)







[1] Gefährdung Schweizer Spitäler gegenüber Cyberangriffen, Martin Darms, 2016
ISBN 978-3-7255-7566-4, Infos auf www.darms.ch
[2] ANATOMY OF AN ATTACK, MEDJACK (Medical Device Hijack), May 7, 2015, By TrapX Research Labs
AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf
[3] ANATOMY OF AN ATTACK. MEDJACK.2 Hospitals Under Siege, 2016, , By TrapX Research Labs
http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_MEDJACK.2.pdf,
[4] Space, the Final Frontier for Cybersecurity? David Livingstone, Patricia Lewis, Sept 2016
https://www.chathamhouse.org/publication/space-final-frontier-cybersecurity
[5] St-Jude Medical Case
http://media.sjm.com/newsroom/news-releases/news-releases-details/2016/St-Jude-Medical-Brings-Legal-Action-Against-Muddy-Waters-and-MedSec/default.aspx
[6] FDA Post market Management of Cybersecurity in Medical Devices, Jan 22, 2016
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf
[7] Cybersecurity for Medical Imaging, *A NEMA/MITA White Paper, CSP 1-2016,* www.nema.org
[8] An Introduction to Computer Security: the NIST Handbook, Oct 1995, doi:10.6028/NIST.SP.800-12,
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-12.pdf
[9] BLACKOUT - Morgen ist es zu spät, Marc Elsberg, 2013
[10] Die grössten Hacks grafisch schön aufbereitet http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
[11] MELANI - Halbjahresbericht 2016/II (Juli - Dez.) www.melani.admin.ch
https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html

[12] Lagedossier Ransomware, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html
[13] WannaCry ein Déjà-vu-Erlebnis? http://www.medizin-edv.de/modules/AMS/article.php?storyid=4251
[14] Homepage www.nlg.nhs.uk, Diana Princess Hospital, Printscreen vom 30. Okt. 2016
[15] Klinik Gut,Fläsch https://www.golem.de/news/gebaeudesteuerung-luxusklinik-vergass-it-im-netz-1702-126362.html
[16] Cyber Attack on Britain's National Health Service – A Wake-up Call for the modern Medicine, 7. June 2017, DOI:10.1056/NEJMp1706754
http://www.nejm.org/doi/full/10.1056/NEJMp1706754#t=article

[17] NHS Hospitals Are Running Thousands of Computers on Unsupported Windows XP,
https://motherboard.vice.com/en_us/article/nhs-hospitals-are-running-thousands-of-computers-on-unsupported-windows-xp

Verwendete Bilder in dieser Präsentation:

(alle letztmals besucht: 08.06.2017)

[P1] Bilder der Schweizer Kantone nach 4 und 7 Tage / Kind entlang der Felswand
http://www.usz.ch/news/veranstaltungen/Documents/20160620_C_RisikoVerwundbarkeitsanalyseSpitaeler_StefanBrem.pdf, Bundesamt für Bevölkerungsschutz BABS, www.babs.admin.ch
[P2] US Airfoce Seal https://de.wikipedia.org/wiki/Datei:Seal_of_the_US_Air_Force.svg
[P3] IEEE Code Of Ethics http://www.ieee.org/about/corporate/governance/p7-8.html
[P4] Low Hanging Fruit https://clarknikdelpowell.com/wp-content/uploads/Low-Hanging-Fruit-Layered.jpg
[P5] Dollar https://cbsstlouis.files.wordpress.com/2012/11/83412771.jpg?w=640&h=360&crop=1
[P6] Schweizer Käse Modell http://update.hanser-fachbuch.de/wp-content/uploads/2014/05/netzpro_62_6.jpg

Herzlichen Dank für Ihre Aufmerksamkeit.

Stefan Peter
Geschäftsleitung

+41 62 508 13 49
info@recretix.ch

recretix systems AG
Murgenthalerstrasse 79
4628 Wolfwil

www.recretix.ch

Christian Beck, Regonial Account Manager
Daniel Bühler, Technical Consultant

+41 44 828 60 80
sales_info@trendmicro.ch

TREND MICRO (Schweiz) GmbH
Husacherstrasse 3
8304 Wallisellen

www.trendmicro.com / blog.trendmicro.ch

Martin Darms

+41 41 558 05 25
Martin@Darms.ch

Darms Engineering
Verenaweg 12
6343 Buonas

www.darms.ch