Cybersicherheit als Herausforderung

Was kommt auf die Krankenhäuser zu?

Gerhard Härdter

Leiter Servicercenter IT

Klinikum Stuttgart

VKD BW 14.03.2016

STUTTGART

Klinikum Stuttgart

Cybersicherheit als Herausforderung

- Spam-Mail-Flutwelle
- Aktuelle Bedrohung durch Ransomware
- Sicherheit medizinische Netzwerke am Bsp. ROKIS
- IT-Sicherheitsgesetz –
- Empfehlungen des AG IT AKG

Was ist Spam

- Als **Spam** [spæm] oder **Junk** (englisch für ‚Abfall' oder ‚Plunder') werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten (Informationen) bezeichnet, die dem Empfänger unverlangt zugestellt werden und häufigwerbenden Inhalt enthalten.

SPAM-Mail

An lokales@az-muenchen.de

Schlagwörter Zu erledigen

DHL

Werter Kunde,

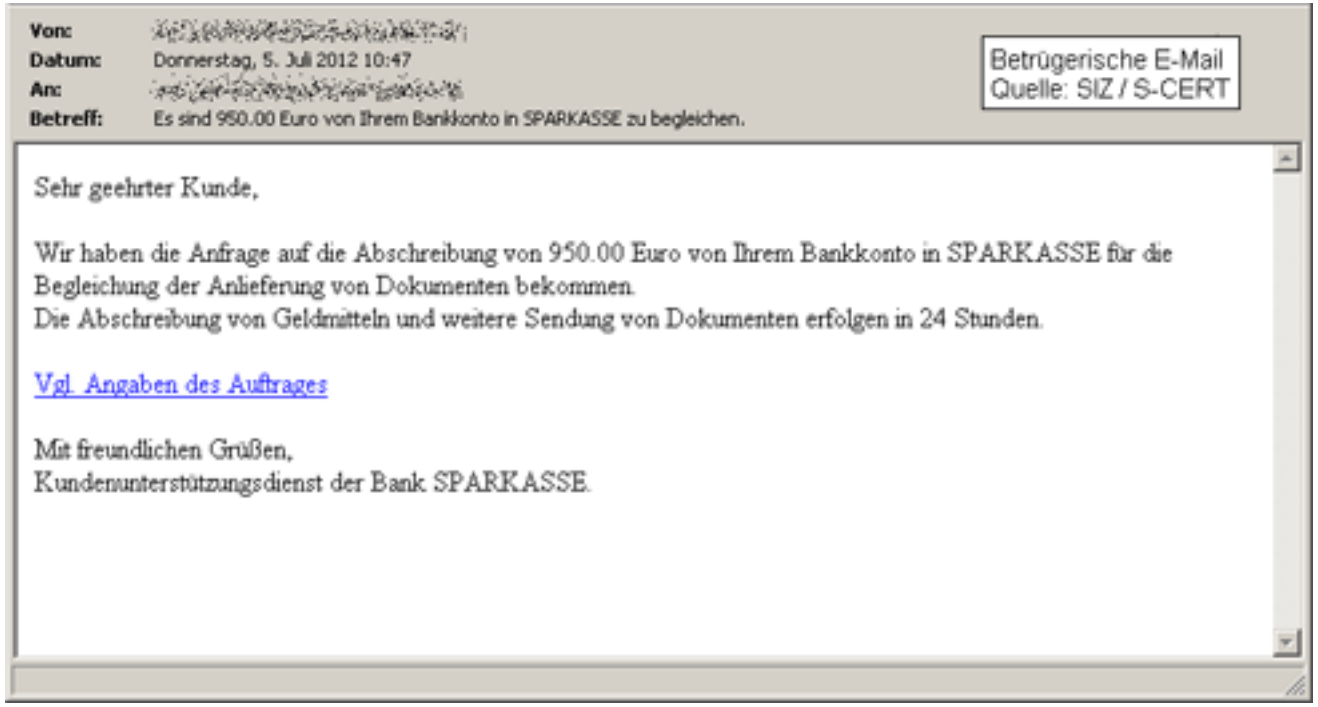
Ihre Sendung **612989020222026198 90** wurde an DHL übergeben und wird voraussichtlich am **03.03.2015** zugestellt.

Über die nachfolgende Verlinkung werden weitere Informationen zu Ihrer Sendung ausgegeben: **612989020222026198 90**.

Mit freundlichen Grüßen,
Ihr Logistik-Team

Spam-Ordner in Outlook

SPAM-Mail mit Trojaner



Von: [redacted]
Datum: Donnerstag, 5. Juli 2012 10:47
An: [redacted]
Betreff: Es sind 950.00 Euro von Ihrem Bankkonto in SPARKASSE zu begleichen.

Betrügerische E-Mail
Quelle: SIZ / S-CERT

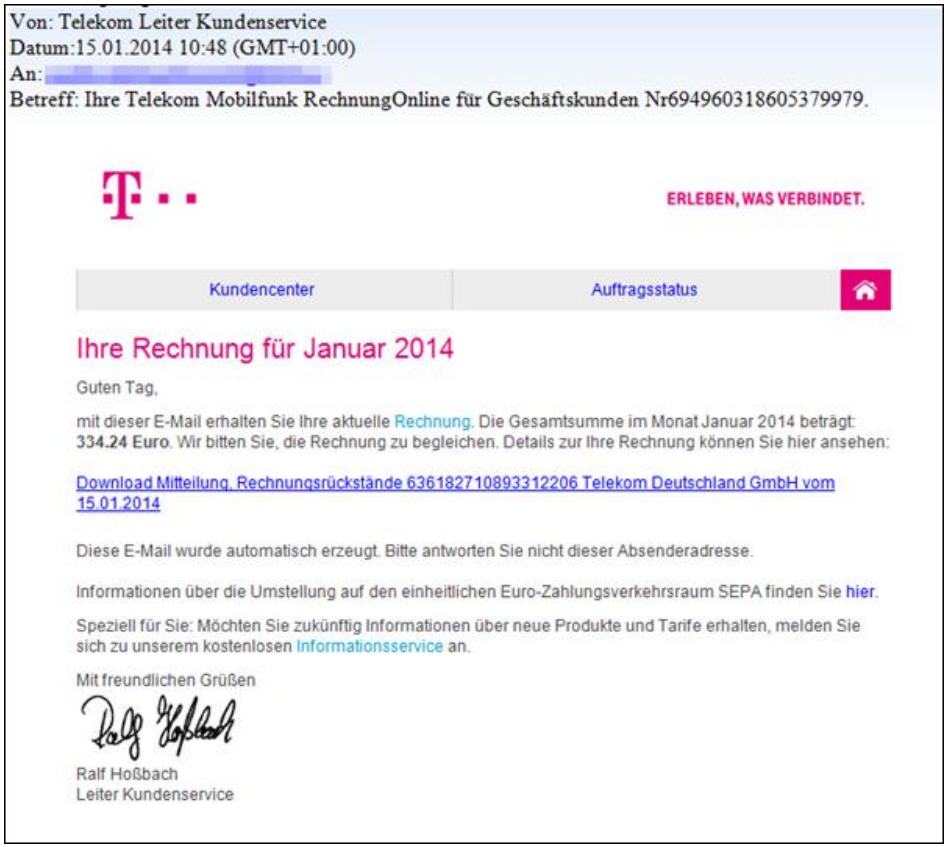
Sehr geehrter Kunde,

Wir haben die Anfrage auf die Abschreibung von 950.00 Euro von Ihrem Bankkonto in SPARKASSE für die Begleichung der Anlieferung von Dokumenten bekommen.
Die Abschreibung von Geldmitteln und weitere Sendung von Dokumenten erfolgen in 24 Stunden.

Vgl. Angaben des Auftrages

Mit freundlichen Grüßen,
Kundenunterstützungsdienst der Bank SPARKASSE.

SPAM-Mail mit Trojaner



Von: Telekom Leiter Kundenservice
Datum:15.01.2014 10:48 (GMT+01:00)
An: [redacted]
Betreff: Ihre Telekom Mobilfunk RechnungOnline für Geschäftskunden Nr694960318605379979.

T · ·

ERLEBEN, WAS VERBINDET.

Kundencenter | Auftragsstatus

Ihre Rechnung für Januar 2014

Guten Tag,

mit dieser E-Mail erhalten Sie Ihre aktuelle Rechnung. Die Gesamtsumme im Monat Januar 2014 beträgt: **334.24 Euro**. Wir bitten Sie, die Rechnung zu begleichen. Details zur Ihre Rechnung können Sie hier ansehen:

Download Mitteilung, Rechnungsrückstände 636182710893312206 Telekom Deutschland GmbH vom 15.01.2014

Diese E-Mail wurde automatisch erzeugt. Bitte antworten Sie nicht dieser Absenderadresse.

Informationen über die Umstellung auf den einheitlichen Euro-Zahlungsverkehrsraum SEPA finden Sie hier.

Speziell für Sie: Möchten Sie zukünftig Informationen über neue Produkte und Tarife erhalten, melden Sie sich zu unserem kostenlosen Informationsservice an.

Mit freundlichen Grüßen

Ralf Hoßbach
Leiter Kundenservice

Ransomware – Definition BSI

- Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und eine Freigabe dieser Ressourcen erfolgt nur gegen **Zahlung eines Lösegeldes** (engl. ransom).
- Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der **Verfügbarkeit** und **eine Form digitaler Erpressung**

Massive Zunahme von Ransomware

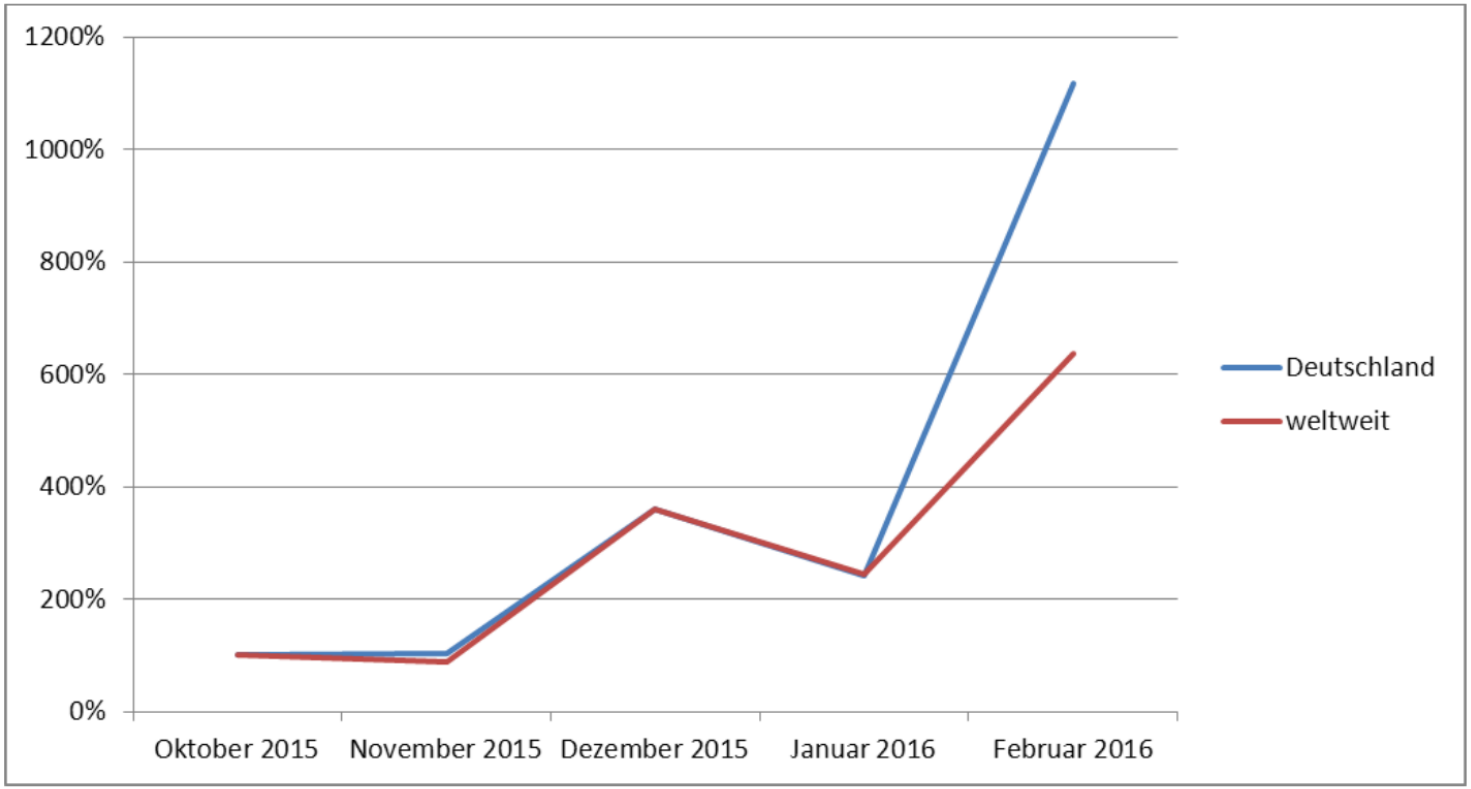


Abbildung 1: Trend der Ransomware-Detektionen in Deutschland Oktober 2015 – Februar 2016, Quelle: BSI

Ransomware


YOUR COMPUTER HAS BEEN LOCKED!
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.
To unlock the computer you are obliged to pay a fine of $200.
You have 72 hours to pay the fine, otherwise you will be arrested.
You must pay the fine through
To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY
OK

Ransomware – Angriffswege

- Spam
  - Bei Angriffen mittels Spam wird versucht, über meist professionelles Social Engineering den Benutzer zum **Öffnen von E-Mail-Anhängen** zu bewegen.
  - So werden angebliche **Rechnungen**, **Bestellbestätigungen**, **Paketempfangsbestätigungen**, eingescannte Dokumente, empfangene Faxe, teilweise **unter Verwendung von echten Firmennamen und –adressen**
  - zum Teil in perfekter **Nachahmung** tatsächlicher Firmen-E-Mails, versendet.
  - Im Anhang befindet sich meist ein sog. Downloader, der die eigentliche Schadsoftware nachlädt.

Ransomware – Angriffswege

- Mailanhänge
  - Zip-Dateien (komprimierte .exe)
  - Officedokumente mit Makros
- Schwachstellen in Webservern
  - Infizierte Webseiten
- Ungeschützte Fernwartungszugänge

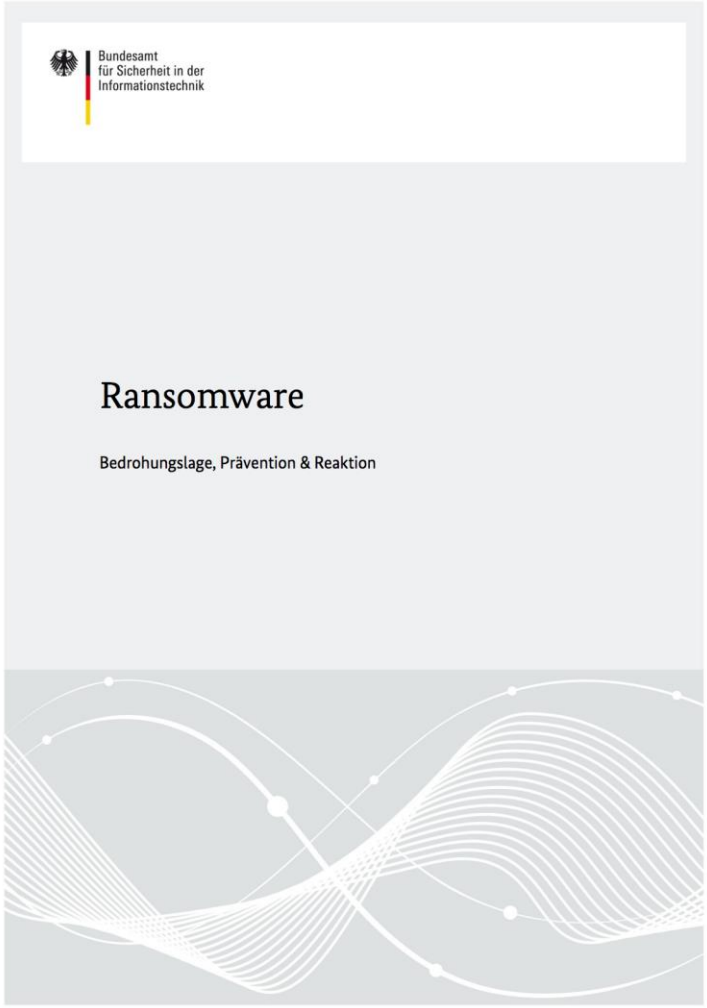
BSI zur Lage in Unternehmen

- Versäumnisse bei der Prävention
  - Schlecht gepflegte Systeme
  - fehlende, veraltete oder nicht überprüfte Software-Backups,
  - schwache Administrator-Passworte,
  - fehlende Netzsegmentierung

BSI Empfehlungen zur Prävention

- Software auf aktuellem Stand halten
  - Updates und Patches sollten **unverzüglich** nach der Bereitstellung durch den jeweiligen Softwarehersteller - **idealerweise über zentrale Softwareverteilung** - eingespielt werden.
- Angriffsflächen minimieren
  - Je **weniger Programme** zum Öffnen von unbekannten Inhalten und zur Ausführung von unbekanntem Code zur Verfügung stehen, desto weniger Schwachstellen und Fehlkonfigurationen können durch einen Angreifer ausgenutzt werden.
  - **nicht benötigte Software** generell deinstallieren
  - In **Web-Browsern** sollte die **Ausführung aktiver Inhalte** eingeschränkt werden
  - nicht zwingend benötigte **Browser-Plugins** (z. B. Flash, Java, Silverlight) sollten **entfernt** werden.
- eMail
  - Ausführung aktiver Inhalte unterdrücken
- Datensicherungskonzept
  - Ein **Backup** ist die **wichtigste Schutzmaßnahme**, mit der im Falle eines Ransomware-Vorfalls die Verfügbarkeit der Daten gewährleistet ist.
  - Jede Institution sollte über ein **Datensicherungskonzept** (IT Grundschutz: B 1.4 Datensicherungskonzept) **verfügen** und dieses auch **umsetzen**.

BSI-Themenpapier - Ransomware



https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Ransomware_11032016.html

aktuelle Herausforderung

Ransomware-Virus legt Krankenhaus lahm

heise online 12.02.2016 12:48 Uhr – Detlef Borchers vorlesen

(Bild: heise Security)

Ein Computervirus hat die IT des Lukaskrankenhauses in Neuss infiziert. Patientendaten sollen dank Backup in Sicherheit sein. Zwei weitere Kliniken sollen auch befallen sein.

Attacke auf Klinik-Computer in Neuss sperrt alle Daten – Mitarbeiter im SRH Waldklinikum Gera sensibilisiert

18.02.2016 - 06:35 Uhr

Anzeige

Geheime Blutwerte

Diese 7 Blutwert-Informatione

geheimwissen-bluthochdruck.

Das Lukaskrankenhaus in Neu

Der Computerschädling sperr

Politik | Wirtschaft | Panorama | Sport | Kultur

Nachrichten > Netzwelt > Web > Computerviren > No

IT-Sicherheit: Comput

Krankenhausmitarbeiter auf dem Flur: Nur A

Befunde mussten per Telefon oder Krankenhaus Arnsberg gestört. Es

Montag, 15.02.2016 – 17:07 Uhr

Drucken | Merken

Nutzungsrechte | Feedback

Kommentieren | 68 Kommentare

THEMA

Abo/Service | ePaper | Anzeige aufgeben

Digitale Prospekte | RP Trauer | Termine | Kalaydo | Scribez | weitere »

RP ONLINE

18. FEBRUAR 2016

Suchbegriff eingeben

NRW POLITIK WIRTSCHAFT SPORT KULTUR PANORAMA LEBEN REISEN DIGITAL

Startseite NRW Krankenhaus-Servern: Hacker-Angriffe auch in Mönchengladbach, Essen und Köln

Login

EXKLUSIV:

Wenn die Rente nicht mehr für die PKV reicht

...mehr

Themen

Computer | Köln | Mönchengladbach | Neuss

Video-Empfehlungen

erbindung wird hergestellt...

3 später lesen

12. Februar 2016 | 19.26 Uhr

17 5 3

Virus auf Krankenhaus-Servern

Hacker-Angriffe auch in Kleve und Kalkar

Ärzte und Patienten in Neus
Flugblättern informiert.

Neuss. Neben dem
auch Computer de
Trägergesellschaf

Teilen Twittern E-Mail

Ein Computervirus hat die digitale Kommunikation eines
in Nordrhein-Westfalen unterbrochen. Das Klinikum Arns
Freitag auf einem Computersystem eine Schadsoftware
ein Sprecher des Klinikums am Montag.

Daraufhin habe man sich
entschlossen, das komplette

xy S7 Android iOS 9 Oculus Rift

eben deutschen Krankenhäusern auch US-Klinik von Viru

« vorige | nächste »

ankenhäusern auch US-Klinik

vorlesen

Computervirus legte Fürther Klinik-Server lahm

Schadsoftware aus Mail-Anhang brachte Arbeitsabläufe im Krankenhaus durcheinander - 17.02.2016 17:04 Uhr

FÜRTH - Ein Virus im Krankenhaus? Das soll vorkommen. Diesmal aber hat es keine Patienten erwischt, sondern einen Server: Ein Computervirus hat die Abläufe im Fürther Klinikum durcheinandergewirbelt. Auch andere Häuser in Deutschland waren betroffen.

Jede Menge Ärger hatte das Klinikum vergangene Woche mit eingeschleuster Schadsoftware.

Charakteristika der aktuellen Infektion

- Infektion durch E-Mail und per WWW
- Programm sucht alle Verzeichnisse, die schreibbar sind
- Diese werden verschlüsselt und damit unbrauchbar.
- Auch Dateien, die für den Betrieb des PCs nötig sind werden ebenfalls verschlüsselt:
  → PC nicht mehr betriebsbereit.

Im Klinikum waren 7 Nutzer davon betroffen, ca. 150.000 Dateien verschlüsselt. Keine Schäden, alles im Backup.

Bedrohungen durch externe Mails - Problemmangement

Ransomware-Virus legt Krankenhaus lahm

heise online 12.02.2016 12:48 Uhr – Detlef Borchers vorlesen

(Bild: heise Security)

Ein Computervirus hat die IT des Lukaskrankenhauses in Neuss infiziert. Patientendaten sollen dank Backup in Sicherheit sein. Zwei weitere Kliniken sollen auch befallen sein.

Erfolgreiche Aktionen im Klinikum

1. Gutes Servicemanagement:
   Schnelle Trennung der PCs vom Netz
2. Schnelle Analyse des Schädlings – Kontakt mit Virenschutzhersteller → Signaturen
3. Fitte IT-Mitarbeiter in der Client-Betreuung
4. Erfolgreiches Krisenmanagement, bereit zur technischen Eskalation
5. Campusweite Ersatznutzer für Ausfallszenarien:
   Wichtigste Anwendungen (SAP, PACS, Archiv) unter maximaler Sicherheit möglich.
6. Alle betroffenen Dateien waren im Backup und konnten wiederhergestellt werden.

Empfehlungen für Anwender - Intranet

Warnung vor E-Mails mit gefährlichen Inhalten

In den letzten Tagen kam es in Deutschland zu massiven Angriffen durch Mails, die über in der Mail enthaltene Dokumente oder Links zur Installation einer Schadsoftware führte, die dann sämtliche Daten im gesamten Netz verschlüsselt, auf die der Benutzer Zugriff hat.

Diese Mails können scheinbar von verschiedensten Absendern kommen, dies können große Unternehmen wie DHL, Amazon, Banken oder Energieversorger sein, aber der Absender kann auch scheinbar ein Kollege aus dem Klinikum oder ein Bekannter sein.

Einige Firmen und auch Kliniken in Deutschland hat es dadurch bereits so stark in Mitleidenschaft gezogen, dass diese ihren IT-Betrieb einstellen mussten, was zu immensen Störungen des Betriebsablaufs führte.

Um uns und Sie zu schützen:

1. **Niemals Links und Dokumente in diesen Mails anklicken.**
   Rechnungen die bezahlt werden müssen werden nicht per Mail zugestellt! Und wenn scheinbar ein Kollege um Rat zu einer Rechnung fragt, rufen Sie diesen Kollegen an, bevor die Anhänge und Links geklickt werden.
2. **Lesen Sie aus dem Kliniknetz heraus keine private Mails über Webmailer**, wie Web.de, GMX.DE, Outlook.Com, usw. – hier besteht ein größeres Risiko, da viele der FreeMail-Accounts keinen Virenschutz haben, das wird als extra Merkmal verkauft.
   Sie tun sich und dem Klinikum keinen Gefallen.
3. Wenn Ihr PC z.B. nach dem Start eine Trojanerwebseite zeigt: **Sofort mit dem Handy ein Foto davon machen und PC schnellstens (hier geht es um Sekunden) ausschalten!**
   Danach bei der **IT-Hotline (DW: 32626)** melden. Stichwort: Befall mit Schadsoftware.

Seien Sie gegenwärtig doppelt vorsichtig! Im Klinikum Stuttgart wurden einzelne Personen bereits mit dem Schädling infiziert, einen größeren Schaden konnten unsere IT-Administratoren aber verhindern.

Wir arbeiten in der IT ständig an Maßnahmen um die Betriebssicherheit zu gewährleisten.

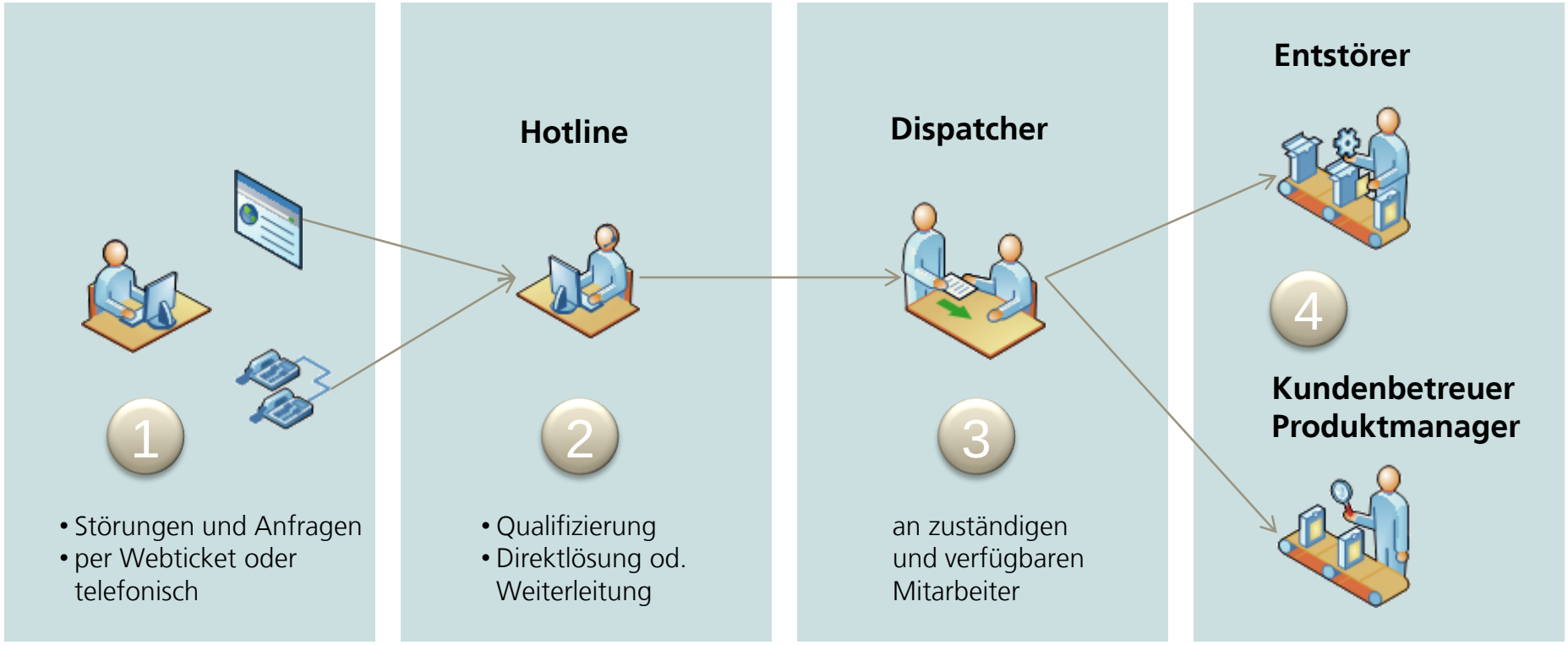
Empfehlungen für Anwender

- **Niemals Links und Dokumente in verdächtigen Mails anklicken.**
  Rechnungen die bezahlt werden müssen werden nicht per Mail zugestellt! Und wenn scheinbar ein Kollege um Rat zu einer Rechnung fragt, rufen Sie diesen Kollegen an, bevor die Anhänge und Links geklickt werden.

- **Lesen Sie aus dem Kliniknetz heraus keine private Mails über Webmaile**r, wie Web.de, GMX.DE, Outlook.Com, usw. – hier besteht ein größeres Risiko, da viele der FreeMail-Accounts keinen Virenschutz haben, das wird als extra Merkmal verkauft.

- Wenn Ihr PC z.B. nach dem Start eine Trojanerwebseite zeigt: **Sofort mit dem Handy ein Foto davon machen und PC schnellstens (hier geht es um Sekunden) ausschalten!**
  Danach bei der **IT-Hotline (DW: 32626)** melden. Stichwort: Befall mit Schadsoftware.

Entstörung


Hotline
Dispatcher
Entstörer
4
Kundenbetreuer
Produktmanager
1
2
3
• Störungen und Anfragen
• per Webticket oder telefonisch
• Qualifizierung
• Direktlösung od. Weiterleitung
an zuständigen und verfügbaren Mitarbeiter
5
6

Management der Restrisiken

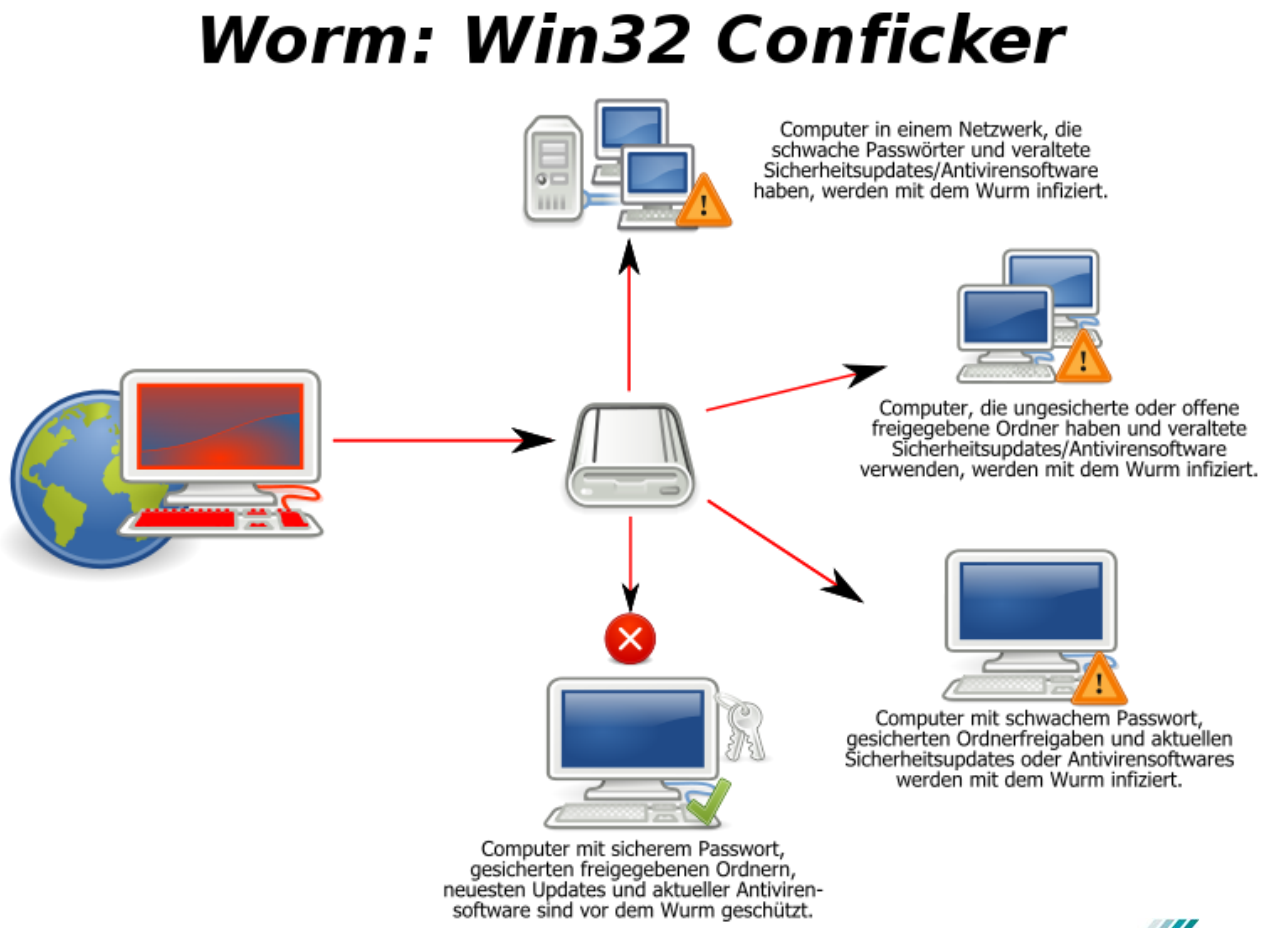
- Nutzer unterscheiden nicht zwischen privaten und dienstlichen Mails in der Mailbox, denn private Nutzung ist erlaubt. Links in Mails werden angeklickt.
  → Verbot der privaten Mail-Nutzung angestrebt (Dienstvereinbarung zum Datenschutz mit PR)
- Mehr Sicherheit am Übergang zum Internet
  → Einsatz von Spezialfiltern (Antispam, Websecurity)
- Vereinzelt noch Daten auf lokalen End-Systemen statt auf Fileservern.
  → Konsolidierung der Datenablagen und Backup

Medizinische IT-Netzwerke

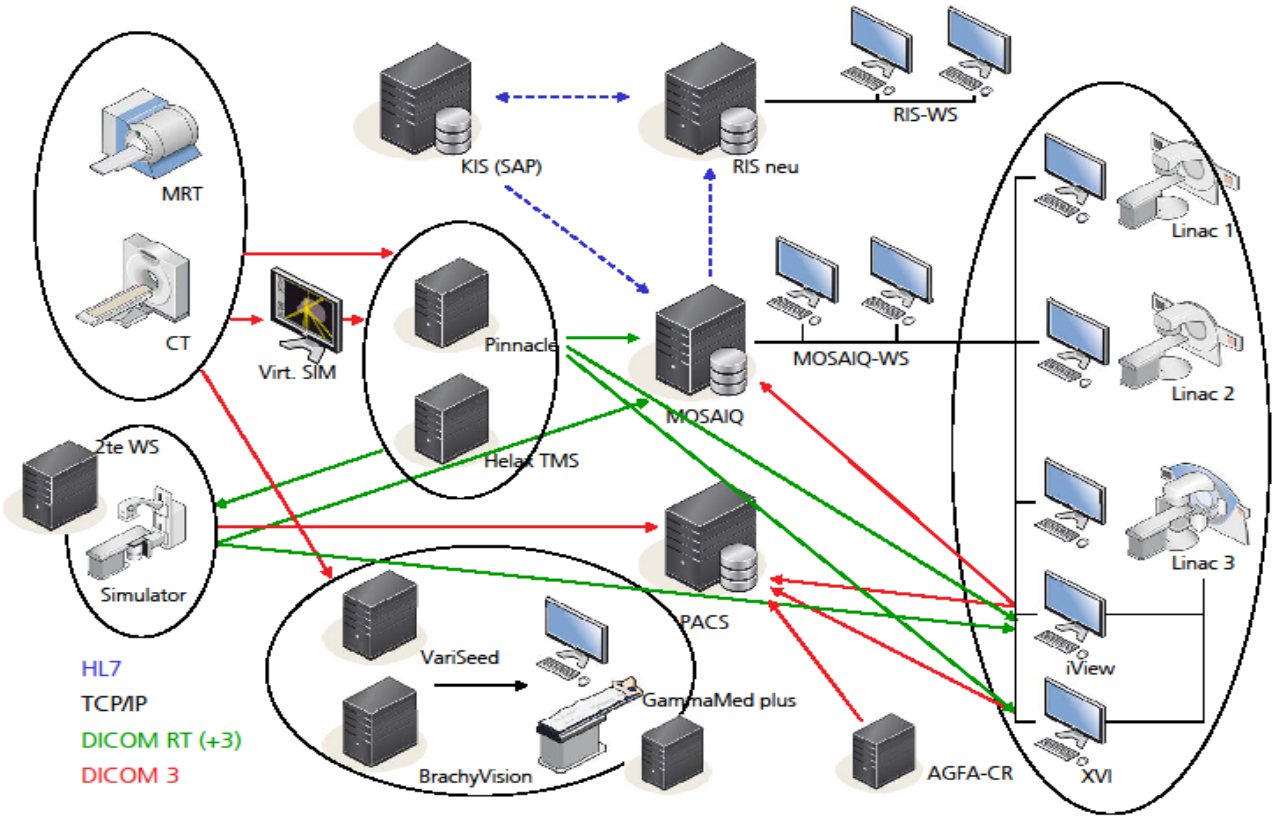
Konfigurationsbeispiel

Rokis – Linearbeschleuniger Fa. Elekta

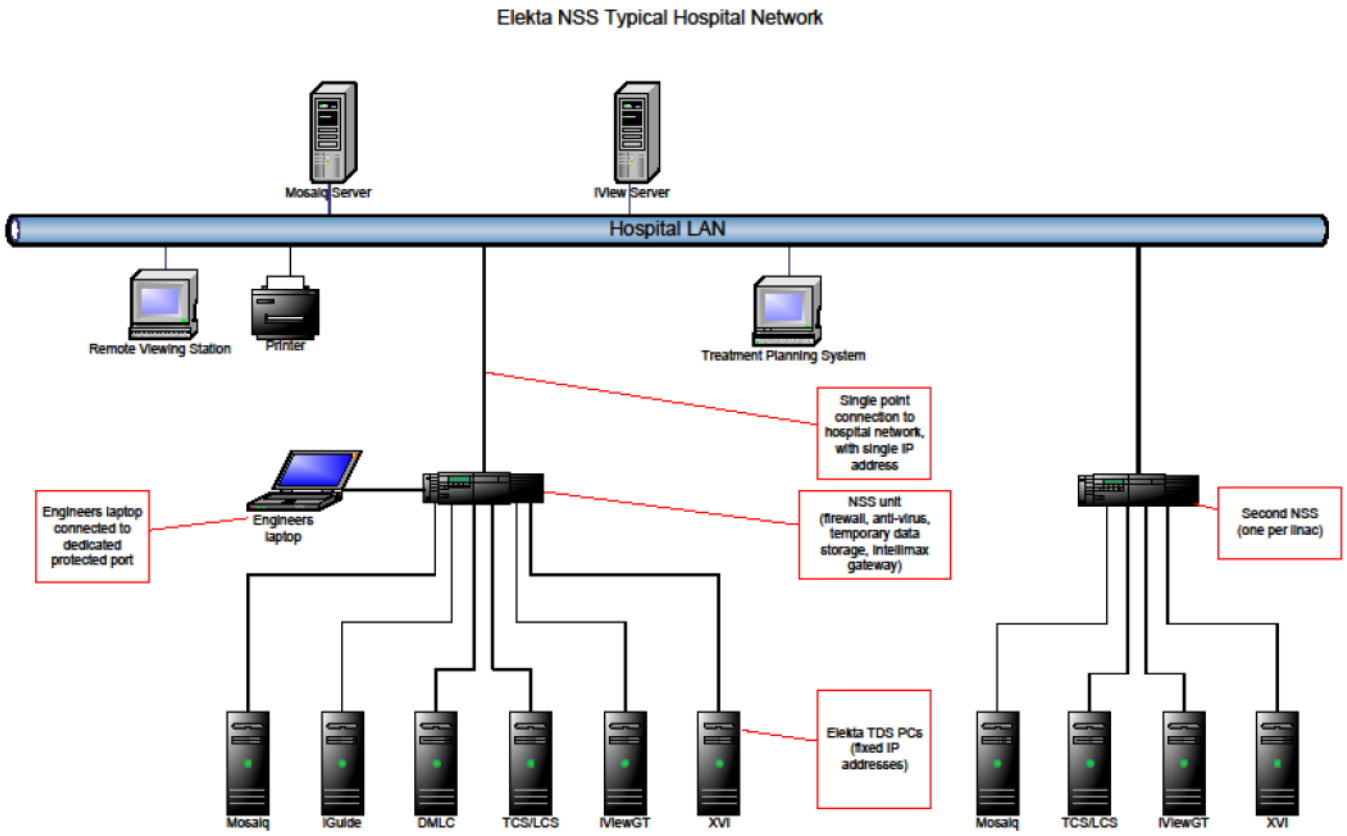
Schadensfall Computerwurm im Medizingerätenetz ROKIS



Medizingerätenetz ROKIS



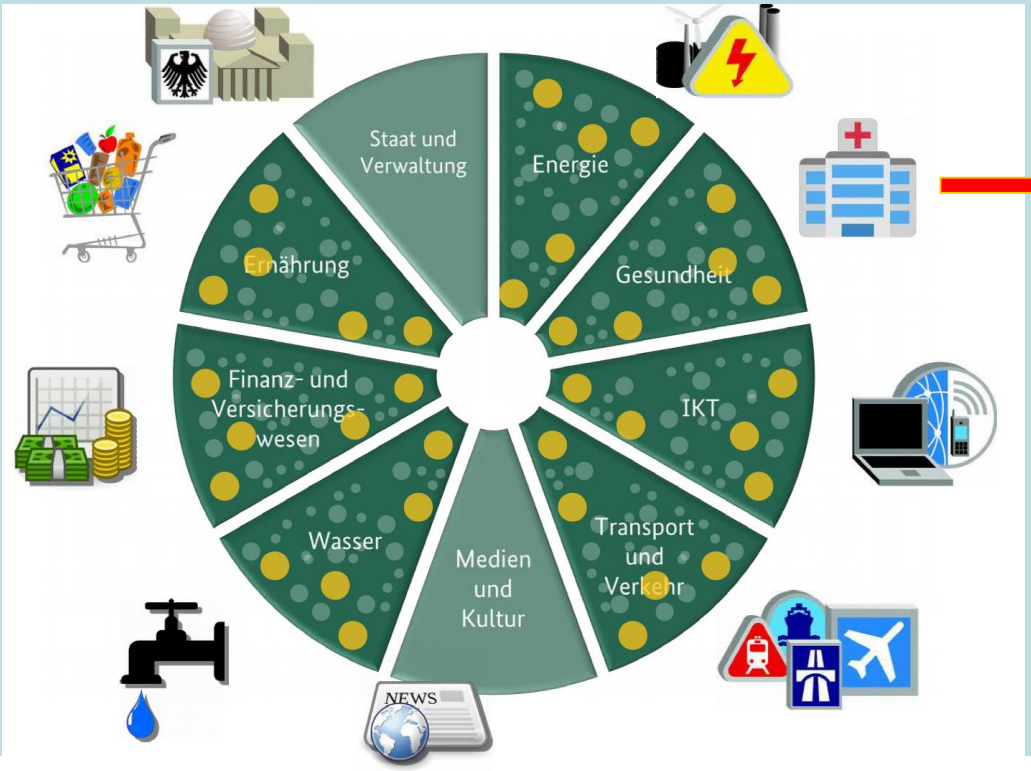
Medizingerätenetz ROKIS – sicherer Betrieb



IT-Sicherheitsgesetz - Ziele

- eine „signifikante Verbesserung der IT-Sicherheit in Deutschland zu erreichen“
- „der Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) verbessert“ werden,
- den „aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können“.

Alle Betreiber kritischer Infrastrukturen, die wesentlich für die Gesellschaft sind



Aufgeteilt auf:
- Labore
- Arzneimittelherstellung
- Med. Versorgung

Quelle BSI

Gesetzliche Vorgabe:
8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung […] 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.

KRITIS – für wen gilt das Gesetz?

Rechtsverordnung durch das BMI – Ende 2016:

Definition, welche Unternehmen genau als „kritische Infrastrukturen“ – KRITIS – gesehen werden und damit unter das Gesetz fallen

Schwellwerte für Krankenhäuser noch unklar

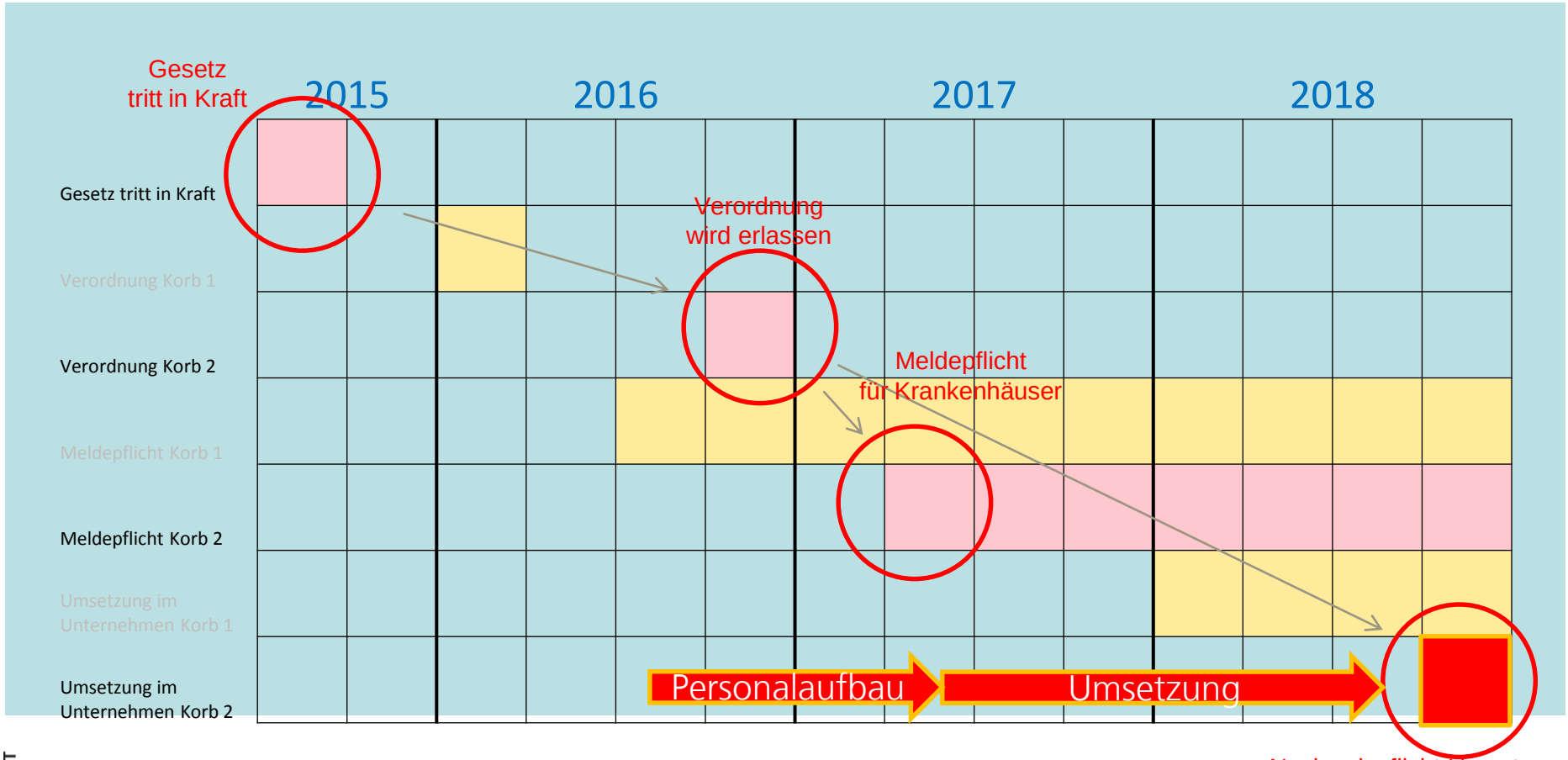
- Welche Größe ein Haus besitzen muss, um teilzunehmen wird in der Rechtsverordnung definiert.
- Die abzusichernden Dienstleistungen werden auch in der Verordnung definiert.
- Unklar, welche Freiheitsgrade ein Haus hat.

Finanzierung

BSI bekommt Stellen, aber öffentliche Betreiber kritischer Infrastrukturen haben aber ebenfalls Aufwände:

- Finanzierung des benötigten Personals
  (3 VK Security-Anforderungen für IT)
- Finanzierung der Maßnahmen zur Absicherung und für die Ersatzverfahren
  (*Erfahrungswerte:*
  Investition: 100k€-200k€ einmalig pro Verfahren
  + 0.2VK pro kritischem Verfahren / Jahr)

Zeitplan IT-Sicherheitsgesetz



STUTTGART

Klinikum Stuttgart

Handlungsempfehlungen BSI

- Für große Einrichtungen: Informationssicherheitsmanagement einführen (ISMS), das ist immer richtig und notwendig!
- Sicherheitsexperten rekrutieren – die werden noch rarer werden!
- Kompetenz für IT Sicherheits- und Risikomanagement im Rechenzentrum aufbauen
- „RiKrIT“ – Methode zur Risikoanalyse Krankenhaus IT anwenden

Handlungsempfehlung AG IT der AKG zum IT-Sicherheitsgesetz

- Pragmatische Herangehensweise

1. Identifikation aller unternehmenskritischen Verfahren des Krankenhauses
2. Erarbeitung und zentrale Dokumentation der organisatorischen und technischen Ausfallkonzepte für die als unternehmenskritisch identifizierten Verfahren
3. Anwendung des IT-Grundschutzes auf besonders kritische Verfahren

Handlungsempfehlung AG IT der AKG zum IT-Sicherheitsgesetz

- Priorisierung

1. Es empfiehlt sich, die Priorisierung nach Kritikalität und wirtschaftlichem Risiko vorzunehmen und mit den Verfahren zu beginnen, bei denen im Falle eines Ausfalls der IT, der „Nacharbeitungsaufwand“ am höchsten ist.

Zusammenfassung

1. Erfolgreiche Lösungen ergeben sich aus einer Gesamtstrategie **technischer** und **organisatorischer** Maßnahmen
2. Pragmatische Herangehensweise reduziert die Komplexität

Expertenmeinung

„Die Wahrscheinlichkeit, dass jemand zielgerichtet versucht, auf ein Medizingerät zuzugreifen, halte ich für gering."

Hannes Molsen, Dräger

Zitat –
Psychologie des Risikos - Gerd Gigerenzer

„Ungewissheit ist gerade die Bedingung, die den Menschen zur Entfaltung seiner Kräfte zwingt."

Erich Fromm