ST. CHRISTOPHORUS-KRANKENHAUS WERNE

Klinikum Lünen
St.-Marien-Hospital
Akademisches Lehrkrankenhaus der
Westf. Wilhelms-Universität Münster

SRC
security consulting

ERFAHRUNGSBERICHT: PRÜFUNG NACH § 8A (3) BSIG AUS PRÜFER- UND KRANKENHAUSSICHT

KritisV-Eindrücke eines Betreibers und einer prüfenden Stelle

Randolf Skerka & Ralf Plomann

ST. CHRISTOPHORUS-KRANKENHAUS WERNE

Klinikum Lünen
St.-Marien-Hospital
Akademisches Lehrkrankenhaus der Westf. Wilhelms-Universität Münster

SRC security consulting

Ralf Plomann

IT-Leiter

Katholisches Klinikum Lünen/Werne

Randolf Skerka

Bereichsleiter „ISMS“

SRC, Bonn

WIR ÜBER UNS

2014 / 2015 erster Kontakt zum Thema

KGNW Krankenhausgesellschaft Nordrhein-Westfalen e. V.

13.11.2014 Rundschreiben Nr. 477/2014
Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz (ITSiG))
zum Dokument im Archiv >>

UNSERE ENTWICKLUNG…

§ 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.

Fachliche Sicht: 

Emotion: 

UNSERE ENTWICKLUNG…

UNSERE AUSGANGSLAGE(N)

Sicht des Klinikums:

- Angemessenheit?
- Stand der Technik?
- Verpflichtung?
- Kosten?

Sicht des Prüfers:

- Die anderen Prüfer sind auch nicht schlauer als wir!
- Das Nachweisverfahren ist jung und unreif!
  - Wir haben Gestaltungsspielraum!
- Das BSI wird fachlich solide Arbeit erwarten!
- Die Prüfungen müssen bezahlbar bleiben!
  - Unsere Kunden möchten möglichst geringe Kosten!

Prüfgrundlage

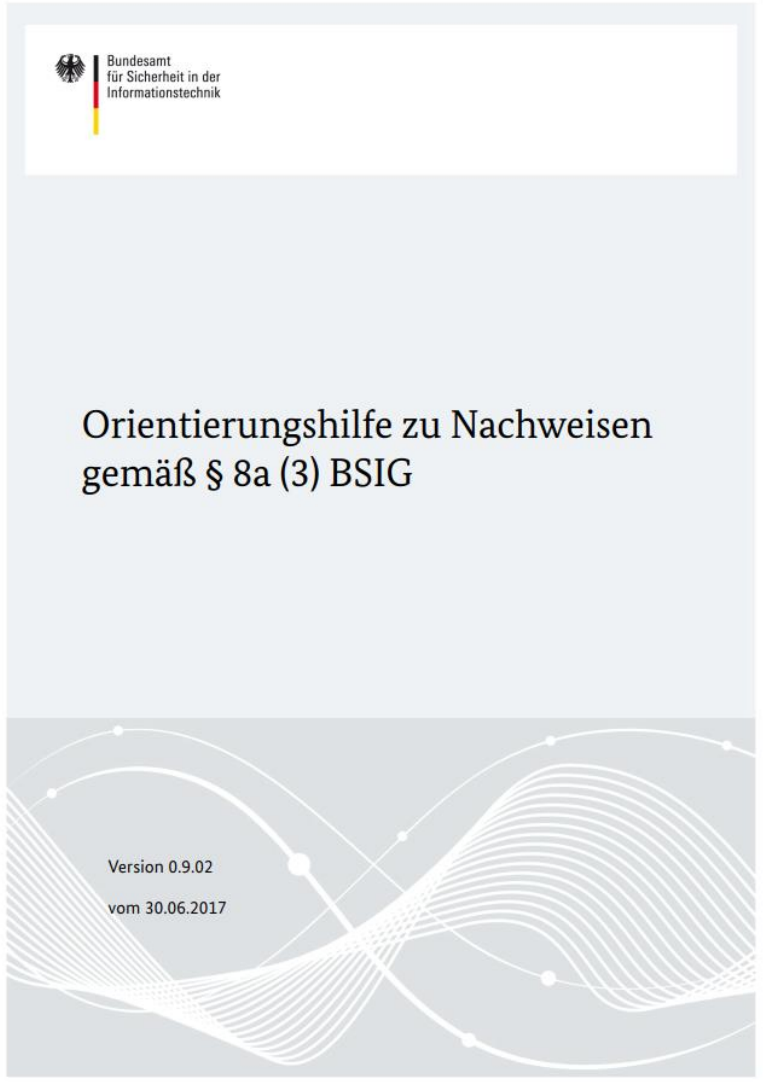
Berücksichtigung eines B3S

Vorhandene Prüfungen & Zertifizierungen

Aufwand der Prüfung

Stichprobenauswahl

ORIENTIERUNGSHILFEN!?



Bedrohungen &
Schwachstellen

Risikomanagement

Technische Informationssicherheit

Asset Management

Bedrohungskategorien

Branchenspezifische Gefährdungslage

Notfallmanagement

ISMS

extern erbrachte Leistungen

ORIENTIERUNGSHILFEN!?

August 2017 Audit „Kick Off“

- Definition des „Scope“
  - Ausgangspunkt „stationäre medizinische Versorgung“
- IT und Risiko
- Interne Kommunikation zum Thema ITSiG

August 2017 Audit „Kick Off“

- IT-„Vorprüfung“
  - Ziel: Ermittlung des Digitalisierungsgrades in den klinischen Prozessem
- Definition „Prüfgegenstand“
- Abstimmung Vorgehen

UNSERE ENTWICKLUNG…

- Beantwortung der Fragen:
  - „Ist der Stand-der-Technik Umgesetzt?“
  - „Ist die Versorgungssicherheit gewährleistet?“

- Ansatz
  - Zerlegung der Frage nach dem „Stand-der-Technik“ in Teilfragen
  - Orientierung am Ziel des IT-Sicherheitsgesetzes (Versorgungssicherheit)

- Herausforderung
  - Wie mit „alter“ Technik umgehen?

DARSTELLUNG DER VORGEHENSWEISE

PRÜFSTRATEGIE

Vorgehensweise

Vorbereitung der Prüfung
- Abstimmung Geltungsbereich
- Festlegung erforderliche Dokumente
- „Vorprüfung IT“

Prüfung IT und IT-Managementprozesse
- Beurteilung technische IT-Sicherheit
- Bewertung der IT-Managementprozesse
- Bewertung der räumlichen Gegebenheiten

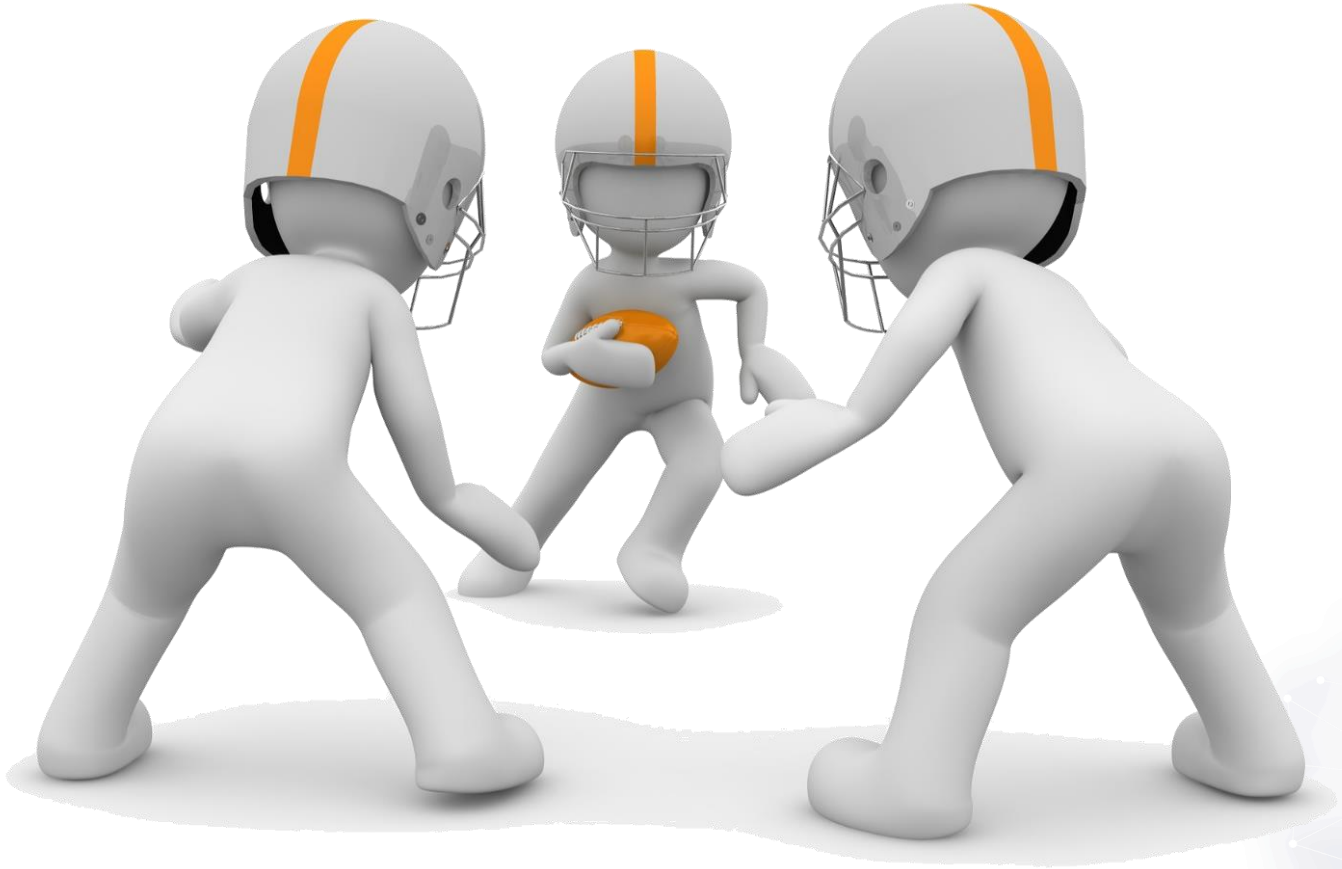
Fachgespräche in klinischen Bereichen
- IT-Durchdringung in klinischen Bereichen
- Resilienz der klinischen Prozessen bezüglich „IT-Problemen“

Dokumentation Schwachstellen
- Dokumentation der Schwachstellen im Prüfbericht
- ggf. Anpassung der Prüfkriterien

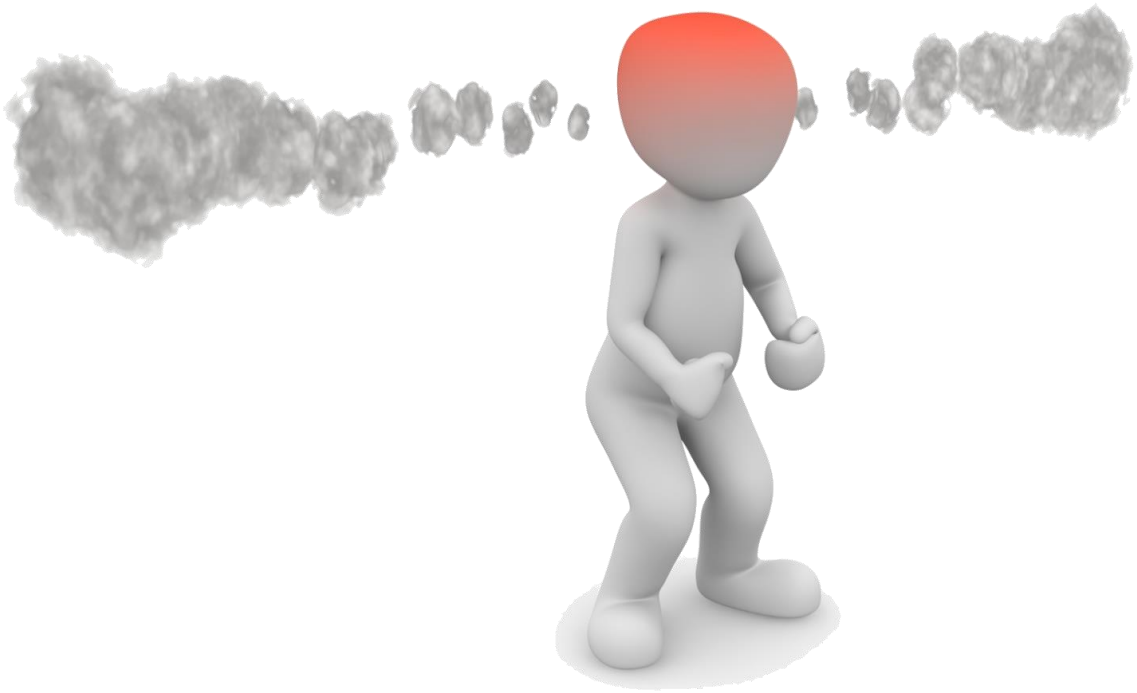
Umsetzung Korrekturmaßnahmen
- Stichwort: „Low-Hanging-Fruits“
- Erstellung Maßnahmenplan

Freigabe Prüfbericht
- Finalisierung Bericht
- Auslieferung an den Betreiber

VORGEHENSWEISE



DIE SITUATION … ZU BEGINN UND WÄHREND DER PRÜFUNG



UNSER ERGEBNIS

Unsere Erkenntnisse während des Audits

Veränderungen im Audit

Anmerkung: ca. 20 Tage Vor-Ort

- 23.04.2018 Übermittlung des Prüfberichts an das BSI

- Aktueller Stand:
  - Anmerkungen des BSI liegen vor
  - Prüfbericht wird angepasst

DAS ERGEBNIS …

… aus Sicht des Betreibers

- Sicherheitsdenken“ wurde aktiviert
- BSI Meldungen sind Wertvoll
- gefühlte Sicherheit (Organisation)
- Ruhe und Gewissheit
- Richtiger Zeitpunkt (Digitalisierungsgrad)
- Wir tragen Verantwortung
- Es gibt noch viel zu tun und das ist gut so!

- Personalresource für ITSiG
- Dringlichkeit hoch halten
- Erwecken nicht drohen
- wenige „Player“
- Keine Alibi Sicherheit

… aus Sicht der Prüfenden Stelle

- Ohne kompetente Fachexperten ist keine sinnvolle Prüfung möglich!
  - Ein IT-Prüfer kann selten klinische und medizinische Prozesse beurteilen!
- Das Wesentliche muss im Fokus stehen!
  - Es geht primär um die Verfügbarkeit kritischer Dienstleistungen.
- Wir definieren die Prüfkriterien individuell!
- Wir halten Kontakt mit dem BSI!

FAZIT

ST. CHRISTOPHORUS-KRANKENHAUS WERNE

Klinikum Lünen
St.-Marien-Hospital
Akademisches Lehrkrankenhaus der Westf. Wilhelms-Universität Münster

SRC security consulting

RuhrNachrichten.de

Suchbegriff

Anmelden/Registrieren

Städte | Nachrichten | Sport | Lifestyle | Bilder | Videos | Meine Themen | Stellen | Immo | Reise | Anzeigen | Abo/Service

Startseite >> Städte >> Lünen >> Dieses Gerät verschafft Herzpatienten lebensrettende Minuten

Neue Technik für Notfälle in Lünen

Dieses Gerät verschafft Herzpatienten lebensrettende Minuten

LÜNEN Wird der Rettungsdienst in Lünen zu einem Notfall mit Herzinfarkt gerufen, zählt jede Minute. Ein neues Gerät der Feuerwehr kann Ärzten und Patienten wertvolle Zeit schenken. Bessere Versorgung in Notfällen – nur durch eine E-Mail.

Da das St.-Marien-Hospital als einziges Krankenhaus in Lünen über ein Herzkatheter-Labor verfügt, wurde die E-Mail-Adresse des Hospitals im Gerätespeicher hinterlegt. Wird nun unterwegs das EKG eines Notfallpatienten gemessen, sendet das Defibrillator-Modul die Aufzeichnungen an das St.-Marien-Krankenhaus, wo Ärzte auf die Daten zugreifen können.

EINE ANEKDOTE ZUM ABSCHLUSS …

ST. CHRISTOPHORUS-
KRANKENHAUS WERNE

Klinikum Lünen
St.-Marien-Hospital
Akademisches Lehrkrankenhaus der
Westf. Wilhelms-Universität Münster

SRC
security consulting

HÖREN SIE AUFMERKSAM ZU.
KOMMUNIZIEREN SIE OFFEN.

Ralf Plomann| plomann.ralf@klinikum-luenen.de | +49 (2306) / 77 2170

Randolf Skerka | randolf.skerka@src-gmbh.de | +49 (228) 2806 - 136