Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

„You ain’t seen nothing yet“ – KRITIS-Highlights 2020

Isabel Münch
Fachbereichsleiterin Kritische Infrastrukturen
Bundesamt für Sicherheit in der Informationstechnik

Worum geht es?

1. Digitalisierung und Cyber-Risiken
2. Erfahrungsbericht KRITIS und Corona
   - Bescheinigungen
   - Umgang mit Vor-Ort-Prüfungen
   - Gefährdungslage
   - Bedeutung Kern-Ressourcen
   - Warum sind Notfallpläne wichtig?
3. Lessons Learned Nachweise: Wie ist die Lage? Wie ist der Umgang damit?
4. Übersicht Branchenspezifische Sicherheitsstandards
5. Ausblick

1. Digitalisierung und Cyber-Risiken

Anwendungen der Digitalisierung

>> Vernetze Lieferketten

Industrie 4.0 / Smart Factory

>> Vernetztes Arbeitsumfeld

>> Smart Factory

>> intelligente Ampelschaltung

Vernetzte Stadt

>> Interagierende Infrastruktur

>> Smart City

>> selbstfahrende Autos

Vernetzte Autos

>> Interaktion mit Infrastruktur

>> Smart Car

>> autonome Haushaltsroboter

Vernetztes Zuhause

>> Vernetzte Haushaltssensoren

>> Smart TV

>> automatisierte Versorgung

Intelligente Stromnetze

>> Vernetztes Arbeitsumfeld

>> Smart Meter

>> automatisierte Versorgung

Vernetztes Gesundheitswesen

>> Neue Möglichkeiten durch Datenauswertung

>> eHealth

Bundesamt
für Sicherheit in der
Informationstechnik

Entwicklung der Digitalisierung

…mehr Datenübertragung

2016	2021
108.000 TB pro Std[1]	*400.000 TB pro Std*[1]

…mehr Geschwindigkeit

2016	2021
27 Mbps (fix)	*53 Mbps (fix)*
7 Mbps (mobil)[1]	*20 Mbps (mobil)*[1]

…mehr Geräte

2016	2021
fünf webfähige Geräte p.K. in D[1]	*neun webfähige Geräte p.K. in D*[1]

…mehr Vernetzung

2016	2021
6 Mrd. M2M fähige Geräte[1]	*14 Mrd. M2M fähige Geräte*[1]

…mehr Angriffe

2016	2021
1,3 Mio. DDoS Angriffe >1 Gbps	*3,1 Mio DDoS Angriffe >1 Gbps*

1 Quelle: CISCO VNI, 2017

Bundesamt für Sicherheit in der Informationstechnik

Wie bedroht ist Deutschlands Cyber-Raum?

- Angreifer nutzen **Schadprogramme für cyber-kriminelle Massenangriffe** aber auch für **gezielte Angriffe** auf ausgewählte Opfer.
- In einer neuen Schadprogramm-Welle **dominiert Emotet die Lage**.
- Rund **117,4 Mio. Variationen von neuen Schadprogrammen** wurden im Berichtszeitraum gesichtet. Das sind durchschnittlich **322.000 pro Tag, in Spitzenwerten 470.000**.
- Knapp **7 Millionen Meldungen zu Schadprogramm-Infektionen** hat das BSI an deutsche Netzbetreiber übermittelt.
- Bei Angriffen auf die Bundesverwaltung wurden rund **35.000 E-Mails mit Schadsoftware pro Monat** abgefangen.
- **24,3 Millionen Patientendatensätze** waren Schätzungen zufolge international frei im Internet zugänglich.
- Cyber-Kriminelle nutzen **COVID-19-Pandemie** für Social-Engineering-Angriffe aus.

Quelle: BSI

Cyber-Sicherheit in der Digitalisierung

Vernetzung

Komplexität

Allgegen-
wärtigkeit

Digitalisierung bedeutet…

…mehr Möglichkeiten,

auf die Deutschland nicht verzichten kann und soll

…mehr Gefahren,

auf die Deutschland vorbereitet sein muss

Cyber-Sicherheit **…unverzichtbare Voraussetzung für das Gelingen der Digitalisierung**

Bundesamt
für Sicherheit in der
Informationstechnik

2. Kritische Infrastrukturen und Covid-19

Kritische Infrastrukturen (KRITIS)

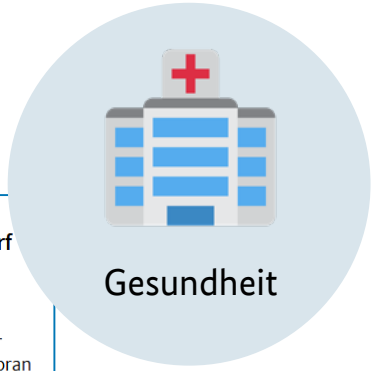
Kritische Infrastrukturen im Sinne des BSI-Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Höhere Gefährdungslage durch die Pandemie

- Erhöhtes Bedrohungsrisiko im Sektor Gesundheit
- Erhöhte IT-Abhängigkeit durch vermehrtes Homeoffice
- Stärkere Belastung der IT-Infrastruktur und Herausforderung für Cyber-Sicherheit aufseiten der Betreiber
- Unsicherheit in der Bevölkerung: Gefahr durch Phishing, Social Engineering, DDoS-Angriffe und Schadprogramme steigt

IT-Sicherheitsmaßnahmen müssen aufrechterhalten und an die neuen Umstände angepasst werden!

Cyber-Sicherheitsvorfälle



IT-Ausfall an der Uniklinik Düsseldorf

- Ab dem 10. September 2020 waren zentrale IT-Systeme des UKD weitreichend gestört.
- Hintergrund war ein Hackerangriff, der eine Schwachstelle in einer Anwendung ausnutzte.
- Die Sicherheitslücke befand sich in einer marktüblichen Zusatzsoftware.

UKD Universitätsklinikum Düsseldorf

17.09.2020

IT-Ausfall an der Uniklinik Düsseldorf

Update (17. September 2020, 10.00 Uhr): Cyberangriff bestätigt – Sicherheitslücke in verbreiteter Software ermöglichte Zugang – Wiederherstellung geht Schritt für Schritt voran

Seit Donnerstag letzter Woche (10.9.) ist das IT-System des Universitätsklinikums Düsseldorf (UKD) weitreichend gestört. Daher ist das UKD weiterhin von der Notfallversorgung abgemeldet und Patienten mit Terminen sollten zur Abstimmung Kontakt mit der behandelnden Abteilung aufnehmen.

Nach Informationen der Staatsanwaltschaft und des Justizministeriums hat die Polizei in Zusammenarbeit mit externen Spezialisten und den IT-Fachleuten der Klinik inzwischen konkrete Anhaltspunkte für die Ursache ermittelt. Hintergrund des Ausfalls ist nach diesen Analysen ein Hackerangriff, der eine Schwachstelle in einer Anwendung ausnutzte. Die Sicherheitslücke befand sich in einer marktüblichen und weltweit verbreiteten kommerziellen Zusatzsoftware. Bis zur endgültigen Schließung dieser Lücke durch die Softwarefirma war ein ausreichendes Zeitfenster gegeben, um in die Systeme einzudringen. Als Folge des damit ermöglichten Sabotageakts fielen nach und nach Systeme aus, Zugriffe auf gespeicherte Daten waren nicht mehr möglich.

Die IT-Experten konnten mittlerweile den genauen Umfang analysieren und den Zugang zu den Daten wiederherstellen. Bisher gibt es keine Anhaltspunkte dafür, dass Daten unwiederbringlich zerstört worden sind. Auch für das Abfischen von konkreten Daten gibt es nach heutigem Stand keine Belege. Eine konkrete Lösegeldforderung gab es nicht.

„Wir danken als Vorstand allen unseren Beschäftigten und insbesondere unseren IT-Fachleuten für die hervorragende Arbeit in dieser schwierigen Situation. Ganz besonders wollen wir die gute Zusammenarbeit mit der Polizei, dem LKA und den hinzugezogenen IT-Experten herausstellen. Sie haben innerhalb kurzer Zeit herausarbeiten können, dass es sich um einen Angriff von außen handelte und nicht um einen Fehler eines Nutzers. Es war also nicht nur das Universitätsklinikum durch die Sicherheitslücke gefährdet, sondern weltweit sehr viele Unternehmen," erläutert Prof. Dr. Frank Schneider, Ärztlicher Direktor des UKD.

Quelle: uniklinik-duesseldorf.de

Erstmaßnahmen des BSI zu Beginn des Lockdowns

- Veröffentlichung von Informationsmaterial zur IT-Sicherheit in der Pandemie-Situation
- Für registrierte KRITIS-Betreiber und Teilnehmer im UP KRITIS:
  - **Schriftliche Bestätigung des Betriebs von kritischen Dienstleistungen**, so dass bei einer (möglichen) Ausgangssperre das Personal zur Arbeitsstelle gelangen kann, TK-Bevorrechtigungen geschaltet werden und weitere Maßnahmen der Kommunen (wie z. B. Bevorrechtigung bei der Kinderbetreuung) greifen können
  - **Aussetzung des Mahnwesens** für Nachweiserbringung, da Personal zur Bewältigung der neuen Anforderungen an IT-Abteilungen gebunden wurde
  - Internetbasiertes **Austauschforum im UP KRITIS**
- Speziell für systemkritische Unternehmen im Kontext von COVID-19: zusätzliches Informationsmaterial zur IT-Sicherheit und Notfall-Kontaktadresse des BSI

Umgang mit Vor-Ort-Prüfungen

Nachweisprüfungen

- Fester Bestandteil einer Prüfung nach § 8a Absatz 1 BSIG sind Prüfungshandlungen, die die prüfende Stelle beim Betreiber vor Ort vornimmt
- Aber Corona?
- Remote-Prüfung an Stelle einer Vor-Ort-Prüfung ist Prüfmangel
- Akzeptiert bis 12/2020

Und danach?

- Vor-Ort-Prüfung oder Risikobewertung:
  - Ausnahmsweise einzelne Prüfschritte remote
  - Voraussetzung sind Risikobewertung und Dokumentation
  - Beispiel: zum Zeitpunkt eines Vor-Ort-Termins für Prüfer und Betreiber erhöhte Infektionsgefahr
  - Beispiele Prüfschritte: Interviews, Einsichtnahme Server, Zutrittskontrolle

Lessons Learned Covid-19

- The Importance of Being Critical Infrastructure
- Entdeckung der Kern-Ressourcen
- BCMS als Stützpfeiler in der Krise

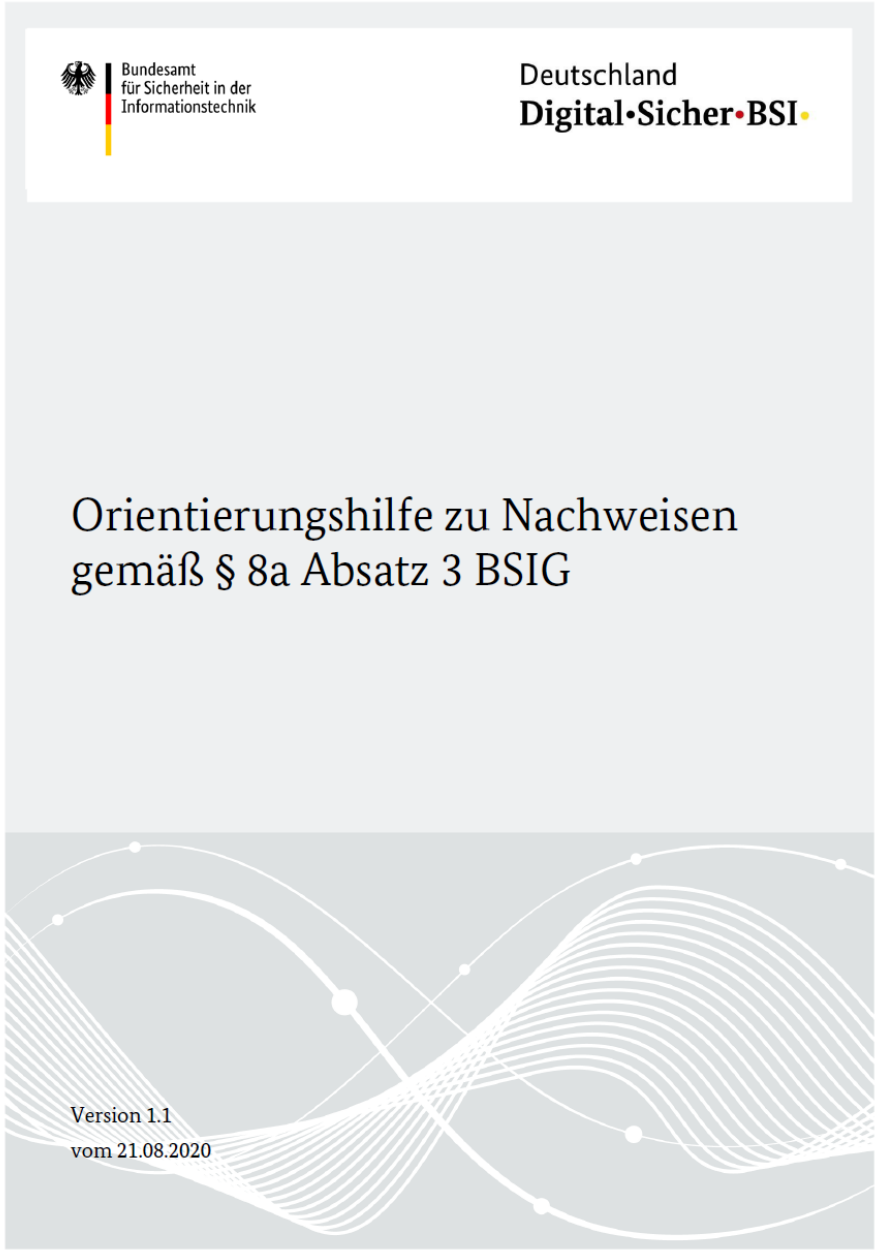
Notfallpläne: Plane den Notfall in der Zeit,
so hast Du im Notfall einen Plan!

3. Lessons Learned Nachweise

Lessons Learned Nachweise

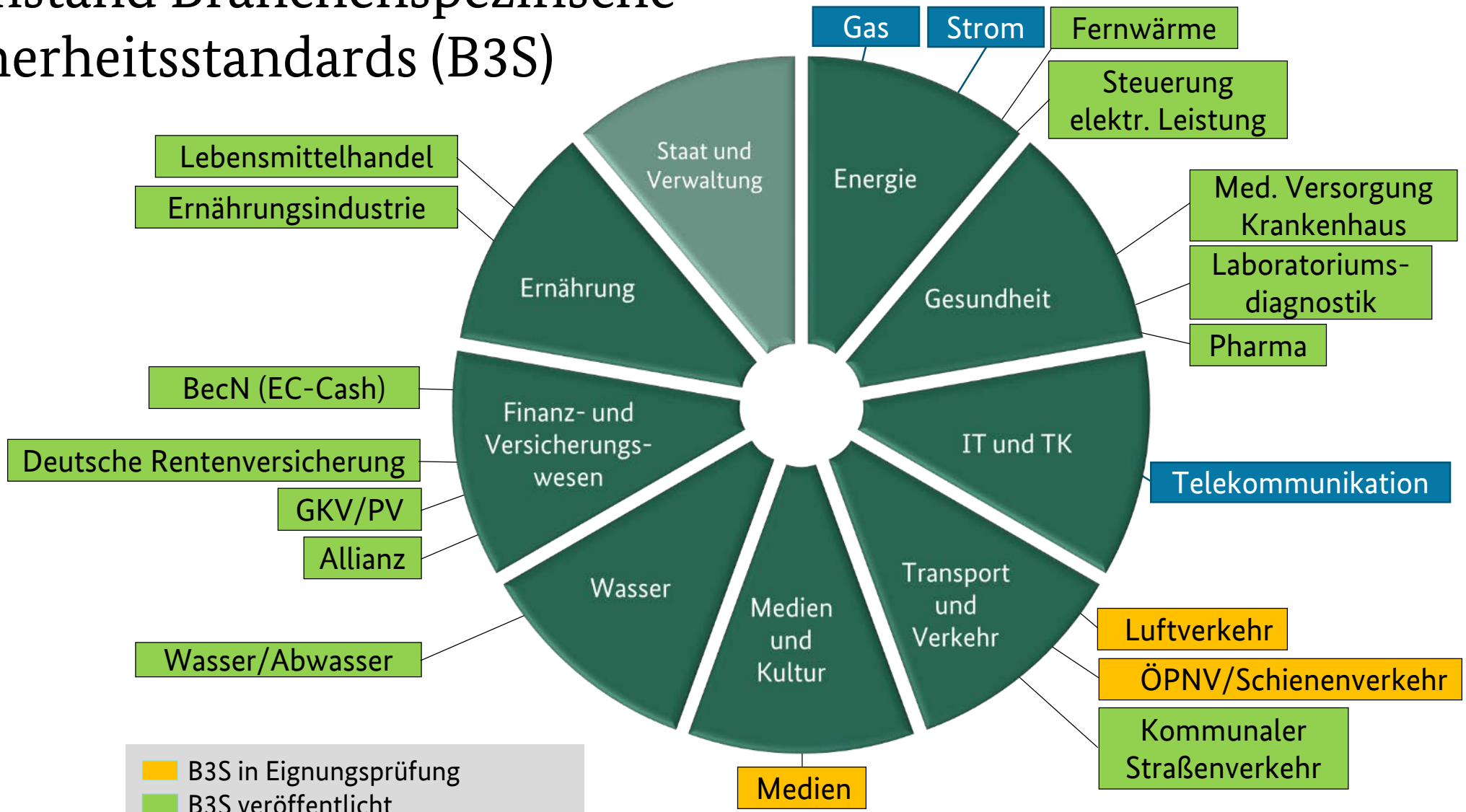
- Was haben wir gesehen?
  - Gefährdungslage
  - Typische Mängel bei KRITIS-Anlagen

- Wie haben wir reagiert?
  - Angepasste Formulare
  - Änderungen in OH Nachweise
  - Reifegrad
  - Geltungsbereich / Anhörung nach §8a (5)
  - Monitoring der Mängelbeseitigung
  - Tiefenprüfungen nach §8a (4)



4. Übersicht Branchenspezifische Sicherheitsstandards

Sachstand Branchenspezifische Sicherheitsstandards (B3S)



Bundesamt für Sicherheit in der Informationstechnik

5. Ausblick

Fazit

- KRITIS ist angekommen
- KRITIS ist erfolgreich
- Mit /als KRITIS gut durch die Pandemie
- KRITIS geht weiter

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

KRITIS-Büro
Postfach 20 03 63
53133 Bonn
Tel: +49 (0)22899-9582-6166
Fax: +49 (0)22899-10-9582-6166
kritis-buero@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik