DMEA Berlin 9.–11. April 2019 Connecting Digital Health

CHARITÉ UNIVERSITÄTSMEDIZIN BERLIN

André Solarek
Stabsstelle Katastrophenschutz und Notfallplanung

Einschränkung Notfallmedizinischer Versorgungsprozesse durch Ausfall IT-gestützter Verfahren im Krankenhaus - Erfahrungsbericht einer Stabsrahmenübung

Agenda

- Motivation
- Ausgangsszenario
- Übungsaufbau
- Übungsablauf
- Konsequenzen
- Fazit

Quelle: pixabay.de

CHARITÉ – Universitätsmedizin Berlin

4 Standorte / Sites	>100 Kliniken und Institute / Departments and Institutes	17 CharitéCentren / Charité Centers	3.011 Betten / Beds	232 Professoren/Professorinnen / Professors	90 Nationen / Nationalities	> 7.200 Studierende / Students	1.210 Mio. Euro Umsatzerlöse im Jahr 2017 / Total Revenue
13.760 Charité-Beschäftigte / Charité Employees	4.395 Pflegekräfte / Nursing Staff	3.952 Wissenschaftler/-innen und Ärztinnen/Ärzte / Researchers and Physicians	> 4.000 Veröffentlichungen in wissenschaftlichen Zeitschriften / Publications in Scientific Journals	162 Mio. Euro Drittmitteleinnahmen / External Funding	148.304 Voll- und teilstationäre Fälle / Inpatients and Day Case Patients	702.367 Ambulante Fälle / Outpatients	5.495 Geburten / Births

Quelle: Jahresbericht 2017 der Charité

Eckdaten Charité IT

Quelle: pixabay.de

Motivation zur Übung:

- Anforderung der Gesundheitssenatorin
- Eigener Antrieb zur Überprüfung der Strukturen und Vorbereitungen
  - Alarmierung
  - Einsatzunterlagen
  - Strategien
- Überprüfung der etablierten übergreifenden Prozesse
- Sensibilisierung der Mitarbeiter

Quelle: pixabay.de

Ausgangsszenario

- bei durch Routine-Wartungsarbeiten eines externen Dienstleisters wurde Schadsoftware mittels eines infizierten USB-Sticks unbemerkt in die IT-Infrastruktur des Krankenhauses eingeschleust
- Anfänglich wurde nur einige Befundarbeitsplätze (RIS/PACS-Workstations) im CT und Röntgenbereich in der zentralen Notaufnahme gestört und im weiteren zeitlichen Verlauf durch die Schadsoftware isoliert
- nach und nach wurden weitere Radiologiearbeitsplätze infiziert so dass keine Notfallpatienten mehr versorgt werden konnten

Übungsaufbau – Teil 1

Übungs-leitung

Steuerung

Helpdesk

GB-IT

Sicherheits-team

Reaktions-gruppe

Email-Einspieler

Telefon-Einspieler

Dokumentation

Übungszenario und Drehbuch

Übungsaufbau – Teil 2

Übungs-leitung

Moderation

Hilfestellung

Steuerung

Krisenstab

Reaktions-gruppe

Email-Einspieler

Telefon-Einspieler

Dokumentation

Übungszenario und Drehbuch

Übungsablauf - Teil 1

- Teil 1 der Übung wurde real im GB-IT durchgespielt
- Ziel:
  - Erfassen der Reaktionszeiten
  - Initiierung der Kaskade „IT-Sicherheitsvorfall“
  - Einleiten erster Eindämmungs-maßnahmen
  - Alarmierung und Einberufen der Gesamteinsatzleitung
  - Risikosensibilisierung

28.02.2019 10:00 Die folgende Nachricht wurde empfangen:
Helpdesk Online-Auftrag
An: Helpdesk
CC:

Der folgende Online-Auftrag wurde über das INTRAnet-Portal der Charité aufgegeben:
Name: Solarek
Vorname: Andre
E-Mail-Adresse:
Telefonnummer:
Geräte-Typ: PC
Inventarnummer: 711
Campus: Charité Campus Mitte (CCM)
Straße / Gebäude: Rettungsstelle Mitte
Ebene / Etage: 1
Raumnummer: 01-082
Beschreibung der Störung: ÜBUNG --- ÜBUNG --- ÜBUNG--- ÜBUNG---In der Rettungsstelle Mitte sind dieser und weitere RIS/PACS-PCs ausgefallen. Beim Neustart kommen komische Meldungen, ohne das etwas passiert. Wir benötigen schnelle Hilfe, da die Rettungsstelle sonst bald nicht mehr arbeiten kann!
10:07 an IT-Servicepunkt CCM weitergeleitet
10:08 von IT-Service Mitarbeiter geöffnet und bearbeitet: Vor Ort das Informationsschreiben erhalten
10:20 Ich als IT-Sicherheitsmanager wurde gerade vom IT-Service Mitarbeiter angerufen bzgl. des eingetretenen Vorfalls (Ausfall mutipler Befundungs PCs) – Ticket wird nun an das IT-Sicherheitsteam weitergeleitet, wir werden und nun zusammensetzen

Übungsablauf - Teil 1

- 10:00 – 11:00
  - Erste Meldungen über PC Störung laufen im IT Helpdesk auf
  - von IT-Service Mitarbeiter vor Ort in der Notaufnahme
  - Meldung IT-Sicherheitsmanager äußert den Verdacht eines Verschlüsselungstrojaners
  - Erste Lagebesprechung GB IT und Weiterführung der Analysen
- 11:00 – 12:00
  - wurde die sofortige radiologische Netzwerkstrennung Charité Mitte vereinbart
  - **CIO und CISO informieren den Krisenstab und setzten für 12:30h die erste Lagebesprechung an**

ÜBUNG --- ÜBUNG --- ÜBUNG --- ÜBUNG --- ÜBUNG ---

Die folgenden Rechner in der Rettungsstelle (Räume siehe unten) wurden im **ÜBUNGSSZENARIO** von einem Verschlüsselungsvirus komplett lahmgelegt:

01-081 – Ultraschall	.charite.de	
01-082 – Demoraum	1.charite.de	.charite.de
	.charite.de, c	1.charite.de
	.charite.de, c	1.charite.de
01-085 – Steuerungsraum	.charite.de, c	.charite.de
	1.charite.de	
01-066 – Schockraum	.charite.de	

Komplett lahmgelegt heißt konkret: kein Booten möglich, USB-Sticks sind gesperrt (DS-Klasse MED)

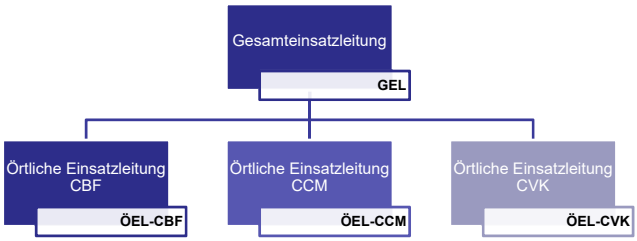
DIES IST EINE ÜBUNG, KEINE AKTIONEN AN DEN RECHNERN DURCHFÜHREN!!!!!

ÜBUNG --- ÜBUNG --- ÜBUNG --- ÜBUNG --- ÜBUNG ---

Übungsablauf - Teil 2

Gesamteinsatzleitung = Krankenhauseinsatzleitung (KhEL)/Krisenstab

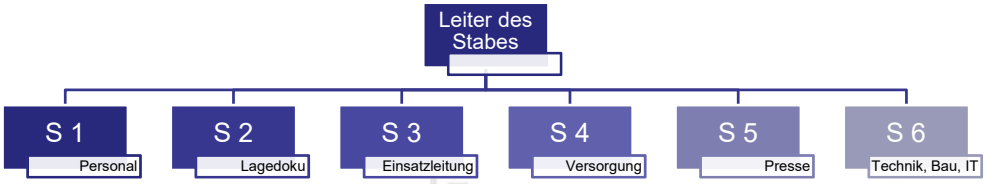
- Höchste klinische Entscheidungsebene im Schadensfall
- Besetzung durch Vertreter der Klinikumsleitung und des Vorstandes
  - Direktor des Klinikums
  - Kaufmännische Leitung
  - Ärztliches Direktorat
  - Stabst. Katastrophenschutz
  - Pflegedirektion
  - Fakultät
  - Presseabteilung
  - Leitung von Technik, Bau und IT



Übungsablauf - Teil 2

Gesamteinsatzleitung = Krankenhauseinsatzleitung (KhEL)/Krisenstab

- Alarmierung bei großen Schadenslagen oder wenn mehr als Standort betroffen ist
  - Aufbau und arbeiten einer Strabsstruktur
  - Aufgabe:
    - geeignete Maßnahmen zu ergreifen, um die Ursache festzustellen
    - Maßnahmen einleiten, um die Patientenversorgung zu sichern
    - Erarbeitung von Strategien zur Wiederherstellung des Krankenhausbetriebes



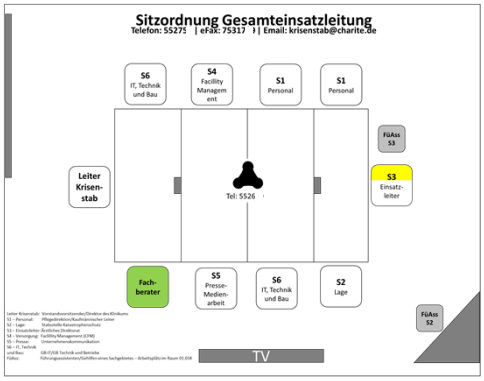
CHARITÉ UNIVERSITÄTSMEDIZIN BERLIN
Stabsstelle Katastrophenschutz und Notfallplanung

Übungsablauf Teil 2

12:30 – 13:00

- Krisenstab nimmt nach Lagebesprechung Arbeit auf
  - Initiierung Ressourcenabfrage an anderen Standorten
  - Information der Mitarbeiter über Lage
  - Meldung an Behörden

- Notfallmanagement
  - Kontrolliertes Beenden von laufenden OP´s
  - Abmelden der ZNA für Regelversorgung
  - Detektion von hochkritischen ICU-Patienten



Übungsablauf Teil 2

13:00 – 15:00

- Personalorganisation
  - Aufstocken der Ressourcen für Krankentransport
  - Externe Mitarbeiteralarmierung
  - Ressourcenaufstockung für Funktionsbereiche

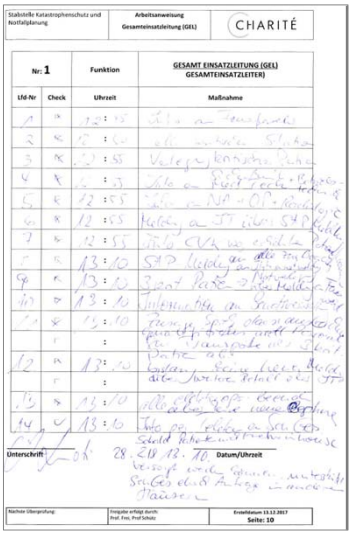
- Sicherung der Notfalldiagnostik
  - Evaluierung Alternative zu CT
  - Bilddaten können nicht an PACS überspielt werden
    - Nur lokale Bildspeicherung möglich

Quelle: pixabay.de

Übungsablauf Teil 2

15:00 – 17:00

- Ausbreitung der Schadsoftware
  - Kurzzeitspeicher durch Datenverschlüsselung an allen Standorten ausgefallen
  - Einleiten einer Wiederherstellung -> ca. 3Std
  - Lokale Befundung am Gerät möglich
    - Datenverlust aufgrund eines eventuellen Speicherüberlaufes möglich
- Informationen und Meldungen:
  - Meldung an das BSI erfolgt
  - Information über Ausbreitung der Schadsoftware in externen Arztpraxen
    - Schadsoftware wurde über Befund-DVD´s verbreitet


Stabsstelle Katastrophenschutz und Notfallplanung | Arbeitsanweisung Gesamteinsatzleitung (GEL) | CHARITÉ

Nr: 1 | Funktion: GESAMT EINSATZLEITUNG (GEL) GESAMTEINSATZLEITER

Lfd-Nr	Check	Uhrzeit	Maßnahme

Unterschrift | Datum/Uhrzeit: 28.10.12.10

Nächste Überprüfung | Freigabe erfolgt durch: Prof. Frei, Prof Schulz | Erstelldatum 13.12.2017 | Seite: 10

Übungsablauf Teil 2

17:00 – 19:00

- aktuelle Virenpatter
  - sind bereitgestellt und werden eingespielt
- vermehrte Presseanfragen
  - Vorbereiten einer Pressekonferenz
  - Fortführen des Monitoring und Bedienern der Sozialen Medien

18:00 – 20:00

- PACS wiederhergestellt
  - Bildversand angestoßen
- Rückführung in den Regelbetrieb

Quelle: Charité

Übungsablauf Teil 2

20:00

- **Pressekonferenz und Lageende**

Quelle: Charité

Konsequenzen

- Reale Lösungszeiten sind zu ermitteln:
  - z.B. tatsächliche Wiederherstellungszeit einer Befundungsworkstation
  - Kalibrieren von Untersuchungsgeräten nach Wiederherstellung
- Vorbereitete Datenschutz/Juristische Bewertungen/Einschätzungen
  - Bewertung von geplanten Maßnahmen (Handzettel)
- Verbindliche Abklärung technischer und Organisatorischer Schnittstellen zur Medizintechnik

Quelle: pixabay.de

Fazit

- 6 monatige Vorbereitung
- Externe Begleitung
- Günstige Infrastrukturvoraussetzung

Erkenntnisse:

- Schnelle Reaktion des IT Sicherheitsteam
- Sensibilität des Vorstandes gegen über dem Themenkomplex „Cybersecurity“ gestiegen
- Gute Zusammenarbeit, Kommunikation und Dokumentation im Stab

HERZLICHEN DANK

CHARITÉ – Universitätsmedizin Berlin
André Solarek | Ärztliches Direktorat
Stabsstelle Katastrophenschutz und Notfallplanung
Chariteplatz 1 | 10117 Berlin
Tel: +4930 450 552662
Email: katastrophenschutz@charite.de

Quelle: Jahresbericht 2017 der Charité