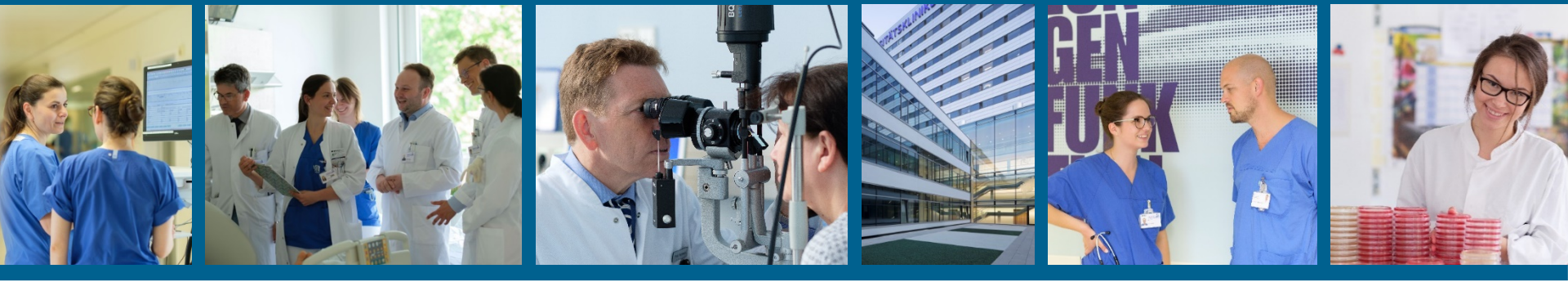
UNIVERSITÄTS MEDIZIN FRANKFURT
GOETHE-UNIVERSITÄT

Cyberangriff entlarvt: Ein einzigartiger Einblick in die Bedrohung



University Center for Digital Healthcare

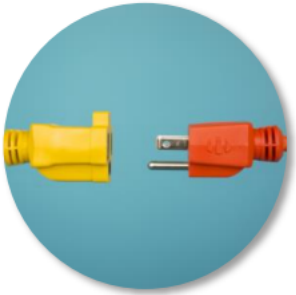
Was ist passiert?

06.10.2023

Entdeckung von Auffälligkeiten im zentralen Benutzerverzeichnis des UKF bei Routine Kontrolle

06.10.2023

Alarmierung relevanter IT-Mitarbeiter, sowie Aktivierung der zentralen Dienstleister.



07.10.2023

Zusammenkunft Krisenstab. Trennung der zentralen Internetverbindung. Kein Webzugriff / Mail mehr für gesamtes UKF.

08.10.2023 ff

Maßnahmen zur Betriebsaufrechterhaltung des UKF.

Wie ist es passiert?

26.09.2023 – Zugriff über Remote-Zugang

Installation Mimikatz und Versuch anderer Tools herunterzuladen und zu installieren

Versuch div. Zugriffe/ Zugänge auf erreichbare Systeme

Passwörter aus Browser und Arbeitsspeicher ausgelesen

Accounts/ Admin-Accounts im AD angelegt

Jumphost mit Screenshot-Tool – 16.000 Bilder

Incident Response Organisation

- Krisenmanager: Vorstandsvorsitzender UKF
- Security Incident Response Kernteam: UKF mit Vertretern aus verschiedenen Dezernaten und Fachbereichen (Krisenstab)
- Dienstleister für IT-Betriebsunterstützung und Dienstleister für DFIR
- u. a. tägliche Status-Meetings, Erkenntnisse und Lagebild, Entscheidungen, z. B. für Notbetrieb
- Incident Response & Digital Forensics: DFIR-Dienstleister
- Notbetrieb & Wiederanlauf: UKF DICT-Abteilungen, Dienstleister

Wichtigstes Ziel in dieser Situation:

Aufrechterhaltung der Patientenversorgung und der Betriebsfähigkeit

Internettrennung und dessen Folgen

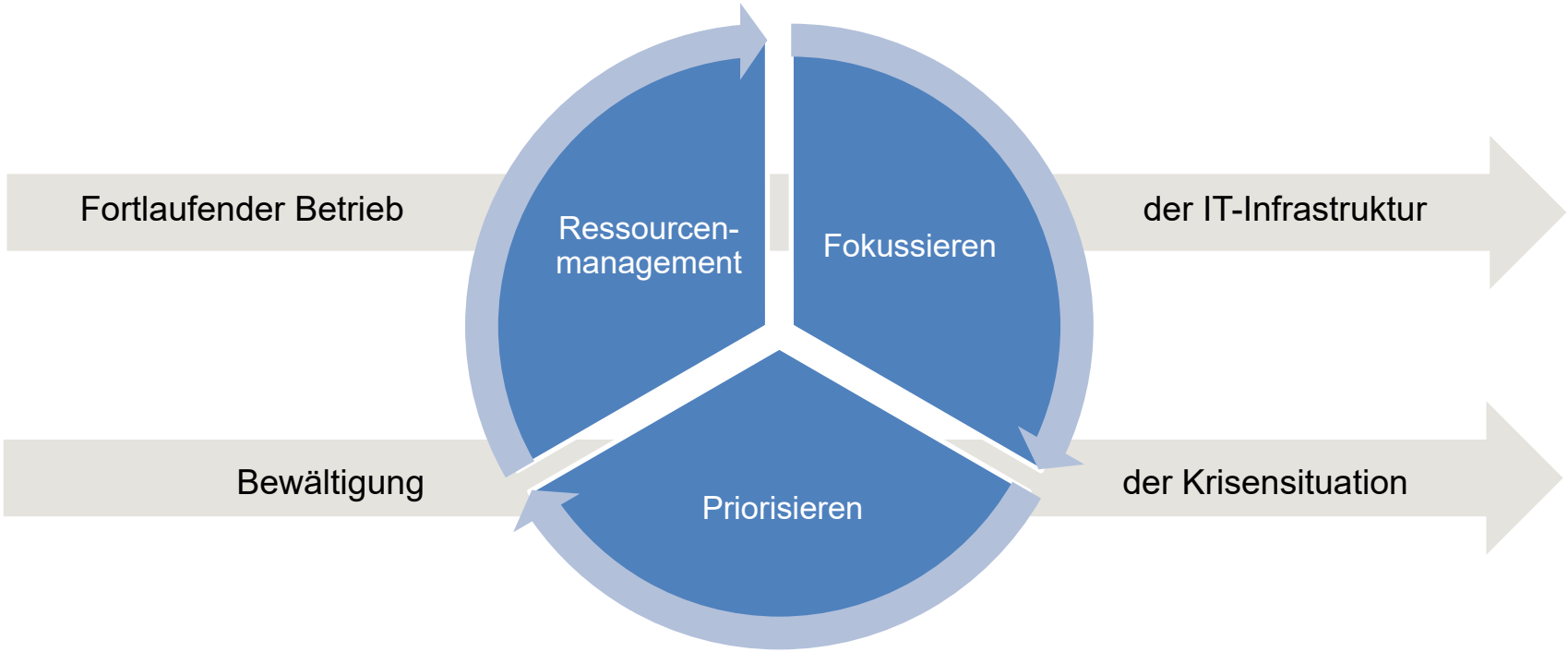
Incident Response – kurzfristige Maßnahmen

- Sperrung der "neuen" AD-Konten mit Dom-Admin-Rechten, die vom Hacker dem System hinzugefügt wurden
- Schutz der Backups durch physikalische Abkopplung von dem internen Netz (LAN)
- Trennung vom Internet und Trennung der internen Netze voneinander, zwecks Isolierung des Angreifers
- Scan der gesamten Infrastruktur auf IoCs und Bereinigung bzw. Neuinstallation betroffener Systeme
- Einspielen von Sicherheitspatches
- Aktivierung eines Spezialdienstleisters für Incident-Response & Forensik und Unterstützung in IT-Sicherheitsfragen
- Konstituierung des internen Krisenstabs unter Leitung des Ärztlichen Direktors
- Definition von verschiedenen Arbeitsgruppen/Gremien auf technischer und politischer Ebene
- Etablierung einer dedizierten, cloudbasierten IT-Infrastruktur (Grüne Zone), um unabhängig von der kompromittierten Infrastruktur (Rote Zone) sicher untereinander, aber auch mit externen Stellen, kommunizieren zu können.

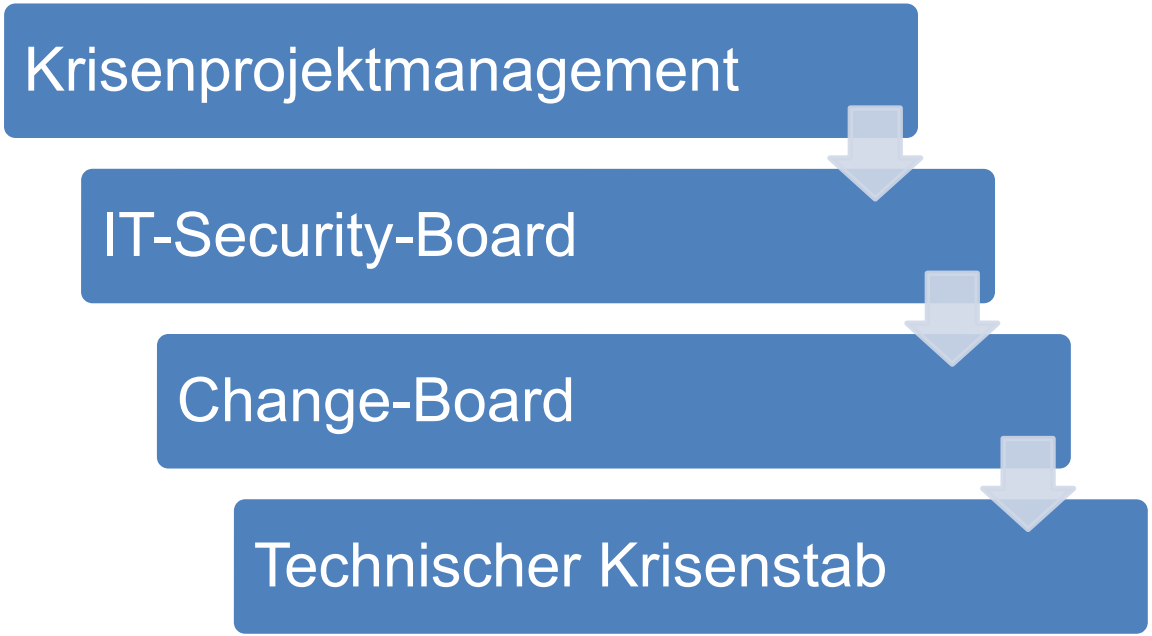
Grüne Zone


https://notfall-kgu.uni-frankfurt.de
UNIVERSITÄTS KLINIKUM FRANKFURT
MEDIZINISCHE FACHABTEILUNGEN
NOTFALL
Herzlich Willkommen auf der Übergangs-Homepage des Universitätsklinikum Frankfurt!
Das Universitätsklinikum Frankfurt hat am 6. Oktober festgestellt, dass ein Hackerangriff auf sein System versucht wird. Deshalb haben wir als Vorsichtsmaßnahme unser Netzwerk vom Internet getrennt. Es gibt bisher keine Hinweise darauf, dass Daten verlorengegangen oder entwendet wurden.
Vermittlungszentrale
T +49 69 63 01 – 0
F 069 6301 6301
E-Mail info@ukffm.de
Medizinische Fach-abteilungen ➔
Direkte Durchwahlen
Lob- und Beschwerde-management
Service- und Telefonzeiten
Montag / Dienstag 09:00 – 11:30 Uhr

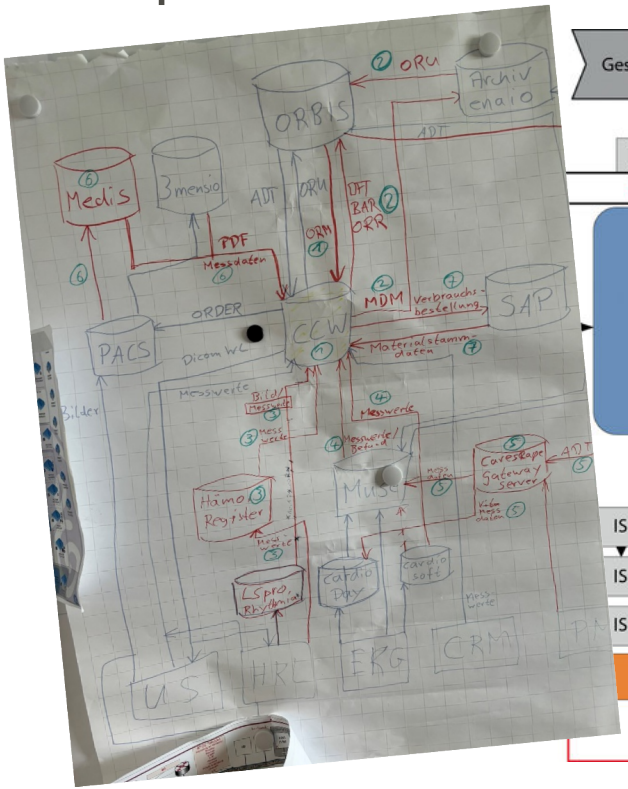
Folgen bewältigen

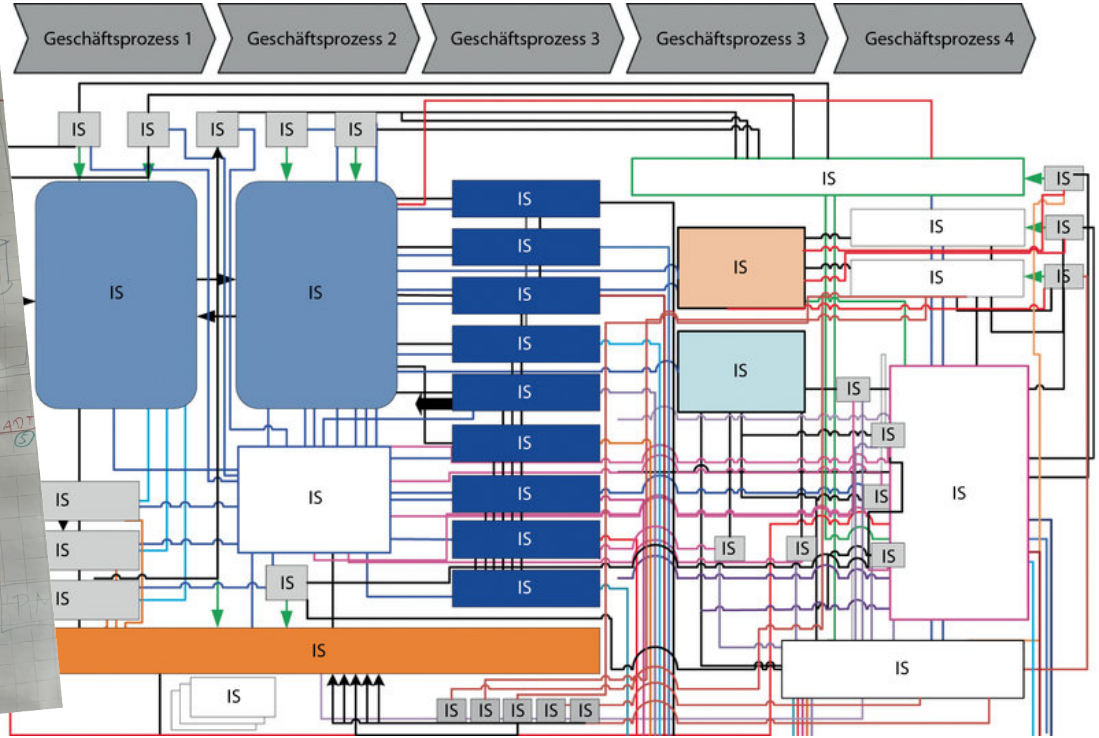


Folgen bewältigen



Komplexe IT-Landschaft





Folgen und Alltag bewältigen

- *Seine IT-Landschaft/ Architektur transparent haben und kennen*
- *Kontaktliste aktuell haben*
  (Darin sollte ein qualifizierter Incident-Response-Dienstleister enthalten sein.)
- *Verträge/ SLAs zentral verfügbar haben und dessen Inhalte kennen*
- *Funktionierende Krisen- und Notfall-Managementstrukturen besitzen*

Mittel-/ Langfristige Maßnahmen

- Härtung der Core-IT (insbesondere Tiering des Active Directorie)
- Beschaffung und Implementierung einer neuen Firewall, inkl. Neu-Konzeptionierung von Fernwartung und Mobiler Arbeit inkl. VPN
- Beauftragung eines „Managed Service“ für SIEM/SOC, inkl. des Anschlusses der Systeme an das SIEM
- Beschaffung und Rollout eines NextGen EDR-Systems
- Beschaffung und Implementierung eines NextGen NDR-Systems und eines Schwachstellen-Scanners

Schutzmaßnahmen der Klinik-IT

- Sichere Passwörter
- Zwei-Faktor-Authentisierung (2FA)
- „Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus“ – B3S als Grundlage des täglichen Handeln nutzen (Informationssicherheit im Krankenhaus | Deutsche Krankenhausgesellschaft e. V.)
- Auf Cyber-Zwischenfall vorbereitet sein
- Externe Dienstleister als verlängerte Werkbank nutzen (…aber auch auf Einhaltung zur Informationssicherheit überprüfen!)

UNIVERSITÄTS MEDIZIN FRANKFURT
GOETHE-UNIVERSITÄT

Vielen Dank für Ihre Aufmerksamkeit!
Fragen oder Anregungen?

University Center for Digital Healthcare