TECHNISCHE UNIVERSITÄT DARMSTADT

!nfoSec

# HEARTBEAT EMERGENCY-SERVER

Vorstellung am 11. Kommunalen IT-Sicherheitskongress Mai 2025

© Axel Becker

TECHNISCHE UNIVERSITÄT DARMSTADT

# ÜBERBLICK

!nfoSec

1 Vorstellung Technische Universität Darmstadt und Informationssicherheit

2 Warum sind wir heute hier? – Informationen zum InfoSec Impact Award

3 HEARTBEAT – Blick unter die Motorhaube

4 HEARTBEAT – Ablauf in einem IT-Notfall

5 Abschluss

TECHNISCHE UNIVERSITÄT DARMSTADT

InfoSec

# VORSTELLUNG

Technische Universität Darmstadt

Informationssicherheit / TUDa-CERT

© Thomas Ott

TECHNISCHE UNIVERSITÄT DARMSTADT

# TECHNISCHE UNIVERSITÄT DARMSTADT

!nfoSec

- Gegründet 1877
- 340 Professuren
- 2.670 wissenschaftlich Mitarbeitende
- 2.056 administrative Beschäftigte
- 108 Auszubildende
- 24.293 Studierende
- 5 Standorte mit 175 Gebäuden
- Fast 30 ausgezeichnete kooperative Forschungsbereiche, -zentren und -schwerpunkte

(Stand: Jahreswechsel 2024/2025)

TECHNISCHE UNIVERSITÄT DARMSTADT

# TEAM INFORMATIONSSICHERHEIT

!nfoSec

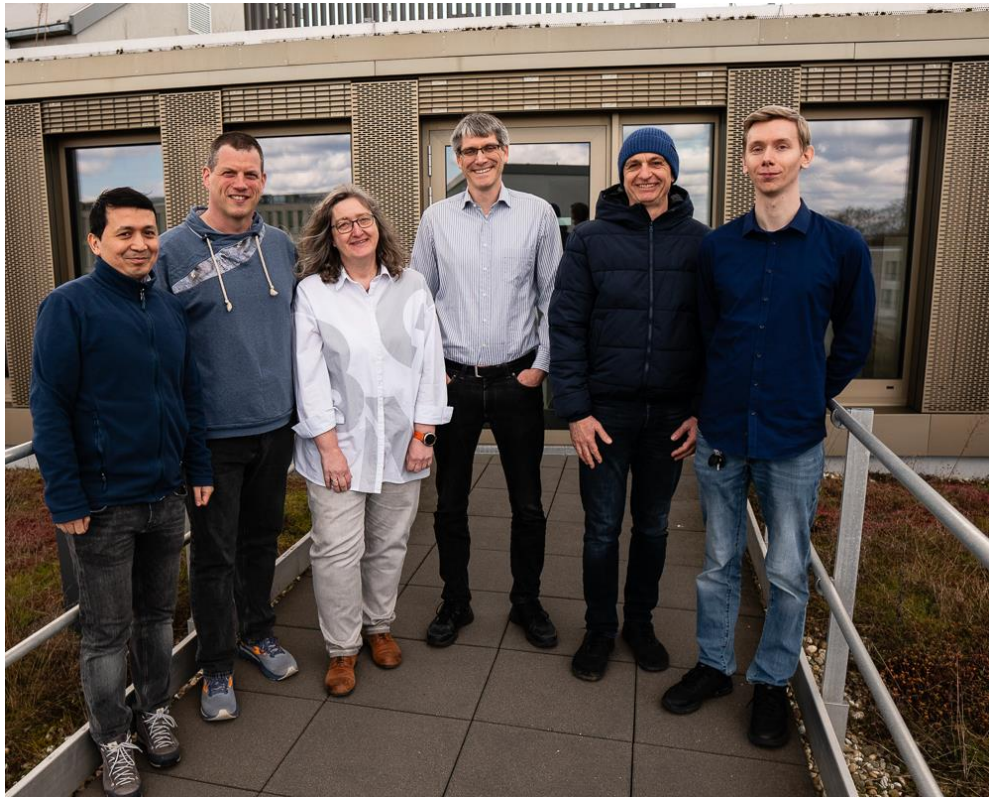
Dr.-Ing. Johannes Braun

Leiter Hochschulrechenzentrum (seit 01/2025)
Chief Information Security Officer der TU Darmstadt (CISO)

Jochen Becker

Leiter TUDa-CERT

- 01/2021 Gründung als Teil des RZ
- 07/2021 Benennung CISO
- 01/2023 Herauslösung aus RZ Ansiedelung ans Präsidium



v.l.: Mau Nguyen, Jochen Becker, Tanja Bollinger, Dr.-Ing. Johannes Braun, Rainer Schwebel, Pascal Widera

# TÄTIGKEITSFELDER

TECHNISCHE UNIVERSITÄT DARMSTADT

## Awareness & Kommunikation

- Schulungen
  - Präsenz, de/en
  - E-Learning
  - IT-Sec Game
  - Awareness Kampagnen
- IT-Sicherheitskommunikation
  → Schwachstellenkommunikation und Vernetzung
- RFC-Prozess für (neue) Richtlinien (Partizipation)
- Webauftritt
  → Alle Informationen rund um Informationssicherheit @ TUDa

## Technische Maßnahmen

- Schwachstellenscans
- Netflow Analyse
- Endpoint Protection
- cisOS
  → Aufbau zentrale IT-Asset-Datenbank: Verantwortungsbereiche, Ansprechpersonen, Netzgeräte, Subnetze, Domains,…

## Organisatorische Maßnahmen

!nfoSec

- Regelwerke & Richtlinien
- Governance & Compliance
- Etablieren und Weiterentwickeln der IT-Sicherheitsorganisation (Aufbau- und Ablauf-Organisation)
- Aufbau Informationssicherheitsmanagement System (ISMS)

IT- Vorfallsmanagement: zentrale Meldestelle, Analyse, Reaktion, Maßnahmenkoordination

Etablierung von Präventionsmaßnahmen, Weiterentwicklung bestehender IT-Dienste bzgl. IT-Sicherheitsaspekten & Anforderungen (Netz, E-Mail,…)

Beratung, Begleitung neuer IT-Projekte bzgl. IT-Sicherheitsaspekten & Anforderungen

Aufbau IT- Notfallmanagement (derzeit Fokus auf zentralem Betrieb)

- Notfall- Kommunikationsplattform
- Notfallwebserver
- Abhängigkeitsanalyse
- Notfallkonzepte / Notfallpläne

# WARUM SIND WIR HEUTE HIER?

Informationen zum InfoSec Impact Award

© Thomas Ott

# INFOSEC IMPACT AWARD – 1. PLATZ

- Auszeichnung bei der ersten Verleihung des InfoSec Impact Awards
- Verliehen durch das BSI und Next e.V.
- Erfolgreich durchgesetzt gegen über 20 Mitbewerber

**Ausgezeichnetes Projekt: "HEARTBEAT Emergency-Server„**

Ein Tool zur schnellen Bereitstellung eines IT-Notfallkommunikationssystems (E-Mail & Chat) für die TU Darmstadt.

- Nachnutzung durch andere Verwaltungseinheiten von Bund und Ländern möglich
- Es besteht Interesse seitens des BSI

TECHNISCHE UNIVERSITÄT DARMSTADT

# HEARTBEAT – EIN BLICK HINTER DIE KULISSEN

!nfoSec

**Schnelle Bereitstellung einer reduzierten Notfallkommunikation (E-Mail & Chat) bei Ausfall der TU-IT-Infrastruktur**

- Individueller separater Account – Zeichenfolge entspricht dem zentralen Nutzendenaccount
- Notfall-E-Mailadresse + kleines Postfach pro Person
- Element-Web
- Webmailsystem

- Externes Hosting → unabhängig von der eigenen IT
- Aktivierung innerhalb 1 Stunde nach Ausruf des IT-Notfallbetriebs
- Keine dauerhafte Personen-Datenhaltung oder Vorabbetrieb nötig
- Manuelle, hierarchische Validierung der Nutzenden vor Freischaltung (Schutz vor Missbrauch)

Status: Aktuell in der Überarbeitung für eine Closed Community Veröffentlichung

TECHNISCHE UNIVERSITÄT DARMSTADT

!nfoSec

# HEARTBEAT

Blick unter die Motorhaube

© Thomas Ott

TECHNISCHE UNIVERSITÄT DARMSTADT

# BSI 200-4 NOTFALLPLAN

!nfoSec

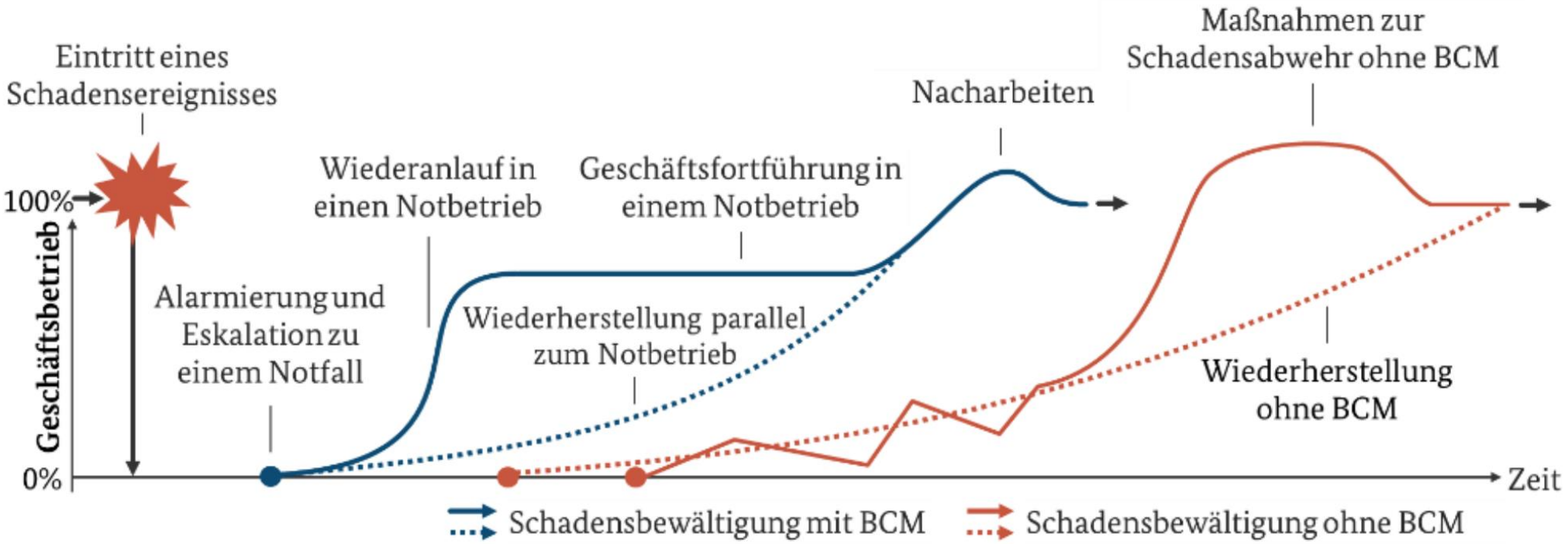



*Abbildung 5: Bewältigung eines schwerwiegenden Schadensereignisses mit und ohne BCM*

Quelle: BSI – Grundschutzstandard 200-4

TECHNISCHE UNIVERSITÄT DARMSTADT

# HEARTBEAT FÜR DEN IT-NOTBETRIEB

!nfoSec

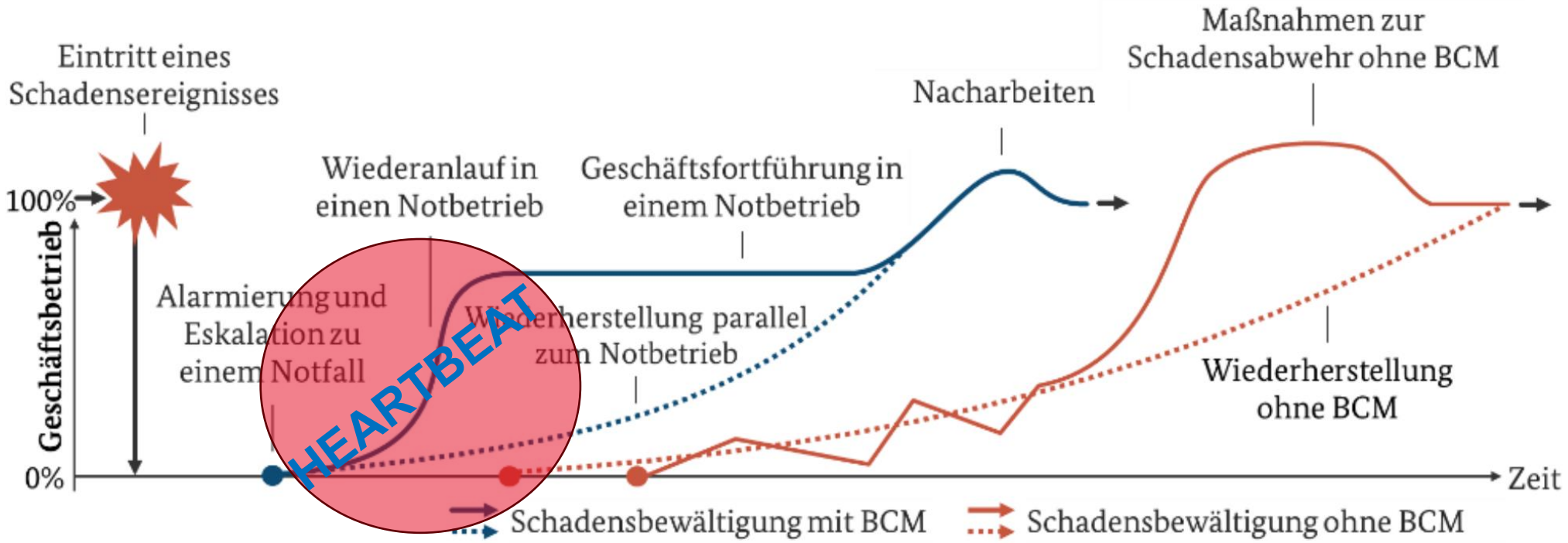



*Abbildung 5: Bewältigung eines schwerwiegenden Schadensereignisses mit und ohne BCM*

Quelle: BSI – Grundschutzstandard 200-4

TECHNISCHE UNIVERSITÄT DARMSTADT

# HINTERGRUND ZU HEARTBEAT ENTWICKLUNG

!nfoSec

- Ransomware an verschiedenen Hochschulen
- Stets steigende Gefahr des Angriffs auf die TUDa mit Abschaltungsgefahr der zentralen IT
- Schnelle schlankes technische Lösung
- Hohe Wiedererkennung für Einrichtungsangehörige
- Aus dem Betrieb heraus entwickelt
- Zentrale IT-Abteilung in den ersten Momenten eines IT-Notfalls entlasten

- Kommunikation ist eines der wichtigsten Führungsmittel
- Handlungsfähigkeit benötigt Kommunikation
- Jeder IT-Notfallbehandlung benötigt Kommunikationsmittel und fängt damit an
- Notfallbewältigungsteams, Führungsebenen und der Krisenstab müssen sich austauschen können
- Klarer Fokus auf die Kommunikation gesetzt

TECHNISCHE UNIVERSITÄT DARMSTADT

# HINTERGRUND ZU HEARTBEAT ENTSCHEIDUNG

!nfoSec

## CHAT

- Direkte Kommunikation ist heute Standardwerkzeug
- 1:1 Chat
- Gruppen-/Teamchats
- Geschlossene Kommunikation im IT-Notfall
- Web- und Rich-Client (Plattform übergreifend)
- Voice- und Video-Calls möglich

## E-Mail

- E-Mail ist universelles Werkzeug
- E-Mail bildet in den meisten Einrichtungen die Basis der Innen- und Außenkommunikation
- Webmail ist gut absicherbar
- Kleine Postfächer ermöglichen Handlungsfähigkeiten
- Private Postfächer werden im IT-Notfall nicht für die Kommunikation benötigt

TECHNISCHE UNIVERSITÄT DARMSTADT

# RAHMENBEDINGUNGEN

!nfoSec

- Aktueller Hoster Hetzner GmbH (DSGVO konform)
- OpenSource Tools (Details folgen)
- Aktuelles Konfigurationsmanagement
- Fokus Kommunikation als Führungsmittel
  - Direkte Kommunikation
  - E-Mail-Kommunikation
- Keine Daten vorab auf den Servern des Hosters
- IT-Notbetrieb bei Totalausfall
- Separate Web-Adressen vorab angemeldet
- Postfachdaten müssen im Nachgang zurück migriert werden
- Getroffene Zugriffsregelungen zum Hostingpartner

TECHNISCHE UNIVERSITÄT DARMSTADT

# TECHNISCHE KOMPONENTEN

!nfoSec

- GNU Debian/Linux
  - OpenSSH (Remote Zugriff)
  - verschiedene Härtungen am System
- OpenLDAP (Personendaten)
- PostgreSQL (Zentrale Datenbank)
- Docker (Containermanagement)
- NGINX (Webserver)
- Postfix (E-Mail Transport Backend)
- Dovecot (E-Mail Postfach Service)

- ansible (Konfigurationsmanagement)

- KeyCloak (IDAM)
- Synapse für Matrix (Chat-Backend)
- Element Web (Chat-Webclient)
- Roundcube (Webmail Client)

- *ES-Verifier* (eine Eigenentwicklung zur Personen-Validierung)

TECHNISCHE UNIVERSITÄT DARMSTADT

# PERSONENDATEN

!nfoSec

- Keine Personendaten im nicht Einsatzfall auf dem Server
- Datenabzüge in unregelmäßigen Abständen
  - schwerer vorhersagbar, nichts tagesaktuell
  - Wenn Kompromitierungszeitpunkt bestimmbar, können Manipulationen erkennbar werden
- Daten direkt importierbar (YAML-Format)
- Daten in CSV-Format parallel vorgehalten
- Einfach Klartextformate
- verschlüsselt vorgehaltene Personendaten und Systemkonfiguration

Vorgehaltene Personendaten (Auszug)

- Accountname (gute Wiedererkennung)
- Name, Vorname, Geburtsdatum
- Persönliche/Private E-Mailadresse
- Organisatorische Zugehörigkeit
- Personenrolle
- Personal-/Matrikelnummer (Identifier)
- Notfall-E-Mailadresse – wird generiert

TECHNISCHE UNIVERSITÄT DARMSTADT

# FRAGEN ZUR TECHNIK

!nfoSec

TECHNISCHE UNIVERSITÄT DARMSTADT

InfoSec

# HEARTBEAT

Ablauf in einem IT-Notfall

© Thomas Ott

TECHNISCHE UNIVERSITÄT DARMSTADT

# HEARTBEAT – PHASE 1

!nfoSec

1. Schadensereignis ist eingetreten/die IT-Störung stellt sich als IT-Notfall heraus
2. Die verantwortlichen Betreibenden melden es dem TUDa-CERT, dass hier eine IT-Notfall vorliegt.
3. TUDa-CERT stellt den IT-Notfall fest und Meldung an CISO und Leiter zentrale IT
4. Lagebeurteilung und Entscheidung, ob IT-Notbetriebssystem HEARTBEAT gebraucht wird
   1. Abwägung bereichsweiser oder einrichtungsvollständiger Einsatz
   2. Entscheidung welcher Stand von Personaldaten eingespielt werden soll
5. TUDa-CERT initiiert das Aufsetzen von HEARTBEAT (etwa 40min)
6. Personaldaten werden importiert (vollständig für die TUDa etwa 3h)

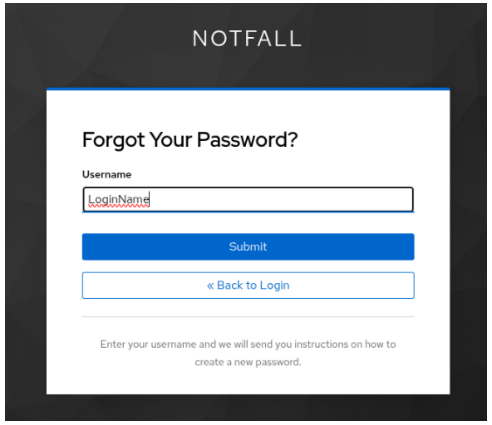
```
TASK [rkhunter : Update rkhunter] ***********************************************************
Dienstag 15 April 2025  15:40:31 +0200 (0:00:00.609)       0:01:00.213 ********
Dienstag 15 April 2025  15:40:31 +0200 (0:00:00.609)       0:01:00.213 ********
ok: [devhost01.dev.emergency-server.de]

TASK [chkrootkit : Install chkrootkit] ******************************************************
Dienstag 15 April 2025  15:40:41 +0200 (0:00:10.674)       0:01:10.888 ********
Dienstag 15 April 2025  15:40:41 +0200 (0:00:10.674)       0:01:10.888 ********
changed: [devhost01.dev.emergency-server.de]

TASK [chkrootkit : Replace in chkrootkit.conf] **********************************************
Dienstag 15 April 2025  15:40:57 +0200 (0:00:15.687)       0:01:26.575 ********
Dienstag 15 April 2025  15:40:57 +0200 (0:00:15.687)       0:01:26.575 ********
ok: [devhost01.dev.emergency-server.de]

TASK [fail2ban : Install Fail2ban] **********************************************************
Dienstag 15 April 2025  15:40:57 +0200 (0:00:00.178)       0:01:26.754 ********
Dienstag 15 April 2025  15:40:57 +0200 (0:00:00.178)       0:01:26.754 ********
changed: [devhost01.dev.emergency-server.de]

TASK [fail2ban : Write new jail.local] ******************************************************
Dienstag 15 April 2025  15:41:10 +0200 (0:00:13.272)       0:01:40.026 ********
Dienstag 15 April 2025  15:41:10 +0200 (0:00:13.272)       0:01:40.026 ********
changed: [devhost01.dev.emergency-server.de]

TASK [fail2ban : Flush handlers] ************************************************************
Dienstag 15 April 2025  15:41:11 +0200 (0:00:00.470)       0:01:40.497 ********
Dienstag 15 April 2025  15:41:11 +0200 (0:00:00.470)       0:01:40.496 ********

RUNNING HANDLER [fail2ban : Restart Fail2ban] ***********************************************
Dienstag 15 April 2025  15:41:11 +0200 (0:00:00.003)       0:01:40.500 ********
Dienstag 15 April 2025  15:41:11 +0200 (0:00:00.003)       0:01:40.500 ********
changed: [devhost01.dev.emergency-server.de]

TASK [psad : Install psad] ******************************************************************
Dienstag 15 April 2025  15:41:11 +0200 (0:00:00.287)       0:01:40.788 ********
Dienstag 15 April 2025  15:41:11 +0200 (0:00:00.287)       0:01:40.787 ********
```

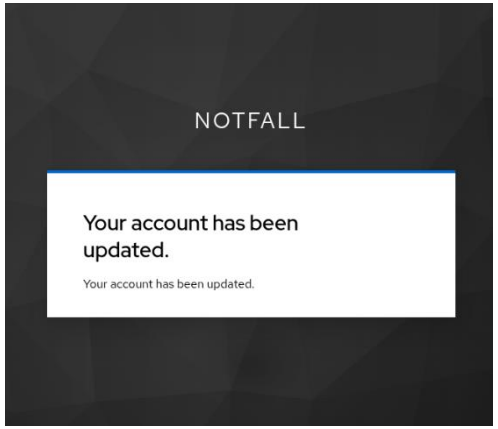
TECHNISCHE UNIVERSITÄT DARMSTADT

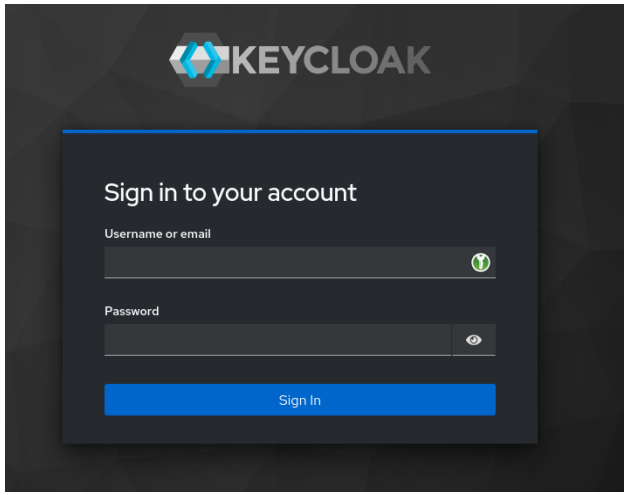
# HEARTBEAT – PHASE 2

!nfoSec

7. Information an die beteiligten Nutzenden über 3ten Kanal
8. Aufforderung an alle betroffenen Nutzenden sich ein Passwort zu setzen.
9. Persönliche Nutzenden Verifikation über Vorgesetzte
   - Nutzung von weiteren Tools Face2Face, WebCam Session, andere Messenger
10. Nutzende erhalten Freischaltung zur Nutzung vom System für Messenger und E-Mail
11. E-Mailadresse wird für die Außenwelt aktiviert und ist zustellbar



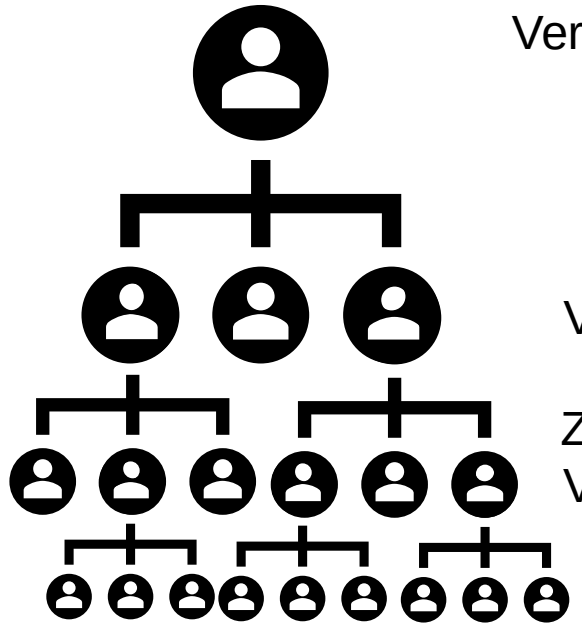



TECHNISCHE UNIVERSITÄT DARMSTADT

# PERSONENVERIFIKATION

!nfoSec

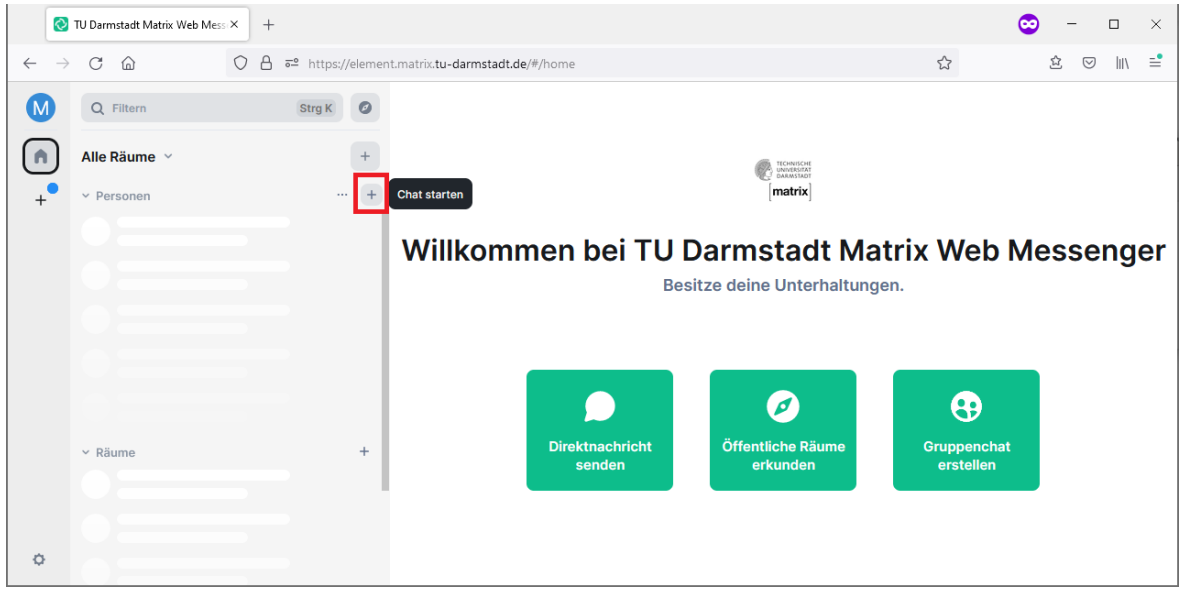
- Vertrauensanker z.B. CERT-Team ist gesetzt.
- Verifizierung der nachfolgenden Verifizierenden z.B. Leitungsebene RZ erfolgt durch Vertrauensanker.
- Die neuen Verifizierende können entsprechend weiter Personen verifizieren.
- Die Sichtbarkeit auf die Zu verifizierenden hat aktuell keine technische Einschränkung für die Verifizierenden (ggf. organisatorische Regelung notwendig).
- Das Folgen der Unternehmensstruktur nutzt den Vorteil, dass regulär miteinander Arbeitende sich entlang der Struktur/Hierarchie kennen.
- Verifizierende sind auch verifizierte Nutzende.

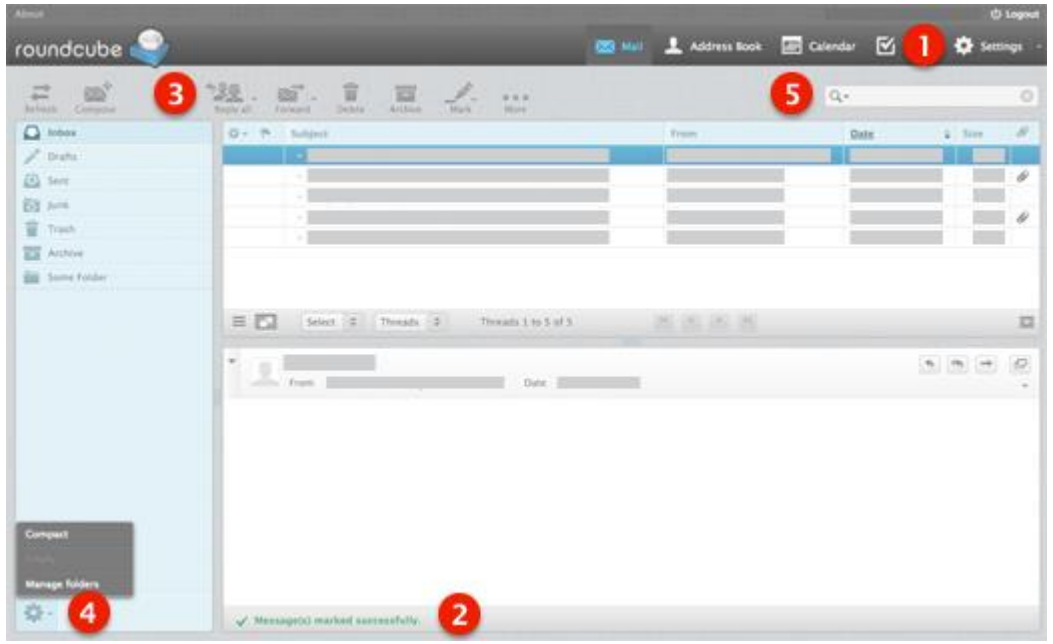


TECHNISCHE UNIVERSITÄT DARMSTADT

# CHAT UND MAIL STEHEN BEREIT

!nfoSec




Standard Messenger- und Webmail-Oberflächen
und damit für Nutzende ein gewohntes Umfeld

Quelle: Dokumentation TU Darmstadt

Quelle: roundcube

TECHNISCHE UNIVERSITÄT DARMSTADT

# FRAGEN ZUM ABLAUF

!nfoSec

TECHNISCHE UNIVERSITÄT DARMSTADT

InfoSec

# ABSCHLUSS

Aktueller Stand

Nächsten Schritte

Offene Fragen

Kontakt und Dank

© Thomas Ott

TECHNISCHE UNIVERSITÄT DARMSTADT

# AKTUELLER STAND

!nfoSec

- Der Code wird zurzeit bereinigt und für eine closed Community Veröffentlichung vorbereitet.
- Beispiel Konfigurationsdateien werden erstellt.
- Nutzendendokumentation wird erstellt.
- Gespräch mit dem BSI und DFN-CERT für Unterstützung der Veröffentlichung und Fortentwicklung beginnen.

TECHNISCHE UNIVERSITÄT DARMSTADT

# NÄCHSTE SCHRITTE

!nfoSec

- Auswahl der entsprechenden OpenSource Lizenz
- Aufnahme von weiteren Partnern für die Fortentwicklung
- Gemeinsame Verbesserung und Verbreitung von HEARTBEAT
  - Ziel eine stete Fortentwicklung und Verbesserung durch Einsetzende
  - Unterstützungen für Proof-of-Concept wird geprüft
- Closed-Community Veröffentlichung (GIT-Repository)

- Kein Hosting für Behörden durch die TUDa

TECHNISCHE UNIVERSITÄT DARMSTADT

# OFFENE FRAGEN

!nfoSec

TECHNISCHE UNIVERSITÄT DARMSTADT

!nfoSec

# DANKE

Jochen Becker
*Leiter TUDa-CERT*

+49 6151 16-71021
jochen.becker@tu-darmstadt.de
contact@infosec.tu-darmstadt.de

Technische Universität Darmstadt
Informationssicherheit (InfoSec)
Postanschrift Karolinenplatz 5, 64289 Darmstadt
Besuchsanschrift Alexanderstraße 2, 64283 Darmstadt