

Was macht die Krise mit Menschen? Wie komme ich wieder gut aus der Krise?

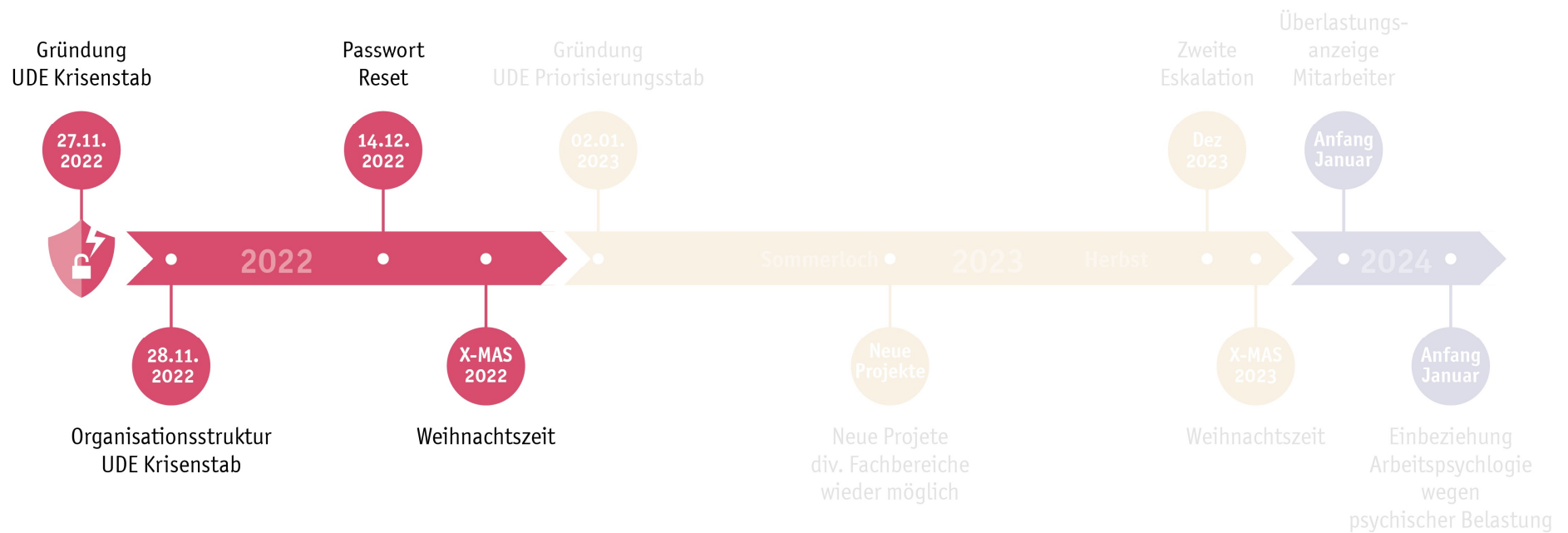
Cyberangriff an der Universität Duisburg-Essen





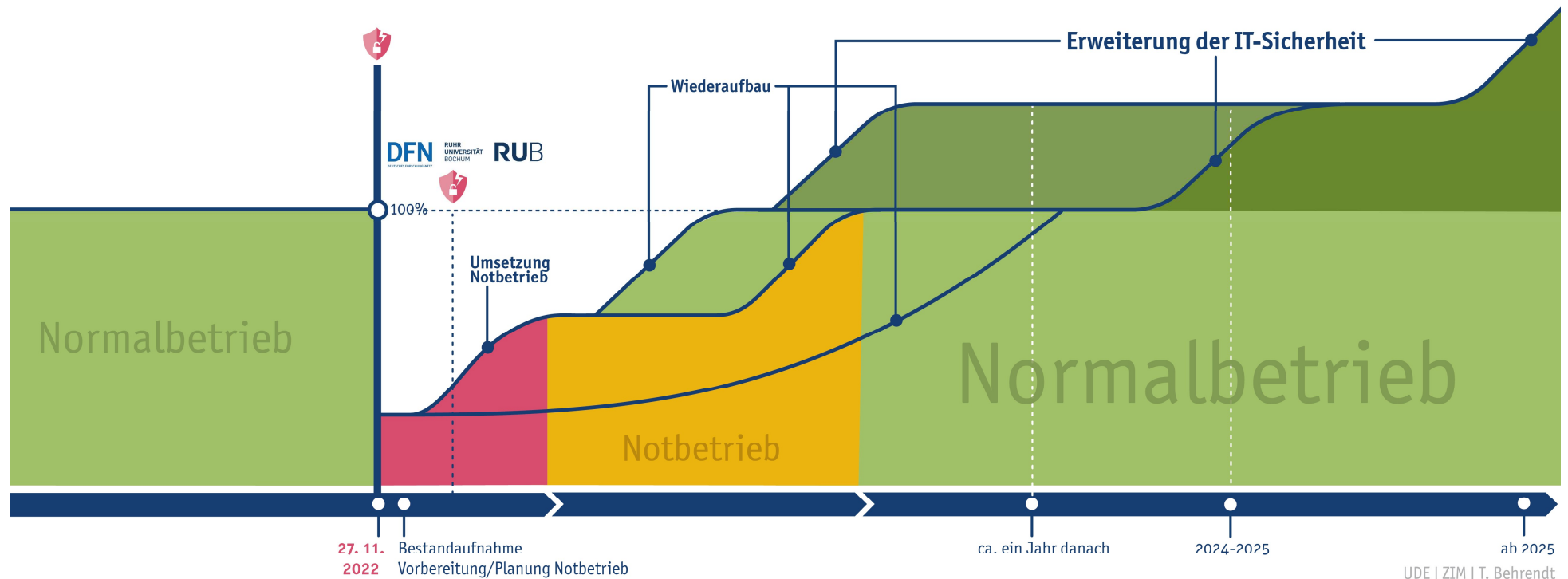
RUHE BEWAHREN!

Chronologie



UDE | ZIM | T. Behrendt

Bestandaufnahme, Vorbereitung des Testbetriebs sowie des Wiederaufbaus

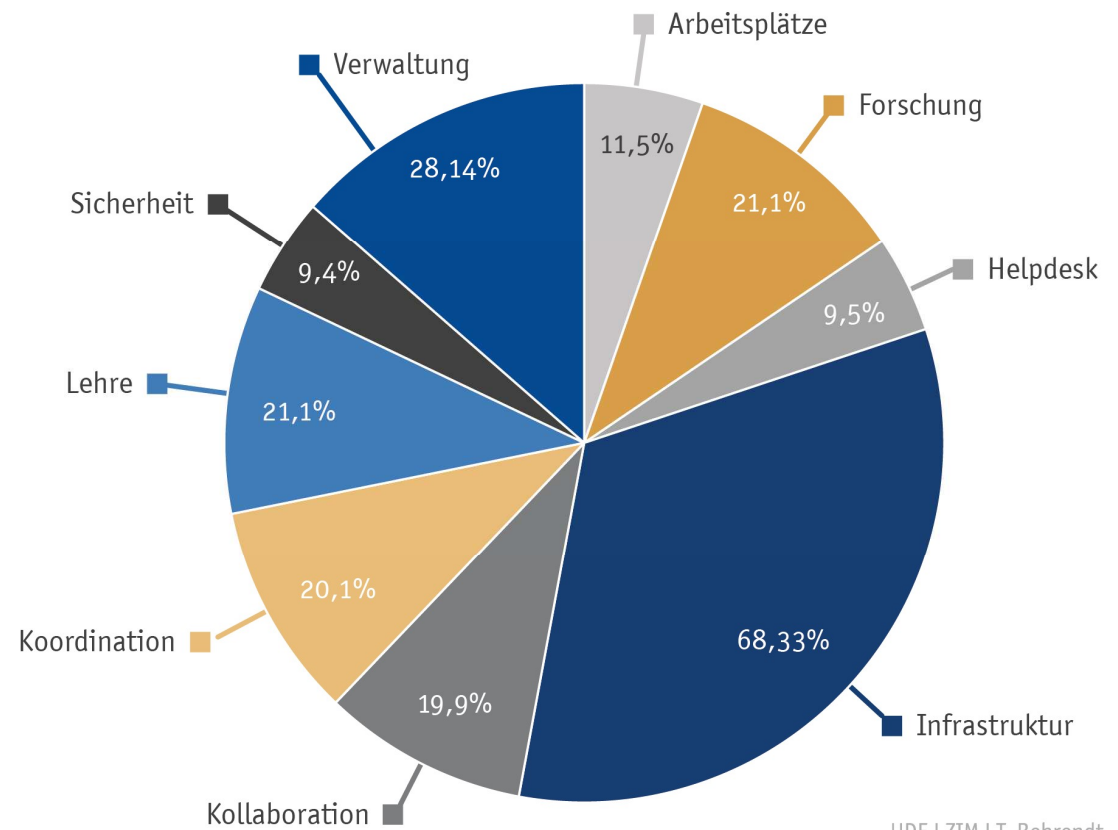


Bestandaufnahme, Vorbereitung des Testbetriebs, sowie des Wiederaufbaus



ZIM Servicekatalog – 206 Services

Aufteilung der Services nach Kategorien

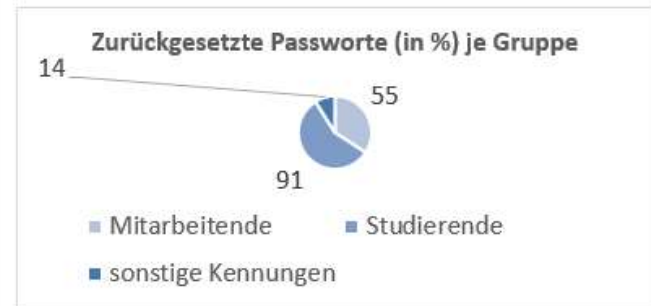
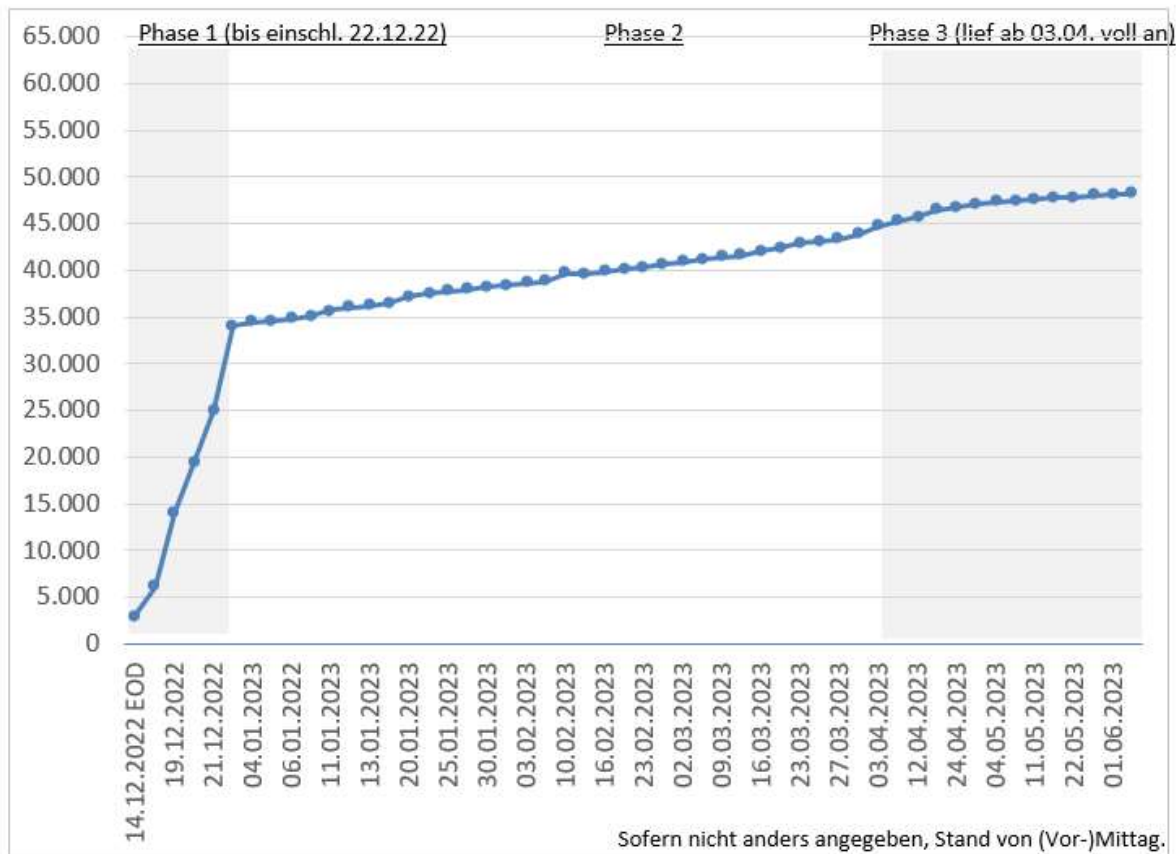


UDE | ZIM | T. Behrendt

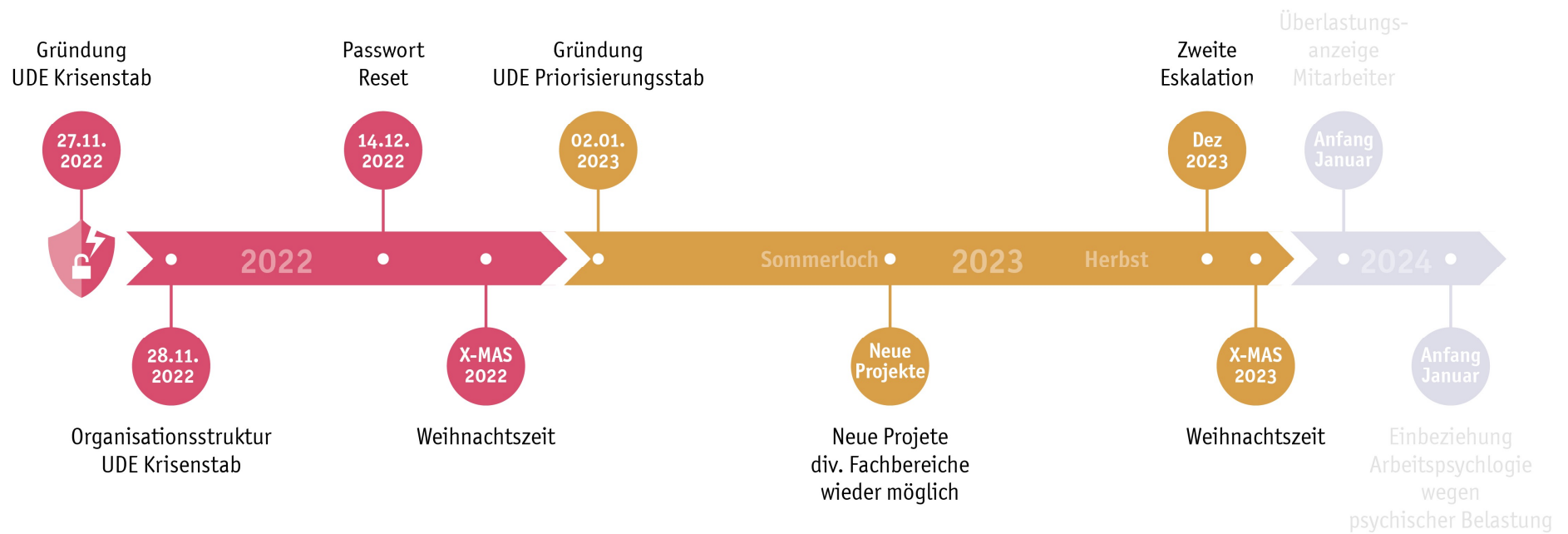
SPRINT ODER MARATHON?



Passwortreset im Zeitverlauf

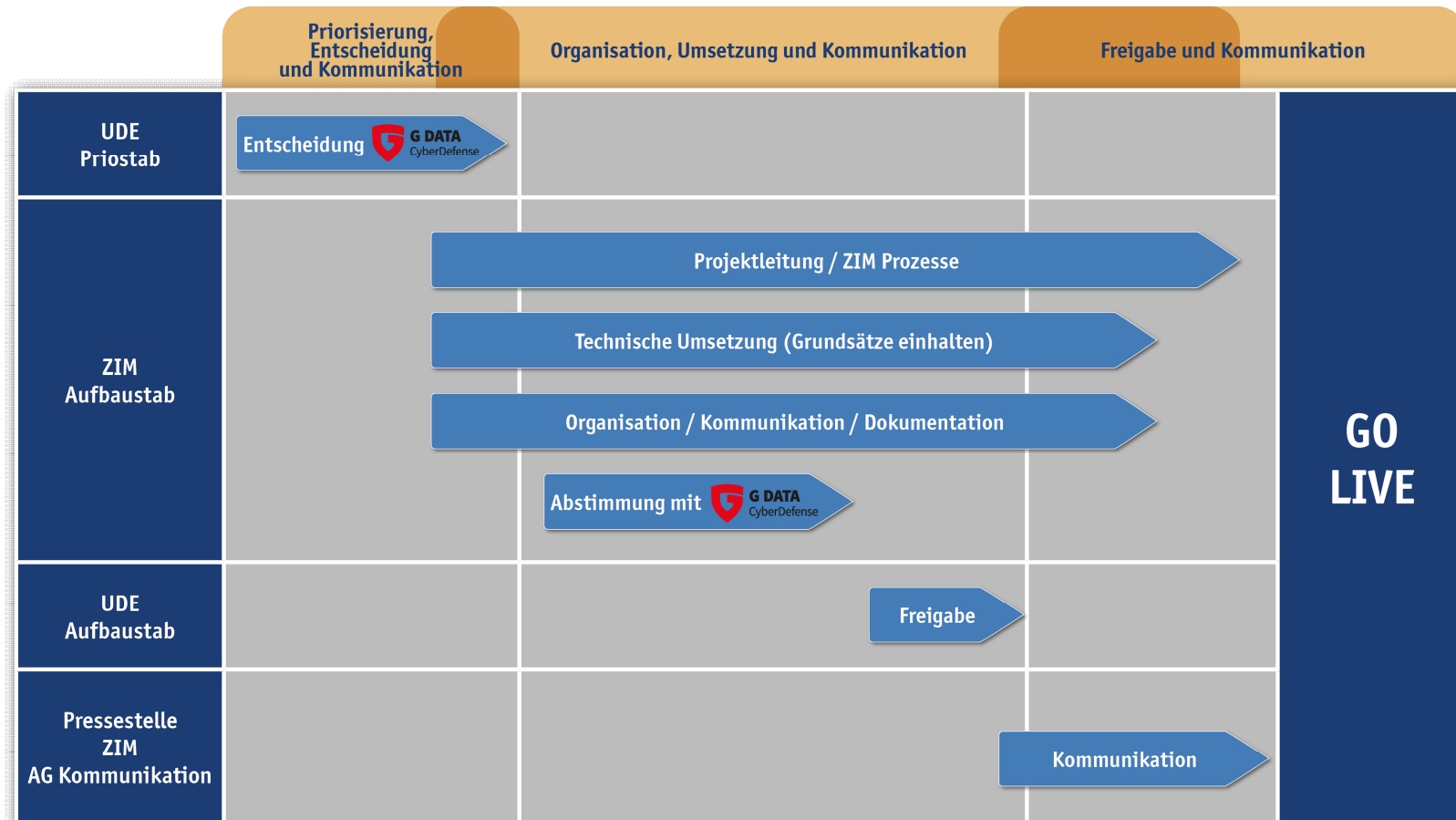


Chronologie



UDE | ZIM | T. Behrendt

Entscheidungs- und Umsetzungs-Prozess



UDE | ZIM | T. Behrendt

Entscheidungs- und Umsetzungs-Prozess

- Organisationstruktur in der Krise
- Berichterstattung der Arbeitsgruppen
- Krisenkommunikation
- Bericht im Krisenstab
- Projektmanagement und Multi-Projektmanagement
- Beratung

UDE IT / ZIM
Agenda

Anwesend in Stabsmeeting

x 2 – Backup / VM / Forensik	x 6 – IT-Sicherheit
x 3 – Netzwerk / Telefonie	x 7 – Forschung
x 4 – CRM	x 8 – Studium und Lehre
x 5 – Kundenservice / Clients	x 9 – Verwaltung / SAP

Übergeordnete Lage offene Fragen aus anderen Stäben/Meetings

- Inkonsistenz bei den Eintragungen in Backup- und Forensik-Liste zu vermeiden
- Wann wird ein Virusscanner zur Verfügung gestellt? Wie können Home Office Nutzer ihren Virusscanner aktuell halten? (z.B. ClamAV)
- FA, versucht Übersicht über weiteren gegangenen Server-Cases mit Zuordnung zu Services und Fakultäten/Erziehungen
- Was ist über Forensik-Gegebenheiten und Einsatzmöglichkeiten bekannt? Ist ein Projekt / eine Aufgabe schon bearbeitet?
- Welche Datenverlust besteht bei SAP? Wie wird ein Fallbearbeitet zusammen? Wenn über Konfigurationsdaten in der Datenbank oder in den virtuellen Servern gespeichert?
- Wann Ressourcen bereit? Organisation wie werden für einen Fall 4er-Case bearbeitet? Versteht man die Logik?
- Umgang mit Druckfällen / Bewertung für Arbeitsplätze und Home Office-Verbindlichkeit
- Unterstützung für Client- & MitarbeiterInnen

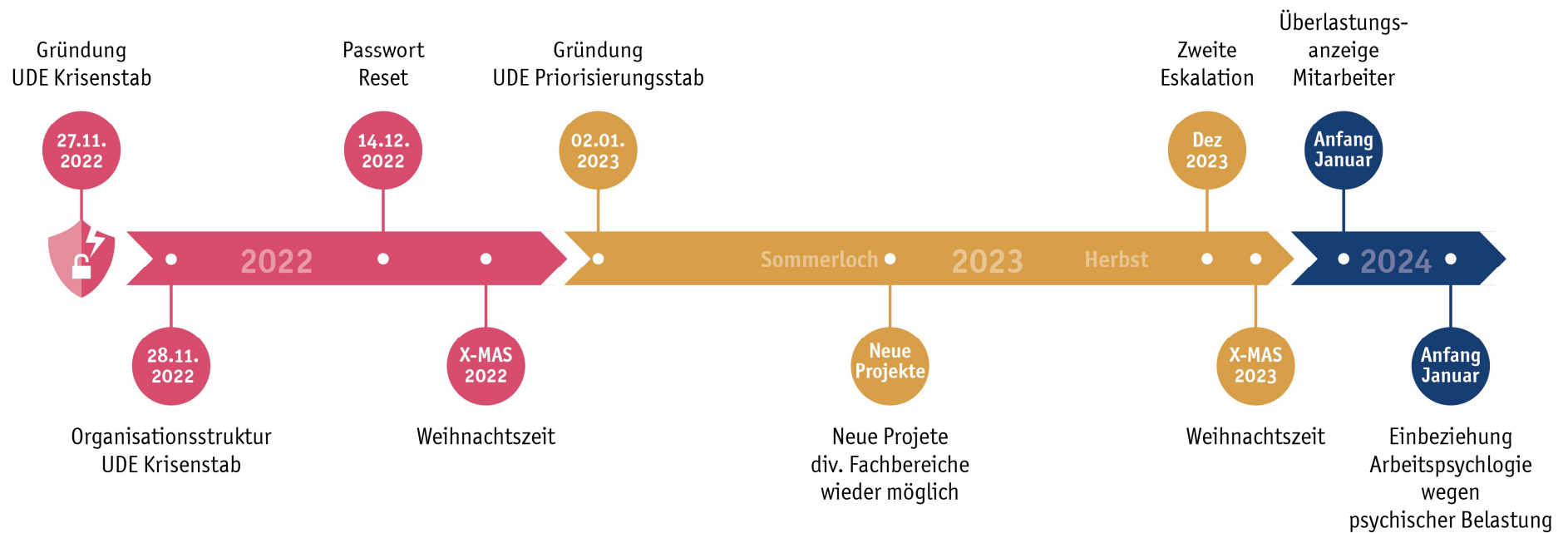
UDE RANSOMWARE ANTACKE
2- Backup / VM / Forensik

Flaserver (Metasploit)	Virtual-Backup	Virtual-Umgebung	TSM-Backup
<p>Voraussetzungen für Host</p> <p>Minimale Rechte</p> <ul style="list-style-type: none"> - Systemverwaltungsrechte (z.B. DllExport) - Zugriff auf den Speicher des Hosts (z.B. über VM-Tools) - Administratorrechte (z.B. über VM-Tools) <p>Wichtige Schritte</p> <ul style="list-style-type: none"> - Anpassen der Datenabfrage und -speicherung - Offene Fragen/Probleme 	<p>Voraussetzungen für Host / VM-Tools</p> <p>Minimale Rechte</p> <ul style="list-style-type: none"> - Remote-Zugriff auf VM-Tools - Zugriff auf die VM-Tools - Zugriff auf die VM-Tools <p>Wichtige Schritte</p> <ul style="list-style-type: none"> - Offene Fragen/Probleme 	<p>Voraussetzungen für Host / VM-Tools</p> <p>Minimale Rechte</p> <ul style="list-style-type: none"> - Remote-Zugriff auf VM-Tools - Zugriff auf die VM-Tools - Zugriff auf die VM-Tools <p>Wichtige Schritte</p> <ul style="list-style-type: none"> - Offene Fragen/Probleme 	<p>Voraussetzungen für Host / VM-Tools</p> <p>Minimale Rechte</p> <ul style="list-style-type: none"> - Remote-Zugriff auf VM-Tools - Zugriff auf die VM-Tools - Zugriff auf die VM-Tools <p>Wichtige Schritte</p> <ul style="list-style-type: none"> - Offene Fragen/Probleme

UDE RANSOMWARE ANTACKE



Chronologie der psychischen Auswirkungen



UDE | ZIM | T. Behrendt

“

*Teamwork ist das Geheimnis,
mit dem **gewöhnliche Menschen**
ungewöhnliche Ergebnisse
erreichen können.* ”

Ifeanyi Enoch Onuoha,
Pädagoge und Bestseller-Autor



Vielen
Dank