ACP

BRAIN SHARE

Notfallplan und Ransomware?

DRaaS als ganzheitlicher Service!

IT for innovators.

Ihr ACP-Trio für die nächsten 60 Minuten

Andreas Karl

Senior Consultant

Infrastructure & Backup

Alexander Fuchs

Consulting Engineer

Datacenter Infrastructure

Lukas Lentner

Solution Engineer

Enterprise Applications

Agenda

01 Aktuelle Lage

02 Ransomware Angriffe

03 Maßnahmen nach Angriff

04 Schneller Wiederanlauf

05 Features Rescue Kit

IT for innovators.

IT-Ausfälle

IT-Ausfälle

IT-Sicherheit

Schwachstellen bei Software auf besorgniserregendem Niveau

Das BSI registriert immer mehr Schwachstellen in Software. Diese Schwachstellen sind oft das Einfallstor für Cyberkriminelle auf ihrem Weg zu einer Kompromittierung von Systemen und Netzwerken. Das BSI hat mit durchschnittlich knapp 70 neuen Schwachstellen in Software-Produkten pro Tag nicht nur rund ein Viertel mehr registriert als im Berichtszeitraum davor. Mit der Anzahl stieg auch ihre potenzielle Schadwirkung: Immer mehr Lücken (etwa jede sechste) werden als kritisch eingestuft.

Quelle: BSI

BSI


bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html
Das BSI
Themen
IT-Sicherheitsvorfall
Karriere
Service
Ransomware ist und bleibt die größte Bedrohung
Bei Cyberangriffen mit Ransomware beobachtet das BSI eine Verlagerung der Attacken: Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen. Insbesondere von erfolgreichen Cyberangriffen auf Kommunalverwaltungen und kommunale Betriebe sind die Bürgerinnen und Bürger unseres Landes oft auch unmittelbar betroffen: So kann es dazu kommen, dass bürgernahe Dienstleistungen eine Zeit lang nicht zur Verfügung stehen oder persönliche Daten in die Hände Krimineller gelangen.

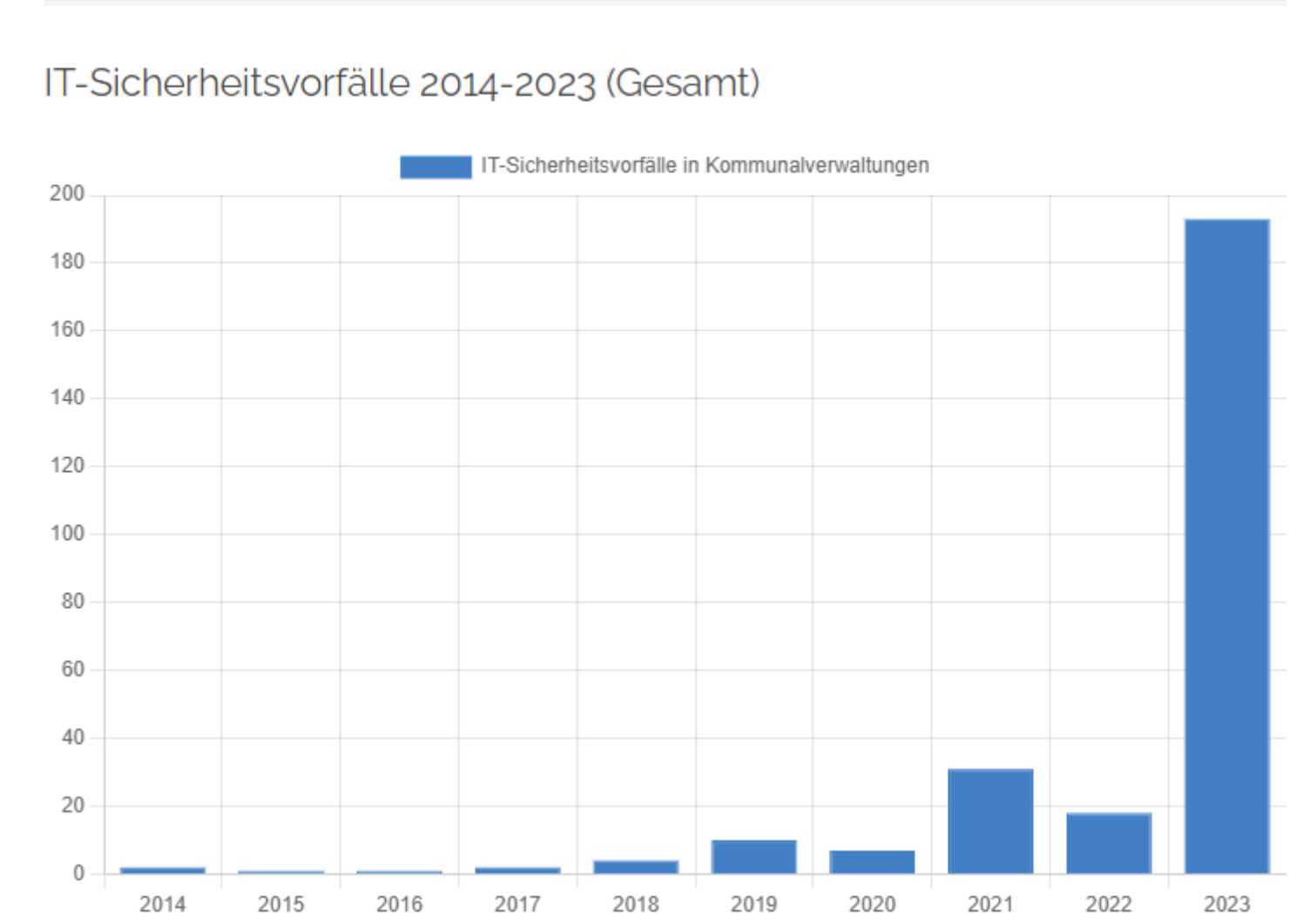
IT-Sicherheitsvorfall in Indonesien

Die Regierung Indonesiens hat offenbar massive Probleme bei der Wiederherstellung von Daten, die am 20. Juni 2024 im Rahmen einer Ransomware-Attacke verschlüsselt wurden. Grund dafür ist der Umstand, dass in den betroffenen nationalen Rechenzentren zwar Backup-Kapazitäten zur Verfügung standen, deren Nutzung jedoch bisher freiwillig war, so dass sich die meisten Behörden aufgrund von Budgetbeschränkungen gegen deren Verwendung entschieden.

> Hinsa Siburian, Leiter der Nationalen Cyber- und Verschlüsselungsbehörde (BSSN) von Indonesien, erklärte laut The Register, dass für 98 Prozent der in einem der beiden kompromittierten Rechenzentren gespeicherten Daten kein Backup erstellt wurde.
>
> *"Dies ist kein Problem der Regierungsführung, sondern ein Problem der Dummheit, nationale Daten ohne ein einziges Backup zu speichern"*, erwiderte daraufhin Meutya Hafid, Vorsitzender der ersten Kommission des Volksvertretungsrates.

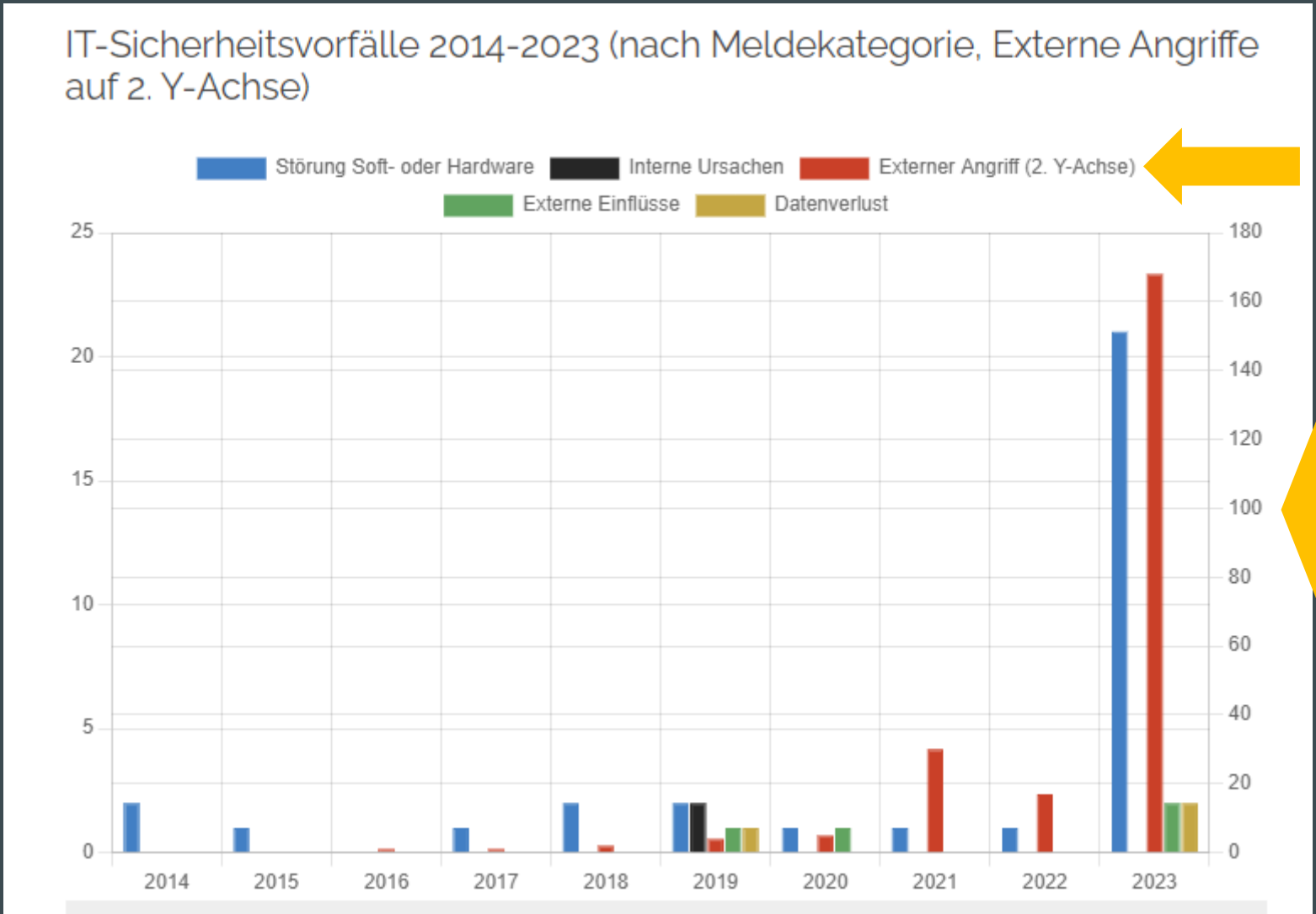
Quelle:
https://www.golem.de/news/cyberangriff-auf-indonesien-fehlende-backups-bereiten-behoerden-massive-probleme-2407-186593.html

IT-Sicherheitsvorfälle in Kommunen



Quelle:
https://kommunaler-notbetrieb.de/zeitleiste/statistik/

IT-Sicherheitsvorfälle in Kommunen



Quelle:
https://kommunaler-notbetrieb.de/zeitleiste/statistik/

ACP

BRAIN SHARE

29.01.2024, 14:31 Uhr

> Hackerangriff auf Bezirkskliniken

Hackerangriff auf Bezirkskliniken

Die Bezirkskliniken [redacted] sind Opfer eines Hackerangriffs. Unbekannte hätten Daten verschlüsselt, so die Kliniken. Wegen des Angriffs haben [redacted] Notfallversorgung abgemeldet.

Von Martin Hähnlein, Henry Lai, Florian Deglmann

Über dieses Thema berichtet: Regional[redacted]chrichten Franken

Hacker haben die IT-Systeme de[redacted] worden, teilten die Kliniken mit[redacted] die Hand der Hacker gefallen.

Audiobeitrag

Unbekannte hätten Daten

Anzeigen

Ausfälle seit einer Woche

Ransomware legt IT-Dienstleister von mehr als 70 Kommunen lahm

Der Dienstleister [redacted] wurde vor einer Woche gehackt. Die Auswirkungen auf die Rathäuser, die zu [redacted] unden zählen, sind gravierend.

Anhören

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

About bitcoin
How to buy bitcoins?
Contact Us

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

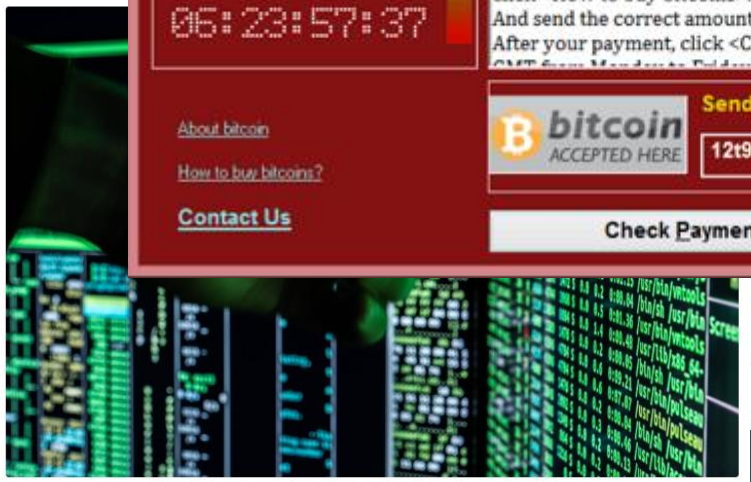
Check Payment

Decrypt

Kripo ermittelt

Digita[redacted]
Unter[redacted]
Bitcoi[redacted]

24.08.2023 | Sta[redacted]



Die Polizei warnt und erläutert Datenbackup-Strategien. –Symbolbild: Imago

1.10.2023 14:39	Dateiordner	
1.02.2022 11:28	Dateiordner	
7.02.2024 10:01	Dateiordner	

Angriff aus dem Netz

[redacted] Firma wird Opfer von Hackern

19. Dezember 2022, 9:27 Uhr aktualisiert am 19. Dezember 2022, 13:30 Uhr

Oliver Berg/dpa/dpa

[redacted] Firma ist Opfer von Hackern geworden.

Ransomware = Erpressung

- verschlüsselte Daten oder „wir haben Ihre Daten“
- i.d.R. organisierte Kriminalität bzw. professionell aufgestellte Hackergruppen/Firmen
  - teilweise mit Kontaktdaten/Hotline
- oder staatlich organisiert (Datenklau)
- es trifft (mittlerweile) auch „kleinere“ Firmen
  - Summe der Forderungen angepasst an Unternehmensgröße

Zahlen - Ja oder Nein ?

Weil der Druck nach einem Ransomware-A s geforderte Lösegeld in de ein.

Es gibt jedoch ser die verschlüsselte e gestohlenen Daten tatsächli

Auch besteht d Verfügung gestellte Entschlüsselun

Das BSI rät da segelds ab.

Zudem müsse ls kompromittiert betrachtet werd

Quelle: Veeam Ransomware Trends Report 2023

Quelle: Sicherheitsjahresbericht 2023

Was passiert bei einem Ransomware Angriff?

- Zugriff verschaffen
- von System zu System hangeln
- ein „Bild von der Umgebung“ machen
- Userverhalten analysieren
- teilweise werden einfachste Mittel genutzt

Das Ziel: **Daten abgreifen oder zerstören, um…**

- Sie handlungsunfähig zu machen
- Sie zu erpressen

Angriffsvektoren und Angriffsmuster I

- externer Zugriff mit User/Passwort
  ohne Multifaktor-Authentication

- Ausnutzen bekannter Schwachstellen
  keine aktuellen Sicherheitspatches installiert

- keine oder unzureichende Netzwerksegmentierung

- zentrale Systeme unzureichend abgesichert
  - Backupserver im selben Netz und im Active Directory
  - Backup Device(s) für alle erreichbar
  - Domänen-Admin wird von allen für alles genutzt

Angriffsvektoren und Angriffsmuster II

- keine Kennwortrichtlinien
  - „altbekannte Kennwörter“ auf vielen Systemen
  - keine Sperren nach X Versuchen
  - Admin-Accounts in use – schlechte Passwörter
- „historisch gewachsenes“ Firewall-Regelwerk
- EndPoint Protection (Virenscanner)
- fehlendes Logging und keine Logging-Historie
- kein SIEM – keine Korrelation von Informationen
- Unvollständige / veraltete Best Practice Empfehlungen

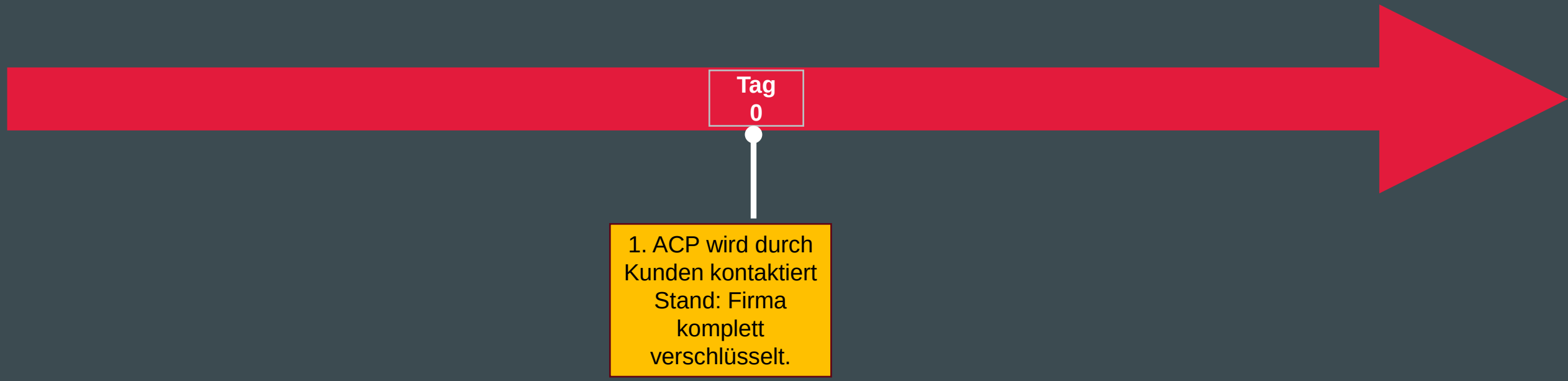
Es ist passiert…

- Was nun?

1. **Theorie**
   - **Notfallplan aus der Schublade holen**

2. **Praxis**
   - **Notfallplan nicht vorhanden oder veraltet**
   - **niemand ist auf diesen Fall vorbereitet**

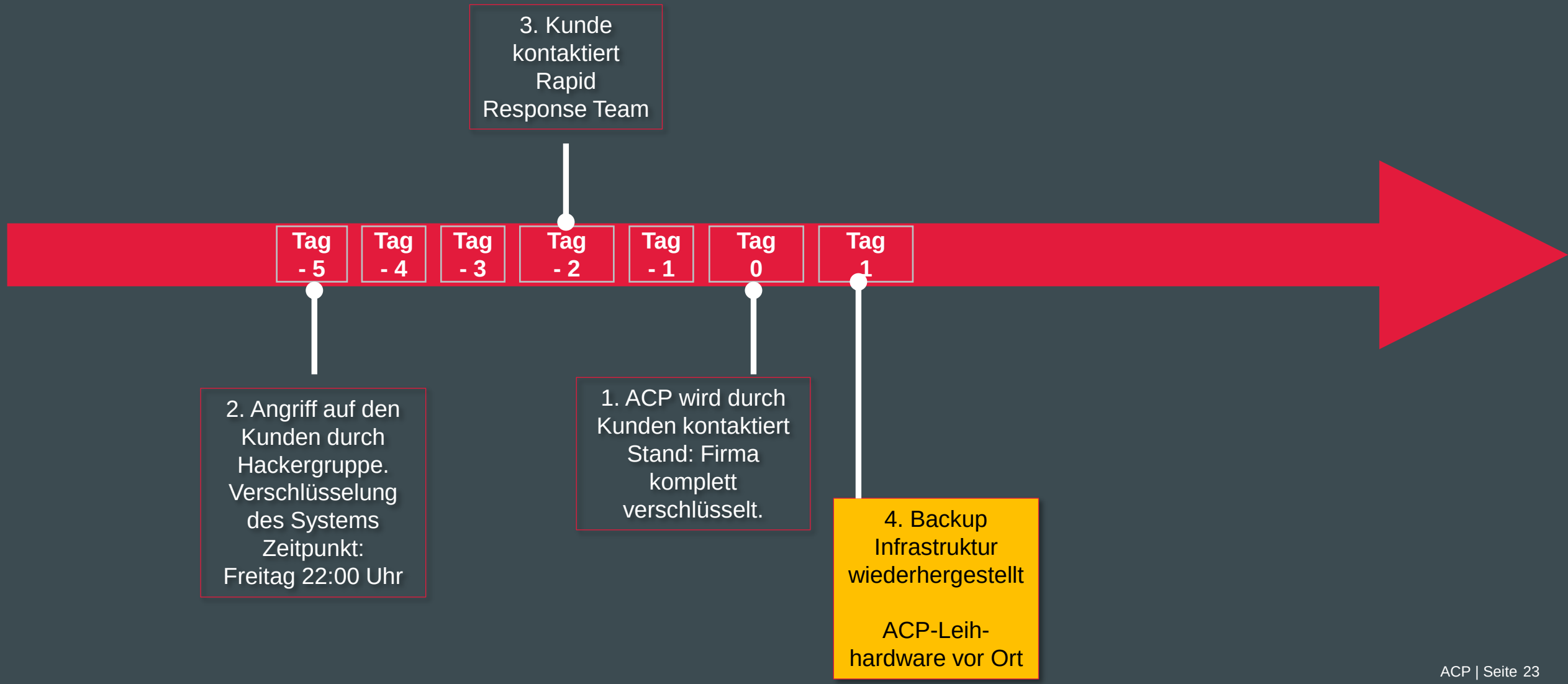
Ganzheitlicher Ablauf



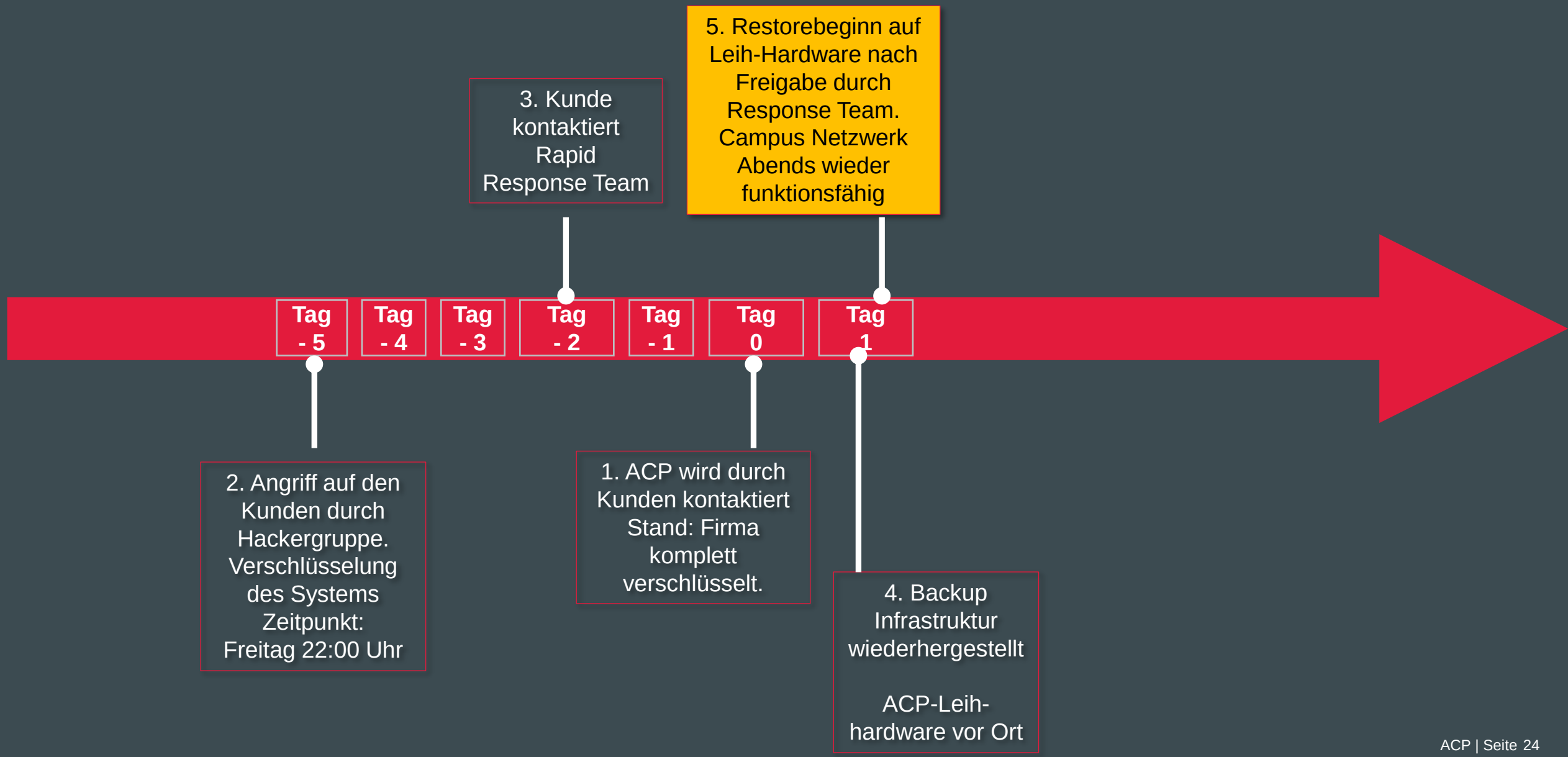
Ganzheitlicher Ablauf

Ganzheitlicher Ablauf

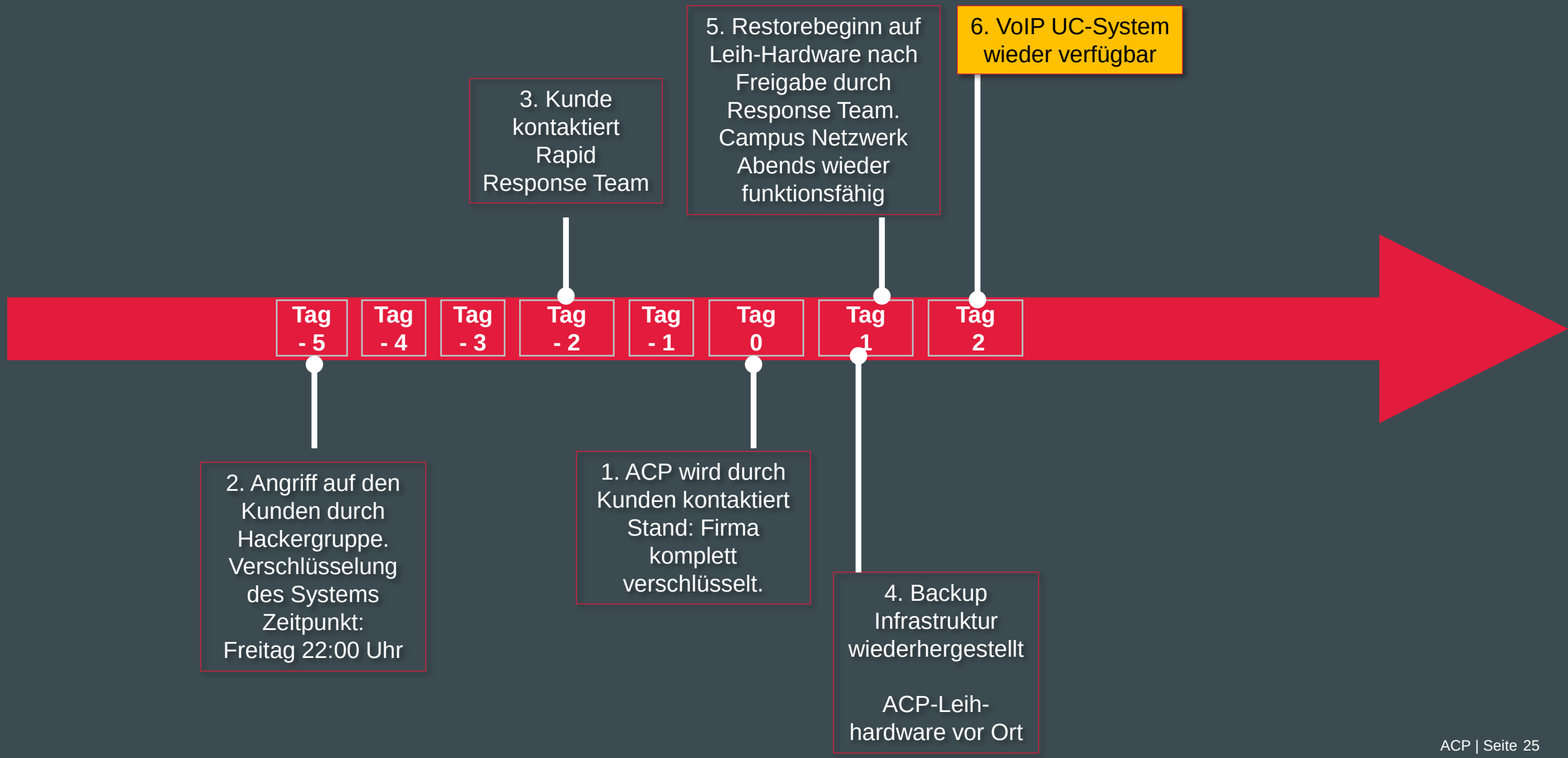
Ganzheitlicher Ablauf



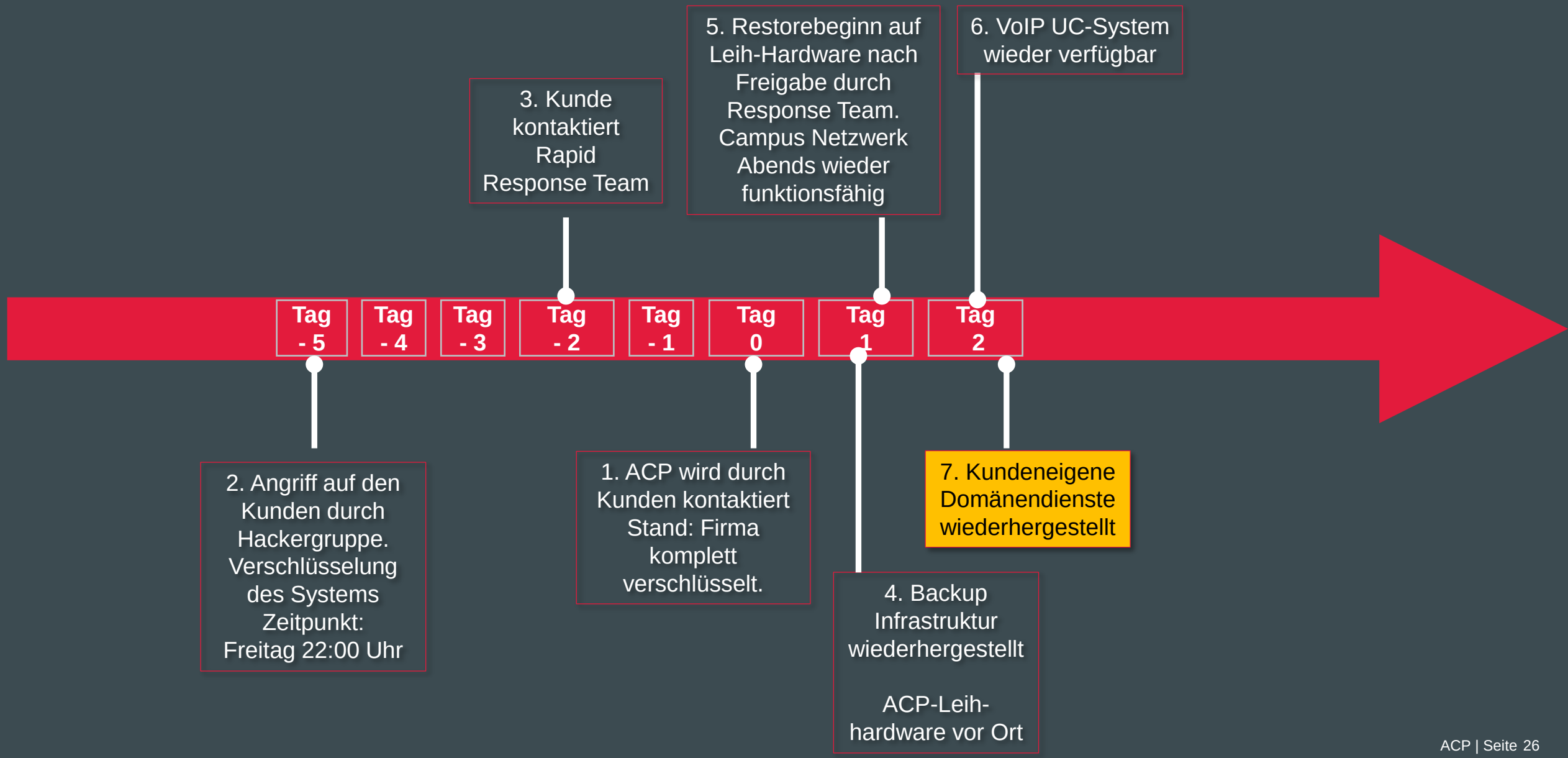
Ganzheitlicher Ablauf



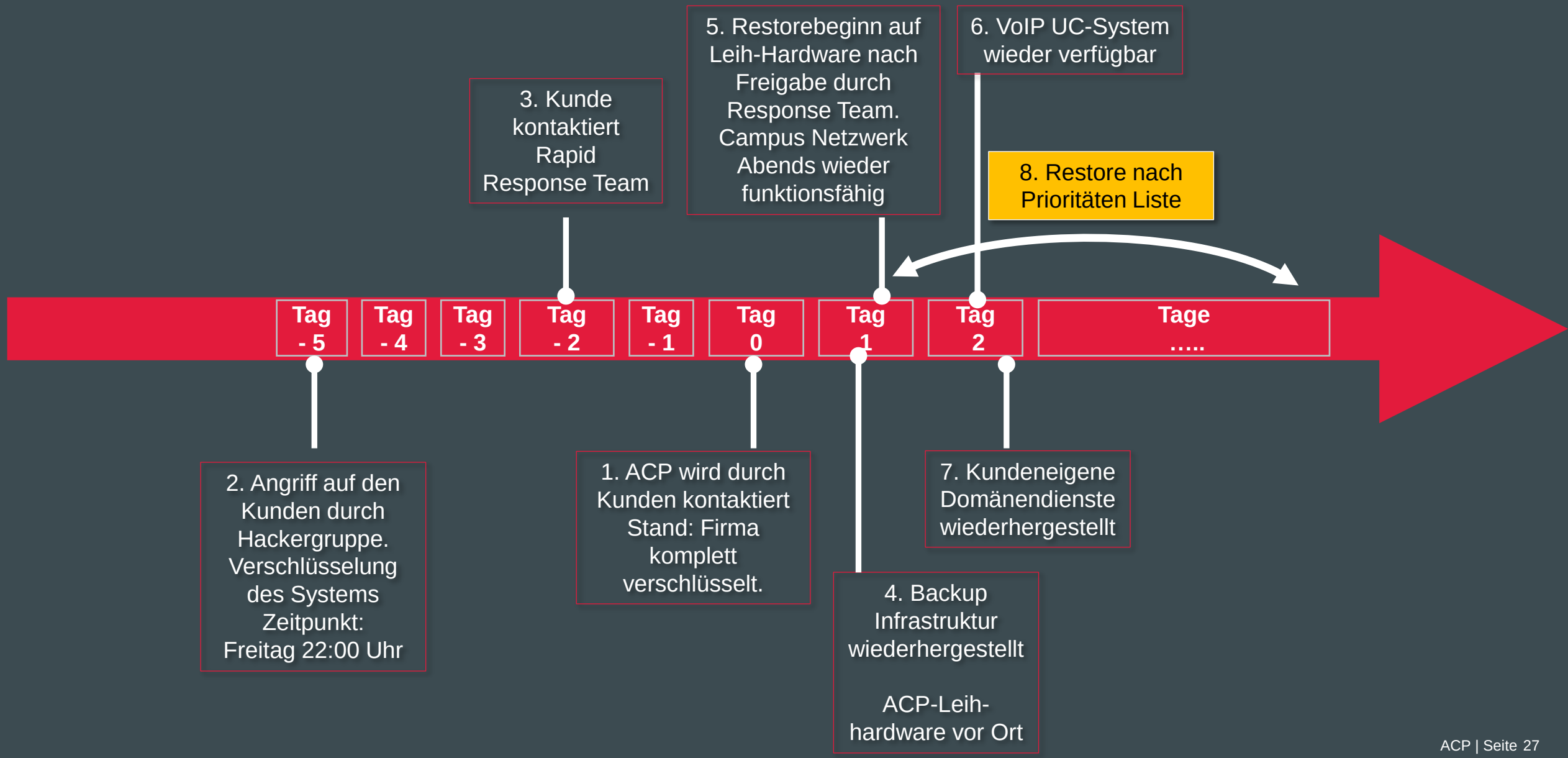
Ganzheitlicher Ablauf



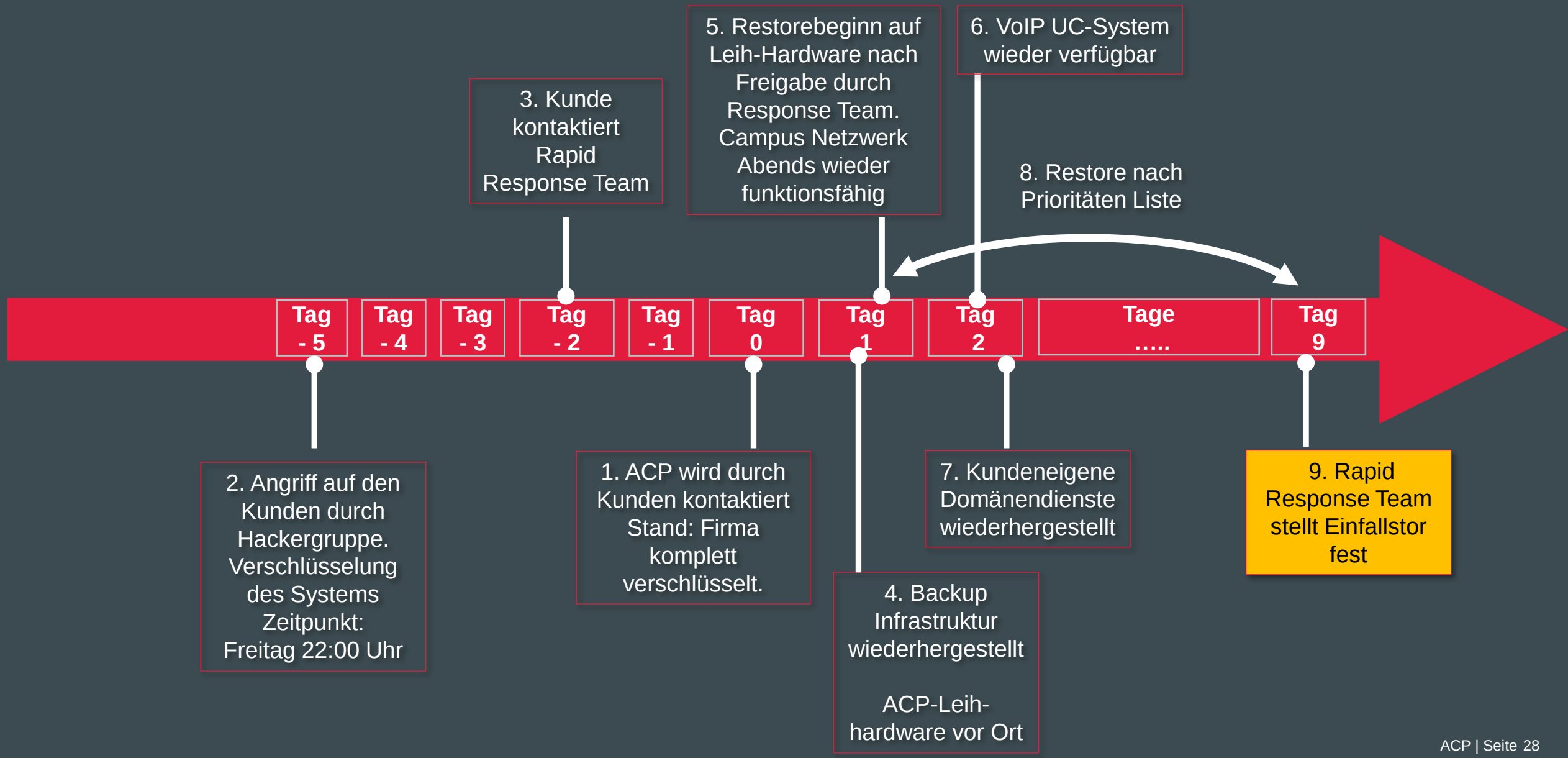
Ganzheitlicher Ablauf



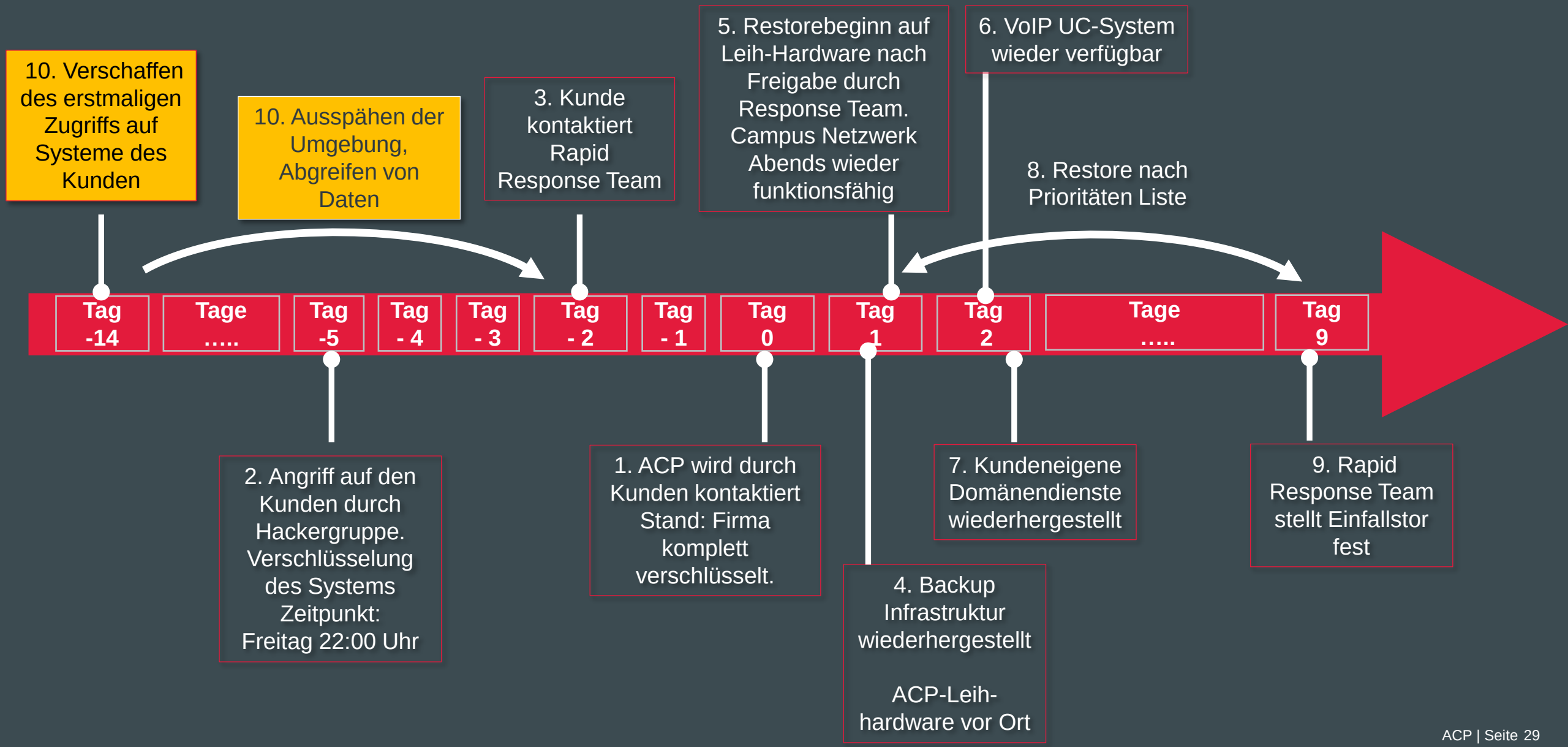
Ganzheitlicher Ablauf



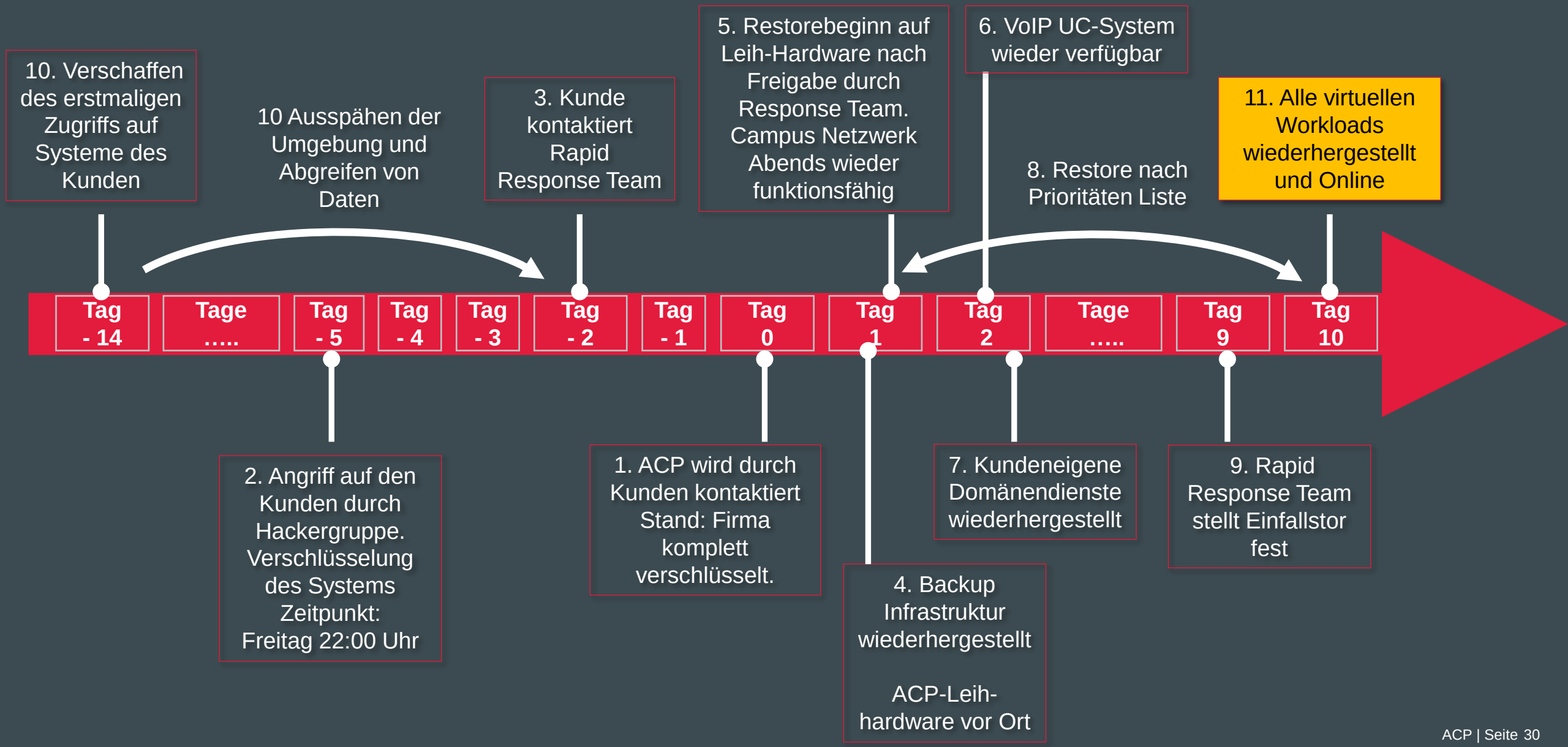
Ganzheitlicher Ablauf



Ganzheitlicher Ablauf



Ganzheitlicher Ablauf



Phasen des Angriffs

1

2

Erstmaliger Zugriff

Tag - 14

14 Tage Aussp[illegible]

Kontaktaufnahme ACP

Tag 0

Angriff
Freitag, 22:00 Uhr

Rapid Response Team stellt Einfallstor fest

Tag 9

Tag 10

Alle Workloads online

Daten-verlust

Betriebs-ausfall

Tatsächlicher Schaden

Sofortmaßnahmen

Kappen der Internetanbindung

Sofortmaßnahmen

Systeme ausschalten Ja/Nein?


RANSOMWARE

Absch


IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

Wiederanlauf

- Notfallplan anwenden

Inhalt Notfallplan

- Meldekette (Wer muss informiert werden?)
  - Notfallkontakte
  - Behörden
- Sofortmaßnahmen festlegen
  - Schadsoftware
  - Elementarschäden (Brand, (Lösch-) Wasser, Überspannung, etc.)
- Kommunikationsmatrix
  - Pressemeldung
  - Extern (Kunden, Partner) / Intern (Mitarbeiter)
- Wiederanlauf und Wiederherstellung der kritischen IT-Services
  - Bedarf Personal (Intern / Dienstleister)
  - Prioritäten der Services / Reihenfolge der Wiederherstellung (incl. Abhängigkeiten)
  - Ersatzinfrastruktur / Ersatzräumlichkeiten

Wiederanlauf - Analyse

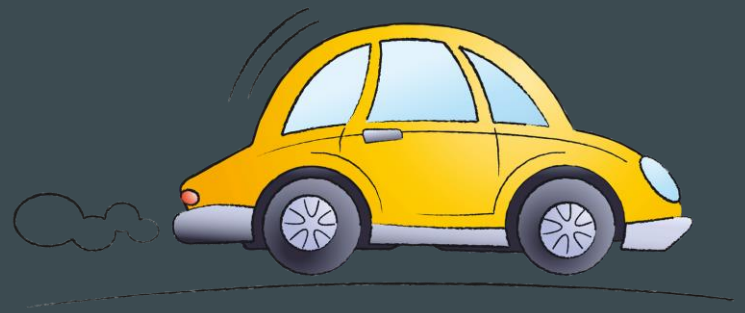
- Response Team + Restore Team (Dienstleister) hinzuziehen
- Analyse durch Response Team
  - Betroffene Systeme finden
  - Angreifer anhand Angriffsschema identifizieren
  - Ausmaß und Zeitrahmen erkennen
  - Betroffene Systeme prüfen
  - **Einfallstore lokalisieren**

WICHTIG:
Response Teams machen Forensik und
<u>keine</u> Restoreaktivitäten

Wiederanlauf - Restore

- Ihre Systeme sind in der Regel nicht nutzbar!
  - da kompromittiert / verschlüsselt
  - diese für Forensik gebraucht werden
  - ggf. Beweissicherung betrieben werden muss
  - keine zusätzliche Kapazität vorhanden ist

Sie haben erstmal kein einsatzfähiges IT-System



Sie brauchen ein Leihauto!

ACP Cloud Rescue Kit

- Mobiles unabhängiges Datacenter
  - **kundenspezifische Konfiguration mit Cloud Replicas**
  - in wenigen Stunden verfügbar
  - für Kooperation mit Response Teams vorbereitet
- isoliertes System, das an Ihre Umgebung gekoppelt werden kann
- virtuelle Umgebung mit zentraler Storage
- unabhängige Backuphardware
- eigenes Routing, eigene IP Services
- dedizierte Firewall mit eigenen WAN-Uplinks
- in verschiedenen (T-Shirt) Größen verfügbar

Warum ACP Cloud Rescue Kit?

- Schnell verfügbare Leihhardware
- Schneller Wiederanlauf in Kombination mit Veeam Cloud Replica
- Kein Warten auf Freigabe der eigenen Hardware
- Response Team kann prüfen, ob die wiederhergestellten Workloads in Ordnung sind
- Optimiert durch einen erfahrenen Partner mit Tools

Vorbereitung

- Welches System hat welche SLA/Priorität?
- Wie sieht die Backupstrategie aus?
  - 3-2-1-Regel
  - Performance (SATA/SSD/Cloud)
  - Verfügbarkeit (Tape, WAN-Bandbreite)
- Wer prüft das regelmäßig, ob das noch passt?

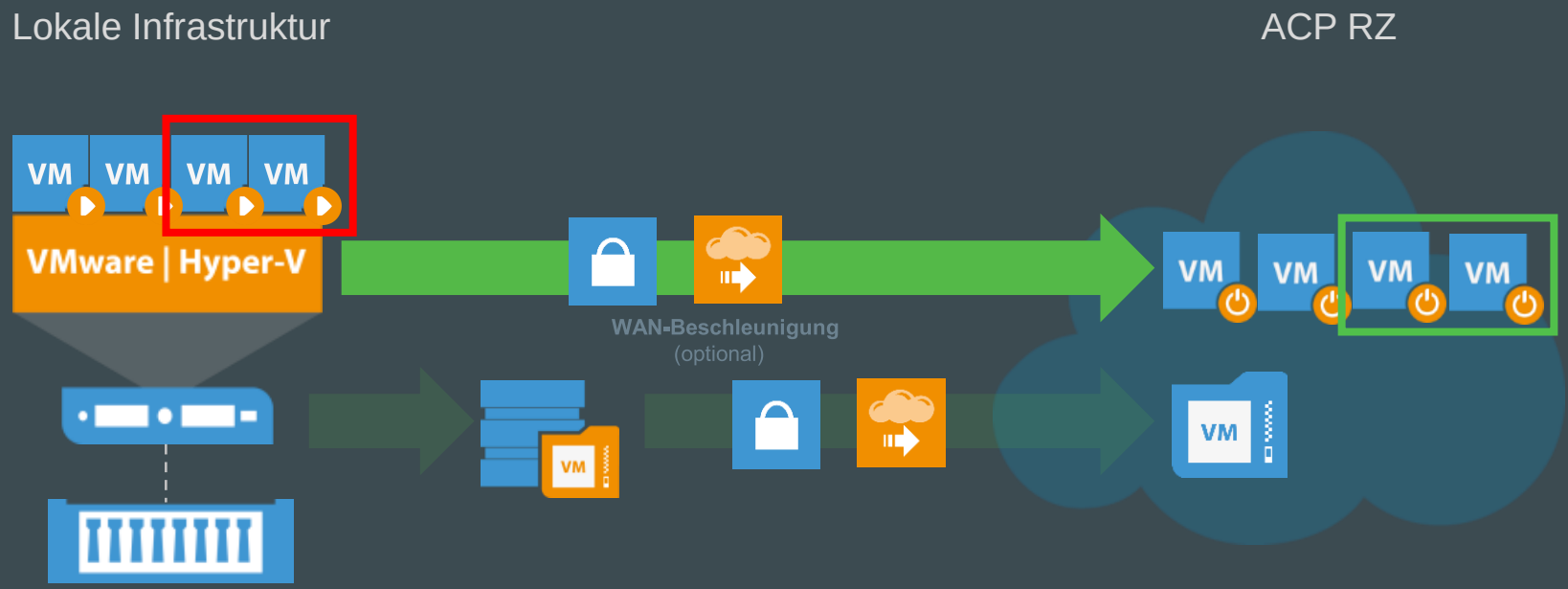
SLA1	• Kritische Systeme
SLA2	• Standard Systeme
SLA3	• Nice to have Systeme

ACP.HZB Onbording Prozess
incl. zyklischer Kontrolle mit dem Kunden!

Cloud Replica

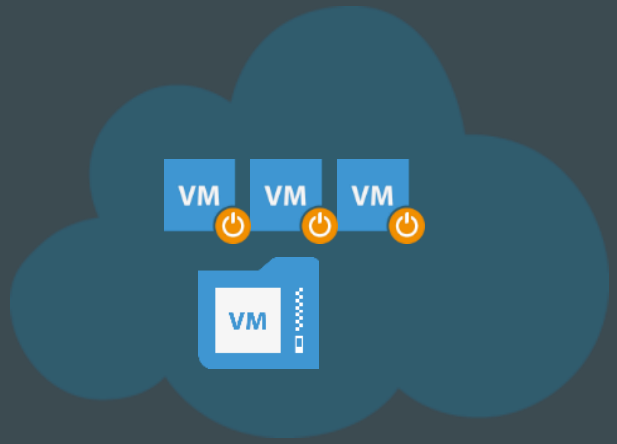
Veeam Cloud Connect Replica (Regelbetrieb vor dem „K“-Fall)

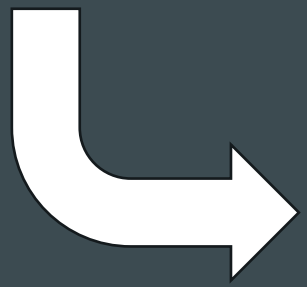
- SLA 1 Workloads



Das ACP.HZB Cloud Rescue Kit

ACP RZ

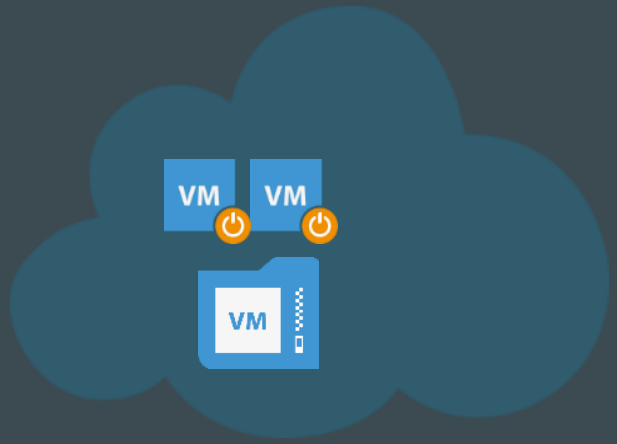


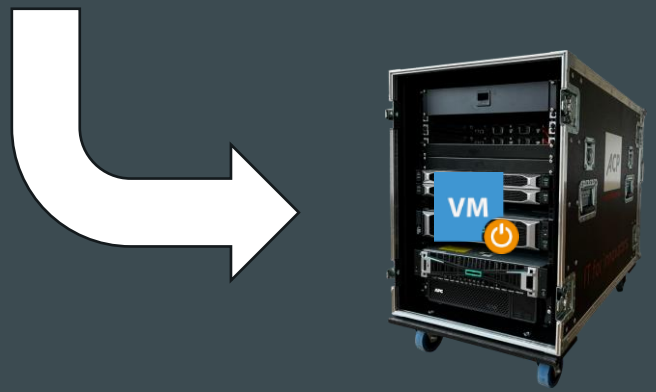


Firewall (incl. LTE)
Netzwerk (>= 10 Gbit/sec)
Compute (ESXi)
Block-Storage (AllFlash)
Backup-Server (Veeam)
zwei Stromkreise incl. USV

Das ACP.HZB Cloud Rescue Kit

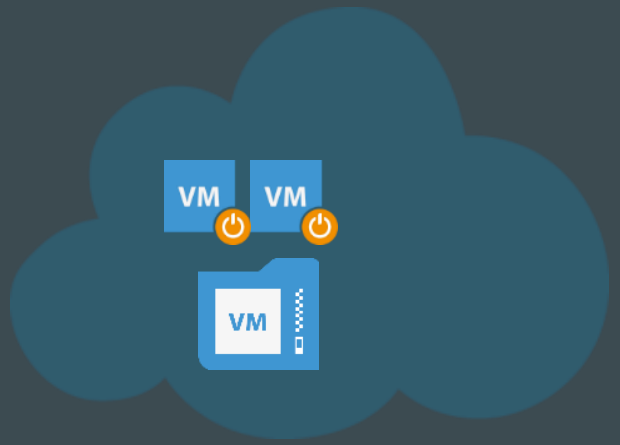
ACP RZ

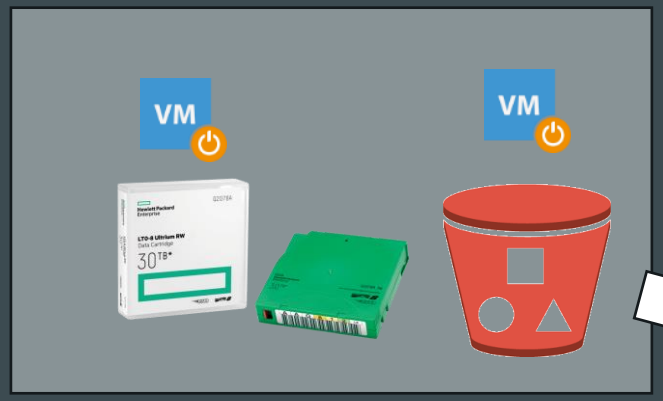




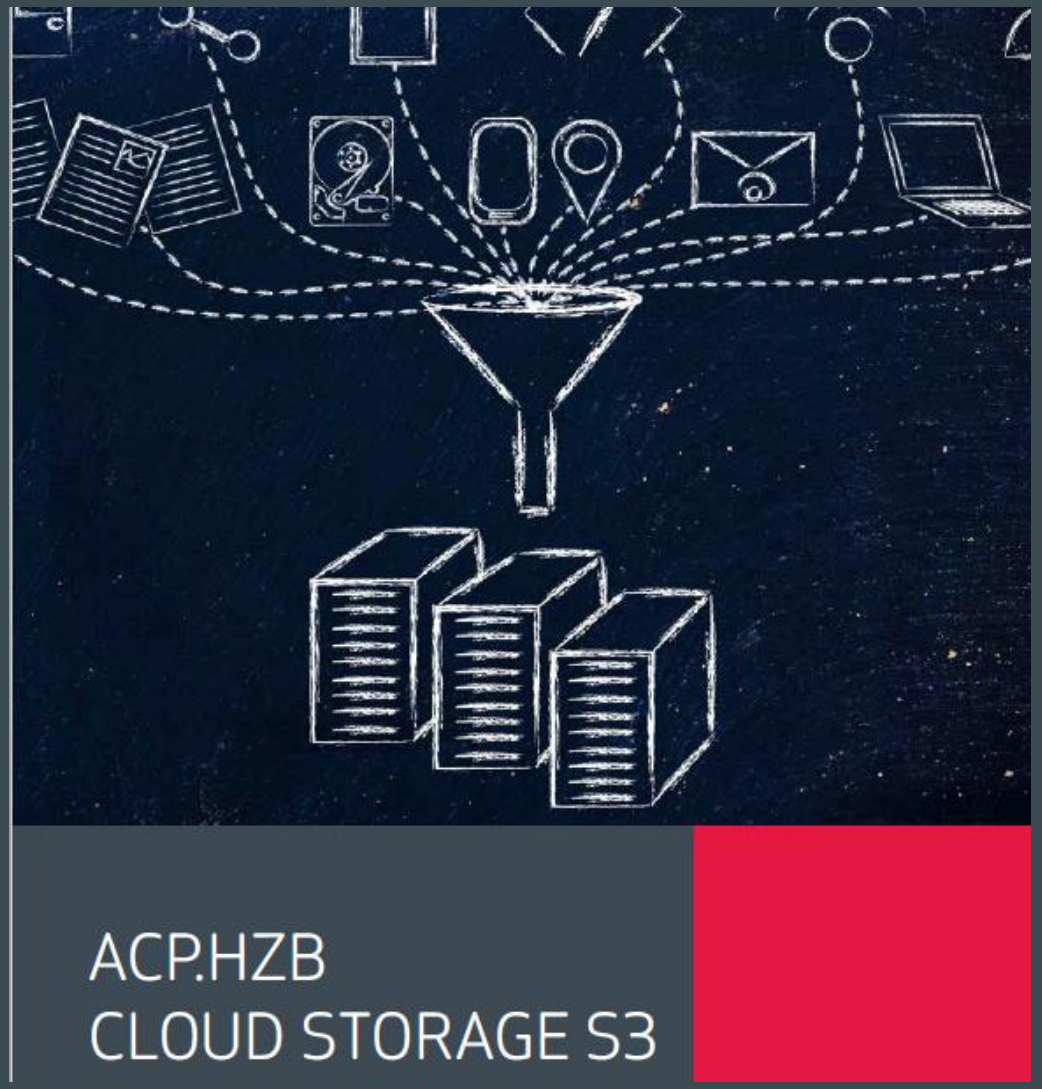
Das ACP.HZB Cloud Rescue Kit

ACP RZ





Backup auf S3



Backup-Ziel für SLA2/SLA3

- Object-Lock
- Versioning
- Immutability

Features / Leistungen im Rescue Kit

- Maßgeschneiderte Leihhardware mit Rescue Service
  - Modulares Baukastensystem
  - Verschiedene „T-Shirt Größen“
- Verkürzung der Wiederanlaufzeit um mindestens 5 Tage
- Wichtiger Bestandteil Ihres Wiederanlaufplans (Ersatzinfrastruktur) -> NIS2!
- Regelmäßige Rücksprache mit dem Kunden über die zu replizierenden Systeme
- **Add-Ons im RZ**
  - **Zusätzliches Backup (Veeam KI)**
  - **SureLab**
- **Test – funktioniert das Konzept denn?**

NIS-2 und Risikomanagement

BCM/Notfallmanagement (Auszug) nach
ISO 22301:2019 & BSI 200-4

Ausfallszenario	BC-Strategie	BC-Lösung	Zuständigkeit	Wirkung
Gebäude	Ausweicharbeitsplätze	Bereitstellung von 50 dedizierten Ausweich-Arbeitsplätzen am Standort Musterhausen	Gebäudeverwaltung	zeitnaher Umzug und Weiterarbeiten im Notfall möglich
Gebäude	Remote-Arbeit	Ausstattung aller Mitarbeiter mit Laptops und VPN-Client	Abteilung IT	zeitlich und örtlich unabhängiges Arbeiten möglich
Gebäude	redundante Stromversorgung	Ausstattung des Gebäudes mit einer Netzersatzanlage, Einsatzzeit 12 Stunden	Gebäudeverwaltung	Sicherstellung der Arbeitsfähigkeit bei Stromausfall bis zu 12 Stunden
IT	**redundantes RZ**	**Betrieb eines zweiten RZ im Hot Standby**	**Abteilung IT**	**Wiederanlauf aller Anwendungen im Rahmen der WAZ möglich**
Personal	Stellvertreter-Regelungen	Festlegung von Stellvertretern für alle Schlüsselfunktionen	jede OE	Reduzierung der Auswirkungen bei Personalausfall
Personal	Springer-Teams	kontinuierliche Schulung und Wissensaustausch mit den Trainees zwecks Einsatz im Notfall als Springer-Teams	Abteilung Personal	Reduzierung der Auswirkungen bei Personalausfall
(…)	(…)	(…)	(…)	(…)

Quelle: Notfallvorsorgekonzept (Dokumentvorlage) Hilfsmittel zum BSI-Standard 200-4

Empfehlungen/Ausblick

- Rescue Kit ist wie eine Versicherung
  - wichtiger Bestandteil des Wiederanlaufplans
  - Ersatzinfrastruktur
  - auch als reine Hardware mietbar
  - Teil des Notfallplanes/-konzeptes
- haben ist besser als brauchen
- ruhiger schlafen
- wissen, dass man einen zuverlässigen Pannendienst hat (ACP)

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

IT for innovators.