Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee
Führungsunterstützungsbasis FUB

In der Cyber-Hölle für 30 Min.

Angriffsszenario auf eine Bahn

18.11.2021, Luzern

Oberstlt Riccardo Sibilia

Führungsunterstützungsbasis

News

https://edition.cnn.com/2021/11/17/politics/us-iran-hackers-warning/index.html
Edition
politics
The Biden Presidency
Facts First
US Elections
US warns that Iranian government-sponsored hackers are targeting key US infrastructure
By Sean Lyngaas, CNN
Updated 1739 GMT (0139 HKT) November 17, 2021
NOW PLAYING
Here's everything you need to know about ransomware
CNN Business
00:00 / 04:04
Source: CNN Business
Here's everything you need to know about ransomware 04:04

US fuel pipeline hackers 'didn't mean to create problems'
By Mary-Ann Russon
Business reporter, BBC News
10 May
COLONIAL PIPELINE
1474

The New York Times
Mysterious Hacker Group Suspected in July Cyberattack on Iranian Trains
An investigation by a cybersecurity company has concluded that a little-known group opposed to the Iranian government was most likely behind the hack that caused chaos on the railway system.

Cyber Wargaming

Spielregeln:

- Sie sind Mitglieder des Verwaltungsrat oder Geschäftsleitung der Bahngesellschaft ABC Bahn AG – Entscheidungsträger
- Sie können Ihre Stimme über *Mentimeter* abgeben – die Mehrheit entscheidet
- Phase 1 startet am 18. November 2022
  - Weg durch die Hölle (Ramsonware-Szenario)
- Phase 2 startet am 22. November 2021 (nächsten Montag)
  - Was würden Sie tun, wenn Sie die Zeit zurückdrehen könnten

Interaktion: Mentimeter

QR CODE

Link:

https://menti.com/

PIN: XXXX XXXX

Charakterisierung des Angreifers

- Name der Gruppe: **InfraBong**
- Verfügt über verschiedene "Intrusion Kits", die ihn erlauben, in vernetzten Systemen im Windows- und Linux-Umfeld einzudringen und sich lateral zu bewegen
- Ist in der Lage – mit einem gewissen zeitlichen Aufwand – eingebettete Systeme (IoT) zu übernehmen und zu manipulieren
- Hat die Infrastruktur und Systeme der Zielbahn auskundschaftet und verfügt über Angaben in der Architektur und Konfiguration aus früheren Kampanien gegen Lieferanten der Zielbahn
- Verfügt über sehr gute sprachliche Kenntnisse in Deutsch und kennt sich in der Schweiz aus
- Hat zahlreiche Verbindungen im Finanzsysteme, um das erbeutete Geld aus der Krypto-Währungen in "echt Geld" umzuwandeln
- Agiert aus einem Land im ehem. Ostblock

Ziele des Angreifers

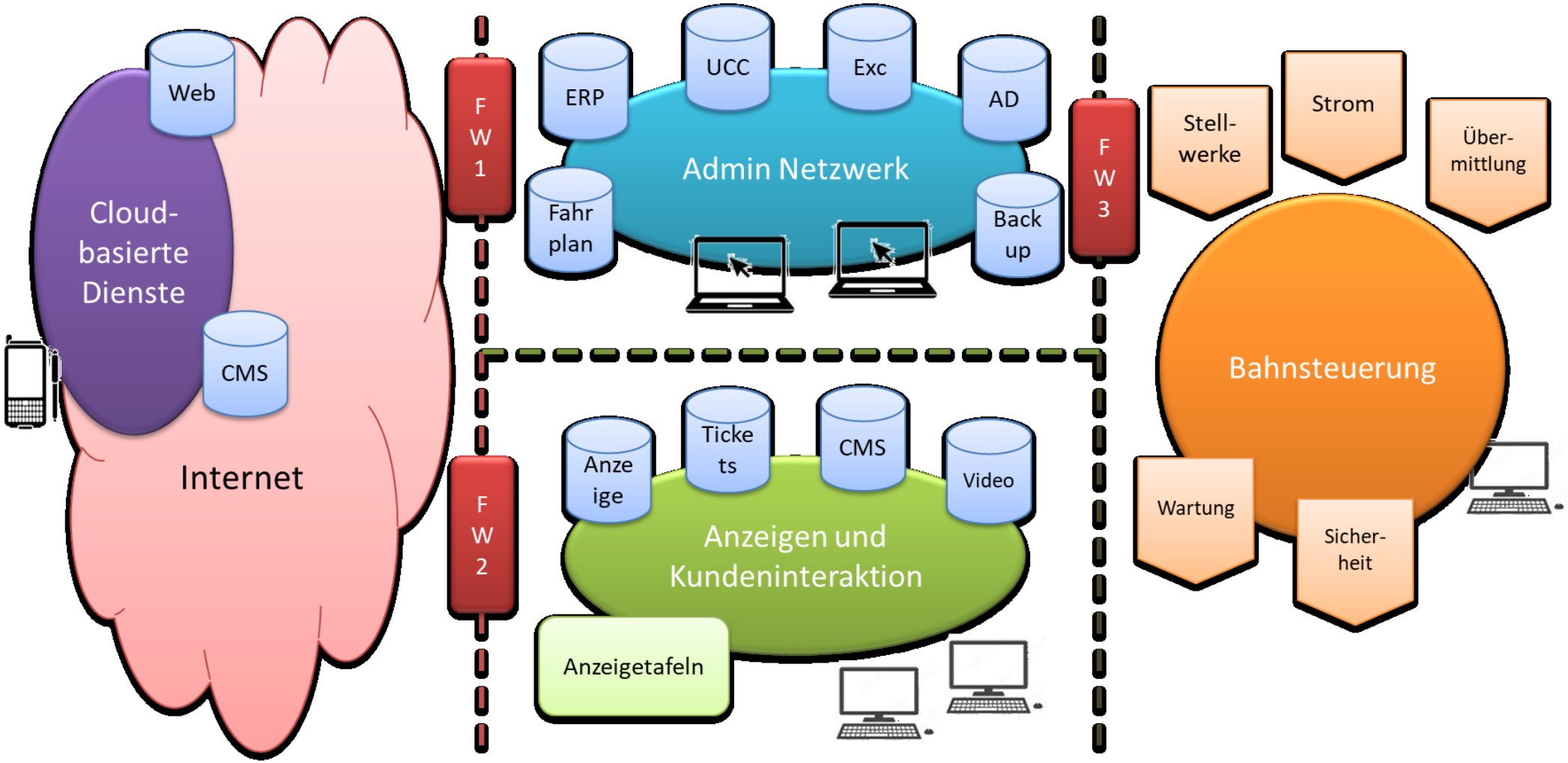
Primär:

- Erbeuten von Geld mittels Erpressung oder Manipulation

Dazu wird er versuchen:

- Den Bahnverkehr zu stören und die Bahnsicherheit zu beeinträchtigen
- Die Passagierflüsse zu beinflüssen
- Die Abrechnung der Bahnleistungen zu verhindern

Eigene Infrastruktur



FREITAG 18.11.2022, 17:23

AUF DEM WEG IN DEN FEIERABEND...

Den Weg durch die Cyber-Hölle

PHASE 1

Input:

Tag 0, 17:23 Telefonanruf aus Ihrer IT-Abteilung

- 12 Rechner in 3 verschiedene Abteilungen sind verschlüsselt
- Ein Drucker-Server und ein Backup-Server sind über das Netz nicht mehr erreichbar
- Es wird ein Major Incident ausgelöst
- Sie werden gebeten, zurück ins Büro zu kommen

Input:

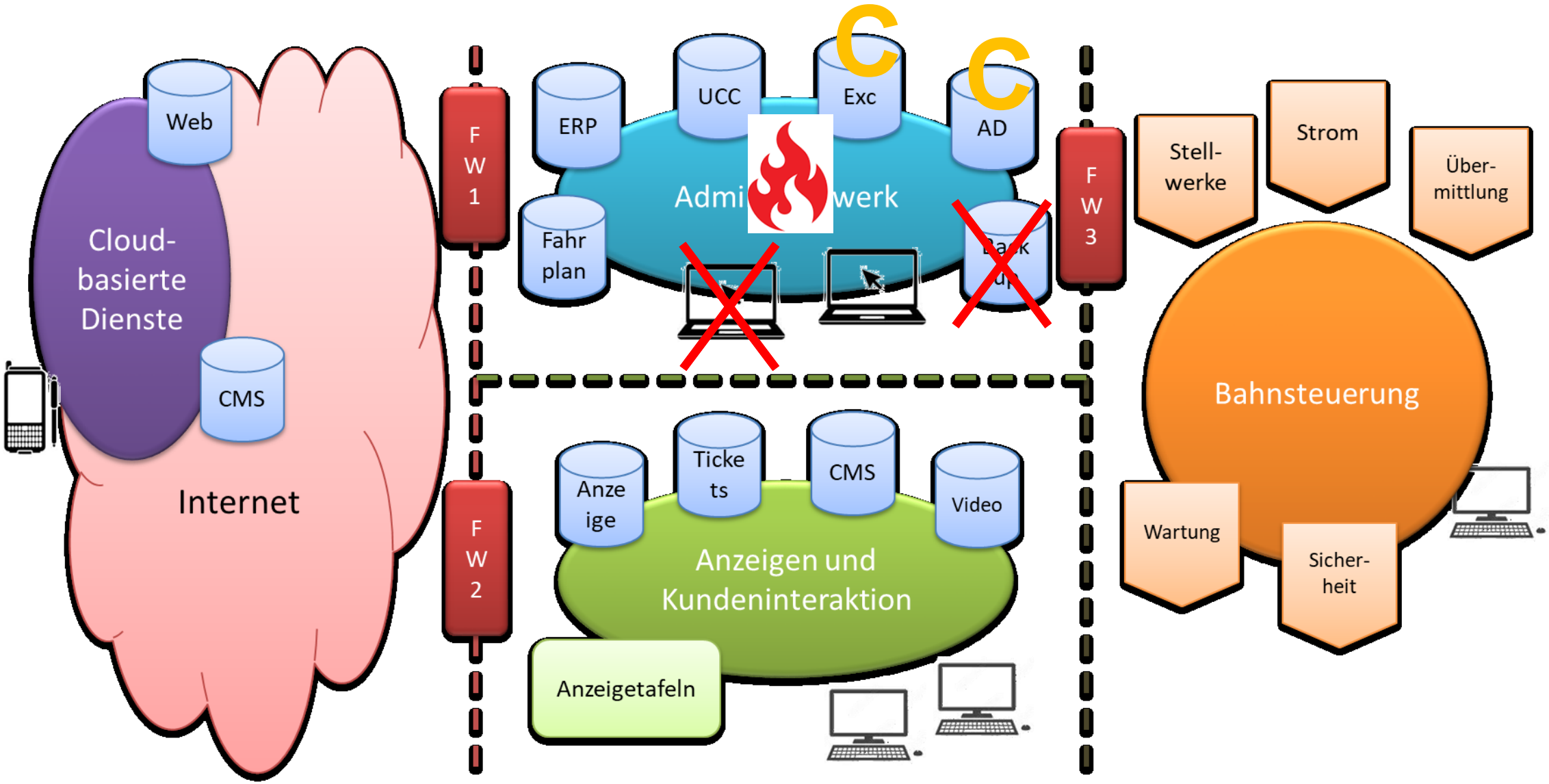
Tag 0, 18:15 Sie betreten das Bürogebäude, Lagebericht

- Der IT-Chef und der Sicherheitschef erwarten Sie dort
- Aktuellen Stand: 22 Rechner in 4 Abteilungen sind verschlüsselt
- Auf den Bildschirme der verschlüsselten Rechner wird eindringlich gebeten, mit der E-Mail infrabong666@gmail.com Kontakt aufzunehmen
- Die Frist für die Kontaktaufnahme beträgt 4 Stunden ab 17:05

Tag 0, 19:53 erste Ergebnisse

- Eine erste forensische Analyse des SOC zeigt, dass das Netzwerk seit 17 Tage kompromittiert ist
- U.a. Domänenkontroller, Exchange-Server und Collaboration Services sind übernommen worden
- Es findet C&C-Datenverkehr zu verschiedene IP-Adressen statt

Lagebild, Tag 0, 19:53



E: Tag 0, 20:15, Trennung der Internetverbindung

- Sie merken, dass die Angreifer ihre Aktion über die C&C-Server aktiv steuern
- Sie kennen der Ausmass des Schaden und die Fähigkeiten des Angreifes noch nicht
- Es werden Ihnen vom SOC folgende Handlungsoptionen angeboten:

Option A:
- Trennen der Internetverbindung
- Wiederherstellung der Systeme aus den Backups

Option B:
- Beobachtung des C&C-Datenverkehrs
- Vertiefte Analyse der Werkzeuge und Tätigkeit der Angreifer
- Kontaktaufnahme zwecks Verhandlung mit den Täter (oder Zeitgewinn)

Option C:
- Beobachtung des C&C-Datenverkehrs
- Vertiefte Analyse der Werkzeuge und Tätigkeit der Angreifer
- Keine Kontaktaufnahme mit den Angreifer

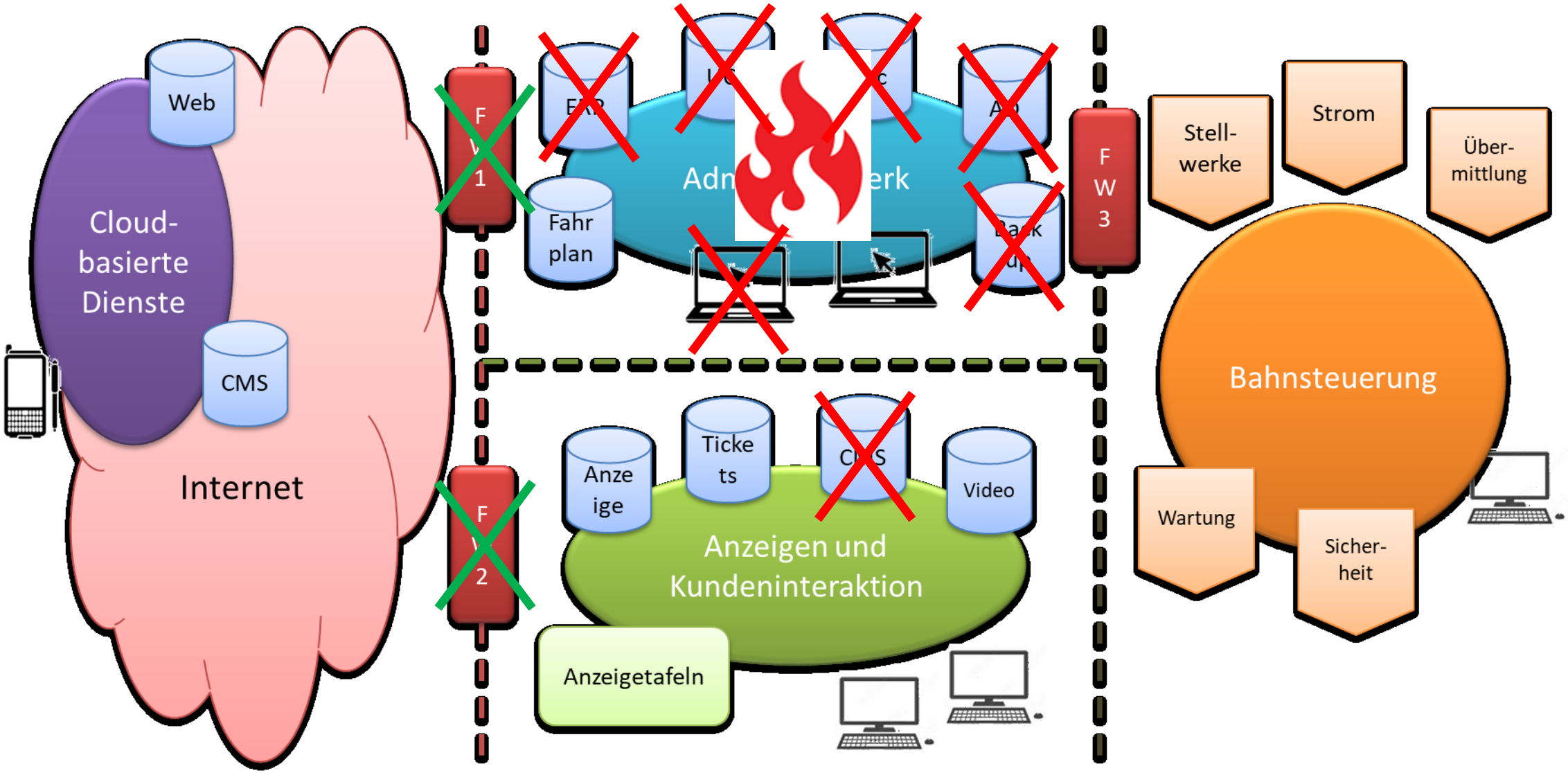
Input:

Tag 0, 21:14 Trennung

- Alle Active Directory Servers werden verschlüsselt
- Mitteilung sagt:

  "Bitte stellen Sie die Verbindung zum Internet wieder her, ansonsten werden alle Systeme verschlüsselt. Die Entschlüsselung kostet zusätzliche 10 Bitcoins."
- Ein Counter fängt an, auf den Server zurückzuzählen.

Lagebild, Tag 0, 21:14



E: Tag 0, 21:14, Internetverbindung wiederherstellen

- Aufgrund der Drohung müssen Sie entscheiden, ob Sie die Verbindung wieder herstellen oder nicht
- Wenn alle Systeme im Admin-Netz verschlüsselt sind, sind Ihre Handlungsoptionen wesentlich eingeschränkt
- Es werden Ihnen vom SOC folgende Handlungsoptionen angeboten:

Option A:
- Wiederherstellen der Internetverbindung
- Kontaktaufnahme zwecks Verhandlung mit dem Angreifer (oder Zeitgewinn)

Option B:
- Wiederherstellen der Internetverbindung
- Kein Kontaktaufnahme mit den Angreifer

Option C:
- Keine Wiederherstellung der Internetverbindung

Input:

Tag 0, 21:03 Sie drucken auf "Mail absenden"

- Mittlerweile sind zahlreiche Endgeräte und Server im Admin-Netz verschlüsselt
- Die Rechner der GL- und Verwaltungsrat Mitglieder sind nicht betroffen
- Sie schreiben eine E-Mail mit dem unterstehenden Inhalt an der angegebene Adresse:

  Ich bin der CEO von ABC Bahn AG und möchte mit Ihnen über Ihre Forderungen reden. Bitte teilen Sie uns mit, was Sie wollen.

Weiter

Input:

Tag 0, 21:06 Sie haben nicht Kontakt aufgenommen

- Mittlerweile sind zahlreiche Endgeräte und Server im Admin-Netz verschlüsselt
- Die Rechner der GL- und Verwaltungsrat Mitglieder sind nicht betroffen
- Die Zeit für die Kontaktaufnahme ist seit 1 Min. abgelaufen
- Ihr Rechner wird verschlüsselt und folgende Botschaft erscheint:

  Sehr schade, wollen Sie nicht mit uns reden. Wir werden leider die Öffentlichkeit über diese Situation informieren müssen. Dieses kostet Ihnen zusätzlich 10 Bitcoins.

- Familienangehörige der Mitglieder der GL- und Verwaltungsrat erhalten eine E-Mail mit Forderungen

Input:

Tag 0, 22:06 Die Forderungen

- Sie erhalten eine E-Mail:

  Wie Sie sicher festgestellt haben, haben wir die Kontrolle über Ihre Infrastruktur übernommen. Wir erwarten eine Zahlung von 151 Bitcoins auf die Adresse

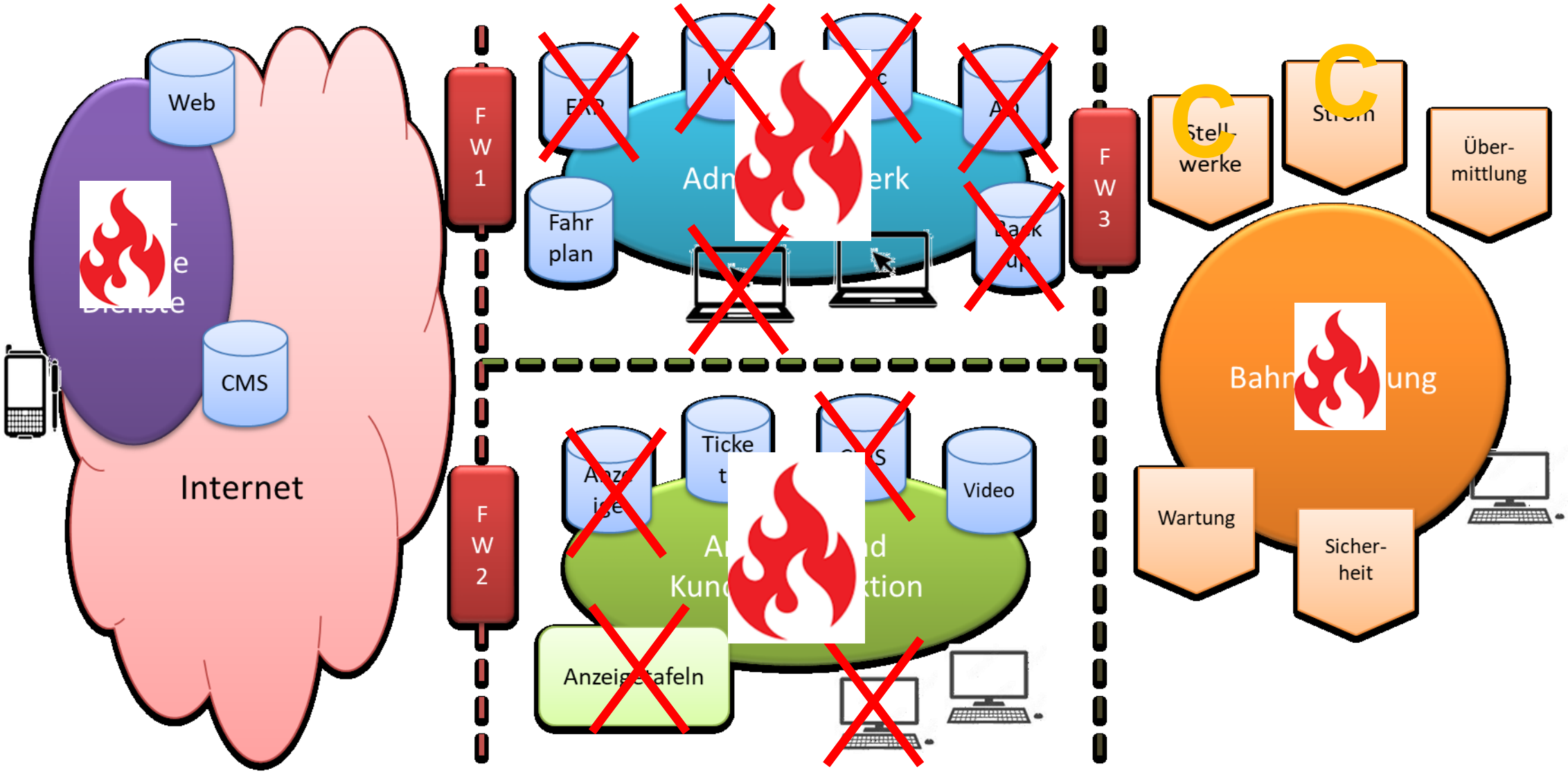
  bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

  Dazu haben Sie ab jetzt 72 Stunden. Danach legen wir Strom und Stellwerke in der ganzen Schweiz lahm. Wir können nicht für die Unversehrtheit von Mensch und Material garantieren. Sollten wir merken, dass Sie versuchen unternehmen, uns auszuschliessen, werden wir sofort handeln.

  Nach der Zahlung werden wir die Schlüssel senden. Sie werden von uns nie mehr was hören.

  Danke für die Angenehme Zusammenarbeit.

Lagebild, Tag 1, 22:15



Freitag, 18.11.2022, 22:15
An den Bahnhöfen mit Digitalanzeige…

E: Tag 1, 06:30, Bezahlen?

- Sitzungszimmer Verwaltungsrat ABC Bahn AG
- Ihre Spezialisten bestätigen, dass verschiedene kritische Komponenten im Bereich Strom, Stellwerke, Sicherheitskontrollen von Rollmaterial, Ticketautomate und weitere mit Malware versehen sind
- Die Kommunikation erfolgt über kompromittierte Rechner im Admin-Netz
- Die Malware fängt an nach Ablauf der Frist alles zu verschlüsseln
- Wird die Kommunikation unterbrochen, legt sie sofort los

Option A:

Sie bezahlen 151 Bitcon (ca. 8.5 Mio. CHF)

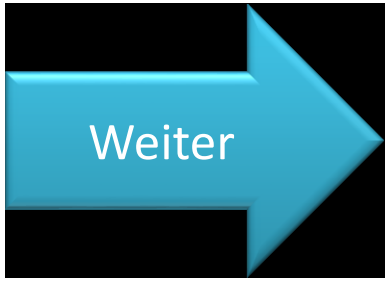
Option B:

Sie bezahlen nicht und versuchen, Ihre Infrastruktur wieder in den Griff zu bekommen

Input:

Tag 0, 21:31 AD Server wird wieder entschlüsselt

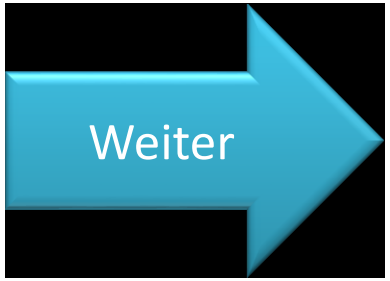
- Die Internet-Verbindung wurde wiederhergestellt
- Die Angreifer haben die Entschlüsselung der AD-Server über den C&C-Server in Gang gesetzt. Diese sind nach ca. 20 Min. wieder Betriebsbereit
- Die Malware ist immer noch drauf



Input:

Tag 0, 21:31 AD Server wird wieder entschlüsselt

- Die Internet-Verbindung wurde wiederhergestellt
- Die Angreifer haben die Entschlüsselung der AD-Server über den C&C-Server in Gang gesetzt. Diese sind nach ca. 20 Min. wieder Betriebsbereit
- Die Malware ist immer noch drauf



Input:

Tag 1, 06:00 … es geht nichts mehr

- Die Malware löst aufgrund der fehlende Verbindung mit den C&C-Server oder Ablauf der Frist die Verschlüsselung aller Systeme aus
- Rechner in verschiedene Bereiche der Bahninfrastruktur fallen aus
- Strom, Stellwerke und andere sind betroffen
- Die Wiederherstellung zum Normalzustand benötigt mehrere Monate und verursacht massive Kosten

Weiter

Input:

Tag 1, 15:30 Sie bezahlen

- Sie bezahlen den verlangten Beitrag
- Innerhalb 15 Min. verschwindet den Betrag auf tausende von Crypto-Currencies accounts und ist nicht mehr zurückverfolgbar
- Danach erhalten Sie eine E-Mail mit einem Schlüssel, mit dem sich die Systeme wieder entsperren lassen
- Die Funktion kann wiederhergestellt werden, auch wenn die Malware ein Teil der Systeme beschädigt hat
- Mehrere Wochen lang bestehen Störungen in Ihrer Infrastruktur
- Die vollständige Bereinigung läuft weiter während Monate

MONTAG 22.11.2021, 08:23

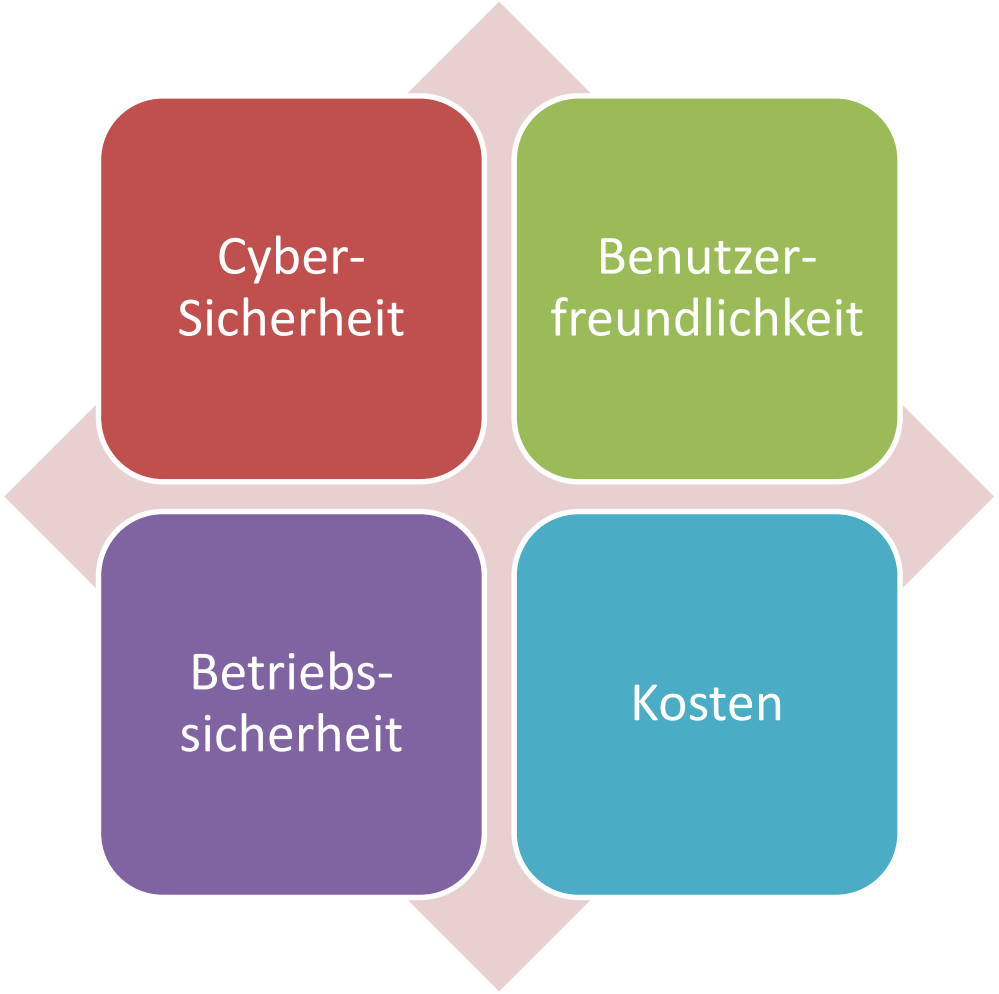
... SIE TREFFEN IM BUERO EIN.

Was würden Sie tun…

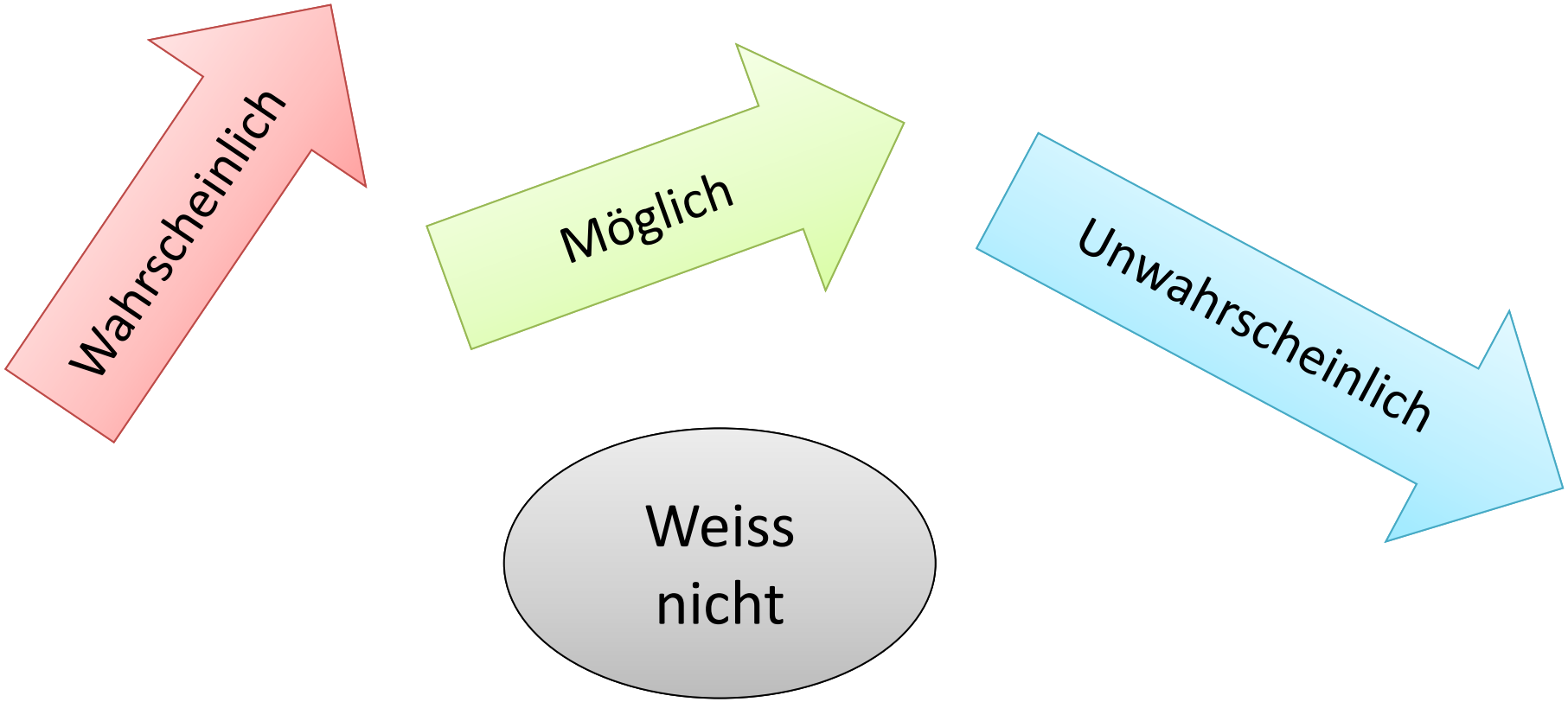
PHASE 2

Was würden Sie tun…

- Das kleine Szenario hat Sie durch eine Reihe sehr unangenehme Situationen geführt
- Es gilt die Voraussetzungen zu schaffen, solche Dilemmas mit minimalen Schaden zu bewältigen
- Dabei gilt es verschiedene Anforderungen und Ansprüche zu berücksichtigen



Wie schätzen Sie das Risiko ein?



Wie schätzen Sie die Bedeutung dieses Risiko ein?

- Wird diese Bedrohung in der Risikowahrnehmung entwickeln?

Ja

unbekannt

Nein, es stimmt schon

Welche Massnahmen würden Sie treffen?

- Was, aus Ihrer Sicht, aus der Perspektive dieser Bedrohung, würde am meisten helfen?
- Ein Vorschlag pro Person, in Form eines Stichwortes oder kurzes Satz

Dankeschön für die Aufmerksamkeit und das Mitmachen!

Und weiterhin viel Erfolg!