Von der Attacke zur Kontrolle: Die Anatomie eines Cyberangriffs und effektive Reaktionsstrategien

@YET

@-yet Fakten:
seit 2002 für Digitale Souveränität im Einsatz

Gegründet 2002 | seitdem inhabergeführt | Sitz in Leichlingen NRW

Über 90 Mitarbeiter:innen | in Deutschland und weltweit tätig

Family Offices | Mittelständler | Konzerne | Organisationen

@-yet Industrial IT Security

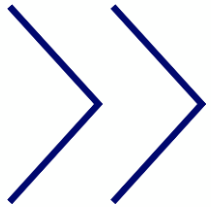
Beratung & Dienstleistungen rund um die Cybersicherheit von Industrieunternehmen

- gegründet 2017
- Hans-Wilhelm Höfken
  Prof. Dr. Marko Schuba
  Wolfgang Straßer
- Sitz in Aachen, NRW
- über 10 Mitarbeiter:innen
- in Deutschland und weltweit tätig
- Betrachtung von IT- und OT-Sicherheit als Prozess
- Sicherheit in der Fertigung
- Sicherheit von Industrienetzen und Steuerungs-komponenten
- Sicherheit in Industrie 4.0 Szenarien

Risiken minimieren – Resilienz aufbauen – Schäden beheben Arbeitsfähigkeit sichern oder wiederherstellen

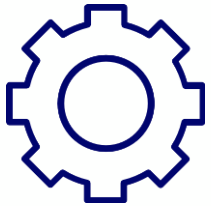
Prevention

Vorbeugen für freies und unbesorgtes Business



Continuity

Unterbrechungsfreie Prozesse schaffen



Digitale Compliance

Rechtliche und externe Anforderungen erfüllen

Notfallhilfe

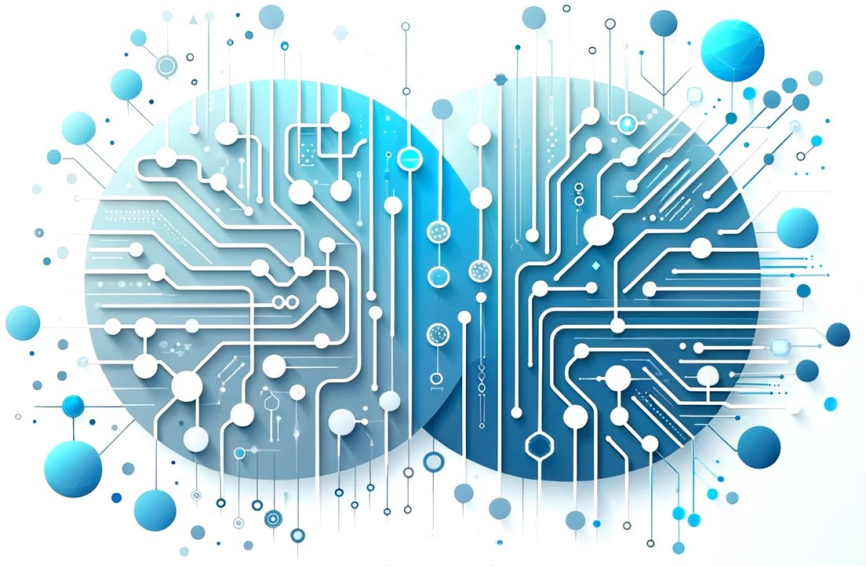
Schnelle Hilfestellung, Forensik und Wiederanlauf

Beratung

ISMS, sicher Infrastruktur, sichere Cloud, sicher Produktion, Notfallplanung

Agenda

- Was ist DFIR und warum braucht man DFIR?
- Ablauf eines Cyber-Angriffs
  und woran man diesen frühzeitig hätte erkennen und abwehren können
- Was benötigt der DFIR-Dienstleister?
- Wie lange dauert es?
- Key Takeaways Prävention



Was ist Digital Forensics & Incident Response – DFIR ?

- **Digital Forensics & Incident Response** (DFIR) kombiniert die Disziplinen der digitalen Forensik und der Incident Response:

- **Incident Response** unterstützt ein Unternehmen in der effektive Reaktion auf IT-Notfälle/Sicherheitsvorfälle

- **Digitale Forensik** liefert idealerweise eine lückenlose Aufklärung des Vorfalls

Cyber-Angriffe in der Presse

Bundeslagebild Cybercrime 2023

2. Polizeiliche Kriminalstatistik

Vor dem Hintergrund eines immer noch sehr hohen Dunkelfeldes im Bereich Cybercrime kommt der PKS vor allem als Datenbasis für Trendaussagen und für die Beschreibung der Entwicklung des Phänomenbereichs eine hohe Bedeutung zu.

Nachdem im Jahr 2021 ein Höhepunkt bei den registrierten Inlands Straftaten im Bereich der Cybercrime-Delikte festgestellt wurde, ist die Entwicklung seit 2022 rückläufig. Im Jahr 2023 konnte mit 1,8% ein weiterer leichter Rückgang an Cyber-Straftaten bei der (Inlands-)PKS verzeichnet werden. Die Aufklärungsquote bei diesen Delikten ist angestiegen (32,2%), liegt damit aber auf dem Niveau der letzten vier Jahre. Der Anteil von Cybercrime-Delikten an den registrierten Straftaten insgesamt nimmt leicht ab und lag für das Jahr 2023 bei 2,2% (vgl. 2021: 2,9%; 2022: 2,4%).

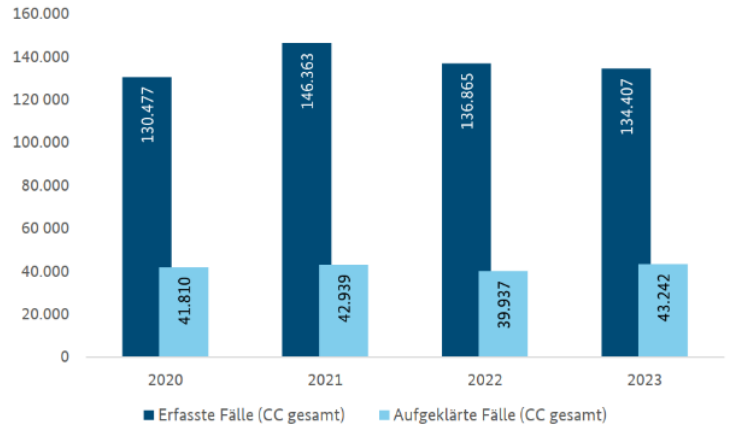


Abbildung 2: Erfasste und aufgeklärte Cybercrime-Fälle in Deutschland 2020 bis 2023

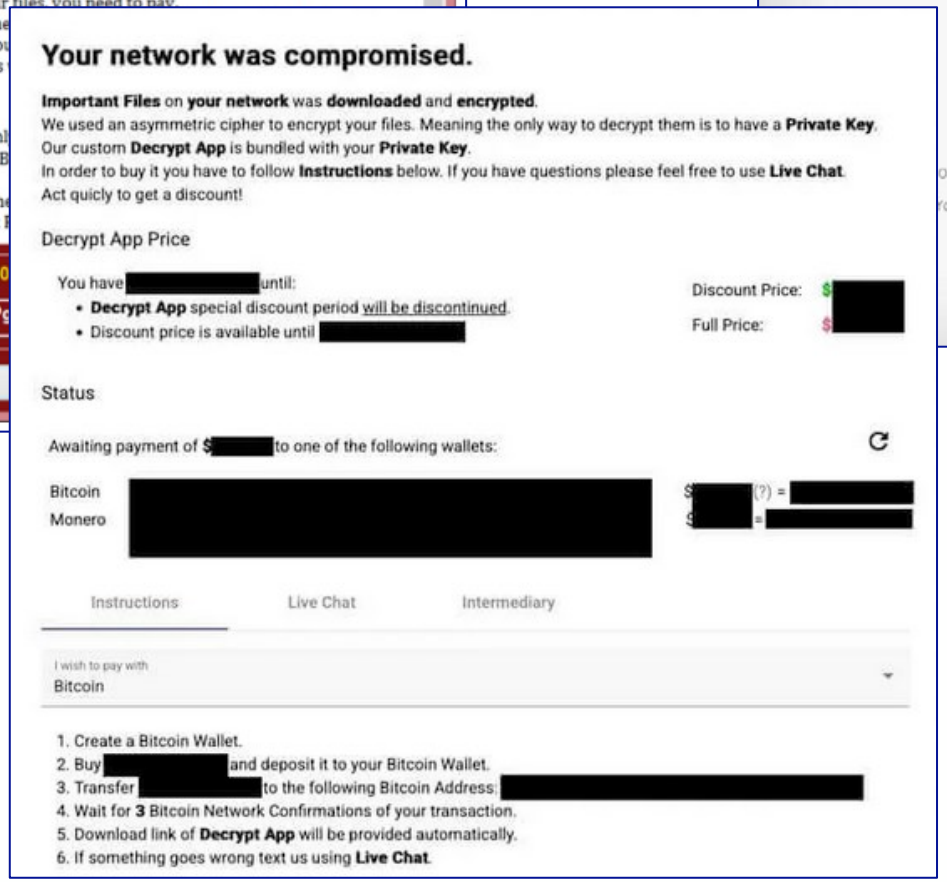
https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.pdf?__blob=publicationFile&v=5

https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/cyberangriff-bkg.html

https://www.golem.de/news/cyberangriff-analysiert-hacker-verschluesseln-unternehmensdaten-ueber-eine-webcam-2503-194073.html

Ransomware – Die sichtbaren Auswirkungen

Wana Decryptr0r 2.0 Ransom Note

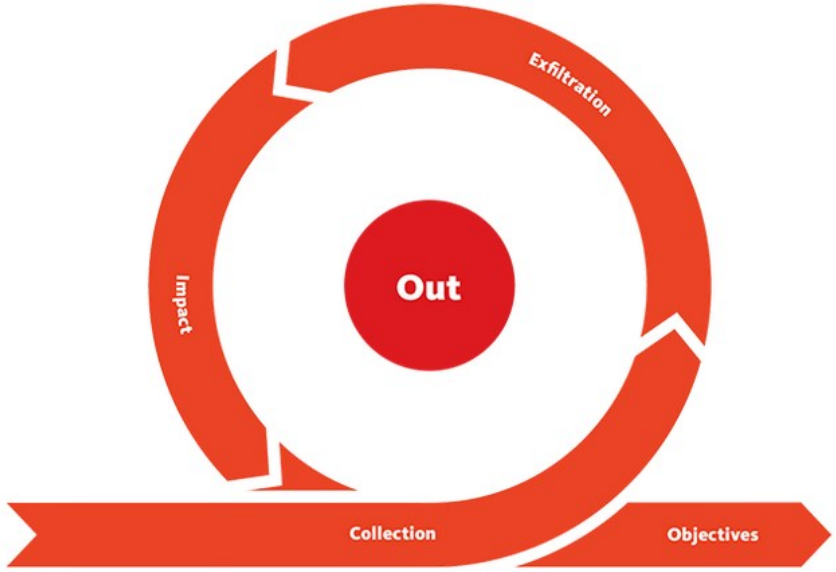


Blackcat / ALPHAV Ransom Note

LOCKBIT 2.0 Ransom Note

Üblicher Ablauf – Unified Kill Chain

- Angriffe sind meist deutlich komplexer, weitreichender und haben früher begonnen, als zunächst angenommen!
- Schematische Darstellung der Phasen eines üblichen Cyber-Angriffs
- Weiterentwicklung der Cyber Kill Chain, entwickelt von Lookheed Martin / Intelligence Driven Defense



Quelle: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf
Autor Paul Pols, Universität Leiden

Warum braucht man Digital Forensics & Incident Response?

- **Ganzheitliche Reaktion** auf einen IT-Notfall bis hin zum vollumfänglichen Krisenmanagement
- **Beweissicherung** und rechtliche Unterstützung
- Detaillierte Ursachen- und **Lagebilderstellung**, z. B.
  - Angriffsvektor und Indicators of Compromise
  - Umfang des Vorfalls
- Erkenntnisse fließen ein in Abwehr und **Bereinigung**
- Nutzung der Erkenntnisse zur **Verbesserung der Sicherheitsstrategie**
- **Schnelle Wiederherstellung** und **Schadensminimierung** durch Aufrechterhaltung des Geschäftsbetriebs
- **Compliance** und Reporting, u. a. Unterstützung durch vollständige Berichte für gesetzliche und regulatorische Anforderungen
- Schutz der **Unternehmensreputation**, u. a. durch schnelle, zielgerichtete und effektive Kommunikation

!

Meist keine Versicherungsansprüche ohne Forensikbericht!

Cyber-Angriff – Sommer 2024 auf einen Kunden der @-yet GmbH

- Der nachfolgend dargestellte IT-Notfall wurde nur unwesentlich verändert und spiegelt weitestgehend den realen Ablauf dar
- Eine Angreifer-Gruppierung drang über abgeflossene Zugangsdaten und einen Citrix Terminal Server in das Unternehmensnetzwerk ein
- Die Angreifer bewegten sich ca. 4 Wochen unerkannt in der IT-Infrastruktur
- Nach erfolgreicher Exfiltration von Daten wurde die IT-Infrastruktur mit einer Ransomware weitestgehend verschlüsselt
- Der Wiederaufbau dauert Monate

Cyber-Angriff – Sommer 2024

Lagebild / Visual Super Timeline

Zeitzone UTC / Times in UTC

Das sichtbare Ende eines Cyber-Angriffs und der Start einer umfangreichen IT-Notfallbewältigung und der Erstellung des Lagebilds:

Cyber-Angriff – Sommer 2024

Lagebild / Visual Super Timeline

Zeitzone UTC / Times in UTC

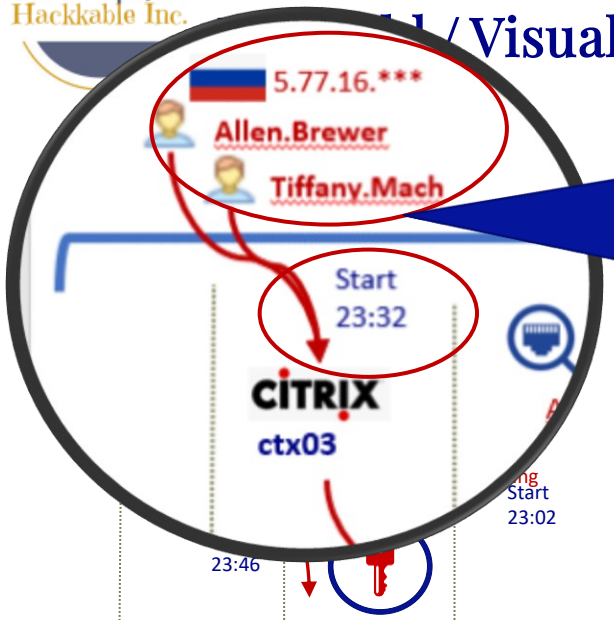
@YET

Wie alles begann:

Cyber-Angriff – Sommer 2024

Zeitzone UTC / Times in UTC

@YET



Erkennung:

- Legitime Benutzerkonten von ungewöhnlicher Geolokation & Uhrzeit

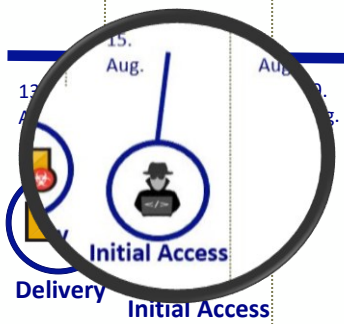
Prävention:

- Conditional Access
- Next-Gen-FW & Detection Rules
- Einwahl mit **MFA** absichern
- Terminal Server erst nach VPN Einwahl

Start
23:02

MFA hätten den Angriff abgewehrt oder zumindest stark erschwert !

Erfolgreicher Phishing-Angriff auf: **Allen.Brewer**, **Tiffany.Mach**



Delivery

Initial Access

Incident Response & Digital Forensics

Internet cut-off

10:30

10. Sep.

11. Sep.

Vorfall identifiziert

Cyber-Angriff – Somm
Lagebild / Visual Super Tim

Zeitzone UTC / Times in UTC

@YET

Erkennung:
- Überwachung von SW-Installationen, hier: Fernwartungs-Tool “Anydesk”

Prävention:
- Application Whitelisting
- Systemhärtung, u. a. keine lokalen Admin-Berechtigungen / Installationsrechte

Erkennung:
- Anti-Virus detektiert Schadsoftware “Mimikatz”

Prävention:
- Monitoring, Alarmierung und Prozesse / Reaktion

13. Aug. — Delivery

15. Aug. — Initial Access

19. Aug.

10. Sep.

11. Sep.

Incident Response & Digital Forensics

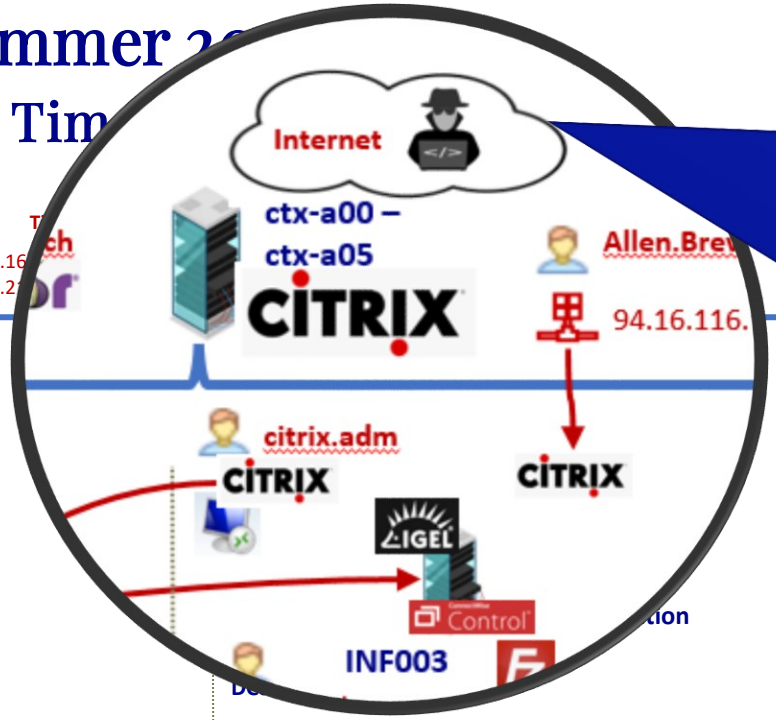
Internet cut-off

10:30

Vorfall identifiziert

Cyber-Angriff – Sommer 2
Lagebild / Visual Super Tim

Zeitzone UTC / Times in UTC



Erkennung:
- Parallele Einwahl der selben Benutzerkonten von verschiedenen Quellen
- Parallele Einwahl mehrerer Benutzerkonten von der gleichen Quelle

Prävention:
- Conditional Access
- Next-Gen-FW & Detection Rules

5.77.16.***
Allen.Brewer
Tiffany.Mach

198.16
206.2

Allen.Brew
94.16.116.

Start
23:32
CITRIX
ctx03

Ausführung
netscan
und
AnyDesk

Ausführung
AnyDesk
23:46

Privilege
Escalation

Persistence

10:59
Ausführung
mimikatz
detektiert
citrix.adm
erlangt

Erfolgreicher
Phishing-Angriff
auf:
Allen.Brewer
Tiffany.Mach

Internet
cut-off
@YET
10:30

13. Aug.
15. Aug.
19. Aug.
25. Aug.
26. Aug.
27. Aug.
28. Aug.
31. Sep.
1. Sep.
2. Sep.
3. Sep.
4. Sep.
7. Sep.
8. Sep.
9. Sep.
10. Sep.
11. Sep.

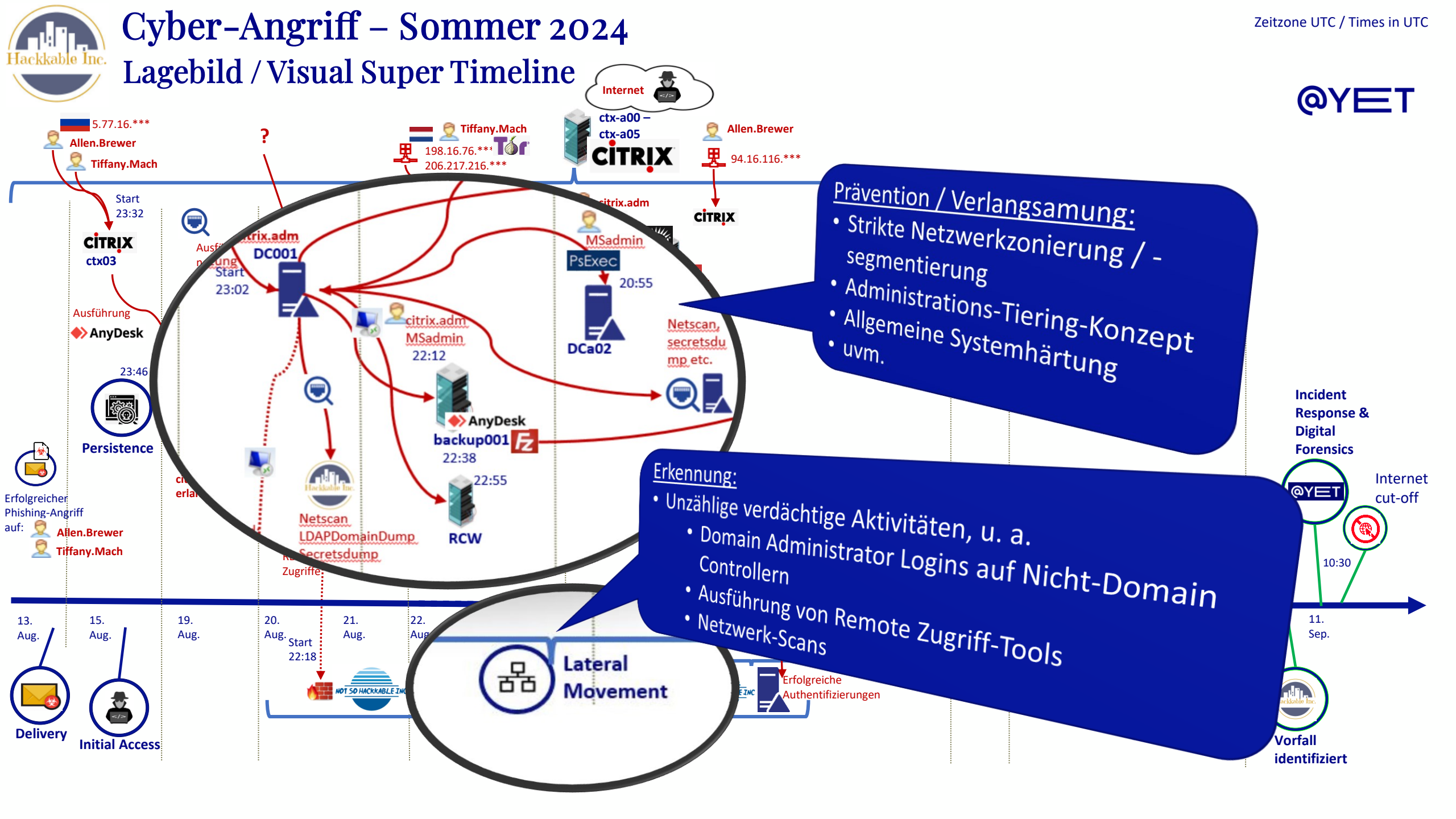
Delivery
Initial Access
Vorfall
identifiziert

Cyber-Angriff – Sommer 2024

Lagebild / Visual Super Timeline

Zeitzone UTC / Times in UTC

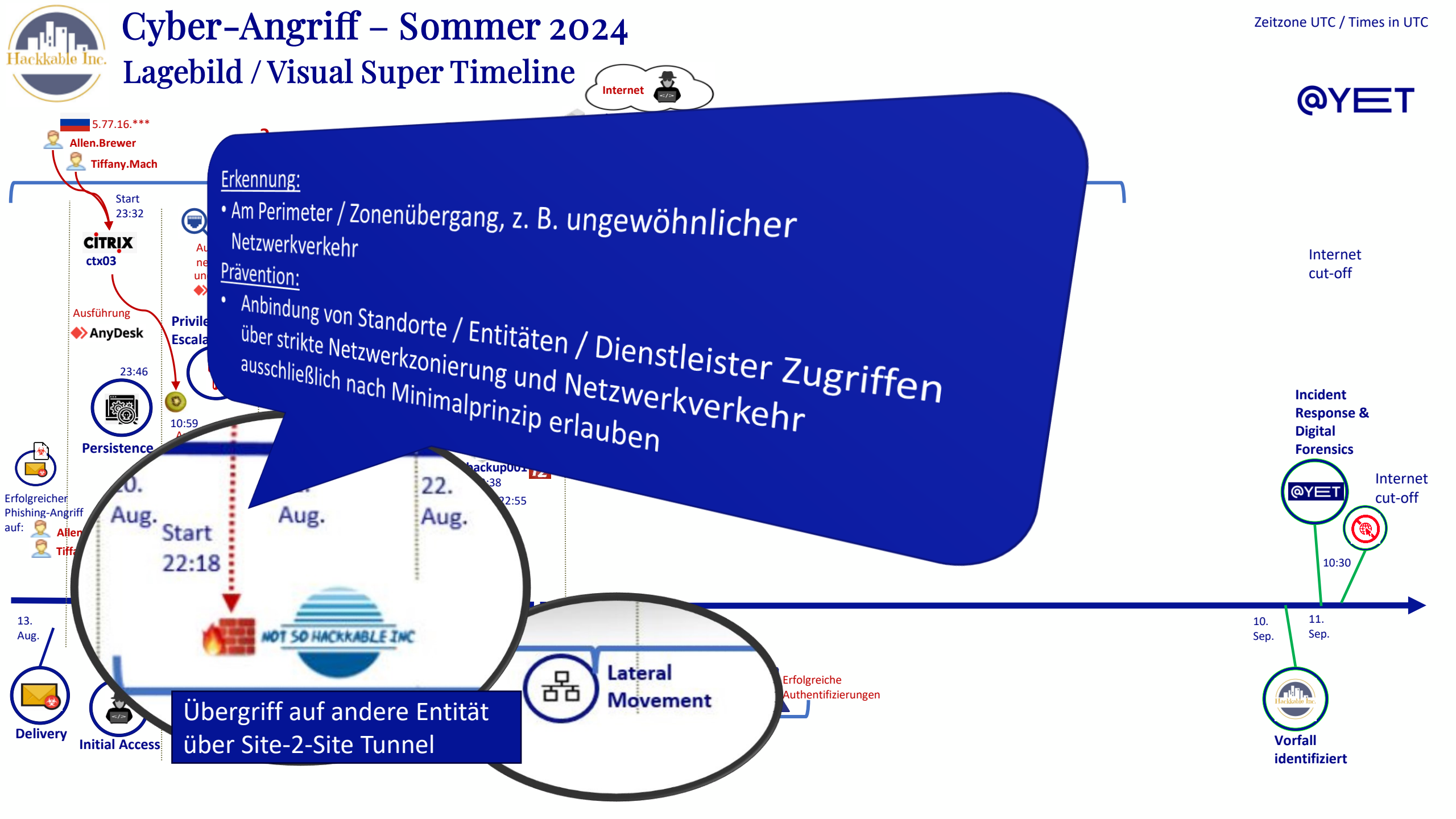
@YET



Cyber-Angriff – Sommer 2024

Lagebild / Visual Super Timeline

Zeitzone UTC / Times in UTC



Cyber-Angriff – Sommer 2024

Zeitzone UTC / Times in UTC

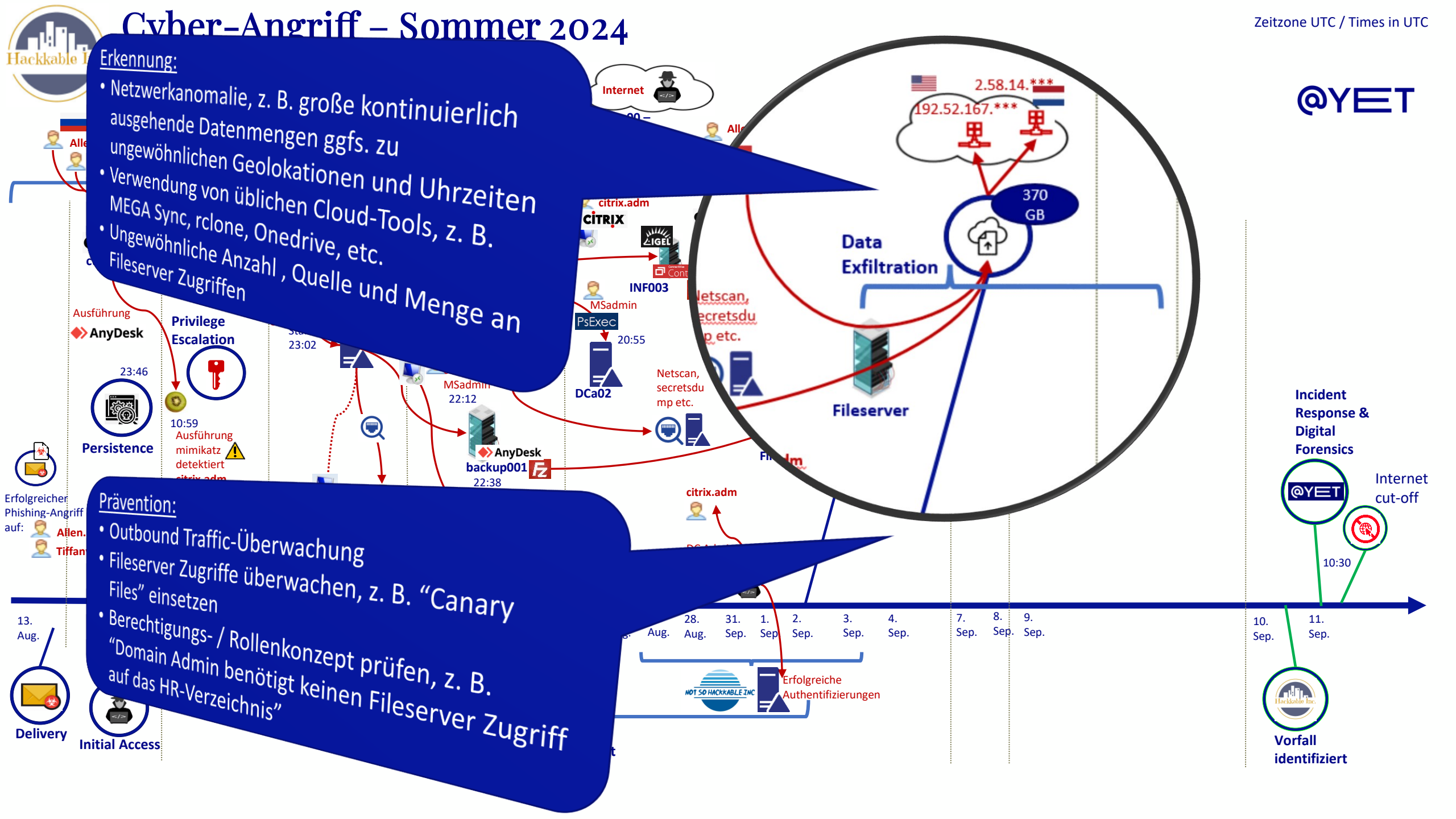
@YET

Erkennung:

- Netzwerkanomalie, z. B. große kontinuierlich ausgehende Datenmengen ggfs. zu ungewöhnlichen Geolokationen und Uhrzeiten
- Verwendung von üblichen Cloud-Tools, z. B. MEGA Sync, rclone, Onedrive, etc.
- Ungewöhnliche Anzahl , Quelle und Menge an Fileserver Zugriffen

Prävention:

- Outbound Traffic-Überwachung
- Fileserver Zugriffe überwachen, z. B. “Canary Files” einsetzen
- Berechtigungs- / Rollenkonzept prüfen, z. B. “Domain Admin benötigt keinen Fileserver Zugriff auf das HR-Verzeichnis”

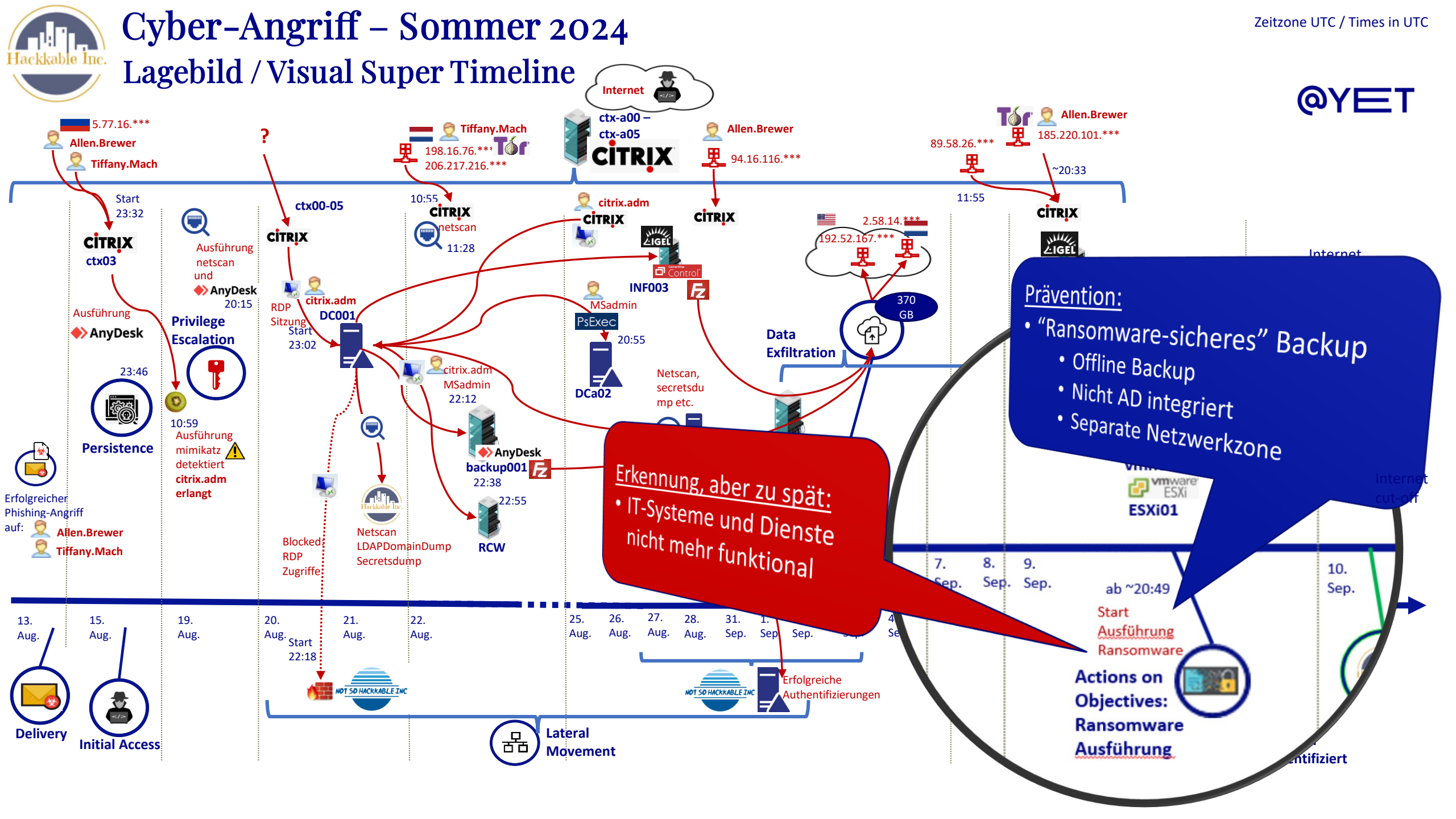


Cyber-Angriff – Sommer 2024

Lagebild / Visual Super Timeline

Zeitzone UTC / Times in UTC

@YET



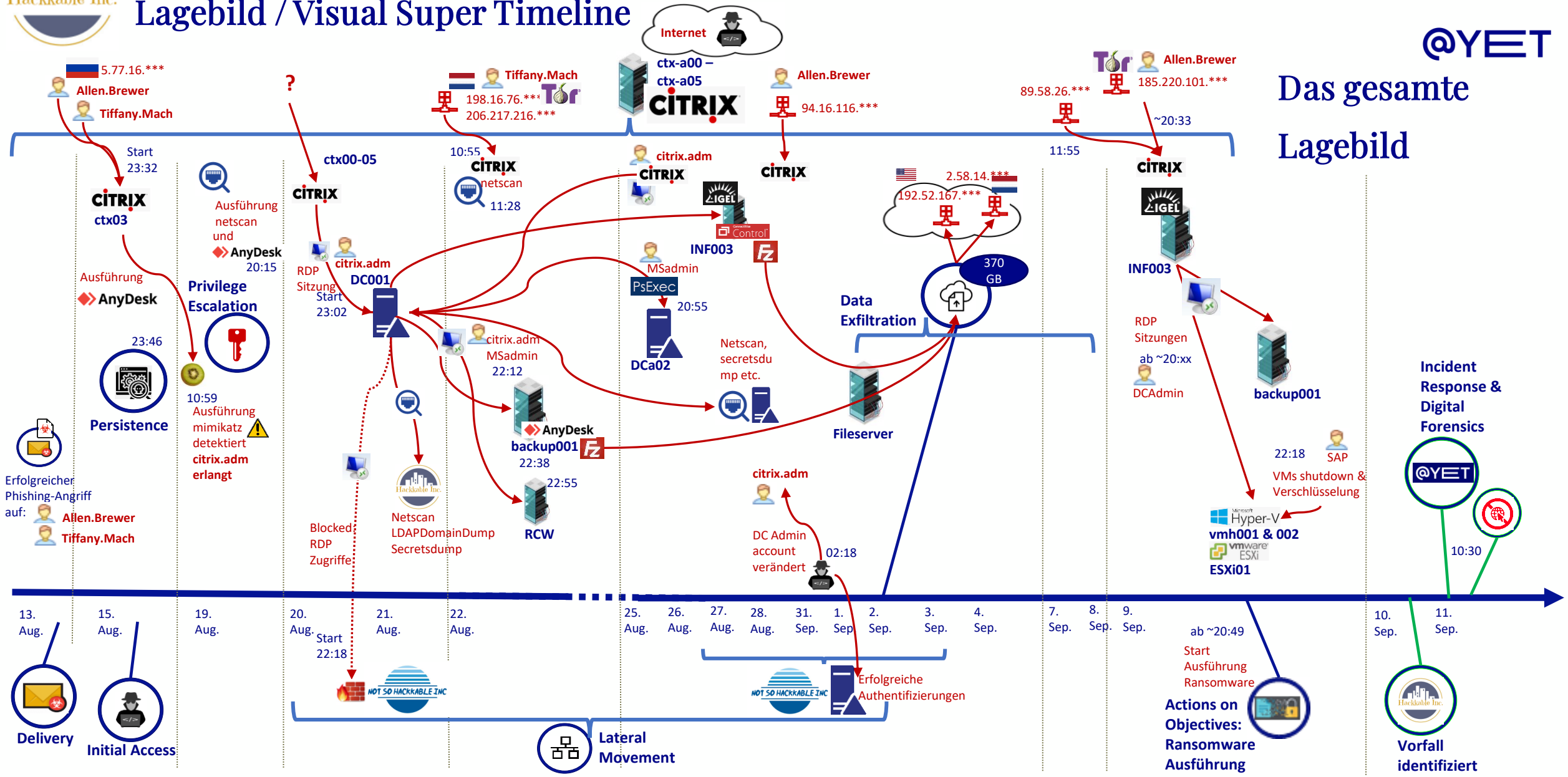
Cyber-Angriff – Sommer 2024

Lagebild / Visual Super Timeline

Zeitzone UTC / Times in UTC

@YET

Das gesamte Lagebild

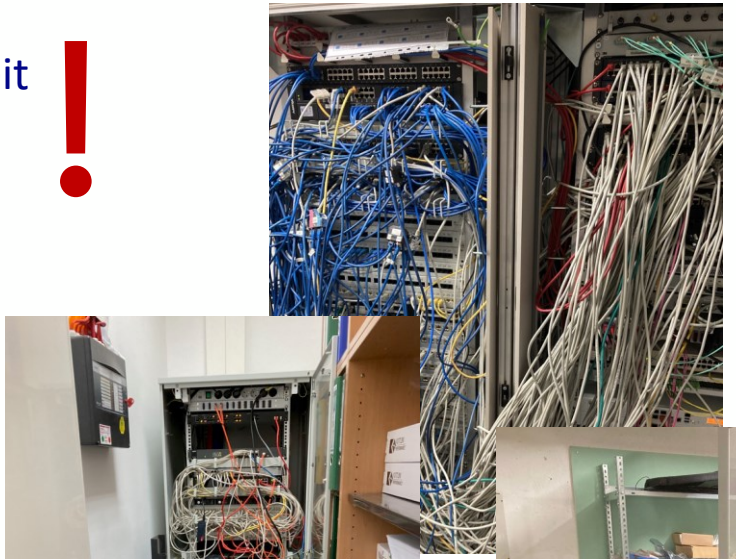


Was benötigt der DFIR Dienstleister?

@YET

Die Analysten müssen die IT-Infrastruktur und Prozesse in sehr kurzer Zeit verstehen, um ein Lagebild erstellen zu können und insgesamt die Krise angemessen zu bewältigen.

!



Quellen: @-yet Fotoarchiv

Ausgangssituation in vielen Fällen:

- Meist historisch gewachsenen IT-Strukturen
- International vernetzte Standorte und diverse Dienstleister
- Dokumentation oft nicht mehr aktuell, fehlt gänzlich oder steht nicht mehr im Zugriff
- Akuter Panikmodus und Notfall-/Krisenprozesse nicht ausgeprägt

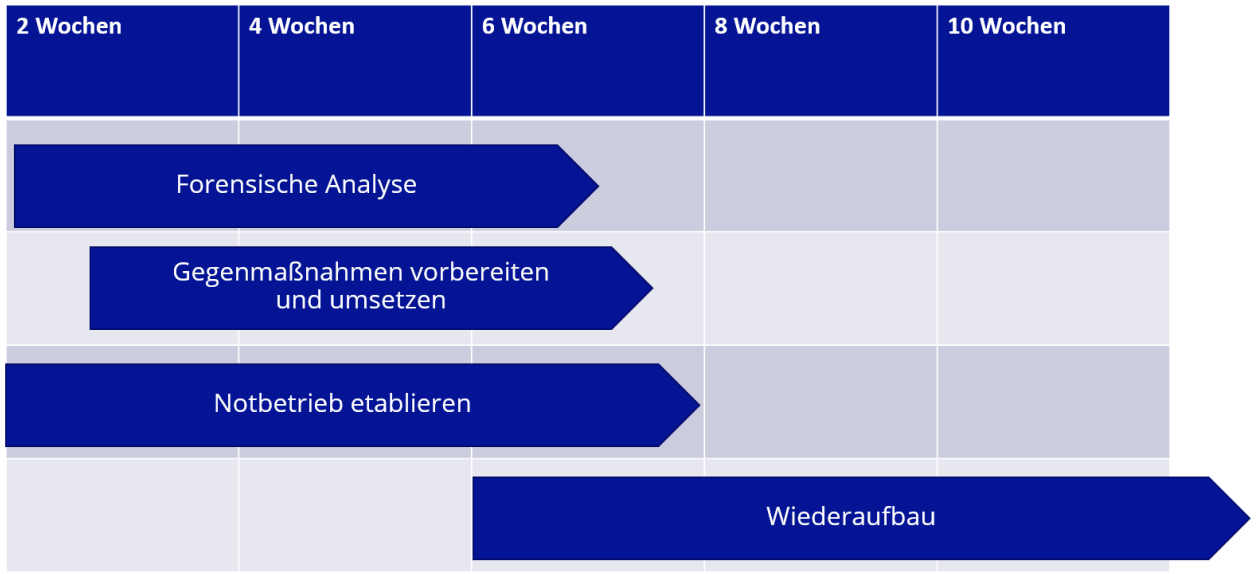
Benötigt werden:

- **Herstellung einer Analysemöglichkeit**
- **Daten**, z. B. Logs und Systemabbilder
- **Zugriffsmöglichkeiten**, um benötigte Daten selber erheben zu können
- **Informationen**, z. B. zu Abläufen, Netzwerkaufbau, etc.
- **Zugriff auf notwendige Mitarbeiter**, z. B. um Plausibilitätsfragen klären zu können und für Zulieferungen

Wie lange dauert der DFIR Einsatz?

It depends !

- **Erstaufnahme und Herstellung der Analysefähigkeit:** meist identisch: 4 h – 3 Tage
- Anfordern erster Daten im „**Triage-Verfahren**“ und erste Erkenntnisse: Stunden bis wenige Tage
- Die zu analysierenden Datenmengen können im Verlauf gigantisch werden.



Idealisierter Ablauf – Realität kann abweichen

Probleme:

- Aufwand steigt mit Größe und Komplexität der IT
- Datenbereitstellung für Unternehmen meist schwierig,
  - Notfallprozesse nicht geübt
  - Logdaten liegen nicht zentral vor
  - Logvorhaltezeiten zu gering (wenige Stunden)
  - Verantwortliche Personen nicht bekannt/greifbar
- Wiederaufbau von unzähligen Faktoren abhängig, z. B. Grad der Kompromittierung und IT-Ressourcen

Incident Response - Projektstruktur / Workstreams

Klare Schnittstellen und agile Anpassung an den konkreten Sicherheitsvorfall

@YET

Krisenstab (Koordination / Schnittstelle Stakeholder / Workstreams)

Incident Response & Digital Forensic

Erste Abwehrmaßnahmen

Tiefenanalyse
- Logdaten
- IT-Systeme

Ermittlung von
- Kompromittierungsgrad
- Lagebild
- Angriffsvektoren (innen/aussen)
- Indicators of Compromise
- Patient Zero
- Datenabfluss

- Darknet Monitoring
- Tägliche Status Updates

Krisen-Management

Kommunikation
- Extern / Medien
- Dritte
- Intern

Rechtsberatung

Strafverfolgungsbehörden / BSI

Angreiferverhandlung

Datenschutz

Cyber-Versicherer

Input

Klärung

Recovery / Support Wiederanlauf

Konzeptionelle, architekturelle und "hands-on" Unterstützung der lokalen IT u. a.
- Datenwiederherstellung
- Notbetrieb in "roter Zone"
- Secure Design neuer "grüner Zone"
- Konzeption sicherer Infrastrukturen
- Erstellung Migrationsstrategien / Road Map "rot" zu "grüner Zone"

- On demand Experts für diverse Themen, z. B. Active Directory, Netzwerk, Firewall, usw.

Threat Hunting / IOC Scanning (Systeme)

Unternehmensweite Suche nach IOCs auf IT-Systemen

Implementierung und Betrieb von Agent basierender IOC Scan-Lösung

1st-Level Analyse der Ergebnisse und Baselining sowie Unterteilung in "Cases"

Bereitstellung von vorgefilterten Ergebnissen an Kunden über dediziertes Web Portal

Bei Bedarf Rückgabe an Forensik

Scan Service (residente Daten)

Scan von ruhenden Daten (Dokumenten, E-Mails, etc.) mit mehreren Signatur/IOC basierten AV-Produkten

Implementierung und Betrieb von "Scan Stations" vor Ort

Trennung "sauberer" und schädlicher Daten als Vorbereitung für eine Migration in "grüne Zone"

Big Picture - Üblicher Ablauf bei Mittel- bis Großschadenlage

Krisenmanagment & Forensische Analyse

- Was ist passiert?
- Was ist wie betroffen (Standorte, Bereiche, Dritte) ?
- Gab es einen Datenabfluss?
- Was und wann war der „Initial Access?
- Indicators of compromise (IOCs) identifizieren
- Was ist die „Root Cause“ / Warum kann der Angreifer rein?
- Kommunikation

Notfallmaßnahmen

- Notfallmaßnahmen definieren & umsetzen
  - Ggfs. Internet Cut-off
  - Systeme isolieren
- Angreifer identifizieren / IOCs finden / Threat Hunting
- Notbetrieb planen

Notbetrieb

- Systeme säubern (AV, THOR)
- Perimeter härten (Schießscharten)
- Wichtigste Systeme isolieren und abgesichert hochfahren
- Kommunikation nach Minimalprinzip

Mischzonen

- Übergangszonen für IT-Systeme und IT-Dienste nach Risikoabschätzung, z. B. Überführung von Systemen, ohne klare Angreiferspuren, aber ohne Neuaufsetzen

Wiederaufbau / Vollständige Bereinigung

- Aufbau einer neuen, grünen Umgebung
  - Secure Infrastructure
  - Neues Active Directory
  - Server und Systeme neu aufsetzen
  - Scan der ruhenden Daten

Business Continuity: Herstellen der Geschäftsfähigkeit mit gerade noch vertretbarem Risiko in der kompromittierten Umgebung

→ Angreiferpräsenz wird in Kauf genommen !

Wann ist ein Notbetrieb notwendig?

- Längerer Geschäftsausfall ist keine Option
- Gefährdung von Partnern und Kunden ist ausgeschlossen oder sehr unwahrscheinlich
- Risiko für Datenexfiltration und große Schäden ist kalkulierbar

Idealisierte Darstellung. Ablauf ggfs. abweichend

Blöcke überschneiden sich in der Regel zeitlich

Wenige Tage bis Wochen | Mehrere Wochen | Mehrere Wochen bis Monate

Key Takeaways: Prävention

- **Backups „Ransomware-sicher“ speichern**
- Kritische und von außen erreichbare Dienste mit **Mehrfaktorauthentifizierung** (MFA) absichern
- **Vulnerability-Management und Patches einspielen** … nicht nur für Windows!
- **Systemhärtung**, mind. nach Security Best Practices
- **Netzwerk schützen und zonieren** / Perimeter-FW, segmentieren und reglementieren
- **Active Directory-Konzept und -Härtung**
  - **Tiering-Modell & Rechte / Rollen** für das Access Management
- **Logdaten zentral sammeln → SIEM/SOC**
  - Technisch: **Monitoring & Alarmierung**
  - **Organisatorische Prozesse**, um auf verdächtige Aktivitäten angemessen zu reagieren
- **Notfallplan** und regelmäßige Übungen
- **Regelmäßige Security Assessments / Audits** (Penetrationtesting, etc.)

Diese Empfehlungen erheben keinen Anspruch auf Vollständigkeit, noch stellen Sie eine Priorisierung / Reihenfolge der Maßnahmen dar.

Kontakt

@-yet GmbH

Schloss Eicherhof
42799 Leichlingen

+49 2175 16 55 0
info@at-yet.de

Kontakt

Wolfgang Straßer