
**SysAdminDay 2026: Komm, wir spielen einen Hack!**

Wie läuft eigentlich so ein echter Hacker-Angriff ab? Und was mache ich, wenn es mir passiert?

Beides gar nicht so einfach. Vielleicht sollten wir uns rechtzeitig vorher mal damit beschäftigen? In dieser Session spielen wir einen fiktiven, aber realistischen Angriff durch. An verschiedenen Stellen halten wir an und überlegen uns: Was tun wir jetzt in der Rolle des angegriffenen Unternehmens? Und wir schauen uns an: Welche Entscheidung haben echte Unternehmen an dieser Stelle getroffen, und was für Auswirkungen hatte das?

Ein Live-Hacking-Adventure zum Mitmachen.

Nils Kaczenski
*Head of Consulting, CTO ATD GmbH*
*MVP Enterprise & Platform Security*

*Bild: Unsplash.com, Jonathan Borba*

Ein Anruf auf der Mailbox:

> *Hi André, hier ist Michael.*
> *Kannst du mich mal dringend zurückrufen? Hier passiert grad irgendwas Komisches. Ich komm nicht auf unsere Systeme.*

- Reales Fallbeispiel als Hintergrund
  - High-Tech-Unternehmen, weltweit tätig, ca. 1500 Mitarbeiter:innen
  - Notbetrieb in der ersten Woche
  - Übergangsbetrieb nach einem Monat
  - Nahe am Normalbetrieb erst nach neun Monaten
- Wie ging es aus Sicht der Admins los?
  - Wir schauen uns bewusst die ersten Stunden an …
  - … denn es geht in der Frühphase nicht um Technik.
- Wir zeigen nicht mit dem Finger auf ein Unternehmen. Es steht als Beispiel für die Vermutung, dass es vielen Unternehmen so gehen würde.


Nils Kaczenski
*ATD | Systemhaus, CTO*
*MVP Enterprise & Platform Security*

N.Kaczenski@atd.de


Sonntagnacht:
Der Hack beginnt

- So, 21:24: Änderungen an zwei Admin-Accounts
- So, 21:31: VPN-Zugriff einer Mitarbeiterin OK
- So, 22:05: Daten werden ausgeleitet
- So, 23:55: Cloud-Software kann sich nicht anmelden
- Mo, 00:48: Manipulationen am Backup
- Mo, 02:04: Verschlüsselungen im VMware-Datastore
- Mo, 02:34: SSH-Zugänge aktiviert
- Mo, 02:41: Sicherheitssoftware abgeschaltet

Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)

Zunächst läuft alles unter dem Radar der Admins. Anomalien fallen niemandem auf, es gibt aber auch keinen durchgehenden IT-Betrieb.


*Bild: unsplash.com, Uladzislau Petrushkevich*

Diskussion mit dem Publikum:

- Woher wissen wir, was passiert ist?
- Wissen wir, ob das stimmt und vollständig ist? Oder sehen wir nur einen kleinen Ausschnitt?
- Was können wir mit diesem Wissen machen?
- Was könnten wir machen, wenn wir mehr wüssten?


Montag früh:
Der Admin schöpft Verdacht

- Mo, 06:03: Admin kann sich nicht anmelden
- Mo, 06:17: Admin bittet DL, sich das anzusehen
- Mo, 06:31: Externer kommt auch nicht drauf
- Mo, 06:39: Externer startet Hosts neu

Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


*Bild: unsplash.com, iSawRed*

Diskussion mit dem Publikum:

- Wann ist der Zeitpunkt, um Alarm zu schlagen?
- Wann würdest du wirklich Alarm schlagen?
- Und wie?

- Mo, 06:03: Admin kann sich nicht anmelden
- Mo, 06:17: Admin bittet DL, sich das anzusehen
- Mo, 06:31: Externer kommt auch nicht drauf
- Mo, 06:39: Externer startet Hosts neu
- Mo, 06:58: Weiter kein Admin-Zugriff
- Mo, 07:28: User-Zugriff scheitert oder ist seltsam
- Mo, 07:44: Ransomware-Nachricht entdeckt
- Mo, 07:51: …

Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)

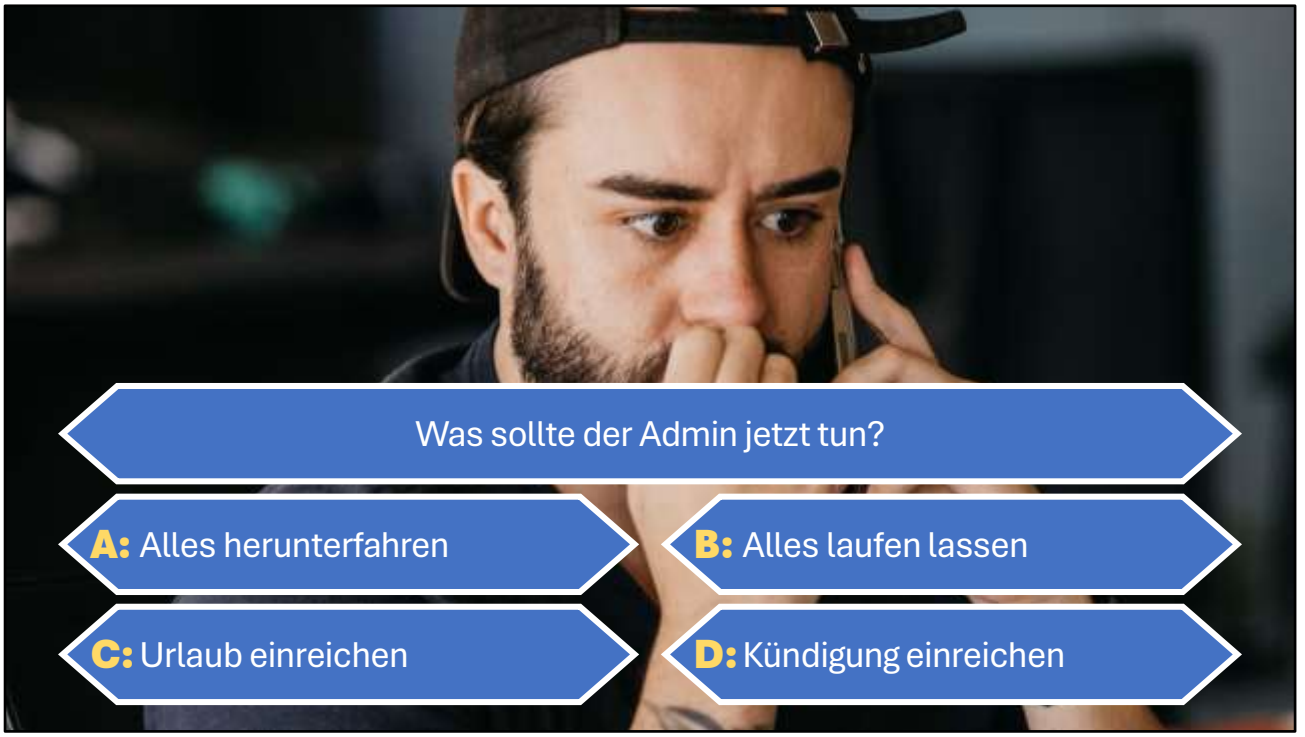



*Bild: Unsplash.com, Jonathan Borba*

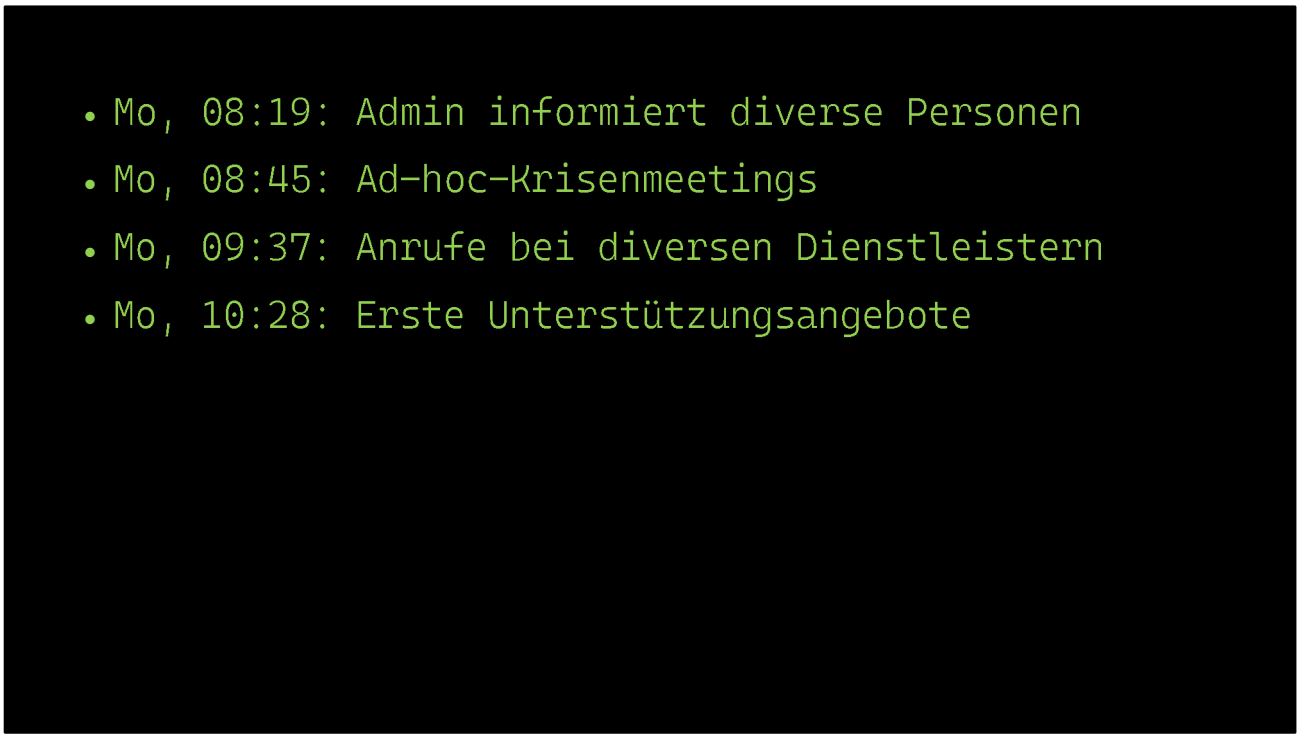
Diskussion mit dem Publikum:

- Was ist nun zu tun?
- Alles abschalten vs. alles laufen lassen

- Mo, 06:03: Admin kann sich nicht anmelden
- Mo, 06:17: Admin bittet DL, sich das anzusehen
- Mo, 06:31: Externer kommt auch nicht drauf
- Mo, 06:39: Externer startet Hosts neu
- Mo, 06:58: Weiter kein Zugriff
- Mo, 07:28: Zugriffe scheitern oder sind seltsam
- Mo, 07:44: Ransomware-Nachricht entdeckt
- Mo, 07:51: Admin fährt alles herunter

Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


Montagvormittag:
Krisensitzungen




Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


*Bild: unsplash.com, Victoriano Izquierdo*

Diskussion mit dem Publikum:

- Welchen IR-DL beauftrage ich?
- Wer hat einen laufenden Vertrag mit einem IR-DL?

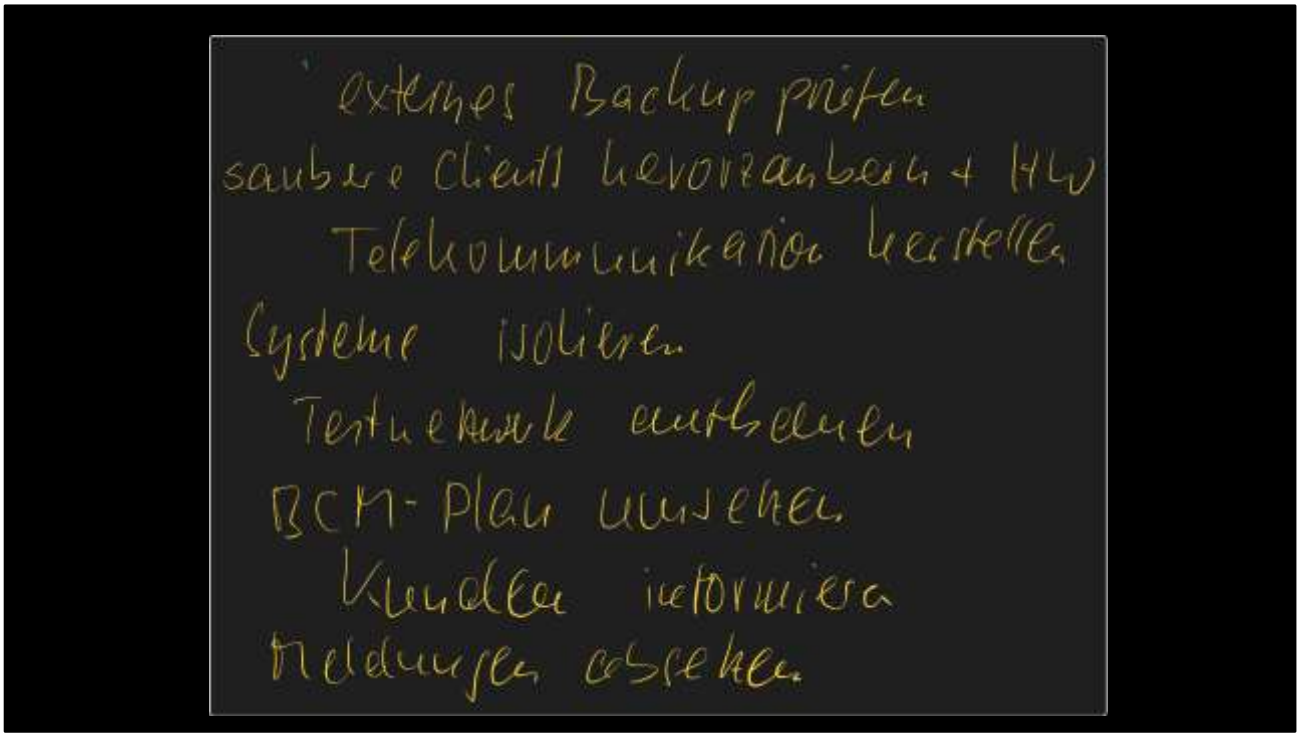
- Mo, 08:19: Admin informiert diverse Personen
- Mo, 08:45: Ad-hoc-Krisenmeetings
- Mo, 09:37: Anrufe bei diversen Dienstleistern
- Mo, 10:28: Erste Unterstützungsangebote
- Mo, 12:38: Vorstand: IR-Team der Versicherung
- Mo, 13:04: Workarounds mit privaten Accounts
- Mo, 13:34: Teile der Produktion nicht betroffen
- Mo, 14:41: Ad-hoc-Notbetrieb beginnt

Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


*Bild: unsplash.com, Huzaifa Ginwala*

Diskussion mit dem Publikum:

- Was gehört bei euch zum Ad-hoc-Notbetrieb?
- Was davon habt ihr wirklich geregelt und vorbereitet?




Diskussion mit dem Publikum:

- Was gehört bei euch zum Ad-hoc-Notbetrieb?
- Was davon habt ihr wirklich geregelt und vorbereitet?


Woran in der IT noch niemand gedacht hat:
Wie kommuniziert man das eigentlich?


Das Business braucht auch intern eine Weile, um das Ausmaß der Krise zu begreifen.


Montagnachmittag:
Das IR-Team beginnt

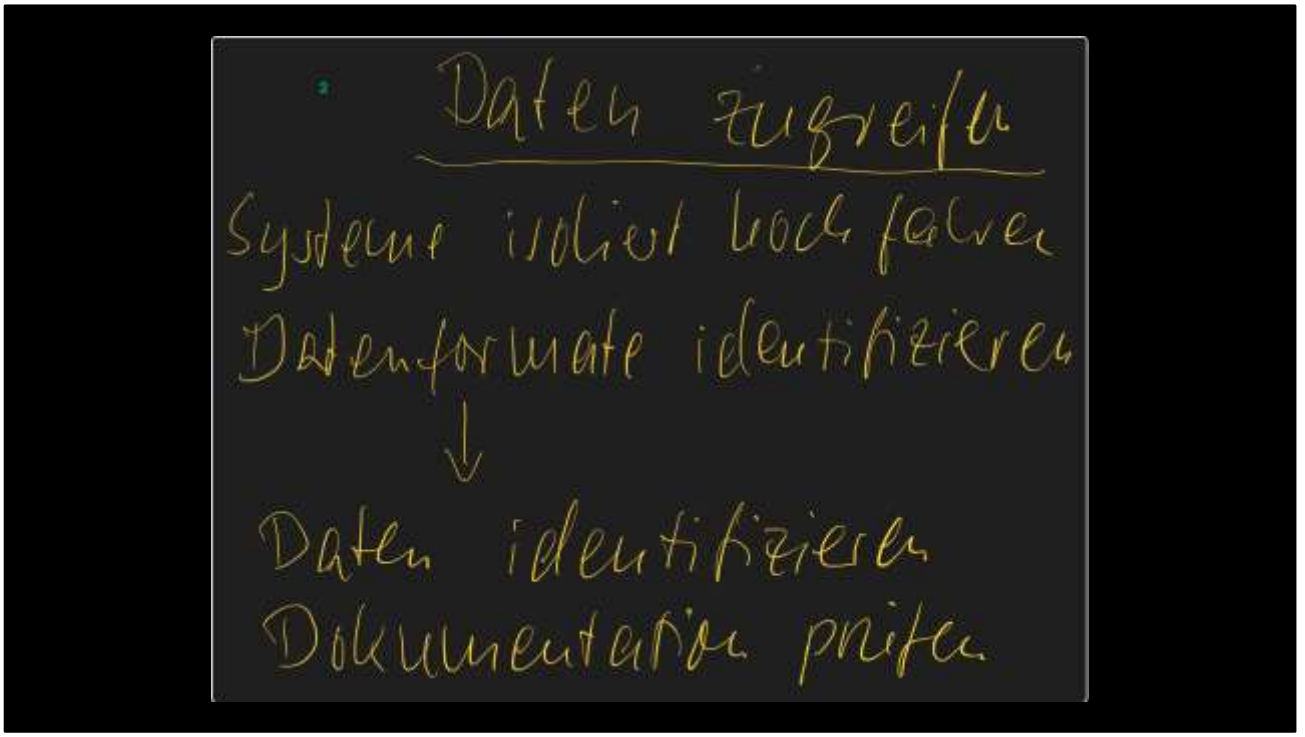
- Mo, 15:24: IR-Team fordert Daten an
- Mo, 16:31: einige Daten können geschickt werden
- Mo, 17:05: … andere nicht
- Mo, 17:55: IR-Team will Systeme starten
- Mo, 18:08: Admins und Externe weigern sich

Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


*Bild: unsplash.com, Laurel and Michael Evans*

Diskussion mit dem Publikum:

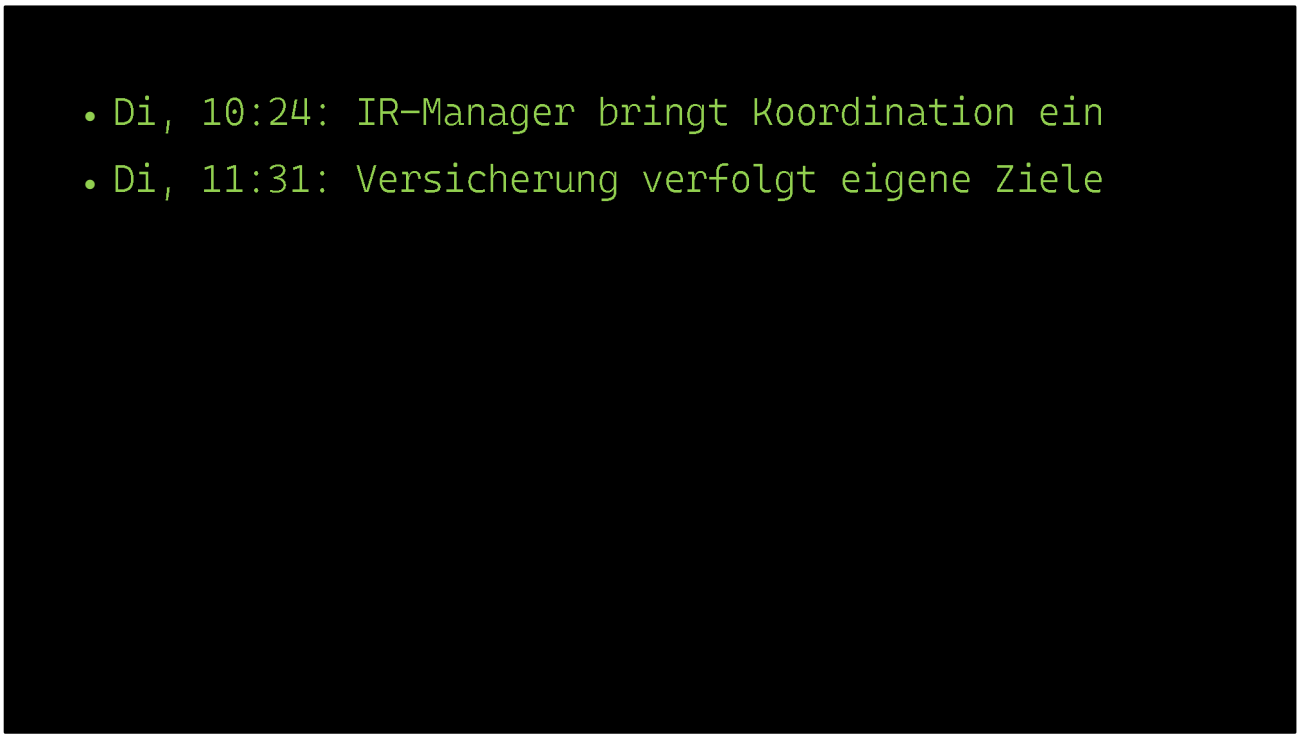
- Was mache ich, um Daten von einem System zu kriegen?
- Wie identifiziere ich überhaupt, welche Daten wichtig und integer sind?




Diskussion mit dem Publikum:

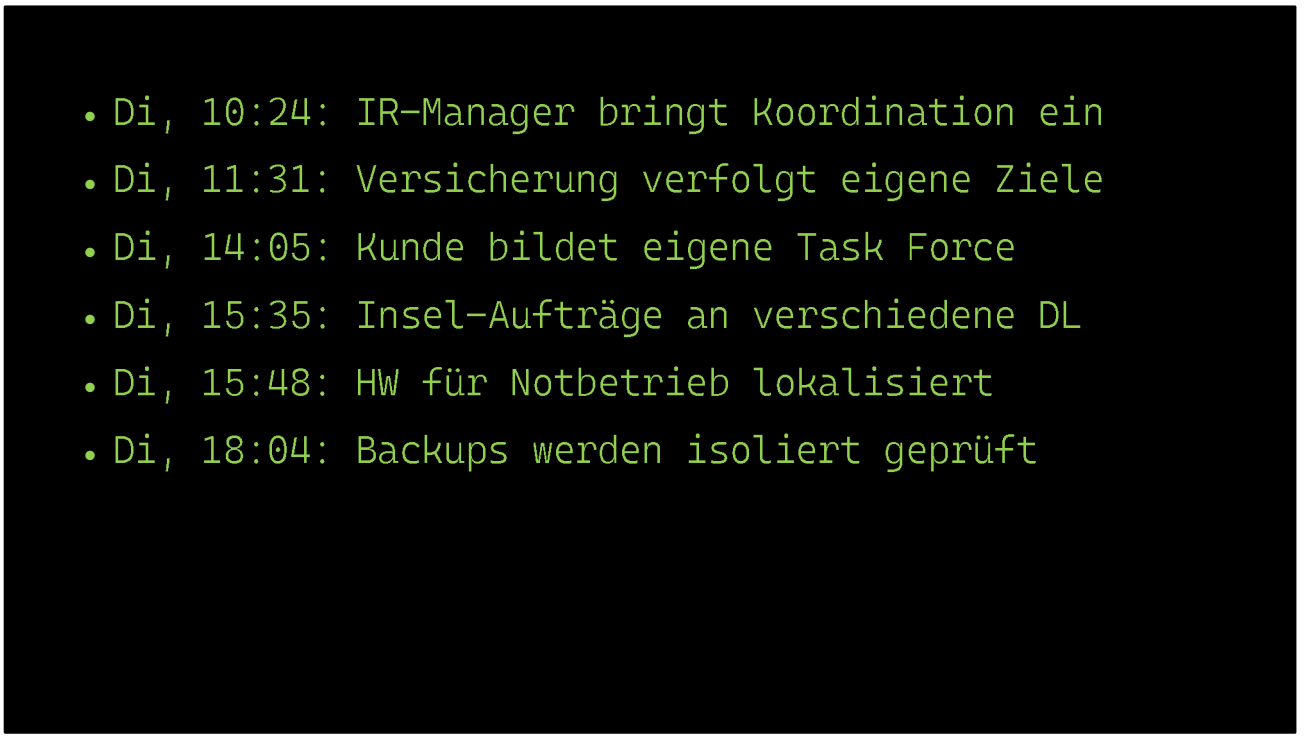
- Was mache ich, um Daten von einem System zu kriegen?
- Wie identifiziere ich überhaupt, welche Daten wichtig und integer sind?

# Dienstagvormittag:
# IR-Team mit Führung




Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


Plötzlich haben das Business und das Management andere Dinge zu tun



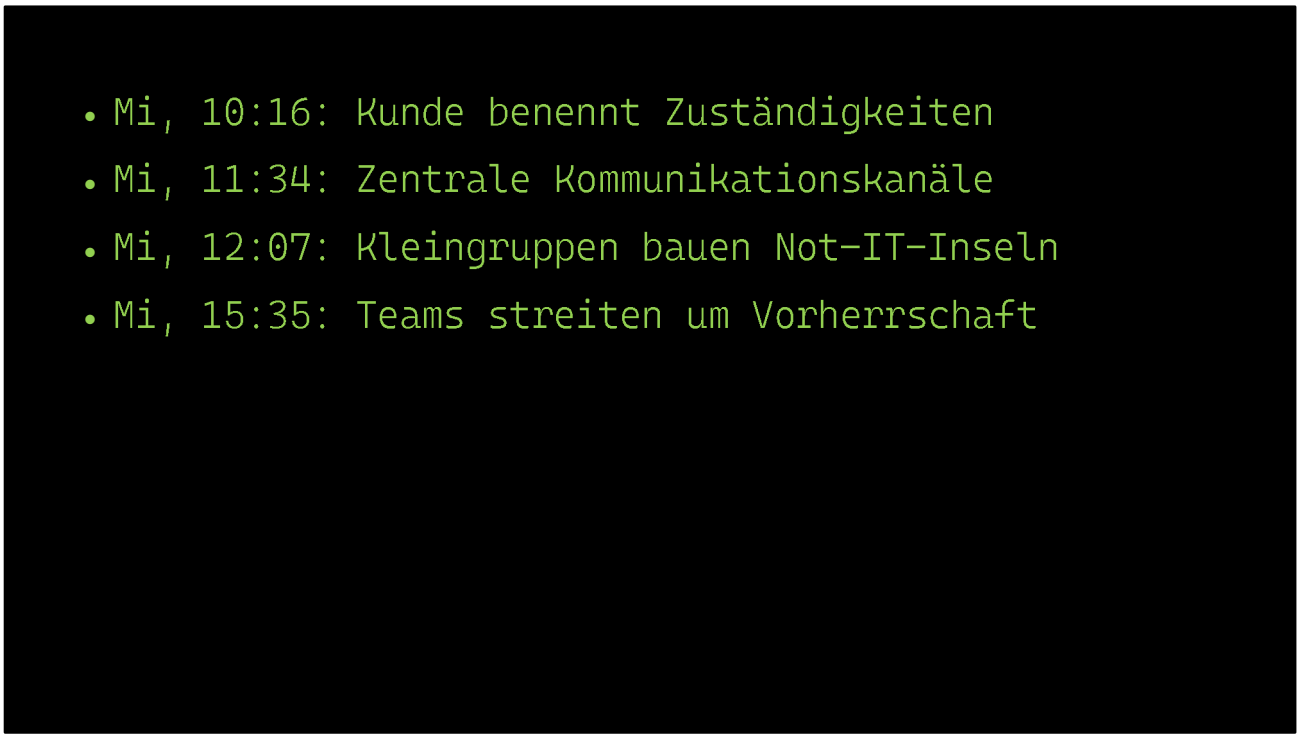

Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


EREIGNIS-FACH
EREIGNISKARTE
Spekulationen und Fake News
verbreiten sich in Social Media.

- Di, 10:24: IR-Manager bringt Koordination ein
- Di, 11:31: Versicherung verfolgt eigene Ziele
- Di, 14:05: Kunde bildet eigene Task Force
- Di, 15:35: Insel-Aufträge an verschiedene DL
- Di, 15:48: HW für Notbetrieb lokalisiert
- Di, 18:04: Backups werden isoliert geprüft
- Di, 18:34: Anforderungen gehen hin und her
- Di, 19:41: Mitarbeiter entscheiden selbst

Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


Mittwoch:
Kunde baut Strukturen




Ablauf eines echten Angriffs: Auszug aus den Log-Dateien einer Umgebung, die gerade gehackt wird (vereinfacht)


*Bild: Unsplash.com, Santiago Lacarta*

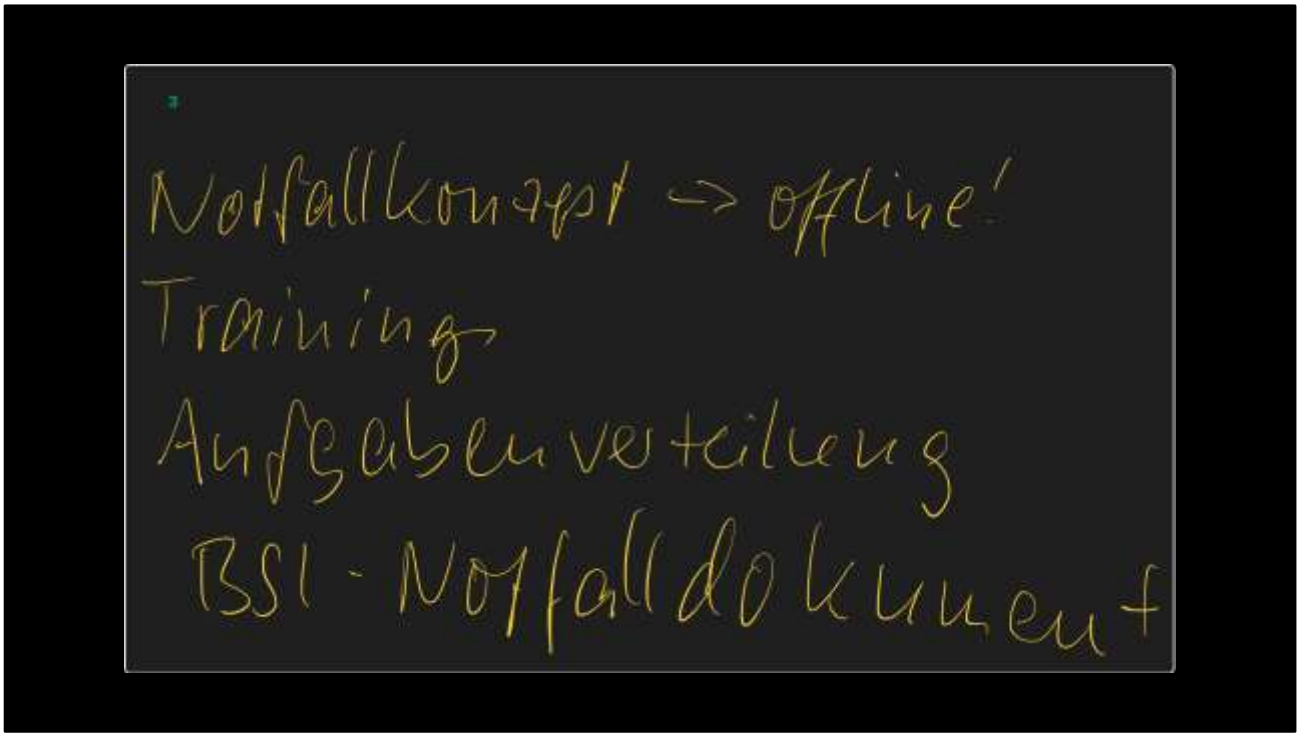
Diskussion mit dem Publikum:

- Wie lege ich die richtigen Prioritäten fest?
- Wie vermeide ich interne Grabenkämpfe?
- Wie beende ich Kompetenz- und Dienstleister-Gerangel?


*Bild: Dimitri Iakymuk, Unsplash.com*

Diskussion mit dem Publikum:

- Was hilft?
- Fragen & Antworten


Notfallkonzept -> offline!
Training
Aufgabenverteilung
BSI - Notfalldokument

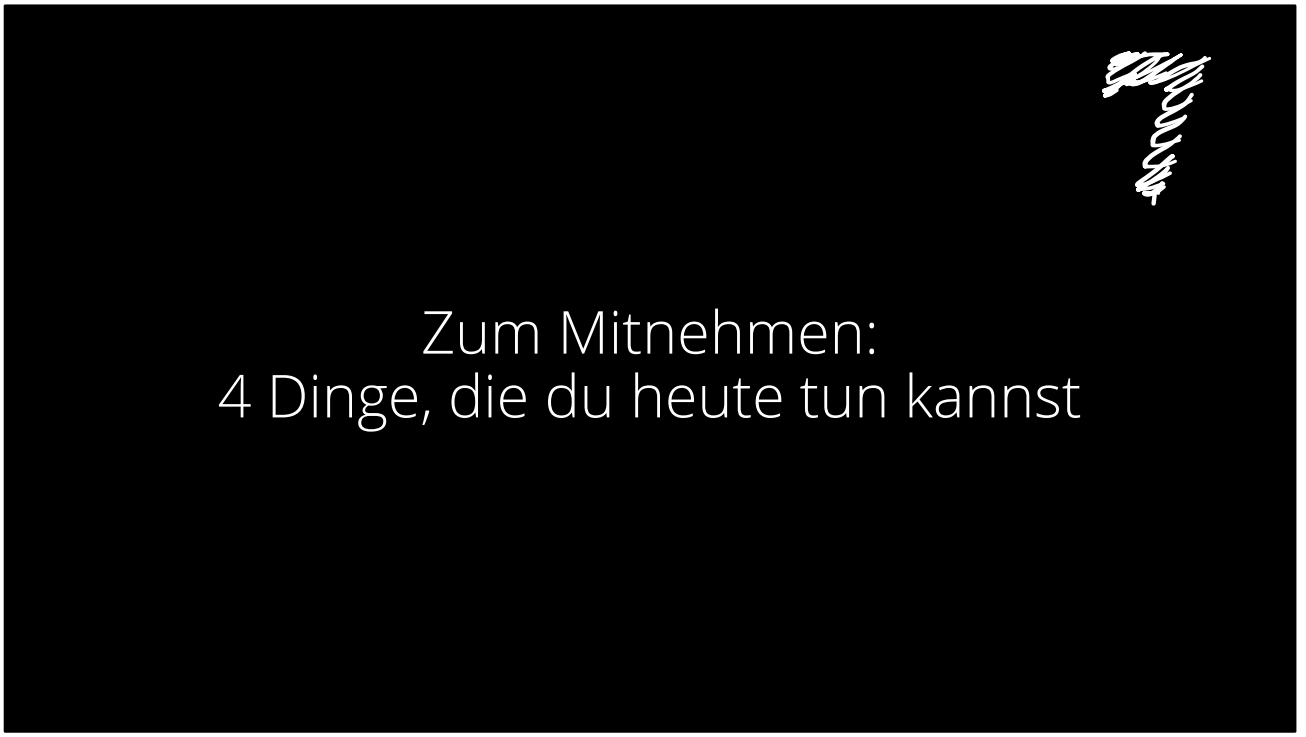

7
Zum Mitnehmen:
4 Dinge, die du heute tun kannst


*Bild: Chris Linnett, Unsplash.com*

4 einfache Dinge für sofort (und ab sofort):

- Backup prüfen
- Malware-Schutz prüfen
- Notfall-Isolierung statt Notfall-Shutdown festlegen
- Digitale Ersthelfer ausbilden


https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Digitaler_Ersthelfer/Onlinekurs/Onlinekurs_node.html

5 Anhang

## 5.3 Checkliste: Verhaltensregeln nach einem IT-Sicherheitsvorfall

Um den Schaden von IT-Sicherheitsvorfällen möglichst auf ein Minimum zu reduzieren oder auch die eine weitere Ausbreitung weitestgehend zu verhindern, ist das korrekte Verhalten nach dem Auftreten von essenzieller Bedeutung.

| Allgemeine Verhaltensregeln |
| --- |
| Ruhe bewahren und nicht in Panik geraten. |
| Weitere Arbeiten mit bzw. an dem IT-System einstellen. |
| Das betroffenen IT-System vom Netzwerk isolieren. |
| Alle bisher durchgeführten Schritte und Unregelmäßigkeiten dokumentieren, sowie Beobachtungen ggf. in Form von Screenshots festhalten. |
| Keine weiteren Maßnahmen eigenständig umsetzen, um das Problem zu behaben. |
| Handelt es sich um eine IT-Störung, die nicht behoben werden kann, ist der Kontakt zu dem entsprechenden IT-Support aufzunehmen. |
| Handelt es sich um einen IT-Sicherheitsvorfall, der nicht behoben werden kann, ist der Kontakt zu einem Vorfall-Experten aufzunehmen. |
| Weitere Maßnahmen erst nach Rücksprache mit dem entsprechenden IT-Support oder einem Vorfall-Experten einleiten bzw. umsetzen. |

*Tabelle 5: Checkliste - Verhaltensregeln nach einem IT-Sicherheitsvorfall*

Aus den Unterlagen für die Digitalen Ersthelfer (BSI).


Nils Kaczenski
*ATD | Systemhaus, Head of Consulting, CTO*
*MVP Enterprise & Platform Security*

N.Kaczenski@atd.de