HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS

(Lessons Learned aus dem) Cyber-Angriff auf die Hochschule Hannover

HIS-HE Forum „Krisenmanagement nach Cyber-Angriffen an Hochschulen“
Hannover, 20./21.06.2024

Aufbau

I. Hochschule Hannover in Zahlen

II. Anatomie des Cyber-Angriffs auf die Hochschule Hannover (HsH)

III. Umgang, Auswirkungen und Herausforderungen

IV. Der Weg zum Stabilen Notbetrieb

V. Lessons Learned

VI. Ausblick / Persönliches Fazit

Daten & Fakten

5

Fakultäten

> 60

Studienangebote

5

Standorte

> 9.000

Studierende

≈253

*Professor*innen*

≈460

Lehrbeauftragte

≈640

*Mitarbeiter*innen*

Anatomie des Cyber-Angriffs auf die HsH

Oktober/November 2023

Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag	Sonntag
23	24	25	26	27 abends: Zugang über VPN-Zugang eines Kontos	28 Rechte eines Domain Admin verschafft	29 abends: Start Verschlüsselung des DC
30 Angriff entdeckt, Abschalten der Server	31 Reformationstag	1	2	3	4	5
6	7	8	9	10	11	12

ERKENNTNISSE

Attacker
Ransom Attacke der Gruppe RTM-Locker

Art des Angriffs
Verschlüsselung des DC, keine sich weiter verbreitende Malware

Datenabfluss
Sehr wahrscheinlich, aber nur in geringem Maße

How To Restore Your Files.txt - Notepad

File Edit View

```
How To Restore Your Files

Your personal ID: 9AB-EC6-523-0D9-F3B2
!!! Your network is infected by the RTM Locker command!!!
All your documents, photos, reports, customer and employee data, databases and other important files
are encrypted and you cannot decrypt them yourself. They are also on our servers! But don't worry,
we will help you recover all your files!
The only way to recover your files is to buy our dedicated software. Only we can provide you with
this software, and only we can recover your files!
You can contact us by downloading and installing the TOR browser
(https://www.torproject.org/download/languages/)
We value our reputation. If we do not fulfill our work and obligations, no one will pay us. It's not
in our interest.
All of our decryption software is perfectly tested and will decrypt your data. We will also provide
support in case of problems.
================================================ ================================================

Login link:
http://nvfutdbq3ubteaxj4m2jyihov5aa4akfudsj5h7vhyrvfarfra26ksyd.onion/1D85262A4B3F59090972E7EE7804FC
641E9CBB6D65E5F4B376DF37D6180CD1/connect
For authorization you need to enter your ID.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Warning!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
If you do not contact the support team within 48 hours, your data will be published in the public
domain, and data compromising you will be sent to your competitors, as well as to the relevant
regulatory authorities.


================================================ ================================================

DO NOT ATTEMPT TO RECOVER THE FILES YOURSELF!
DO NOT MODIFY ENCRYPTED FILES!
OTHERWISE YOU MAY LOSE ALL YOUR FILES FOREVER!
```

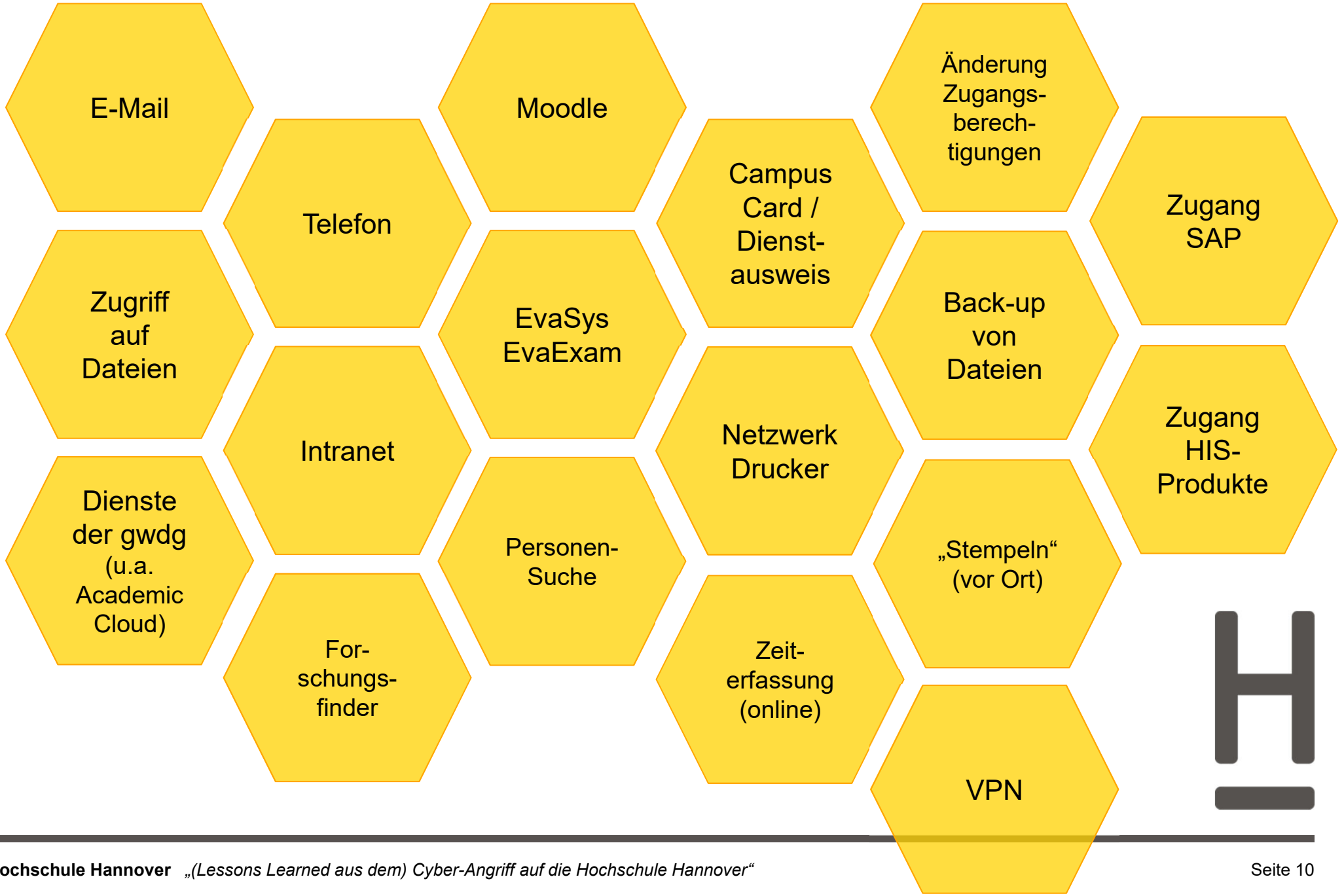
Ln 23, Col 48 | 100% | Windows (CRLF) | UTF-8

Umgang mit dem Cyber-Angriff (1)

- binnen weniger Stunden (alle) Server der Hochschule vom Netz getrennt und abgeschaltet
- Meldung Polizei und Verfassungsschutz
- Meldung Niedersächsisches Ministerium für Wissenschaft und Kultur (MWK)
- (Vorbereitung) Meldung Datenschutz
- Alternative Kommunikationswege aufbauen, denn:

  → **die meisten Systeme und Kommunikationswege waren durch das Abschalten der Server nicht mehr verfügbar**

Auswirkungen: Nicht mehr möglich waren zunächst

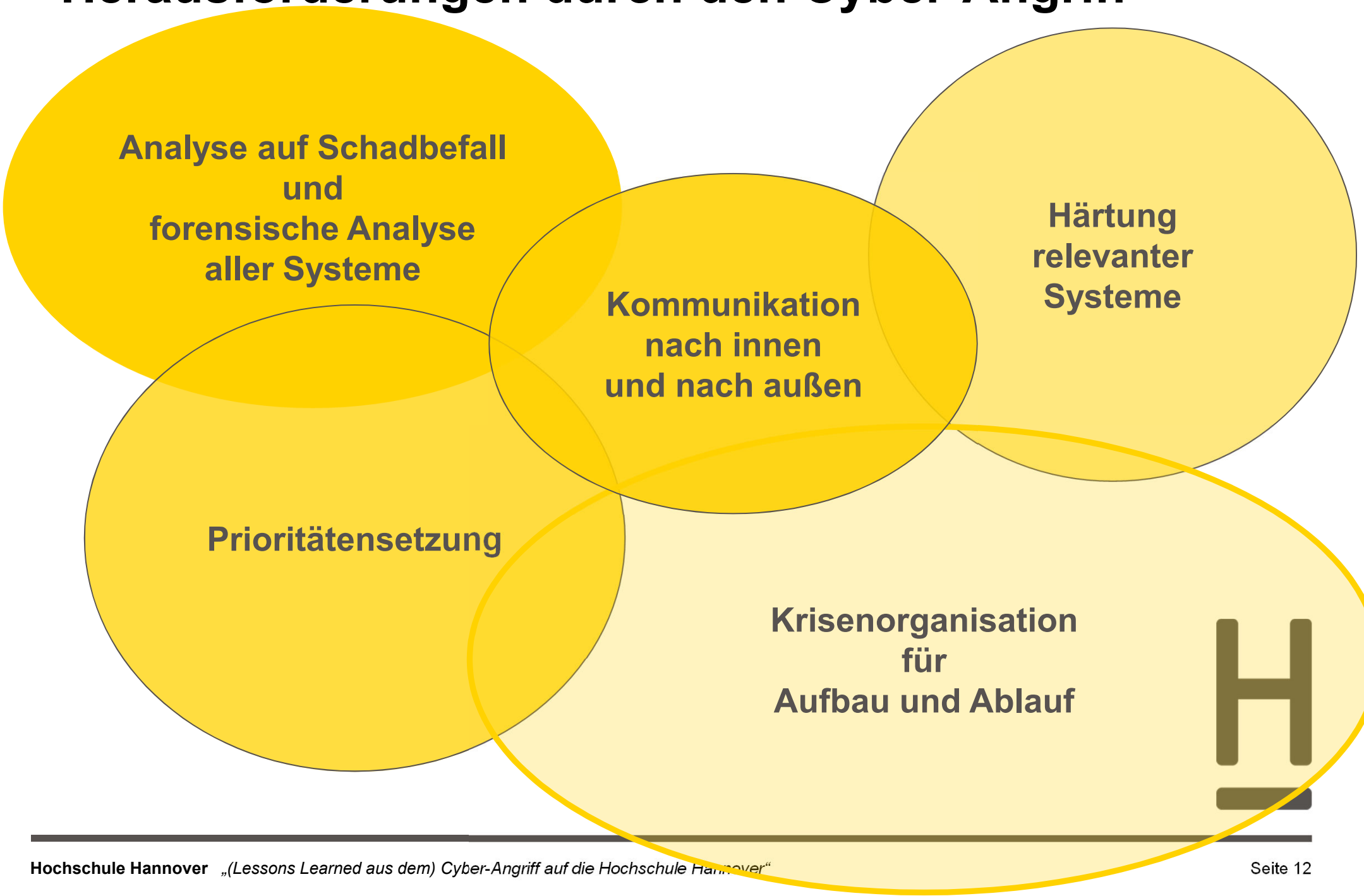


Auswirkungen -2-

- SAP und HIS-Produkte selbst nicht betroffen, nur der Zugang
- was hat noch funktioniert?
  - ✓ Webseiten der HsH (mit Einschränkungen)
  - ✓ Strom und Klimaanlagen
  - ✓ Zugang zu den Gebäuden und den einzelnen Büros
  - ✓ WLAN inkl. eduroam (mit Einschränkungen)
  - ✓ Zugriff auf die Rechner mit lokalem Profil
  - ✓ Teams (in der Lehre und in einigen wenigen Verwaltungsgruppen genutzt)
  - ✓ Zoom (und andere Internet-basierte Dienste mit unabhängiger Authentisierung)

Wiederherstellung von Kommunikationswegen und Erreichbarkeit als zentrale erste Schritte

Herausforderungen durch den Cyber-Angriff

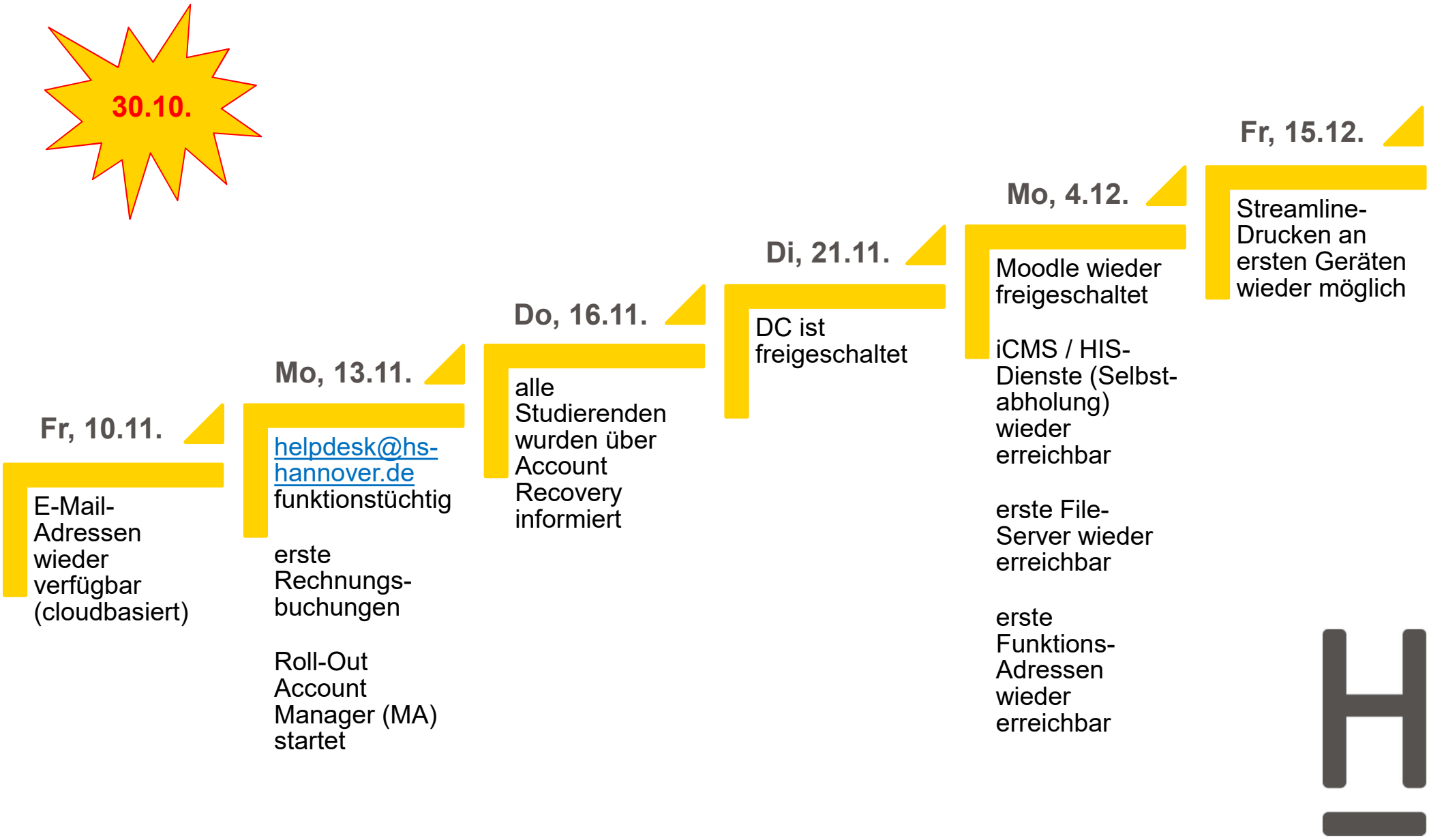


Umgang mit dem Cyber-Angriff (2)

- Einrichtung eines Krisenstabs (strategisch)
  - Präsidium
  - Leitung Kommunikation und Marketing
  - Externe Kollegen
- Einrichtung eines Krisenstabs (operativ)
  - Unterstützung über den LANIT:
    4 Kollegen aus unterschiedlichen Hochschulen / Wissenschaftseinrichtungen mit Fachexpertise, Erfahrungswissen und Projektmanagement-Skills
  - Mitarbeiterin aus der Personal- und Organisationsentwicklung der HsH
  - Aufbau Helpdesk@ mit Kolleg*innen aus der HsH

➔ **Erreichen eines stabilen Notbetriebs zum Jahresende**

Der Weg zum stabilen Notbetrieb



Der Weg zum neuen „Normalbetrieb“ 2024

Mitte Januar

Erste Nach-erfassung (Nov/Dez) der Zeiterfassung möglich

Intranet wieder verfügbar (im Hochschulnetz)

Ende Januar

VPN (ohne MFA) verfügbar, aber kein Zugriff auf Netz-Laufwerke

Academic Cloud und damit verbundene Services nutzbar

Lizenserver wieder verfügbar

Februar

Erste Schulungen MS365 (Teams, Outlook, OneDrive)

„Rückschlag“ bei den Home-laufwerken mit Datenverlust bei einigen Bediensteten

Skype for Business aus dem Netz der HsH möglich

Verteiler eingerichtet

März

Start #Itdoesmatter zur Zukunft der IT an der HsH

April

EvaSys und EvaExam wieder verfügbar (mit Ein-schränkungen)

Zweiter Anlauf zur Wiederher-stellung der Homelaufwerke erfolgfreich

Mai

Online-Zeiterfassung wieder möglich

Lessons Learned – Kommunikation

- Notfall-Webseite, die schnell hochgefahren werden kann
- Alternative Kommunikationskanäle (zu E-Mail) vorbereiten, insbesondere für „Massenkommunikation ohne Verteiler“
- Zentrale „Anlaufstelle“ (helpdesk@ o.ä.)
- Notwendige Übersetzungsleistungen
  - IT -> Anwender*innen:
    technisch -> praktisch und vollständig
    (auch: was wurde von IT nicht gesagt)
  - ins Englische (oder andere Sprachen)
- Kommunikation zu externen Partnern / Partnerorganisationen (der Organisation / einzelner Projekte)

➔ **Abhängigkeiten von Art und Zeitpunkt des Angriffs**

Lessons Learned – Organisation gesamt (1)

- Notfallhandbuch und Struktur für ein Krisenmanagement
  - Wer macht was? Wer darf was?
  - kann sofort greifen
  - inkl. Verbündete andere HS
- „Kopf-Monopole“ beseitigen

- Kernprozesse sollten priorisiert sein – in Abhängigkeit von Art und Zeitpunkt des Angriffs
  - Alternativen für unverzichtbare Kernprozesse vorhalten
  - Vorteil, wenn manche Dienste extern betrieben werden [HsH: SAP, Gehaltsabrechnungen, HIS]

- User-Awareness regelmäßig schärfen
- MFA für zentrale Dienste, ebenso hohe Passwortanforderungen

Lessons Learned – Organisation gesamt (2)

- Resilienz der einzelnen Bereiche sehr unterschiedlich
  - viele sehr erfinderisch und leistungsfähig
  - einige wenige sind wie gelähmt

- Belastung durch den Cyber-Angriff ebenfalls sehr unterschiedlich:
  - Wie bekomme ich das rechtzeitig mit?
  - Welche Unterstützung kann ich ggf. anbieten? (aufgabenbezogen für OE, Gesunderhaltung individuell)

- Risiken abwägen und eingehen
  - völlige Risikofreiheit gibt es nicht, egal, was ich tue

Lessons Learned – IT-Organisation & IT-Architektur

Für die IT-Organisation

- Notfallhandbuch
- Umgang mit Intrusion Detection und Intrusion Prevention prüfen und aufbauen (falls nicht ausreichend vorhanden)
- Abhängigkeiten zwischen verschiedenen Diensten klären und berücksichtigen

Für die IT-Architektur

- Klarheit über die IT-Struktur zentral / dezentral (dokumentiert)
- Vor- und Nachteile einer verteilten IT-Architektur analysieren und entsprechend umsetzen
- Redundanzen systematisch und gezielt aufbauen

Lessons Learned – Niedersachsen

- Zusammenarbeit und Abrufbarkeit von Kolleg*innen innerhalb des LANIT ein großes Plus, kann und soll aber noch besser strukturiert werden
- Hochschule.digital Niedersachsen https://hochschuledigital-niedersachsen.de
  - Verbundprojekt „Sicherung der Resilienz“ zur Stärkung der IT-Sicherheit der niedersächsischen Hochschulen (Volumen: 10 Mio. €)
  - Gemeinsame(r) IT-Strategie(prozess) der niedersächsischen Hochschulen
  - sinnvolle landesweit oder länderübergreifend IT-Strukturen und Services entwickeln

Ausblick / persönliches Fazit

Gemeinsam sind wir stärker.

Es hätte noch viel schlimmer kommen können.

Man kann sich nicht auf jedes Szenario vorbereiten.

Nach dem Cyber-Angriff ist vor dem Cyber-Angriff.

Auf eine Cyber-Attacke vorbereitet zu sein, ist eine Daueraufgabe für die Organisation!

Vielen Dank.

Rückmeldungen und Fragen gerne an

Josef von Helden, Präsident der HsH
(praesident@hs-hannover.de)
oder
Isabel Kassel, Personal- und Organisationsentwicklung
(isabel.kassel@hs-hannover.de)