RUB

RUHR-UNIVERSITÄT BOCHUM

Cyberangriff auf die Ruhr-Universität

IT.SERVICES

Haiko te Neues

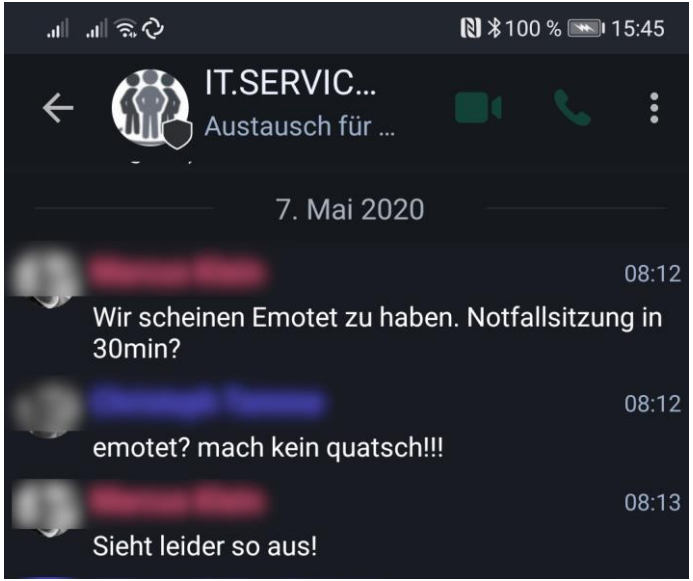
DFN Nutzergruppe Hochschulverwaltung 04.05.2021

Agenda

- Ablauf und Auswirkungen
- Wiederaufbau und Notbetrieb
- Kommunikation und Information
- Lessons Learned

Situation

- Corona Lockdown seit dem 16.03
- Alle im Homeoffice
- Ausrichtung und Arbeitsschwerpunkt:
  - Digitalisierung und Homeoffice ermöglichen



- Sofortmaßnahme: Windows Systeme runterfahren
- Krisensitzung im Leitungskreis gegen 9:00 Uhr
- Analysebeginn mit externen Spezialisten ab 11:00 Uhr

Prozess der Analyse

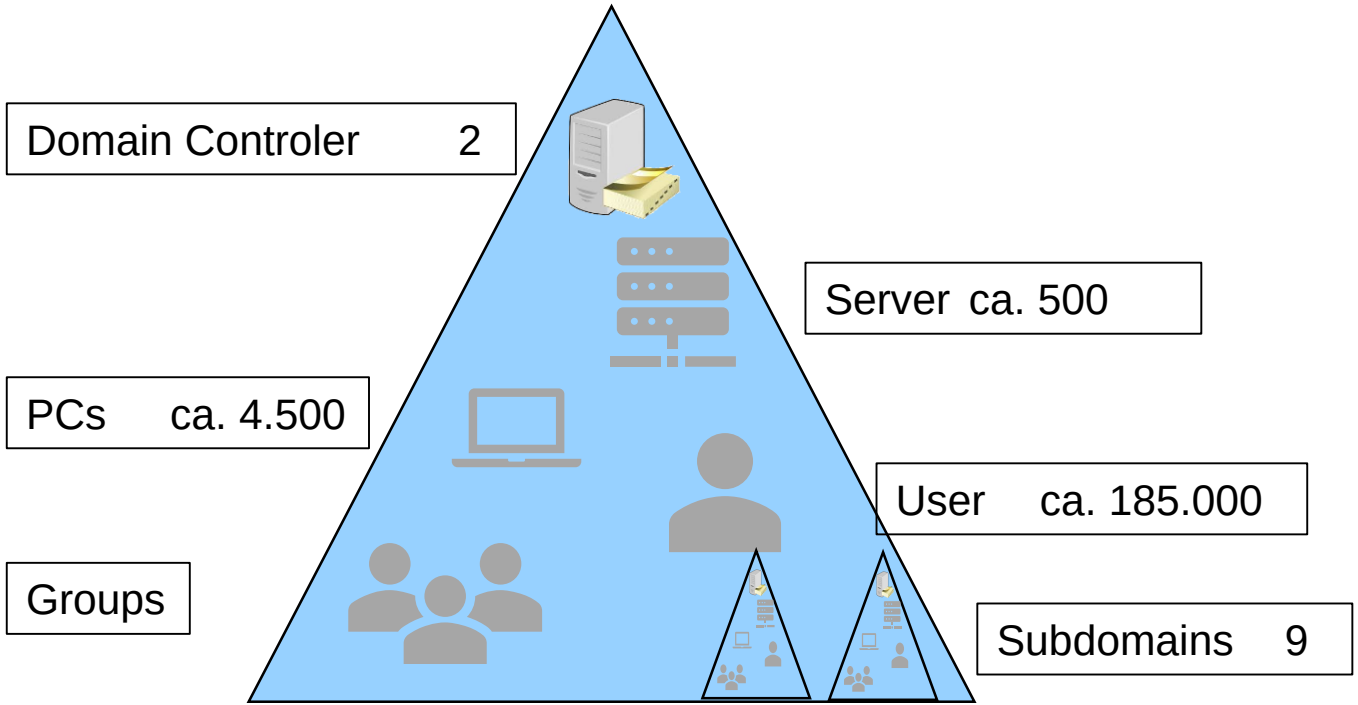
Videokonferenz nonstop

Wechselnde Teilnehmer

- Daten anfragen
- zur Verfügung stellen
- Auswerten
- weitere Daten nötig

Dauer: 1 Woche

Active Directory der Ruhr-Universität Bochum



Ablauf des Angriffs auf die Ruhr Universität

- Vorbereitungen ab 27.02.2020 über einen lokalen PC
- Warnung des DFN-CERT dazu am 07.04.2020
- Weitere Vorbereitung ab 01.05.2020
- Aktiver Angriff auf Subdomänen Server ab 06.05.2020 5:11 Uhr
- Warnung des Bund-CERT am 06.05.2020 12:00 Uhr
  (PC mit offenem RDP Port)
- Start des Cryptolaunchs auf zentralen Domänenserver
  ab 07.05 0:30 Uhr
- Bemerkt am 07.05.2020 ca. 6:30 Uhr

t46rfq6d-readme.txt

---=== Welcome. Again. ===--- [+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension t46rfq6d.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.

If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practice - time is much more valuable than money.

Auswirkungen des Cyberangriffs

Verschlüsselte Server: 60
(45 virtuell / 15 physisch)

- Alle DCs verschlüsselt
- Kein Active Directory
- Kein Exchange
- Kein SharePoint
- Keine SQL Server

Verschlüsselte PCs: keine

Verwaltung quasi arbeitsunfähig

- Keine E-Mail / Kalender
- Keine Personalverwaltung
- Keine Finanzverwaltung
- Studierendenverwaltung stark eingeschränkt

Presse


Ruhr Nachrichten

CORONA BVB LOKALSPORT DORTMUND LÜNEN CASTROP-RAUXEL SCHWERTE WERNE SELM OLFEN

KRIMINALITÄT

Hacker-Angriff legt Systeme der Ruhr-Uni Bochum lahm


heise online heise+

IT Mobiles Entertainment Wissen Netzpolitik Wirtscha

TOPTHEMEN: IPHONE 12 E-AUTO SECURITY WINDOWS 10 CORONAVIRUS

Security) 7-Tage-News) 05/2020) **Ransomware-Infektion: Ruhr-Universität Bochum ruft zur…**

Ransomware-Infektion: Ruhr-Universität Bochum ruft zur Passwortänderung auf

Die RUB kämpft weiter mit Ransomware-Folgeschäden. Studierende, Mitarbeiter und Alumni sollen ihre Zugangsdaten ändern.


ZEIT ONLINE

Suche

Politik Gesellschaft Wirtschaft Kultur Wissen Digital Campus Arbeit Entdecken Sport ZEITmagazin Podcasts mehr

Computerangriff

Ruhr-Universität Bochum durch Cyberangriff größtenteils offline

Die IT-Infrastruktur der RUB ist von außen zu großen Teilen lahmgelegt worden. Studierende und Mitarbeiter sind aber aktuell auf Onlineangebote angewiesen.

7. Mai 2020, 14:39 Uhr / Quelle: ZEIT ONLINE, and / 59 Kommentare


München 9°

Süddeutsche Zeitung

SZ.de Zeitung Magazin

Shop Jobs Immobilien

Coronavirus Politik Wirtschaft Meinung Panorama Sport München Bayern Kultur Gesellschaft Wissen Reise Auto mehr…

Home > Panorama > Bochum > Kriminalität - Bochum - Hackerangriff auf die Ruhr-Uni Bochum

7. Mai 2020, 19:34 Uhr Kriminalität - Bochum

Hackerangriff auf die Ruhr-Uni Bochum


Bochumer Uni erstattete Anzeige

Keine Kommentare

Urheber der Cyber-Attacke auf Ruhr-Universität weiter unbekannt

8. Mai 2020 um 16:54 Uhr | Lesedauer: Eine Minute

Bochum. Nach dem Cyber-Angriff auf die Verwaltung der Ruhr-Universität Bochum ist weiter unklar, wer dahinter steckt. Der Angriff war in der Nacht auf Donnerstag bemerkt worden. Online-Lehrangebote seien aber nicht betroffen.

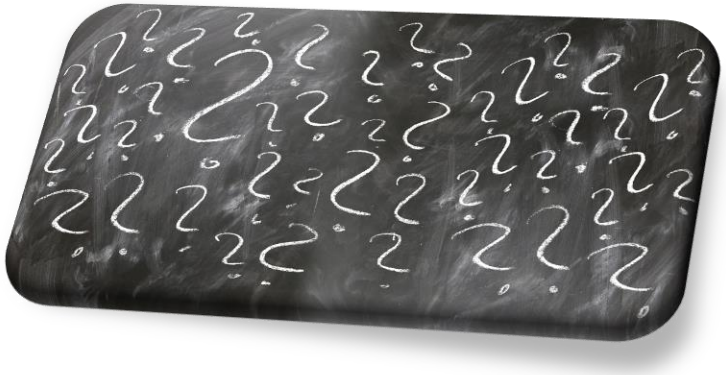
Was tun?

Krisenstab & Taskforce

Neu-/Wiederaufbau

Notbetrieb

Information / Kommunikation



Krisenstab

Rektor

Kanzlerin

Kanzlervertreter

Dezernent für Hochschulkommunikation

Dezernent für Personalwesen und Recht

Direktorin IT.SERVICES

2 Abteilungsleiter IT.SERVICES

Entscheidungen

Erpressung wird nicht nachgegeben

Wiederaufbau und kein Neuaufbau des ADs

Subdomänen werden nicht weiter betrieben

Reihenfolge für Wiederanlauf der Systeme

Taskforce – Technologie & ...

- 8 Personen
- 1 – 3 ext Experten
- 85 m^2 Raum
- 18 Werktage

- Pizza
- Kaffee
- Kekse
- Wasser

Wiederaufbau

- Entscheidung zum Wiederaufbau (nicht Neuaufbau) am 12.05
- Aufruf zum Passwortwechsel am 12.05
- 3 Tage prüfen und dann 5 Tage Konzeptionierung
- Ab 18.05 Neue Domänen Controller mit Backup der AD Struktur bespielt
- Alle Nutzer & Computer gesperrt; Alle Tickets gelöscht
- Neue Struktur gemäß (Brandschutz-) Konzept ist aufgebaut (27.05)
- Fileshares und AD am 02.06 wieder zur Nutzung freigegeben
- 22.06 Exchange und SharePoint freigegeben

Notbetrieb

Reihenfolge für Notbetrieb am 12.05 getroffen

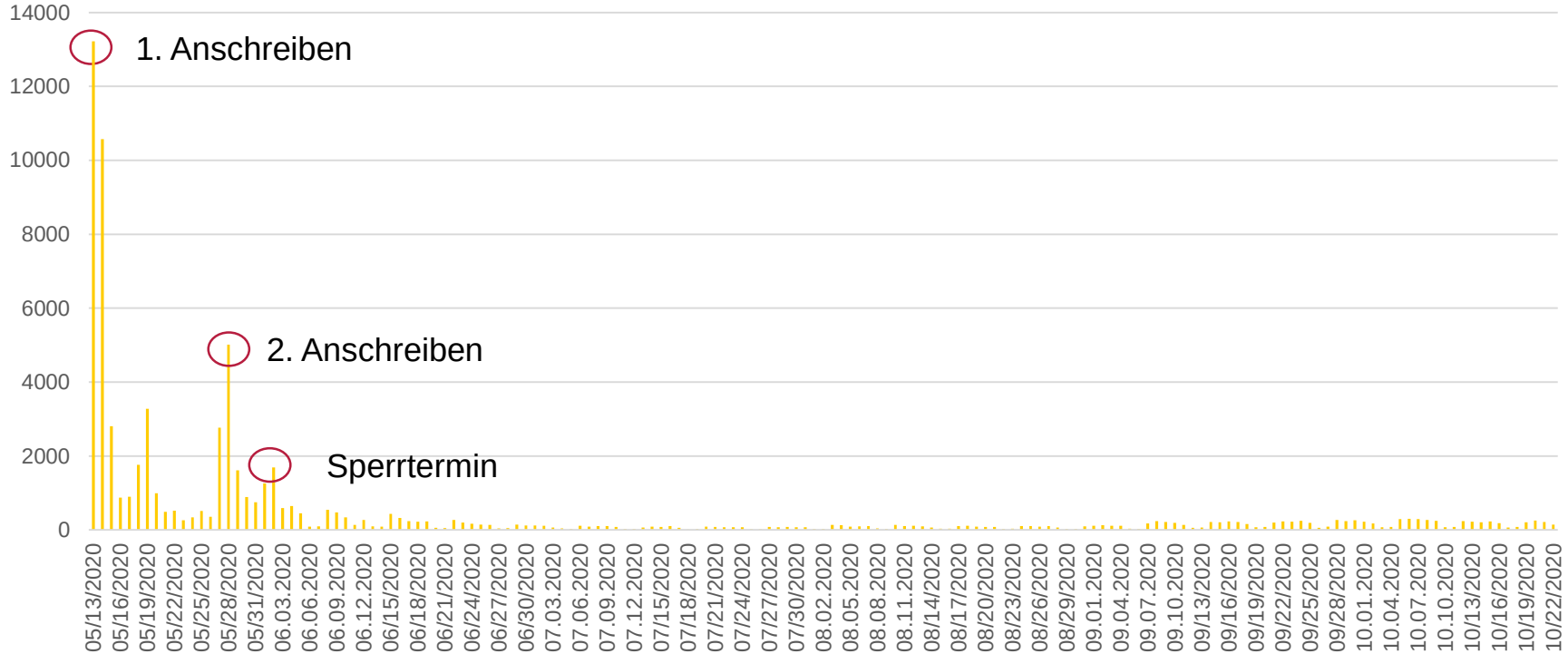
Ab 19.05 kontrollierter Start des Notbetriebes mit Ampelfunktion

1. Studierendenservices
2. Personal- / Finanzwesen
3. E-Mail (alternatives System)

Kommunikation

- Riot / Element
  - IT.SERVICES-intern
  - Technische Ansprechpartner (Moderiert; Täglich bzw. bei Bedarf aktualisiert)
  - Technische Ansprechpartner (Bulletinboard; Täglich bzw. bei Bedarf aktualisiert)
- Videokonferenz (Zoom) & WhatsApp im Krisenstab
- Webseiten (täglich aktualisiert)
  - Öffentlich für alle (Studierende)
  - Für Bedienstete intern
- E –Mail (RUB/Privat) für bilaterale Kommunikation

70.857 Passwortänderungen



Helpdesk

RUHR UNIVERSITÄT BOCHUM RUB

Lessons Learned (persönliche Statements)

- Enorme Überstundenanhäufung – starke Belastung !
- Personal lässt nicht parallelisieren
- Kommunikation ist sehr vielschichtig
- Gute Experten sind das A & O
- Teamwork und gute Kollegen bewegen sehr viel und fangen viel auf
- Sehr gute Rückendeckung der Hochschulleitung

Lessons Learned

- Verwendung von privilegierten und hoch-privilegierten Konten
- Erweiterung der Speicherung von Logdateien
- Flächendeckende Installation von Antiviren-Software
- Schutz der Fernzugriffe
- Einführung einer Sicherheitsüberwachung
- Segmentierung und weitere Absicherung des internen Netzes
- Einführung organisatorischer Strukturen zur Behandlung von Sicherheitsvorfällen
- Awareness / Schulung

Es wird wieder passieren!

Danke!

Fragen?