Dominik Helble

COMBATING RANSOMWARE-AS-A-SERVICE WITH PUBLIC-PRIVATE PARTNERSHIP

RANSOMWARE – A GERMAN PERSPECTIVE

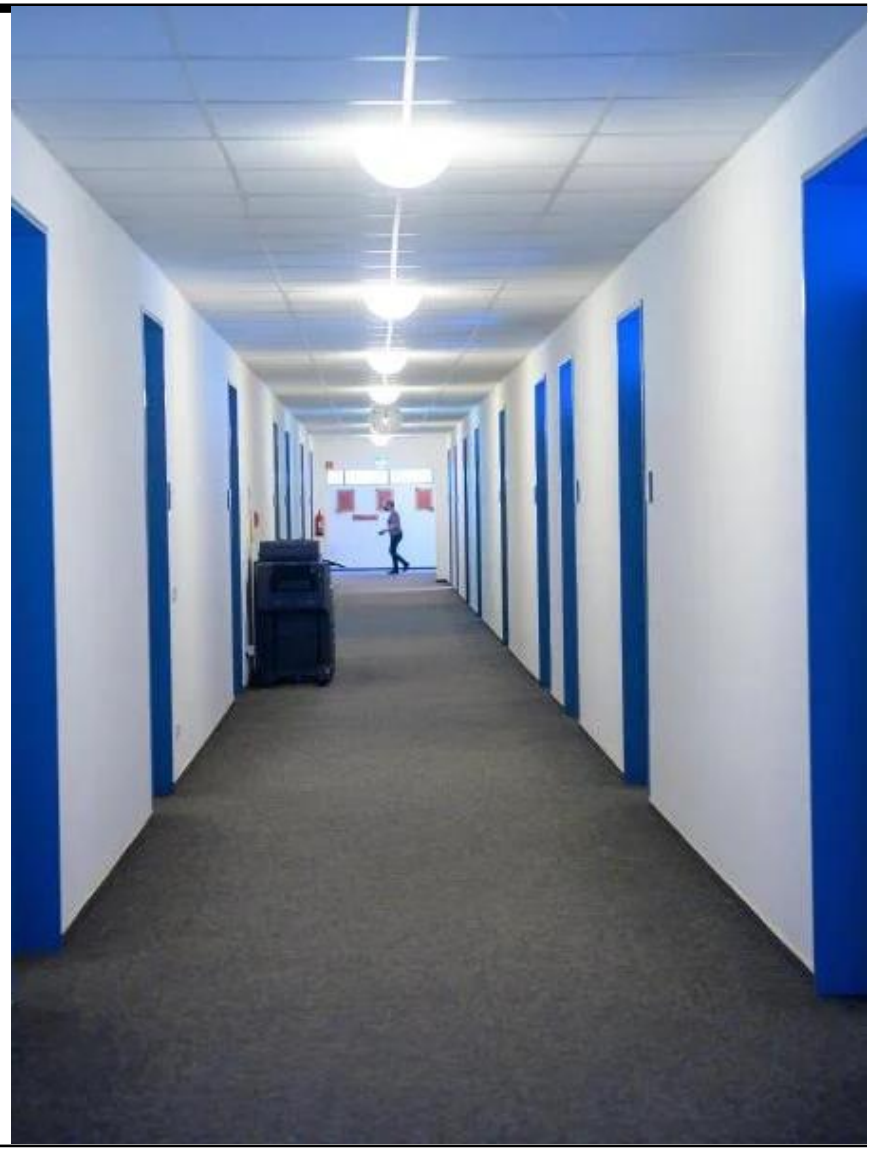
RANSOMWARE THREATENS NOT ONLY DATA BUT ALSO HUMAN LIVES

- September 2020: Ransomware attack on University Hospital Düsseldorf (UKD) (allegedly by “DoppelPaymer“ threat actor)
- IT infrastructure affected massively; not even phone calls possible
- Planned and outpatient treatments and emergency care could not occur at the hospital
- People seeking emergency care were redirected to more distant hospitals for treatment
- A patient in a life-threatening condition was redirected to a more distant hospital in Wuppertal receiving care an hour later and died

Picture: Roland Weihrauch / dpa

…AND SOCIETY

- July 2021: Ransomware attack on Anhalt-Bitterfeld district administration (allegedly by “Pay or Grief“ threat actor)
- Entire IT infrastructure affected: No government services possible for 2 weeks,
  e.g. no car registration possible, no social security or child support benefits paid out
- “Cyber” disaster declared for the first time in Germany
- Assistance from the Bundeswehr, the German armed forces, requested
- Data (e. g. non-public meeting minutes, personal data of local politicians) published on Darknet



Picture: Klaus-Dietmar Gabbert/dpa-Zentralbild/dpa (Foto: dpa)

BUT: ATTACKERS TRY TO AVOID PUBLIC ATTENTION

- Ransomware actors want to avoid public attention, and therefore do (normally) not target critical public infrastructure
- More popular victims are business enterprises and organizations
- Example: Ransomware attack on University Hospital Düsseldorf
  - About 30 servers were found encrypted with a ransom note addressed to the Heinrich Heine University Düsseldorf
  - Police informed the attackers they had hit the ‘wrong’ target and that lives were in danger
  - In return, the ransom demand was withdrawn and decryption keys were provided

Picture: dpa/Jens Büttner

ATTACK TARGET: GERMAN ECONOMY

- Federal Criminal Police Office Germany (BKA): “Cybercriminals are currently increasingly focusing their attacks on the so-called "big game", i.e. large companies and public institutions.
- German economy has never “been attacked as much as today” according to federation of German industries (BDI)
- Virtually every German small medium-sized companies has already been the victim of a cyberattack

Picture: Andrey Popov/stock.adobe.com

223 BILLION EUROS IN DAMAGE CAUSED BY CYBERATTACKS ON GERMAN COMPANIES

- Representative study by the digital association Bitkom in 2020/2021, for which >1.000 companies across all industries were surveyed
- 88 percent of companies in Germany were affected by data theft, espionage or sabotage in 2020 and 2021
- Losses more than quadrupled (+358%) compared to previous years in 2018/2019
- According to the study, ransomware attacks are particularly frequent and dangerous.

THE WINNING FORMULA AGAINST RANSOMWARE: INTERNATIONALLY AND TOGETHER

- Combating ransomware in Germany with 16 independent federal states is impossible without cross-state coordination and bundled investigations
- Investigations should be focused on RaaS providers to achieve sustainability in the fight
- Investigations must be coordinated internationally, as against Emotet

Picture: https://commons.wikimedia.org/wiki/File:Germany_on_the_globe_(Germany_centered).svg

PUBLIC AND PRIVATE SECTOR MUST WORK CLOSELY TOGETHER

- Victim companies must report ransomware attack in order to allow LE investigations
- However, police must include victims' concerns and needs
  - No investigations and forensics at any price
  - Not prolonging negotiations to the disadvantage of the victims in order to make investigations possible
  - Share threat intelligence data with threatened companies, even if this may endanger investigations
  - Think more in terms of prevention than repression, as arrests are difficult and the Hydra only gets another head cut off.

Picture: https://www.vergabe.nrw.de/wirtschaft/public-private-partnership-projekte

OPEN DISCUSSION

- Ransom payments - are they reasonable and appropriate?
- Combating ransomware #1 –
  Fight the RaaS providers or their affiliates?
- Combating ransomware #2 –
  Does a public-private partnership help?

LIST OF SOURCES

- https://www.euractiv.com/section/cybersecurity/news/german-county-targeted-by-ransomware-asks-military-for-help/
- https://www.dw.com/en/rural-german-district-declares-disaster-after-cyberattack/a-58227484
- https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/krankenhaus-derzeit-nur-sehr-eingeschraenkt-erreichbar-patientenversorgung-eingeschraenkt
- https://www.bleepingcomputer.com/news/security/ransomware-attack-at-german-hospital-leads-to-death-of-patient/
- https://www.wired.co.uk/article/ransomware-hospital-death-germany
- https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident
- https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr
- https://www.thestar.com.my/tech/tech-news/2021/08/06/cyberattacks-have-hit-almost-all-german-companies-during-past-year
- https://www.cryptovision.com/en/223-billion-euros-in-damage-caused-by-cyberattacks-on-german-companies/
- https://www.euractiv.com/section/cybersecurity/news/germany-not-sufficiently-prepared-to-tackle-ransomware-threats/
- https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.pdf;jsessionid=1E88DD62DA83CC2ABCBA2B5425672E19.live292?__blob=publicationFile&v=4
- https://krebsonsecurity.com/2021/01/international-action-targets-emotet-crimeware/
- https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
- https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html