

## Cybersecurity – IT Infrastructure & Blockchain



# Secure Information Technology Center A-SIT

- › Information security competence for the Austrian public sector
- › Non-profit association of public sector members
  - › Federal Ministry of Digital and Economic Affairs
  - › Federal Computing Center
  - › Graz University of Technology
  - › Danube University Krems
  - › Johannes Kepler University Linz
- › E.g., eIDAS conformity assessment and certification body

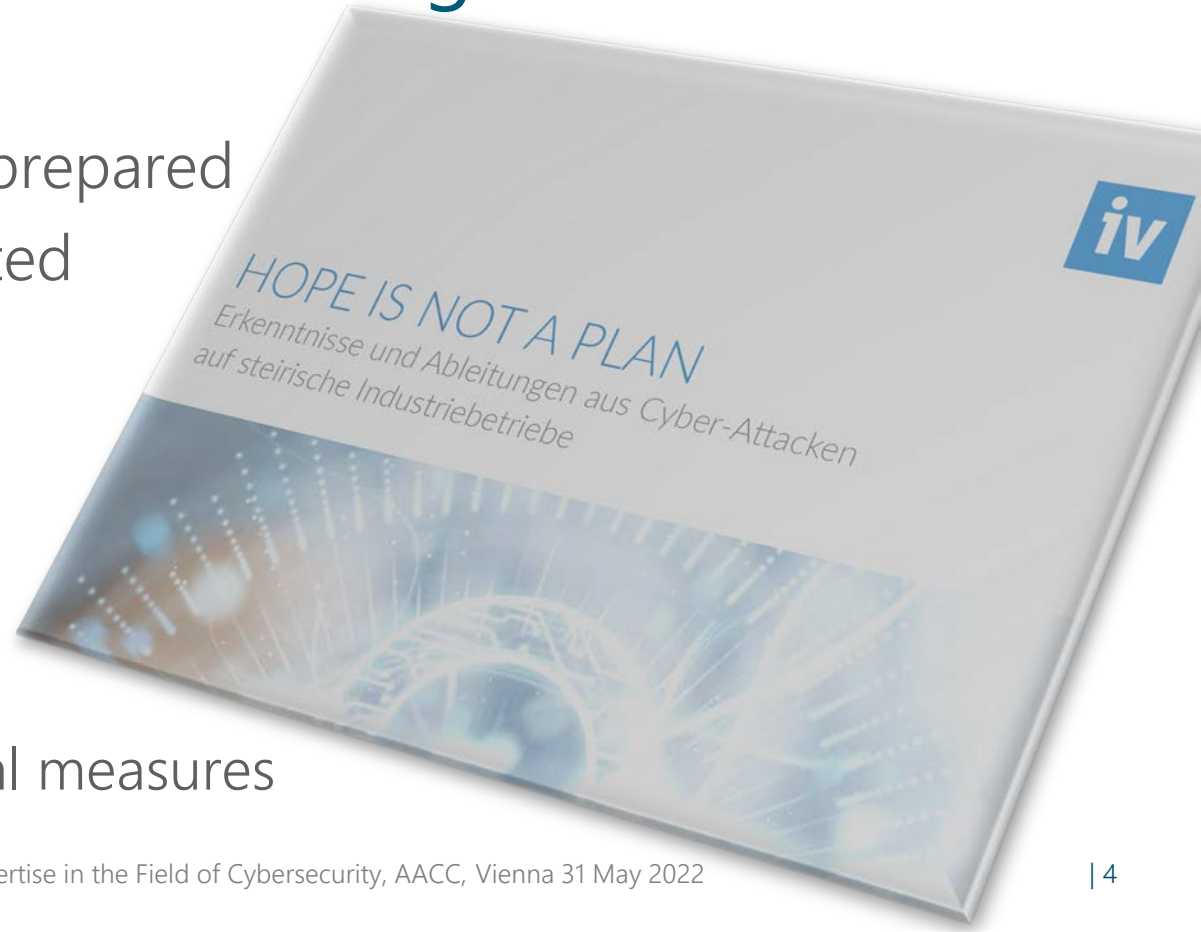
# Ransomware, an 21<sup>st</sup> century plague

- › WEF Global Risk Report 2022: 435 % increase in 2020
- › Study with Federation of Austrian Industries, Styrian Chapter
  - › Interview with victims
  - › Lessons learned
  - › Advise based on the actual experience made



# Some findings

- › Organisations were prepared
- › Impact underestimated
- › “Entry door” human
- › Key is to enter in a planned situation
- › Risk mitigation
  - › Organisational and preventive technical measures

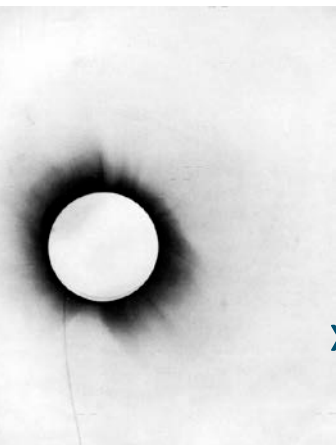


# A few mitigation measures

- › Multifactor authentication should become default
  - › cf. eID session in the afternoon
- › Client barely need Word macros or powershell
- › User awareness is important
  - › but responsibility cannot be only with the end-user
- › Resilience in the infrastructure

# Blockchain - the decentralisation promise?

- › Security assumptions based on massive distribution
  - › But it's an assumption, not a infallible dogma
    - › Some examples of A-SIT results
      - › "Total Eclipse of the Heart – Disrupting the InterPlanetary File System" (Prünster, et.al. 2022)
      - › "A Security Analysis of FirstCoin" (Marsalek et.al., 2018)
      - › "Spoof-of-Work - Evaluating Device Authorisation in Mobile Mining Processes" (Ziegler, et.al., 2018)
    - › Governance and liability, if there is fraud
      - › Whom to turn to, if decentralised?



[a-sit.at/](https://a-sit.at/)