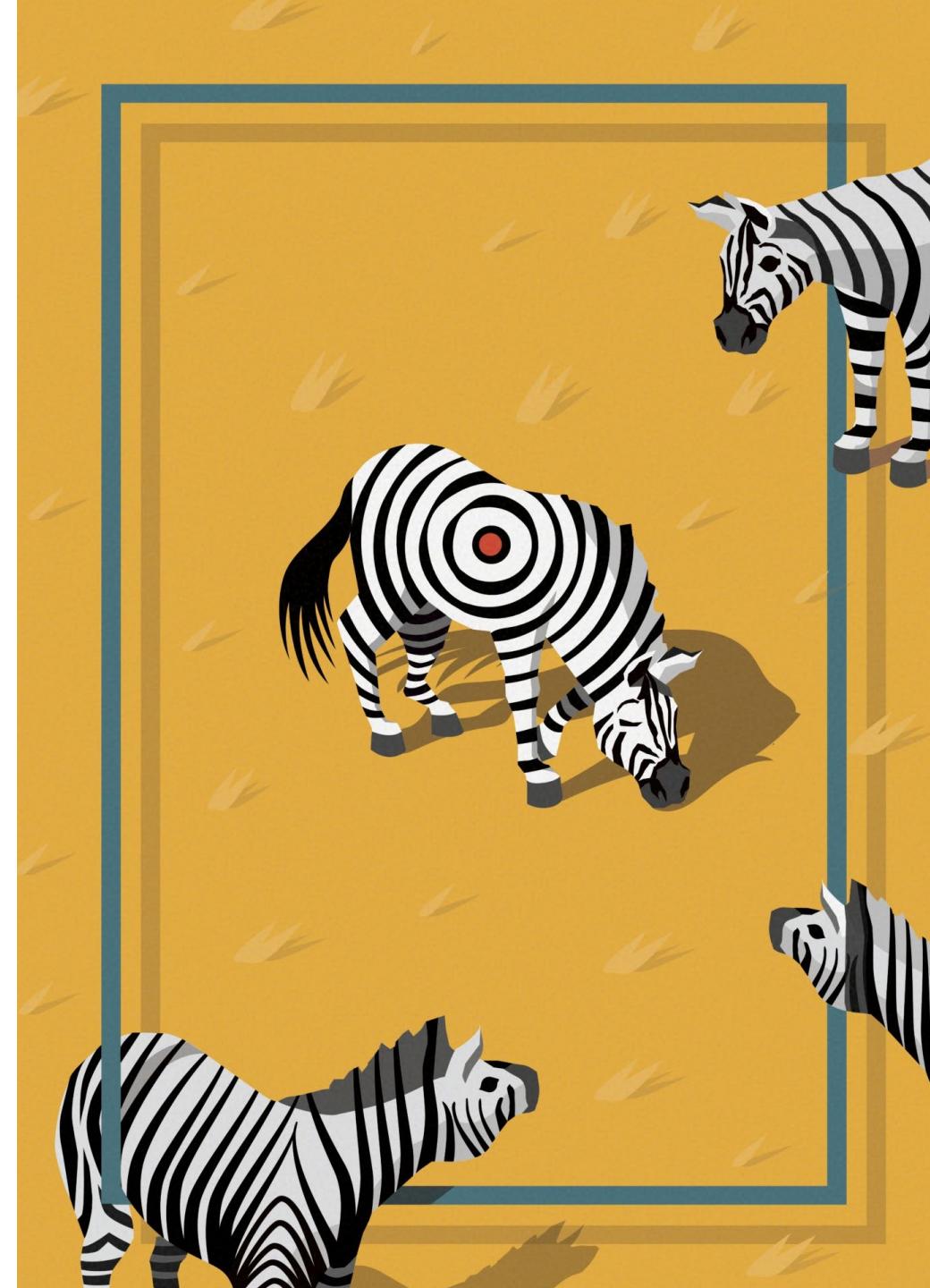


Die Kommune als Ziel von Cyberangriffen

Ausgewählte Malwares und was wir von ihnen
lernen können

Dr. Karoline Busse – 15.09.2021



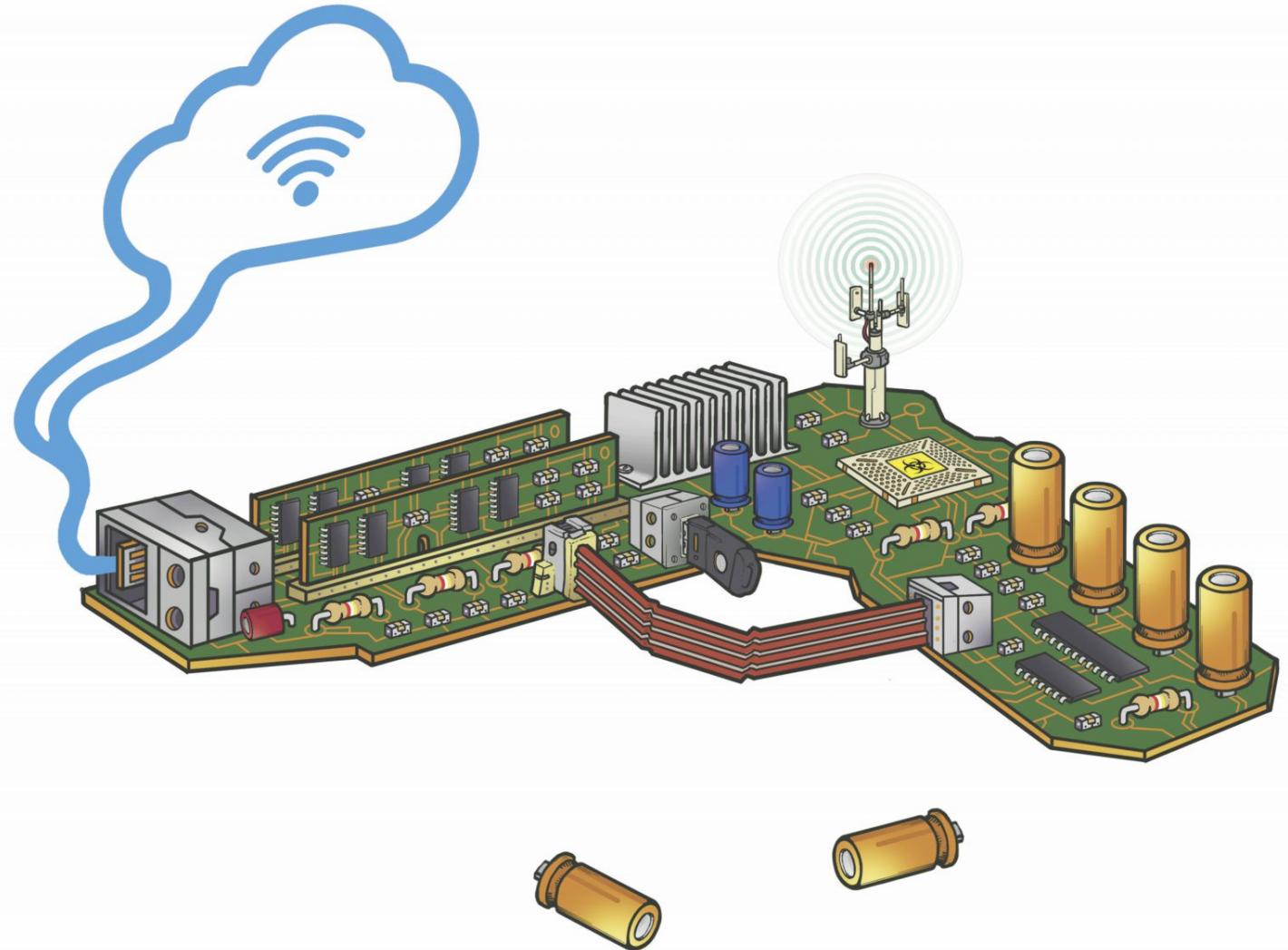
Wer ich bin

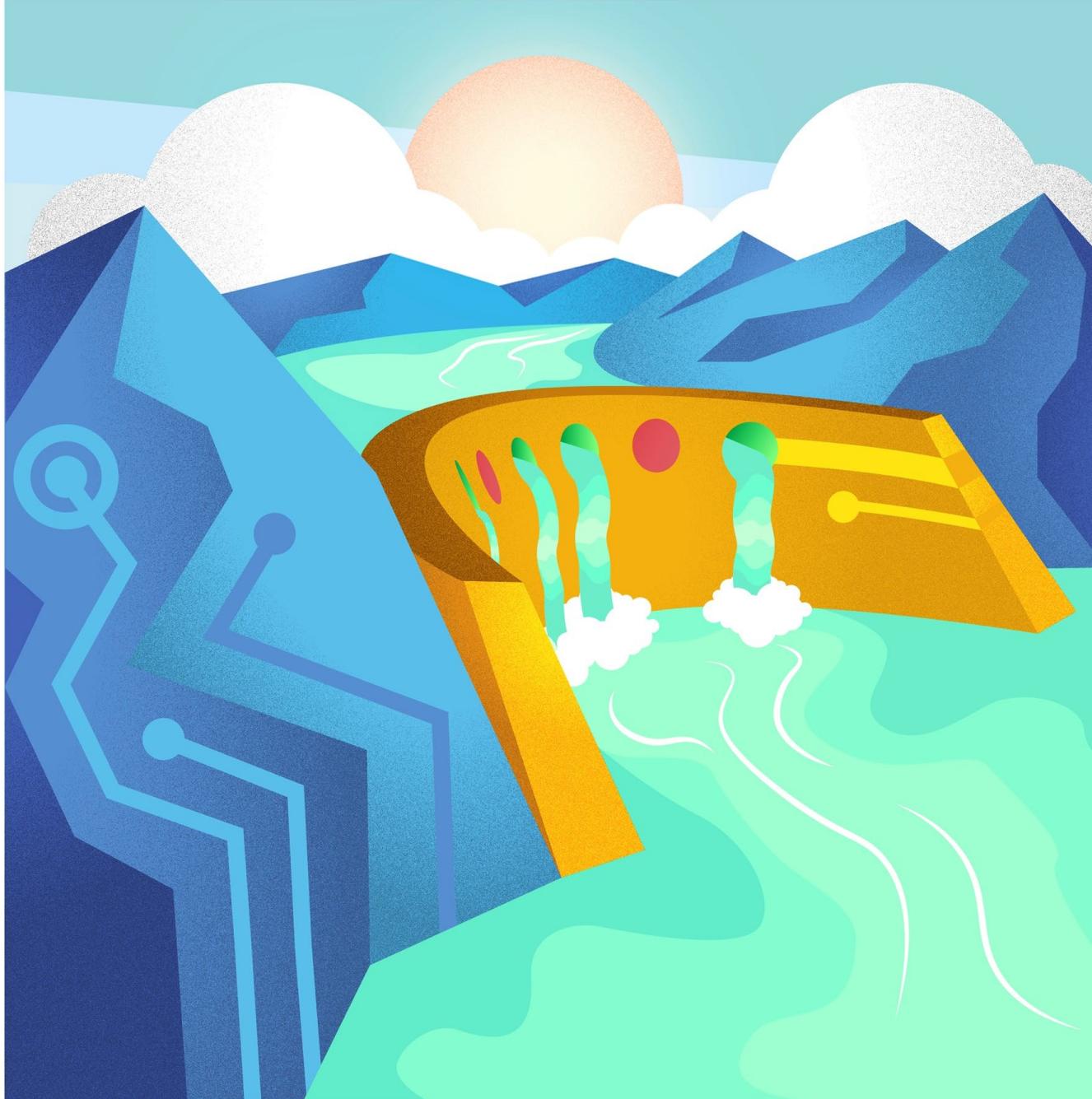


- Dozent*in für Datenschutz und Datensicherheit am NSI seit Mai 2020
- Vorher Studium der Informatik: Bachelor + Master LUH, Promotion Uni Bonn
- Forschungsschwerpunkt: Mensch-zentrierte IT-Sicherheit

Worum geht es heute?

Ausgewählte
Cyberangriffe auf
den öffentlichen
Sektor und was wir
daraus lernen
können



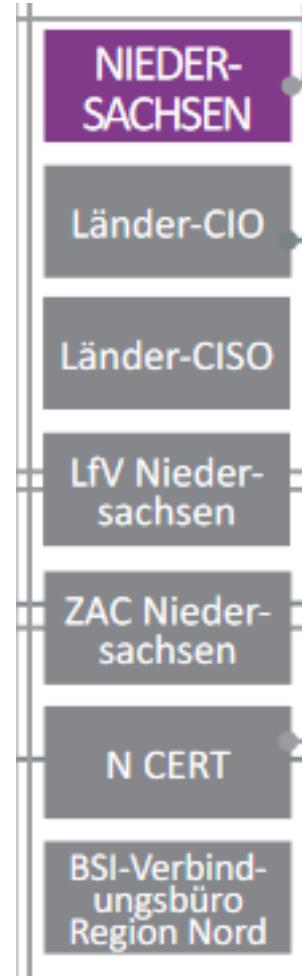


Emotet

Mehr als Ransomware

Was ist Ransomware?

- Eine spezielle Schadsoftware, welche die Dateien des Opfers verschlüsselt und erst nach einer Lösegeldzahlung wieder freigibt
- Im Ernstfall: Nicht zahlen! Polizei (ZAC), ggf. N-CERT und/oder BSI benachrichtigen



Aus: „Deutschlands staatliche Cybersicherheitsarchitektur“, Stiftung Neue Verantwortung,
<https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur>

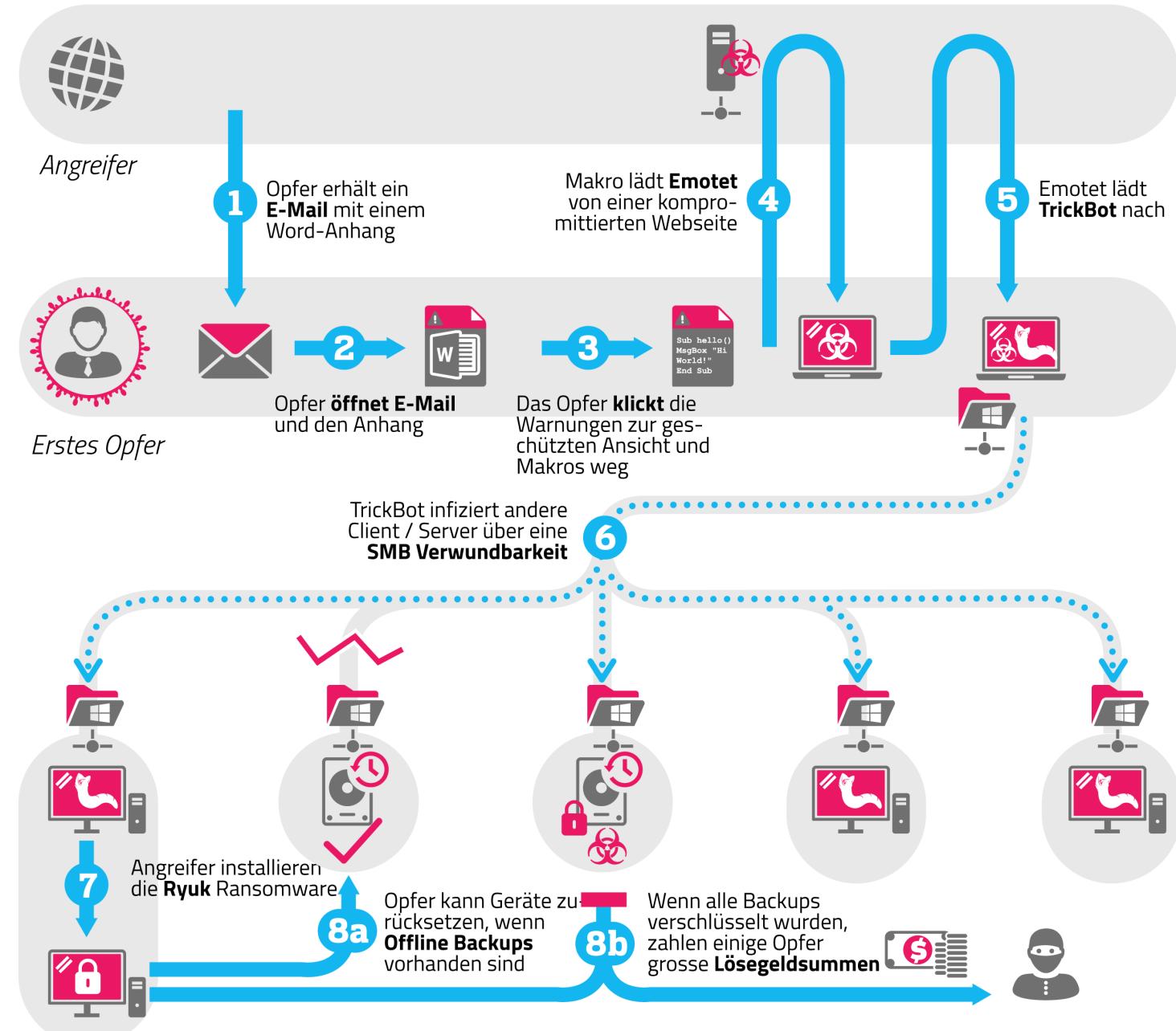
Was ist Emotet?

„Am Montag, den 13. Mai, um kurz vor 15 Uhr öffnete ein Mitarbeiter eine Mail, die sich auf einen zitierten, echten Geschäftsvorgang bezog. Die Mail stammte scheinbar von einem Geschäftspartner und forderte dazu auf, die Daten im angehängten Word-Dokument zu kontrollieren und bei Bedarf zu ändern. Beim Öffnen des Dokuments erschien eine (gefälschte) Fehlermeldung, die dazu aufforderte, „Enable Editing“ anzuklicken. Dieser Aufforderung kam der Mitarbeiter nach – und das Unheil nahm seinen Lauf.“

Emotet Infektionsablauf

Attribution
CC BY GovCERT.ch

Wie funktioniert Emotet?



Berühmte Opfer von Emotet

- Heise Gruppe, Hannover
- Berliner Kammergericht
- Stadtverwaltung Frankfurt am Main
- Stadtverwaltung Neustadt am Rübenberge
- Justizministerium Quebec, Kanada
- Stadtverwaltung Allentown, Pennsylvania,
USA



Emotet in Neustadt am Rübenberge

„Am Morgen des 6. September 2019 bemerkte ein Mitarbeiter der IT-Abteilung der Stadtverwaltung von Neustadt am Rübenberge etwas Seltsames. Sein Monitor zeigte ihm eine extrem hohe Auslastung der Server im Rechenzentrum der Kommune – obwohl keine Tests oder Wartungsarbeiten anstanden. Es könnte Schadsoftware am Werk sein, folgerte der Mitarbeiter. Sicherheitshalber fuhr er die Server sofort herunter.“

Emotet in Neustadt am Rübenberge

„Doch da war es längst zu spät. Schon am Vorabend oder in der Nacht hatten Unbekannte damit begonnen, die Server der Verwaltung der niedersächsischen 45.000-Einwohner-Stadt zu verschlüsseln. Mails und Formulare, Flächennutzungspläne und Bauzeichnungen, die Hochzeitstermine des Standesamts und Elterngeldanträge – der eingeschleuste Kryptotrojaner machte vor nichts Halt.“

Emotet in NRÜ: Der Ablauf

- 6 Monate vor dem Datenverlust: Vereinzelte VirensScanner schlagen Alarm. Systeme neu aufgesetzt, Antivirus zufrieden.
- Wahrscheinlich wurde ein schadhafter Anhang einer gefälschten Email geöffnet und Office-Makros wurden aktiviert.
- Ransomware „Ryuk“ aktiviert sich mit einem Bekennerschreiben



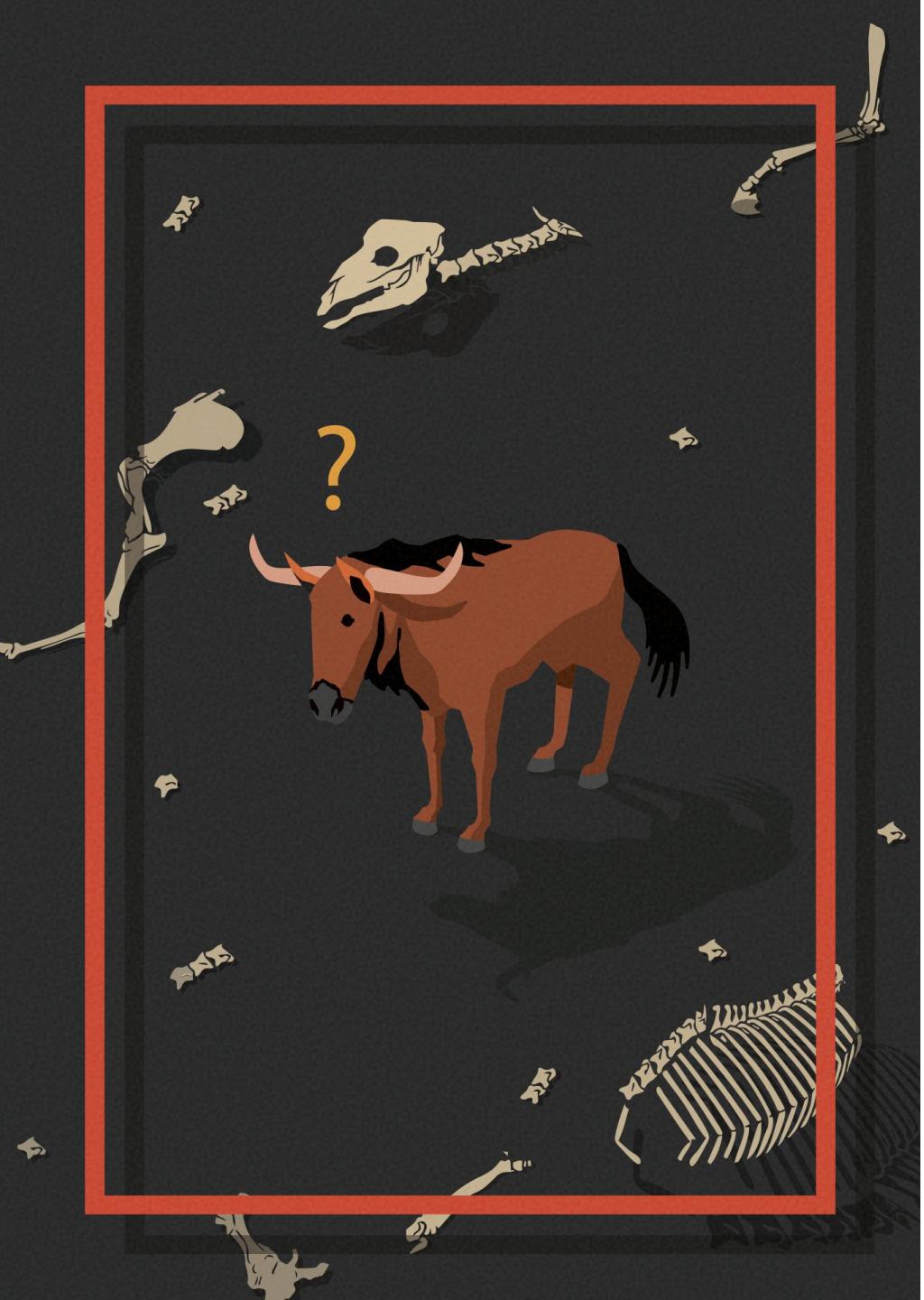
Der Ablauf (2/2)

- Alle Angestellten werden angewiesen, ihre Rechner herunterzufahren
- Externe Partner werden angerufen: Keine Mails aus NRÜ öffnen!
- Sperrung der Konten der Stadt wird veranlasst
- Polizei und LfD werden informiert



Emotet in NRÜ: Schadensbilanz

- Große Teile der Verwaltungsserver verschlüsselt: insg. etwa 550 000 Dateien
- Fast alle Bürger*innendienste nicht verfügbar
- Zahlungen (z.B. Elterngeld) konnten nicht mehr geleistet werden
- IT komplett neu aufgebaut, Kosten ca. 100 000 – 150 000 €
- Pläne für ein Neubaugebiet mussten neu erstellt werden
- 4 Monate später „zu 95% wieder einsatzfähig“



Emotet in NRÜ: Lessons Learned

- Strengere Regeln für Mail-Anhänge: .doc und .zip werden abgewiesen
- Strenge Segmentierung der Netzwerke
- Sicherheitstests durch externe Expert*innen
- Backups auch auf Magnetband, z.T. aufbewahrt im Tresor oder Bankschließfach

Quo Vadis Emotet?

Emotet malware self-destructs after cops deliver time-bomb DLL to infected Windows PCs

Uninstall code, distributed from backend servers seized in January, fired on Sunday

Gareth Corfield

Mon 26 Apr 2021 // 05:33 UTC

Quo Vadis Emotet?

- Januar: Europol-Razzien u.a. in Deutschland, Litauen, Ukraine, Niederlande; mehrere 100 Server beschlagnahmt
- Opfer wurden auf von der Polizei kontrollierte Server umgeleitet
- 25. März: Deinstallationsprogramm wird über die Kontroll-Server der Polizei an Opfer in aller Welt gesendet

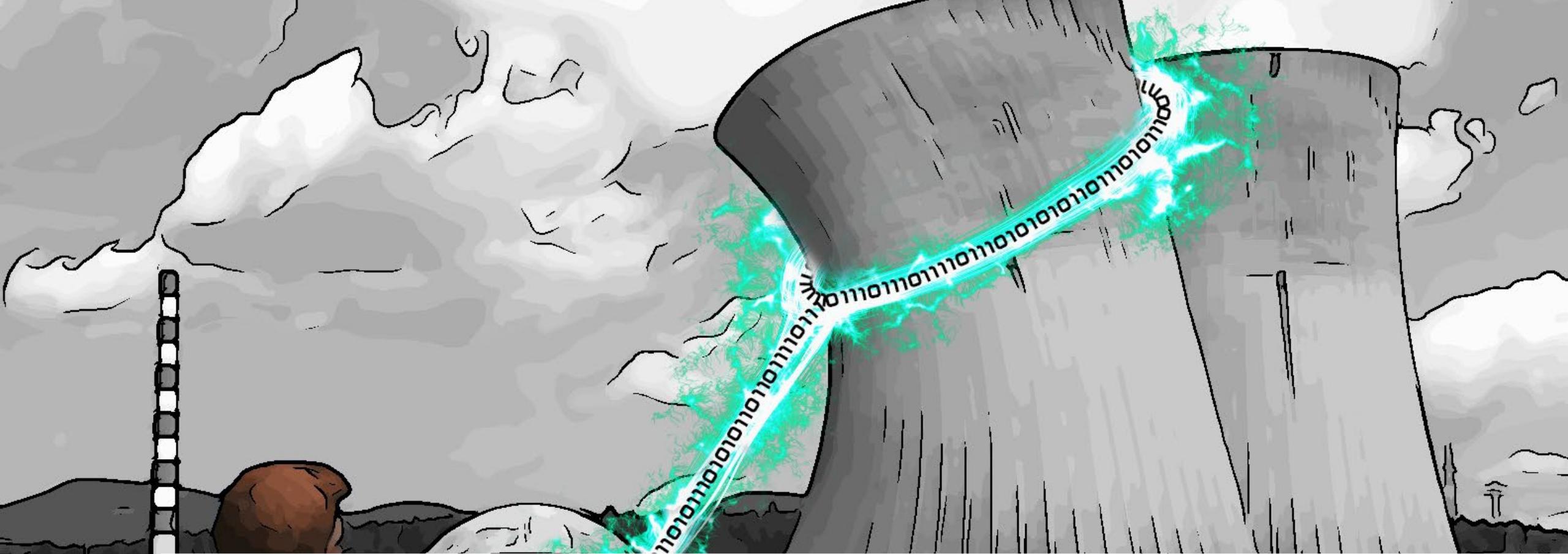


Quo Vadis Ransomware?

First death reported following a ransomware attack on a German hospital

Death occurred after a patient was diverted to a nearby hospital after the Duesseldorf University Hospital suffered a ransomware attack. 17.09.2020

- Die Branche boomt, durchschnittliche Lösegeldzahlung: 570 000 USD
- Vierfach-Erpressung im Trend: Verschlüsselung, Datendiebstahl, DoS, Belästigung von Kunden und Geschäftspartnern
- Neu: Ransomware-as-a-Service mit Supportdienstleistung für Opfer



Angriffe auf kritische Infrastruktur

Hier: Wasser- und Kraftwerke

Was ist kritische Infrastruktur?

„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“

Was ist kritische Infrastruktur?



KRITIS im Visier

KRITIS-Sektor
Wasser

Hackerangriff auf Trinkwasseranlage

Stand: 09.02.2021 08:25 Uhr

In Florida haben Hacker einen Angriff auf eine Aufbereitungsanlage für Trinkwasser verübt. Laut Behörden dabei wurde der Anteil von Natriumhydroxid im Wasser mehr als verhundertfach - eine "potenziell gefährliche" Erhöhung.

- Fernzugriff über die Systeme der Stadt Oldsmar (15 000 Ew.)
- NaOH-Menge von 100 auf 11100ppm geregelt
- Ein Mitarbeiter hat den Eingriff sofort entdeckt und rückgängig gemacht
- Risiko: Hautreizzungen, Erbrechen, Durchfall

KRITIS im Visier

Pipelines in den USA

Hackerangriff verteuert Benzin und Öl

10.05.2021 11:41 Uhr

Ein Hackerangriff hat die Pipelines von einem der größten US-Öllieferer stillgelegt. Die US-Regierung arbeitet am Beheben des Schadens - währenddessen steigen Öl- und Benzinpreise.

- Angriff mit Ransomware
- Gesamtes Pipeline-Netzwerk des Anbieters musste über Wochenende abgeschaltet werden
- Ausfall von 50% der Kapazitäten zur US-Ostküste
- Regionaler Notstand ausgerufen
- Barrel-Preis +1,5%; Benzin +4%

KRITIS im Visier

KRITIS-Sektor
Energie

Bericht: Bundesamt warnt vor Hackerangriffen auf Kraftwerke

Die Gefahr durch Cyberattacken sorgt aktuell in den USA und Europa für Aufsehen. In Österreich wurde das Außenministerium Ziel eines solchen Angriffs. In Deutschland sind Kraftwerke womöglich nicht genug geschützt.

05.01.2020

- In einer Untersuchung von Kaspersky wurden 54 Sicherheitslücken in Siemens-Steuerungstechnik für Kraftwerke gefunden
- BSI warnt vor „erheblichem“ Schadenspotenzial

Die TRITON-Malware

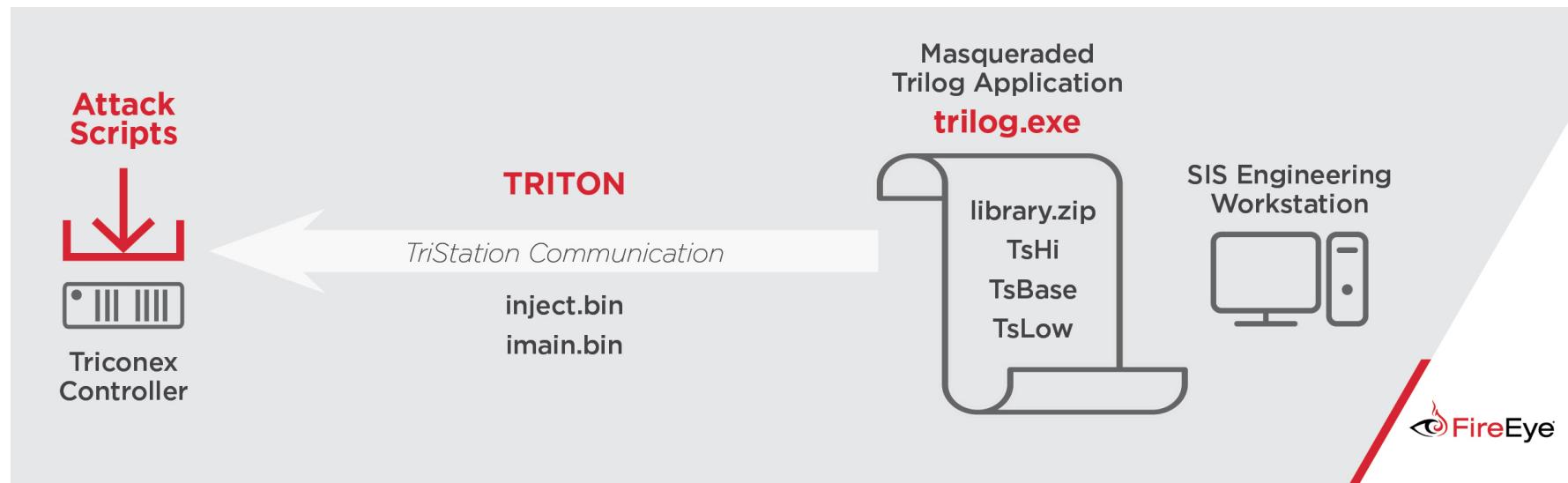
Fallstudie aus dem KRITIS-Sektor Energie



Die TRITON-Malware

- Wurde zuerst in 2017 in Saudi-Arabien bekannt und in letzter Sekunde gestoppt
- Gezielter Angriff auf Kraftwerk-Steuerungsanlagen
- Schadenspotenzial: Explosionen, Freisetzung von Schwefelwasserstoffgas, verheerende Umweltschäden
- Auch weitere Anlagen in „westlichen Ländern“ unter Angriff
- Expert*innen vergleichen die Malware mit STUXNET

TRITON: Angriffsmuster



TRITON: Schwachstellen im Fall 2017

- Erster Zugriff in 2014, vtml. über schlecht konfigurierte Firewall
- Weiterer Zugriffsweg über Workstations, durch eine ungepatchte Lücke in Windows oder über abgefangene Zugangsdaten
- Angeschlossene Triconex-Einheit im Programmiermodus





TRITON: Empfohlene Gegenmaßnahmen

- Updates!
- Für alte Systeme und als Fallback: Antivirus
- Vom Internet getrennte Netzwerke für „sensible“ Infrastruktur (plus „Desinfektion“ für Datenträger von außen)
- Ernstfall-Übungen
- Audits, Penetrationstests

TRITON: Empfohlene Gegenmaßnahmen

„All controllers should [...] never be left in the ‚PROGRAM‘ mode.“

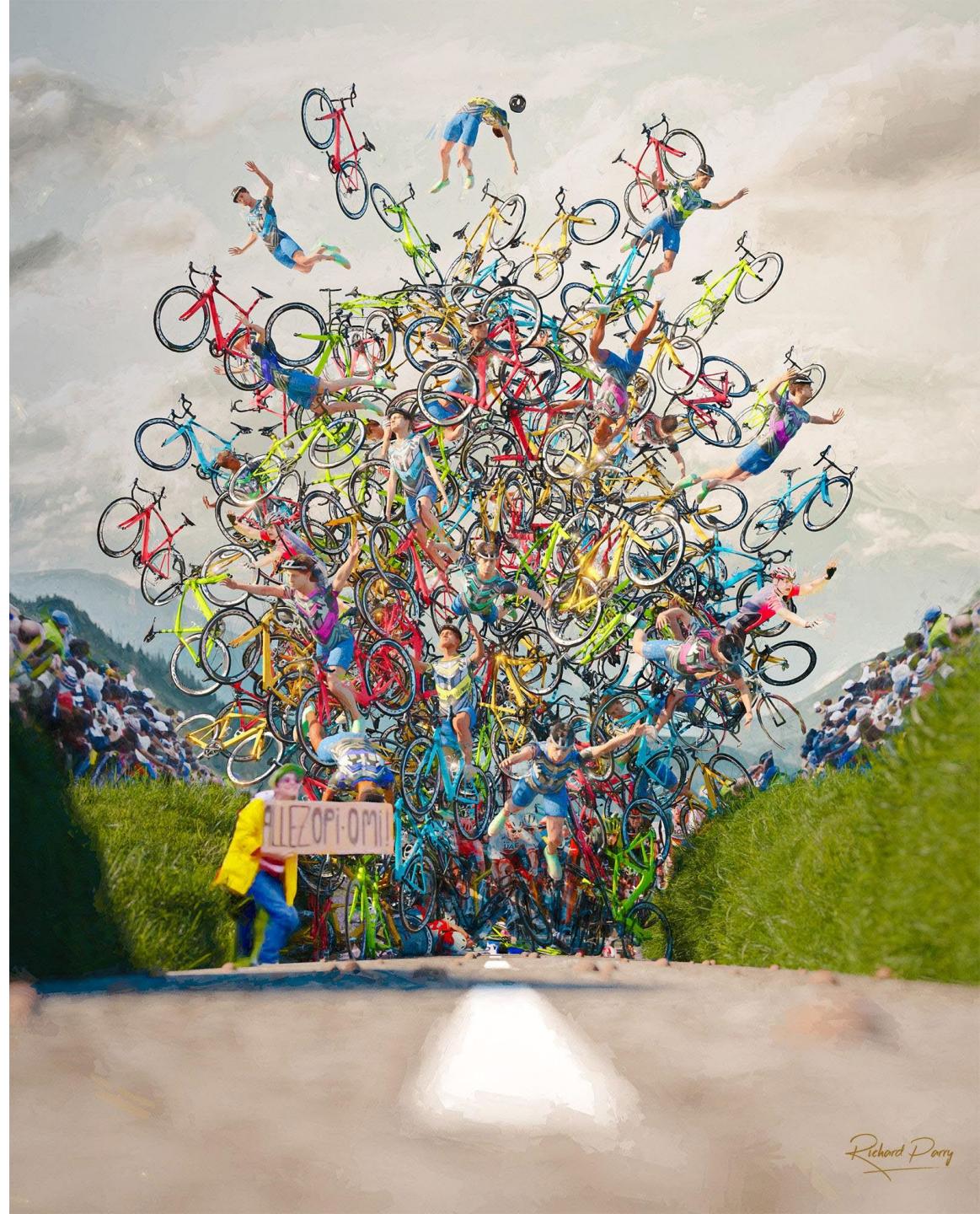
Der Faktor Mensch

Tipps für TOM



Mensch und IT

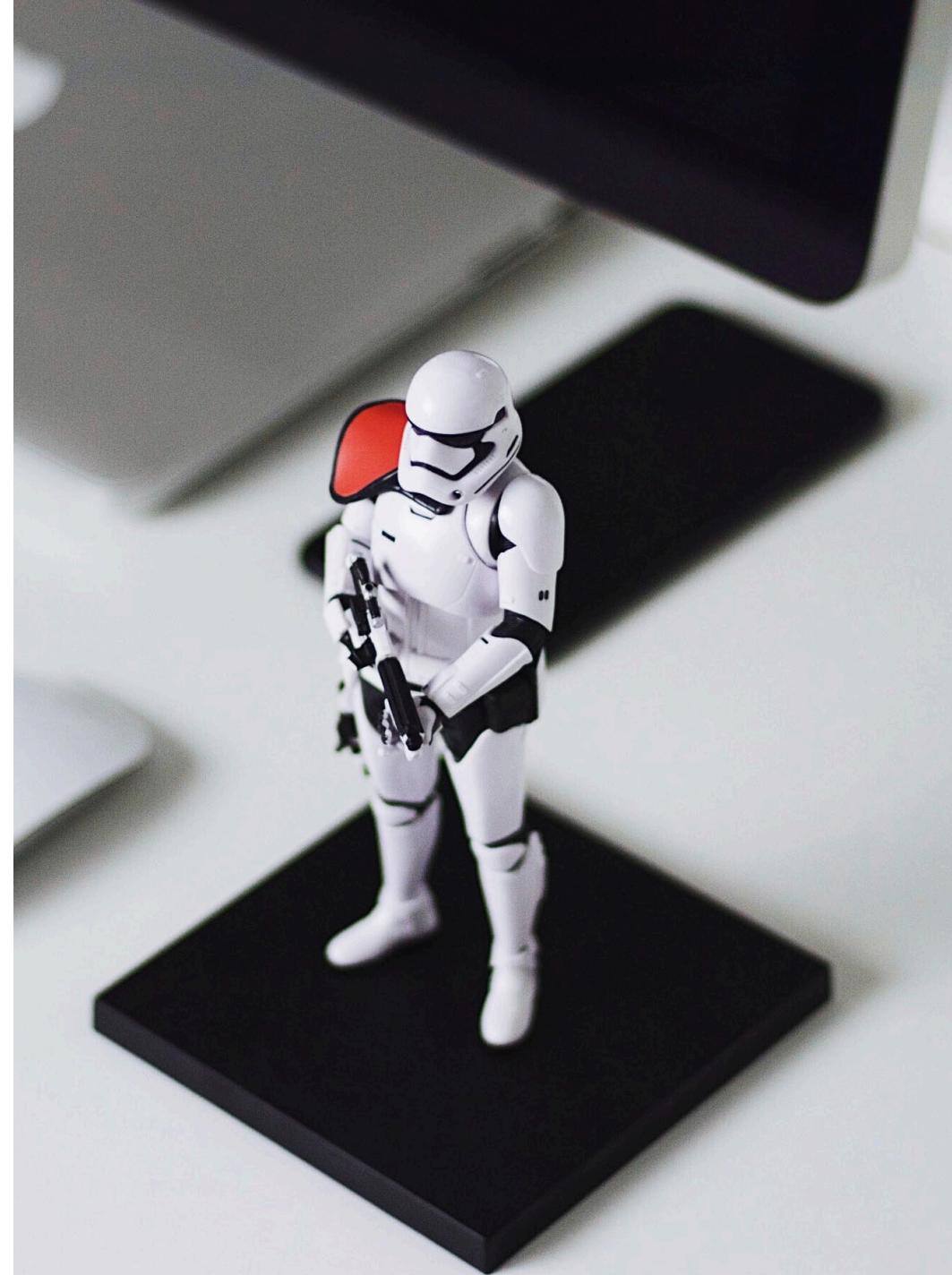
- Kein Mensch ist perfekt.
- Das wirkt sich auch auf alle von Menschen gemachten Dinge aus, z.B. IT.
- Menschen sind Gewohnheitstiere



Richard Derry

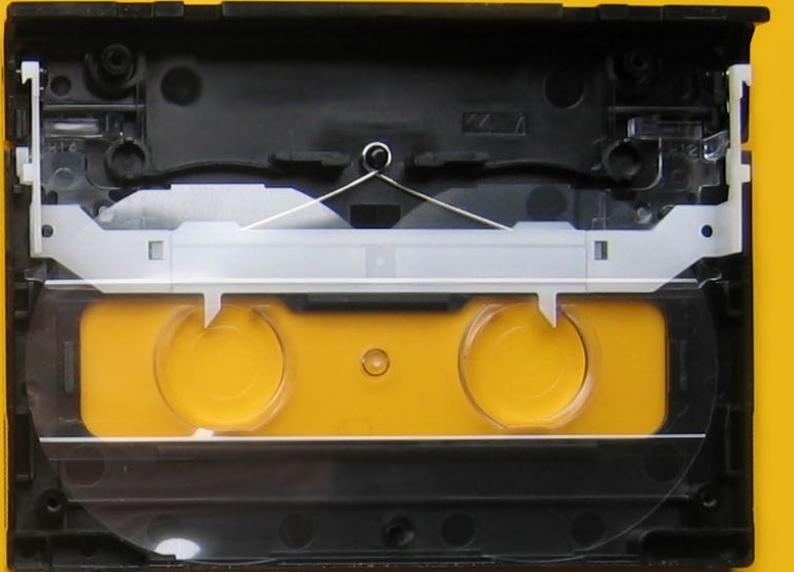
Mensch und Security

- Sicherheit ist quasi immer ein sekundäres Ziel
- Sicherheit sollte deshalb soweit wie möglich im Hintergrund stehen
- Soziale Probleme mit Technik lösen klappt nur selten wirklich gut

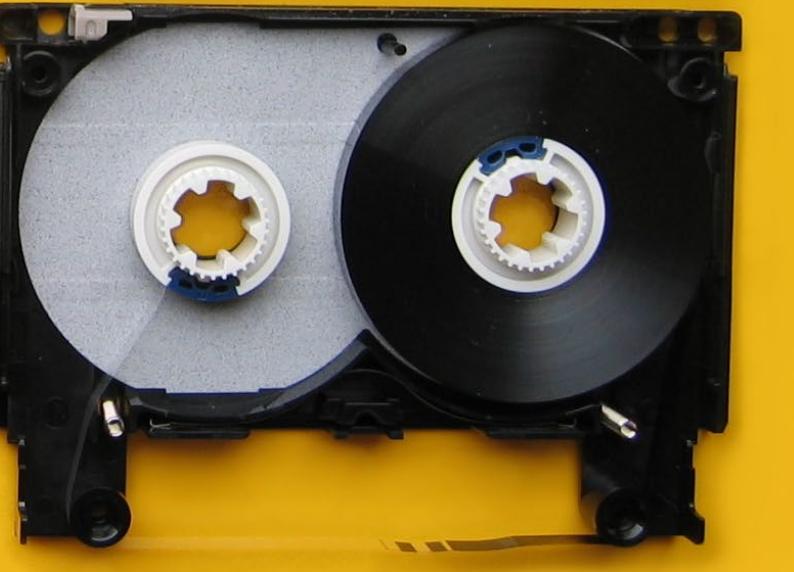


Mensch und Security

„[Security] should be designed and implemented so it is easy for users to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens.“



Mensch und Security: Tipps für die Praxis

- 
- Den Ernstfall antizipieren
 - Sinnvolle und umfassende Maßnahmen zur Eindämmung und Wiederherstellung ergreifen (denken Sie auch an das IoT in Ihrer Kommune!)
 - Maßnahmen regelmäßig üben! (Warntag)
 - Lehre aus Neustadt: Bandsicherungen

Werbeblock

Diesen Herbst neu am NSI: Auftakt der Seminarreihe IT-Sicherheit in Kooperation mit NSGB, AG KRITIS und anderen Schwerpunktthemen

- BSI-Grundschutz
- IDS und SIEM nach NDIG
- KRITIS
- Awareness für Anwender*innen und Führungskräfte

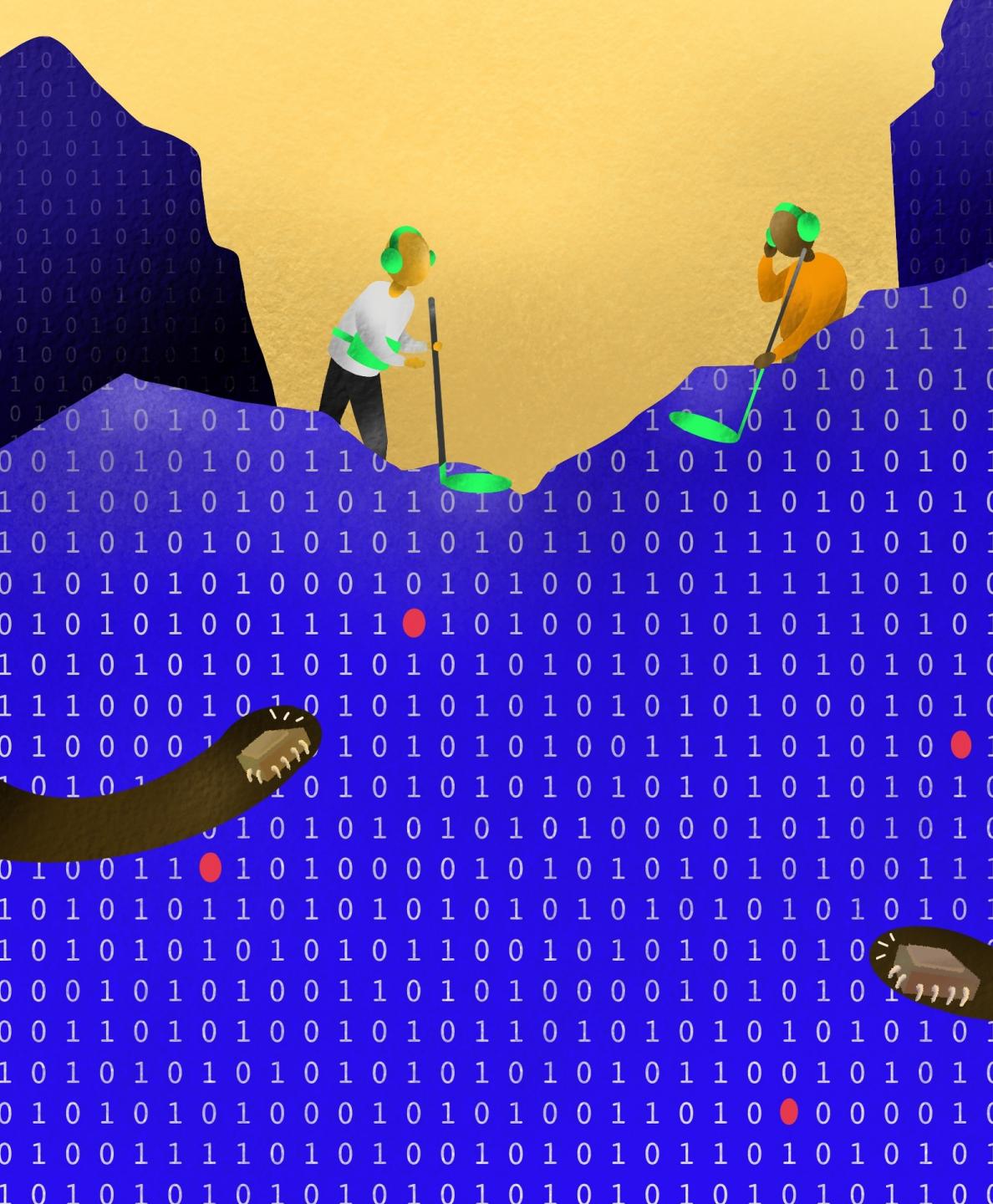
Interesse? Mail an antonia.ladwig@nsi-hsvn.de für Updates und Neuigkeiten



Werbeblock

Außerdem: ID2-Netzwerk
kommunale IT-Sicherheit ab Q1/22
nach Vorbild des ID2-Netzwerks
Datenschutz

Interesse? Mail an
antonia.ladwig@nsi-hsvn.de für
Updates und Neuigkeiten



Fragen & Diskussion

- Sind Sie als DSB/DSK für örtliche Stadtwerke, Wasserwerke etc. zuständig?
- Haben Sie Desaster Recovery-Konzepte für Ransomware o.ä.?
- Konnten Sie bereits Erfahrungen mit Cyberkriminalität sammeln?

Dr. Karoline Busse

Dozent*in für Datenschutz und
Datensicherheit
NSI e.V.

karoline.busse@nsi-hsvn.de

@kb_usec

Folien-Lizenz: CC-BY
Stand: 14.09.2021

Bildquellen (wo nicht anders vermerkt)

- <https://cybervisuals.org/visual/dont-be-an-easy-target/>
- <https://cybervisuals.org/visual/image-post-test-3/>
- <https://cybervisuals.org/visual/control-your-personal-data-stream/>
- <https://unsplash.com/photos/tmuArUNS1TI>
- <https://cybervisuals.org/visual/m-is-for-marie/>
- <https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/>
- <https://cybervisuals.org/visual/trust-your-instincts/>
- <https://cybervisuals.org/visual/aspects-of-cyber-conflict-pt-4/>
- <https://unsplash.com/photos/qNbe1RLo06M>
- <https://www.fotocommunity.de/photo/in-deckung-gehen-t-peters/41003311>
- <https://pixabay.com/de/photos/junge-kind-verwirrt-person-ratlos-61171/>
- „Tour de Farce“, Richard Parry
- <https://unsplash.com/photos/cVMaxt672ss>
- <https://commons.wikimedia.org/w/index.php?curid=57116831>
- <https://cybervisuals.org/visual/cyber-specialists/>