SIT

Netzwerk sii Baden-Württemberg

37. (Konferenz des) ChaosComputerClubs

Januar 2024

Udo Besenreuther, SIT-Heroldstatt

Zur Person

Udo Besenreuther

- verheiratet, 3 Kinder
- Dipl. Ing. Fahrzeugbau
- Tätig als **IT-System-Architekt** und IT-Projektmanager eines weltweiten Internet-Datenportals (Business to Business, 24/7-Betrieb)
- **DSGVO-KnowHow** wegen der Tätigkeit als Datenschutzbeauftragter für Kirche und Jugendarbeit
- Tätig in der lokalen Seniorenarbeit **SIT-Heroldstatt** und engagiert in mehreren Vereinen.
- KSR Alb-Donau-Kreis,
  Koordinator **Digitalpakt Alb-Donau-Kreis**
- Stv. Vorstand des **Netzwerk-sii-BW**.

SIT

Programm

Netzwerk sii Baden-Württemberg

- Chaos Computer Club
- Bahn Mining
- Security Nightmares
- Schwachstellen finden
- Ransomeware
- Hirne Hacken – Verhandlungen mit Erpressern
- Tonie – Reverse Engineering
- Telematik Infrastruktur
- Sicherheit in Gesundheitsapps
- Elektroniesche Patientenakte
- Blick ins neuronale Netz
- Wie baut man ein U-Boot
- Olaf Scholz für AfD-Verbot
- Cyber-Astrologie und KI-Karma

SIT

ChaosComputerClub

Netzwerk sii Baden-Württemberg

Homepage

- https://www.ccc.de/

Aufzeichnungen

- https://media.ccc.de/c/37c3

Streamed Sessions

- https://streaming.media.ccc.de/37c3/

Self-organized Sessions

- https://events.ccc.de/congress/2023/hub/de/sos/

Event Blog

- https://events.ccc.de/category/37c3/

Bahn Mining

Bahn Mining – Pünktlichkeit ist eine Zier

- Referent: David Kriesel
- Inhalt: Analyse der Bahnpünktlichkeit
  https://www.youtube.com/watch?v=0rb9CfOvojk

Scurity Nightmares

Security Nightmares

- Referentin: ron und frank
- Inhalt: Talk über sicherheitsrelevante IT-Themen
  https://media.ccc.de/v/37c3-12224-security_nightmares#t=154
  https://youtu.be/EHGfbqhbXCU?si=-FXfwNG6PWvjh1mR

Schwachstellen finden

Schwachstellen finden in Geräten, die mit dem Internet verbunden sind (englisch)

- Referentin: Christoph Wolff & Pascal Zenker
- Inhalt: Einführungskurs in Hardwareanalyse
  https://media.ccc.de/v/37c3-11919-finding_vulnerabilities_in_internet-connected_devices

SIT

Schwachstellen finden

Netzwerk sii Baden-Württemberg

Poly Develops Video and Voice Communication Devices

Trio 8800

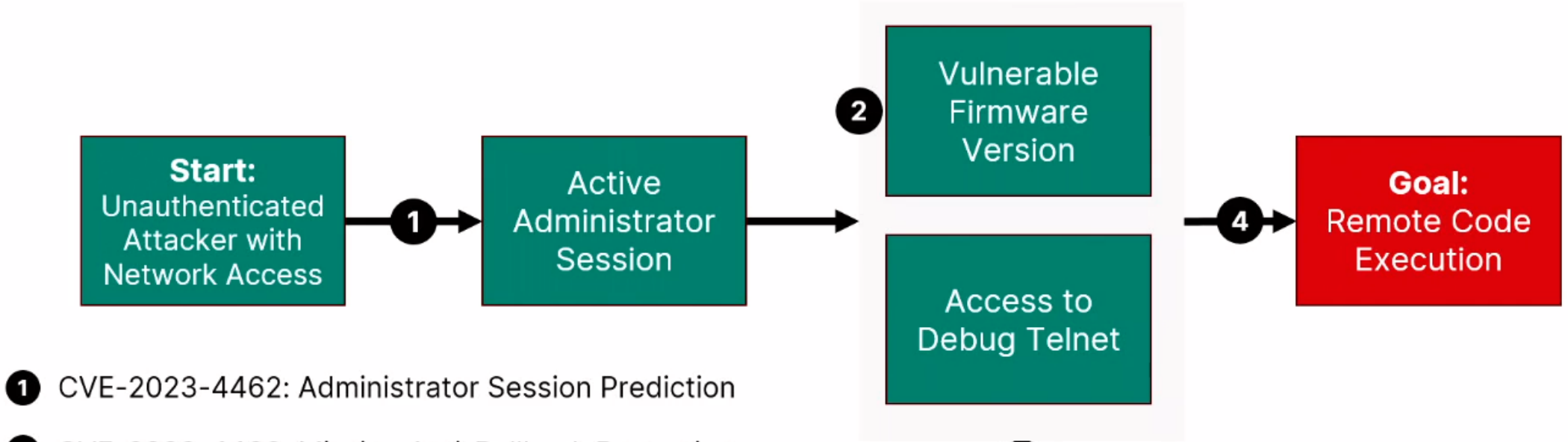
CCX 400

SIT

Schwachstellen finden

Netzwerk sii Baden-Württemberg

Showing Impact by Chaining Vulnerabilities



1. CVE-2023-4462: Administrator Session Prediction
2. CVE-2023-4466: Missing Anti-Rollback Protection
3. CVE-2023-4465: Unverified Password Change
4. CVE-2023-4464: Command Injection

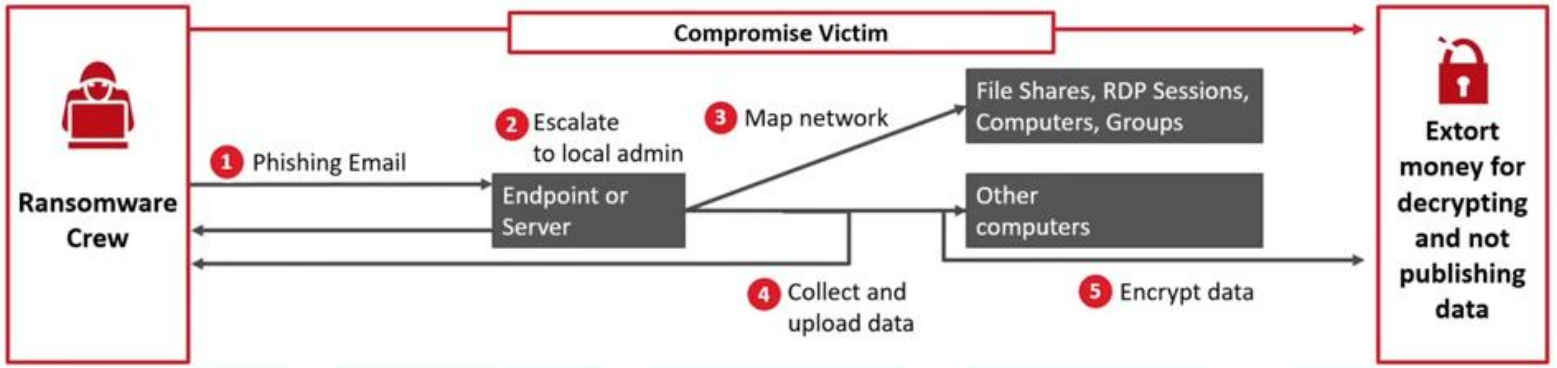
Ransomware

Randsomware: Technik dahinter und Schutz davor (englisch)

- Referentin: Tobias Müller
- Erläutert Grundlagen zu Ransomware
- Ggf. können die Daten entschlüsselt werden
- Wie man richtiges Backup macht und es testet.

https://media.ccc.de/v/37c3-11903-unlocked_recovering_files_taken_hostage_by_ransomware#t=569

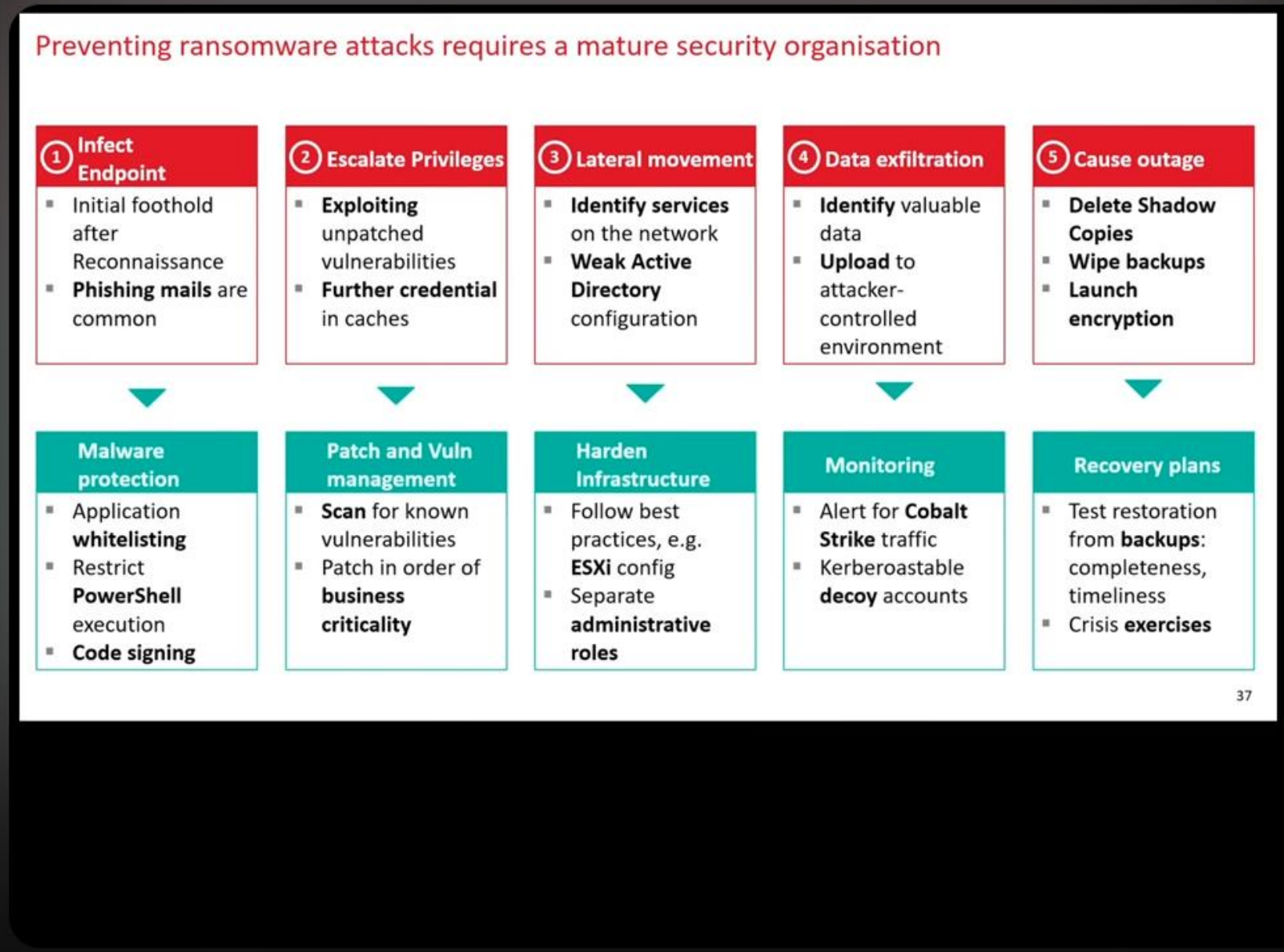
Recall: Ransomware attacks typically follow a well-known pattern



1 Infect Endpoint	2 Escalate Privileges	3 Lateral movement	4 Data exfiltration	5 Cause outage
▪ Initial foothold after Reconnaissance ▪ **Phishing mails** are common	▪ **Exploiting** unpatched vulnerabilities ▪ **Further credential** in caches	▪ **Identify services** on the network ▪ **Weak Active Directory** configuration	▪ **Identify** valuable data ▪ **Upload** to attacker-controlled environment	▪ **Delete Shadow Copies** ▪ **Wipe backups** ▪ **Launch encryption**

35

37C3 - Unlocked! Recovering files taken hostage by ransomware


Preventing ransomware attacks requires a mature security organisation
1 Infect Endpoint
Initial foothold after Reconnaissance
Phishing mails are common
2 Escalate Privileges
Exploiting unpatched vulnerabilities
Further credential in caches
3 Lateral movement
Identify services on the network
Weak Active Directory configuration
4 Data exfiltration
Identify valuable data
Upload to attacker-controlled environment
5 Cause outage
Delete Shadow Copies
Wipe backups
Launch encryption
Malware protection
Application whitelisting
Restrict PowerShell execution
Code signing
Patch and Vuln management
Scan for known vulnerabilities
Patch in order of business criticality
Harden Infrastructure
Follow best practices, e.g. ESXi config
Separate administrative roles
Monitoring
Alert for Cobalt Strike traffic
Kerberoastable decoy accounts
Recovery plans
Test restoration from backups: completeness, timeliness
Crisis exercises
37

We described ransomware threats, our Black Basta decryption technique, and how to prevent ransomware

Ransomware Threats

- Remains a **severe threat**
- Causes **billions** in damage
- Run as **organised** crime
- Black Basta is **very active** in Germany

Decrypting Files

- **Re-use of the ChaCha keystream** weakens Black Basta's encryption
- **64 byte of plaintext** required
- **Decryption tools** are provided here: https://github.com/srlabs/black-basta-buster

Preventing Ransomware

- **The next ransomware will come**, do not rest assured with the decryptor, prepare your organisation now!
- **Backup!**
- **Prioritised recovery plan** with documented dependencies of business-critical apps and infrastructure

Dr. Tobias Mueller

- **Cryptographer** by training
- **Information Security** and **Privacy professional** during the day
- Free- and **Open-Source** Software Hacker by night

Send (**Linux**) samples, intelligence about other **Ex-Conti** groups:
tobias@srlabs.de 18D5 15FC 880A 446D 6E6A 6EF0 ABA1 BBE7 BBAF AE69

- Unlocked! Recovering files taken hostage by ransomware

Hirne Hacken: Hackback

Hirne Hacken: Hackback Edition

- Referentin: Linus Neumann und Kai Biermann
- Inhalt: Bericht aus den Verhandlungen mit Erpressern
  https://media.ccc.de/v/37c3-12134-hirne_hacken_hackback_edition#t=0

SIT

Toniebox Reverse Engineering

Netzwerk sii Baden-Württemberg

Toniebox Reverse Engineering

- Referentin: g3gg0, 0xbadbee, Moritz and Gambrius
- Inhalt: Kinderspielzeug, nicht nur für Kinder
  https://media.ccc.de/v/37c3-12134-hirne_hacken_hackback_edition#t=0

SIT

Telematik Infrastruktur

Netzwerk sii Baden-Württemberg

15 Jahre deutsche Telematikinfrastruktur (TI)

Die Realität beim Arztbesuch nach 15 Jahren Entwicklung einer medizinischen Digitalstrategie

Christoph Saatjohann

15 Jahre Telematik Infrastruktur

- Referentin: Christoph Saatjohann
- Inhalt: Überblick über die Telematik Infrastruktur (Stand 2019)
  https://media.ccc.de/v/36c3-10895-15_jahre_deutsche_telematikinfrastruktur_ti

SIT

Sicherheit Gesundheitsapps

Netzwerk sii Baden-Württemberg

All Your Gesundheitsakten Are Belong To Us

"So sicher wie beim Online-Banking": Die elektronische Patientenakte kommt - für alle.

Martin Tschirsich

REFRESHING :MEMORIES

Einführung der elektronischen Patientenakte (Stand 2018)

- Referentin: Martin Tschirsich
- Inhalt: Sicherheitsthemen rund um die verschiedenen Gesundheitanwendungen https://media.ccc.de/v/35c3-9992-all_your_gesundheitsakten_are_belong_to_us#t=77

SIT

Elektronische Patientenakte

Netzwerk sii Baden-Württemberg

"Hacker hin oder her": Die elektronische Patientenakte kommt!

Martin Tschirsich, cbro - Dr. med. Christian Brodowski and Dr. André Zilch

Hacker hin oder her, die elektronische Patientenakte kommt (2019)

- Referentin: Martin Tschirsich, Dr. med. Christian Brodowski, Dr. André Zilch
- Inhalt: Sicherheitsthemen zur elektronischen Patientenakte
  https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt

Blick ins neuronale Netz

Blick ins neuronale Netz?

- Referentin: … Informatikerin
- Inhalt:
  Einfacher Einblick

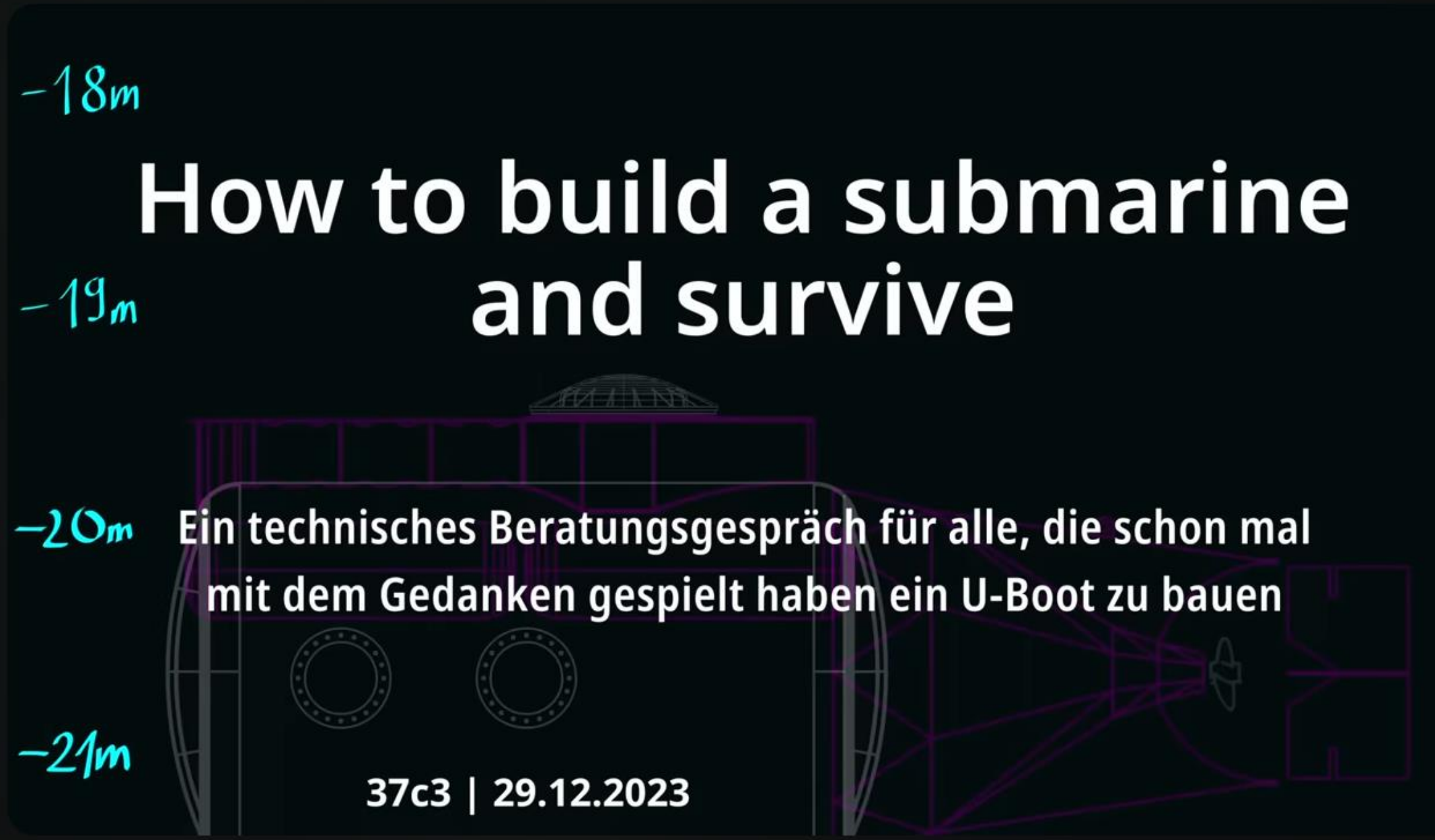
https://media.ccc.de/v/37c3-11784-lass_mal_das_innere_eines_neuronalen_netzes_ansehen

Wie baut man ein U-Boot baut

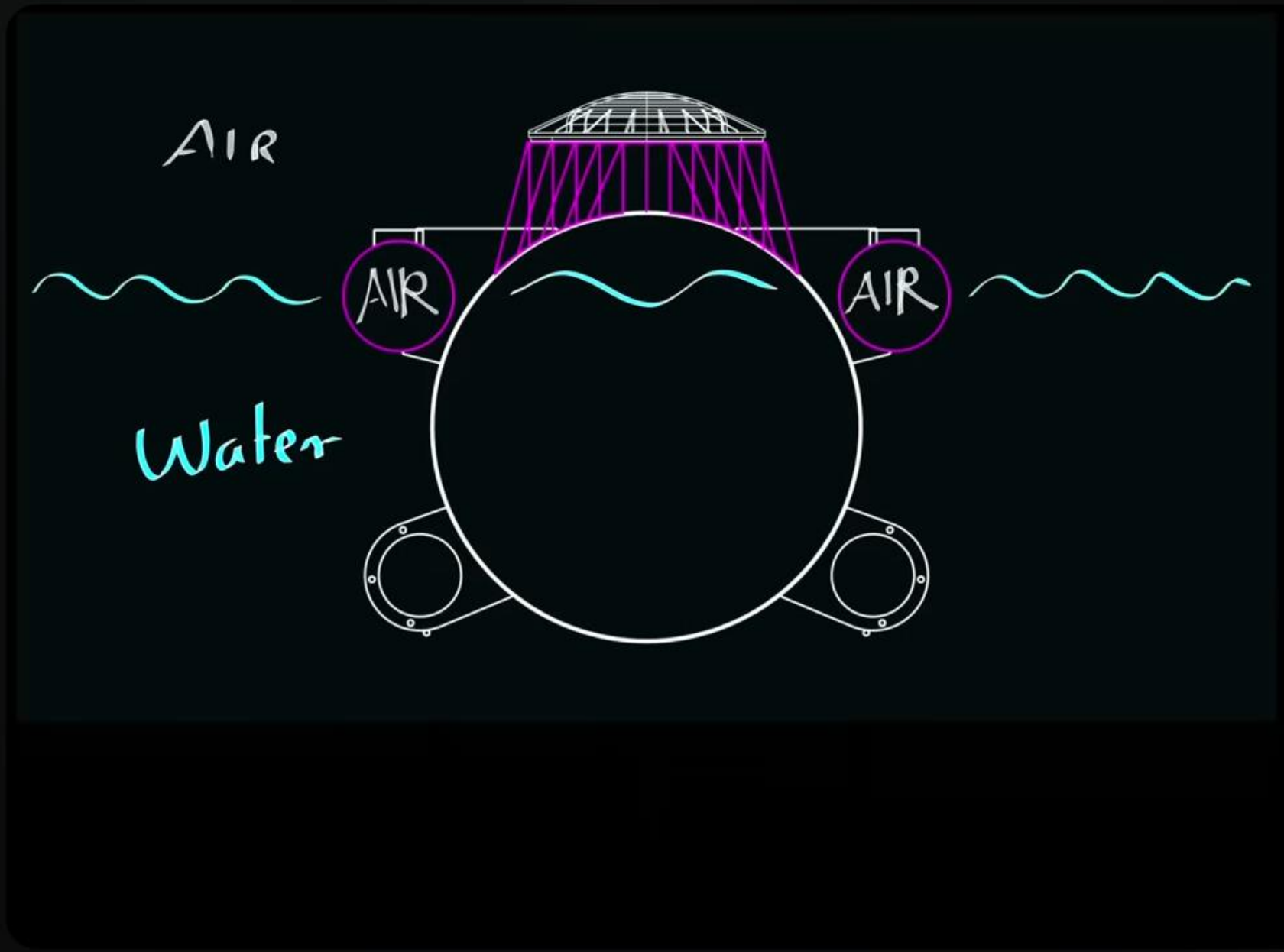
How to build a submarine and survive

- Referent: Elias, Theateringeneur, und Nico, Seenotrettung
- Inhalt: DIY U-Boot bauen

https://media.ccc.de/v/37c3-11828-how_to_build_a_submarine_and_survive



37C3 - How to build a submarine and survive (deu)



37C3 - How to build a submarine and survive (deu)

- How to build a submarine and survive (deu)

C3 - How to build a submarine and survive (deu)

mail:

uboot@tiefenruder.de

blog:

tiefenruder.de

film:

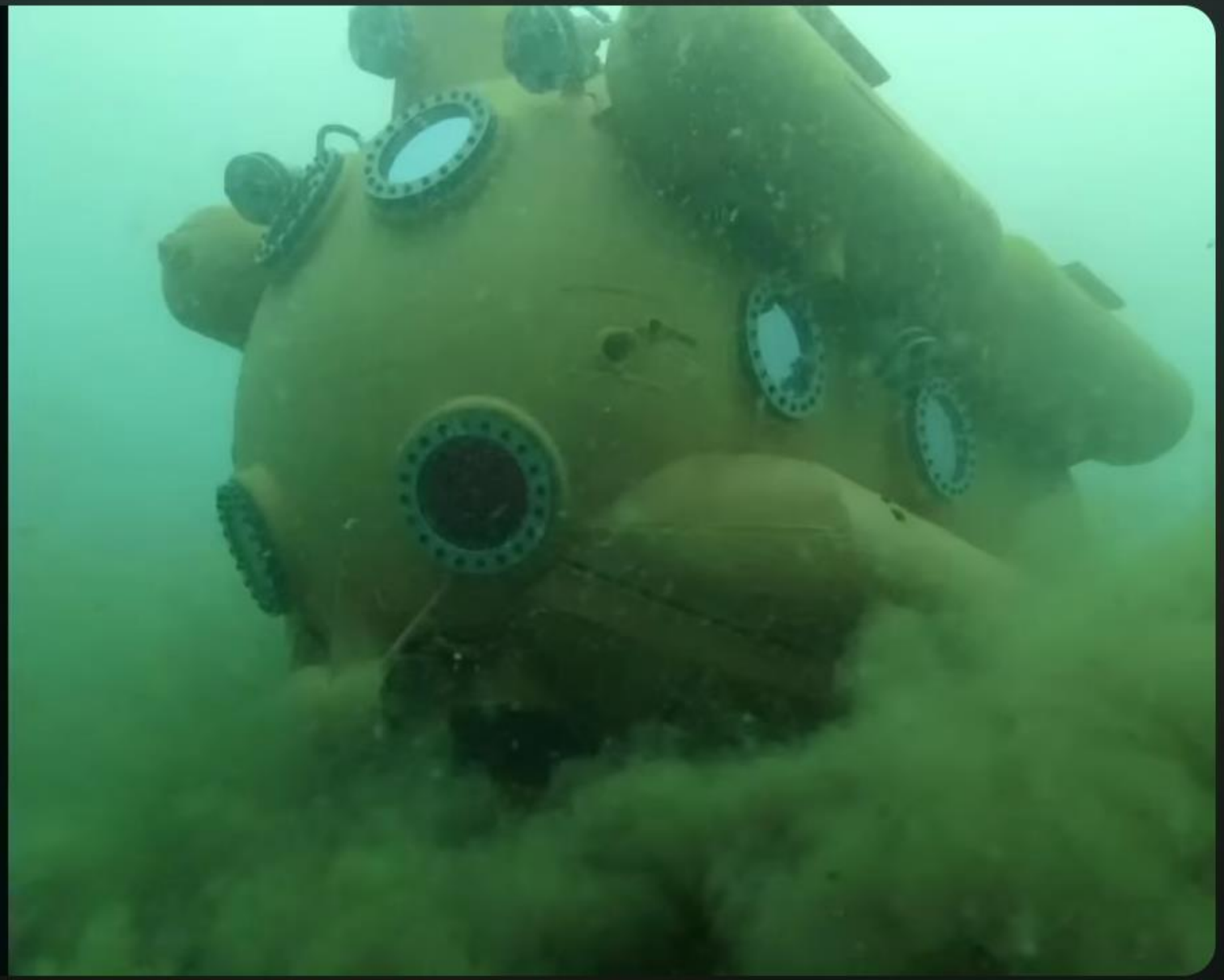
traumtaucher-film.de

Credits

photos:

Selene Magnolia

selenemagnolia.com



- How to build a submarine and survive (deu)

SIT.

Olaf Scholz für AfD-Verbot

Netzwerk sii Baden-Württemberg

- Zentrum für politische Schönheit

https://media.ccc.de/v/37c3-12345-scholz_greift_durch_die_afd_wird_verboten_-_deepfakes_auch#t=1053

Von Zebrastreifen und offenen Daten

https://media.ccc.de/v/37c3-11983-von_zebrastreifen_offenen_daten_und_verschlossenen_verwaltungen

- torben, SaaS Produktentwickler und fedus, Entwickler – Finanzsoftware
- Luxenburg
- ZUG – Zentrum für urbane Gerechtigkeit

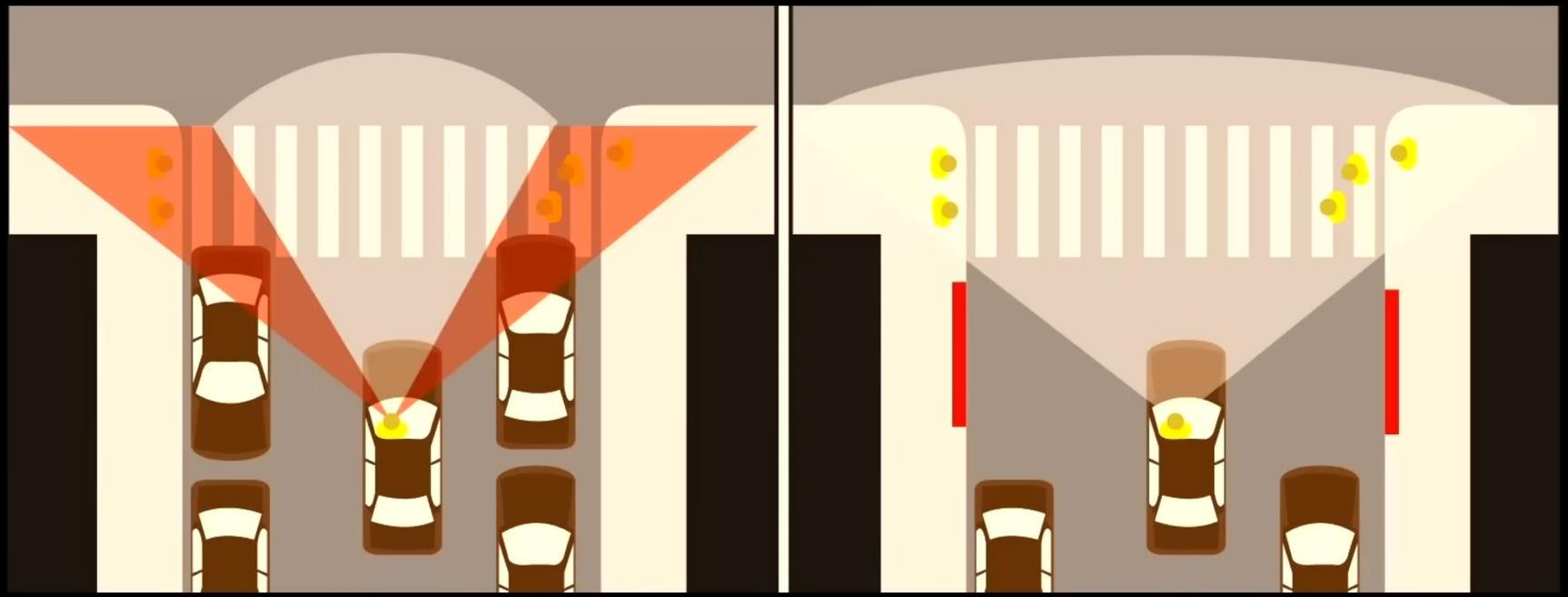
- Sie nehmen sich des Problems an, dass Parkplätze bis zum Zebrastreifen gehen und der Sicherheitsabstand nicht eingehalten wird.
- Fußgänger (insbes. Kinder) sind dadurch gefährdet.

Gesehen werden.

4

Quelle: Zentrum fir Urban Gerechteskeet a.s.b.l.

Warum ist das Gesetz wichtig? 6



Quelle: San Francisco Municipal Transportation Agency (SFMTA)

Von Zebrastreifen und offenen Daten

- In der Meldedatenbank der Stadtverwaltung wird sichtbar, dass dieses Problem schon mehrfach gemeldet wurde.
  Aber nie gab es eine Antwort.

- Die Referenten haben dann über Geoportale die Zebrastreifen erfasst.

Hallo, Tinder

14

37C3 28.12.2023

37C3 UNLOCKED

Von Zebrastreifen und offenen Daten

- In der Meldedatenbank der Stadtverwaltung wird sichtbar, dass dieses Problem schon mehrfach gemeldet wurde.
  Aber nie gab es eine Antwort.

- Die Referenten haben dann über Geoportale die Zebrastreifen erfasst.

- Dann wurde eine App erstellt, mit welcher Bürger die verschiedenen Zebrastreifen bewertet haben.
- Von 1787 Zebrastreifen war OK
  475 sind gesetzeswidrig
  162 sind unklar

21

Safe Crossing

2023: MISSING CROSSWALKS | 2021: UNSAFE CROSSWALKS

Unsafe crosswalks

Uses aerial imagery from 2020.

This is the original "Safe Crossing" project, crowd-sourced and released in 2021.

The map shows dangerous pedestrian crossings in Luxembourg-City. They are dangerous because designated parking spots (including bus stops) are located less than 5 metres away from them. This reduces drivers' visibility of the crosswalk and the people using it, putting them in unnecessary danger. In fact, setting up parking spots so close to crosswalks is also in violation of the Highway Code ("Code de la route").

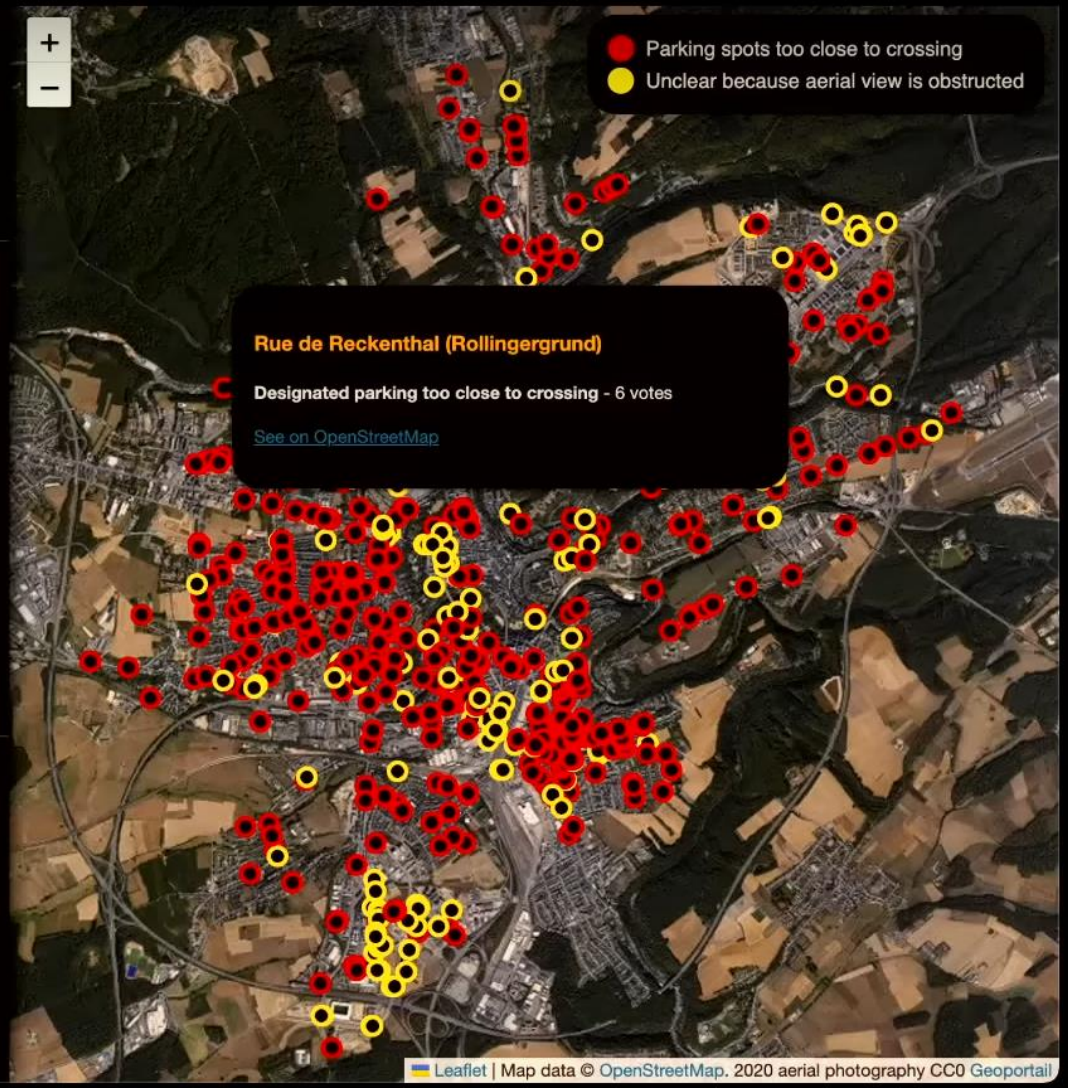
How to read the map

Red and orange dots mark the relevant crossings:

Red (475 crossings, 27%): Dangerous crosswalk due to illegal parking spots nearby

Yellow (162 crossings, 9%): Unable to determine whether the crosswalk is dangerous

Safe crosswalks which are not affected by dangerously close parking spots are not shown on the map (1150



37C3 28.12.2023

Quelle: ZUG a.s.b.l.

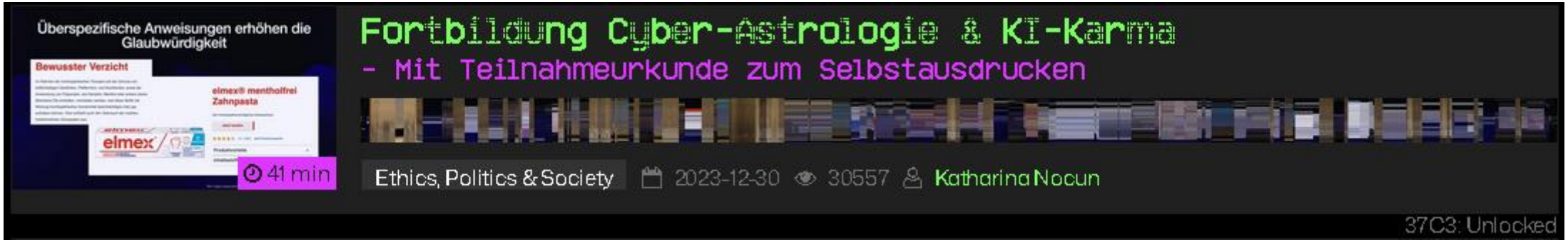
10:57 / 36:37

Von Zebrastreifen und offenen Daten

- Die Referenten haben das Projekt dokumentiert und bekam viel öffentliche Presse. (2021)
- Die Verwaltung reagierte nicht.
- Nach einer Gemeinderatssitzung reagierte die Stadtverwaltung mit der Aussage, dass die Daten falsch sind. Nur 32 müssen genauer analysiert werden.
- Die Herausgabe der zugrunde liegenden Informationen lehnt die Stadt ab. Auch bei einer ‚Frag den Staat-Anfrage‘
- Aktuell (8.2024) kommt es zu einer Gerichtsverhandlung.

SIT. Cyber-Astrologie & KI-Karma

Netzwerk sii Baden-Württemberg



- **Fortbildung Cyber-Astrologie & KI-Karma**

https://media.ccc.de/v/37c3-12019-fortbildung_cyber-astrologie_ki-karma#t=34

SIT

Netzwerk sii Baden-Württemberg

Herzlichen Dank!

Bleibt neugierig und engagiert!