IT-Sicherheit und digitale Kompetenzen – Von der Ausbildung bis zum täglichen Geschäft

3. Digitalkonferenz des Landkreises Vorpommern-Greifswald

Gemeinsame Regionalkonferenz mit dem

Digitalen Innovationszentrum Greifswald

Anklam, 30. November 2023

Kofinanziert von der Europäischen Union

MV tut gut.

WITENO

digitales MV

Gefördert durch:

Bundesministerium für Ernährung und Landwirtschaft

aufgrund eines Beschlusses des Deutschen Bundestages

LANDKREIS VORPOMMERN-GREIFSWALD

Herzlich Willkommen!

- Joanna Hüffelmann, Prognos AG
- Matthias Canzler, Prognos AG

Agenda

"Die unsichtbare Gefahr: Wie öffentliche Einrichtungen sich vor Cyberangriffen schützen können" - Katharina Clausohm & Stefan Otto (Clausohm-Software GmbH)

Next Gen Education – Aus-und Weiterbildung für eine sichere Zukunft - Radosław Chinalski (Akademie der angewandten Wissenschaften Wałcz)

Digitalisierung und Sozialstrukturwandel - Darinka Kriegel (Hochschule Neubrandenburg)

Netzwerk bei kleinem Imbiss

Agenda

„Die qualifizierenden Vier“ - Ellen Grull (IHK Neubrandenburg)

IT-Sicherheit und digitale Kompetenzen - Danis Kotliarov, Kai Düwell, Roberto Krämer (Weber Maschinenbau GmbH Neubrandenburg)

Sicherheit durch Medienkompetenz – Pro. Dr. Ines Sura (Universität Greifswald)

Ausblick

Jörg Hasselmann

Beigeordneter und 1. Stellvertreter des Landrates
Landkreis Vorpommern-Greifswald

Dr. Wolfgang Blank

Geschäftsführer Witeno GmbH
Präsident IHK Neubrandenburg

Tweedback Umfrage

https://tweedback.de/znds

Session-ID: znds

Stefan Otto

Clausohm-Software GmbH

cyber security by clausohm

Cyber Security

Einstieg, Beispiele & Vorgehensweisen

CLAUSOHM. Software++ Automation

Die Clausohm-Software GmbH entwickelt innovative und intelligente IT Lösungen, die Grenzen überwinden und es den Individuen und Organisationen erlauben, ihr Potential frei zu entfalten.

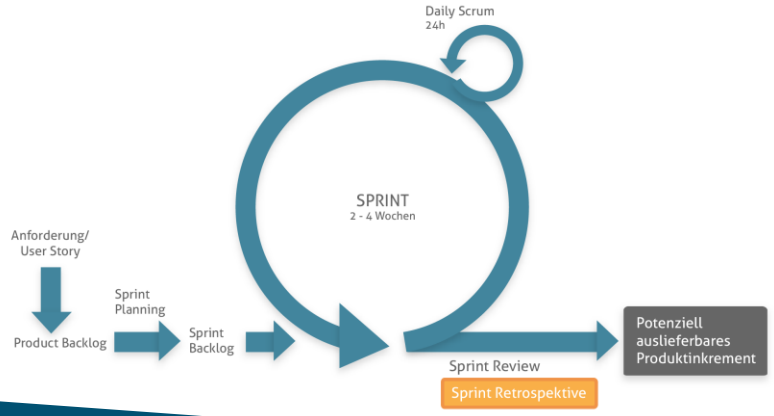
CLAUSOHM. Software++ Automation

Software Engineering

Die Clausohm-Software GmbH ist Ihr Partner für Datenbankentwicklung, die Abbildung von Geschäftsprozessen und E-Commerce

Software-Entwicklung

- ✓ Datenbankentwicklung SQL
- ✓ Backend + Frontendprogrammierung (Ajax, Java, JavaScript, C++, VisualBasic, JSON API und Html 5)
- ✓ Webprogrammierung + Mobile, RAP, GWT
- ✓ Schnittstellenmanagement

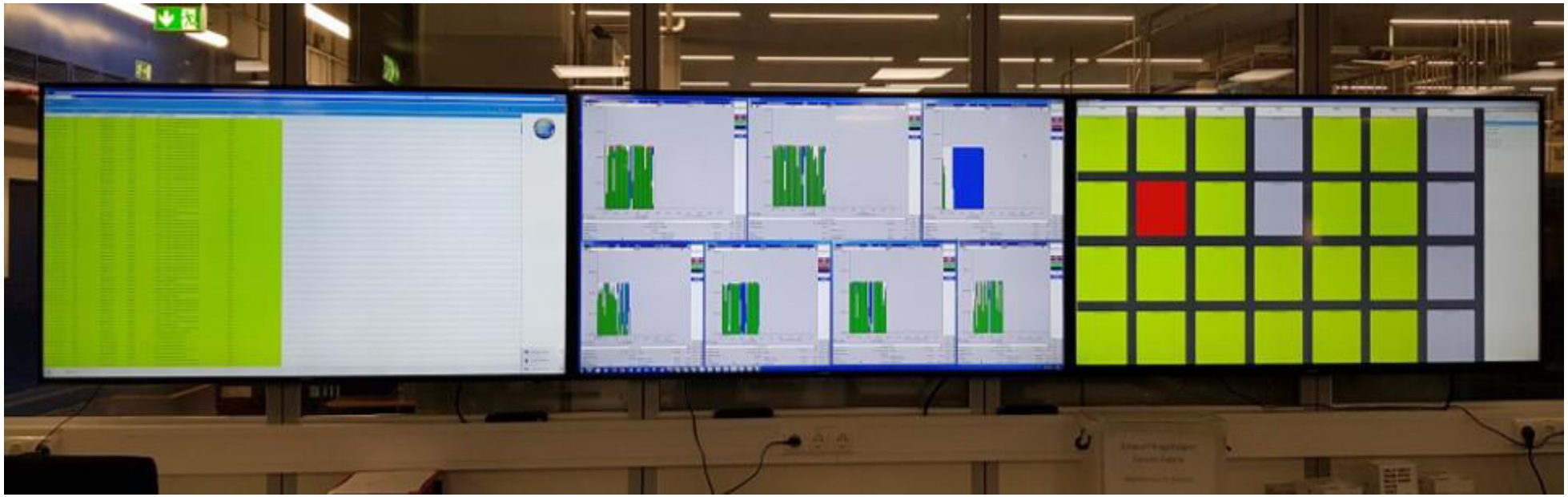


Software Qualitätssicherung

- ✓ Testplanung und Steuerung - Beratung bei der Auswahl der optimal auf Sie passenden Methoden und Leistungen konzeptionelle und operative Umsetzung im Software Testing
- ✓ Testanalyse und Testdesign - funktionale Test, Testautomatisierung, Komponententest, Integrationstest, Systemtest, Regressionstest
- ✓ Testrealisierung und Testdurchführung
- ✓ Testauswertung und Bericht

CLAUSOHM. Software++ Automation

Automation



CIRCLE

CIRCLE ist ein verlässliches Informationssystem zur Optimierung von Produktionsabläufen.

CIRCLE überwacht, steuert und wertet Ihre Maschinen-, Prozess- und Produktdaten
in der industriellen Industrie aus.
Damit ermöglicht Ihnen unsere Software zu jeder Zeit eine vollständige Übersicht über
komplexe Produktionsschritte und produktionslinienübergreifende Daten.

Cyber Security

Continuous Protection

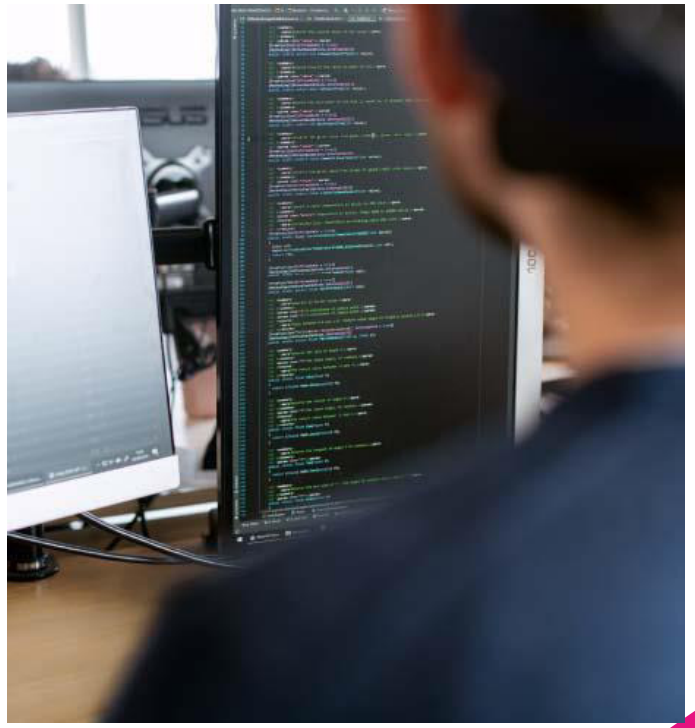
- Penetrationstests und Schwachstellenanalysen
- Externes Monitoring as a Service
- Internes Monitoring as a Service
- IT-Beratung

Sicherheitsüberprüfung / Red Teaming

- gezielte Angriffsversuche ohne vorherige Informationen auf die IT-Infrastruktur
- direkte Angriffsversuche über Social Engineering für den Datenzugriff über Mitarbeiterinformationen
- Physische Gefährdungsbeurteilungen von Objekten

Continuous Awareness

- Phishing Mailkampagnen
- Schulungsmaßnahmen und Einsatz AWAP Lernplattform



I Herausforderungen

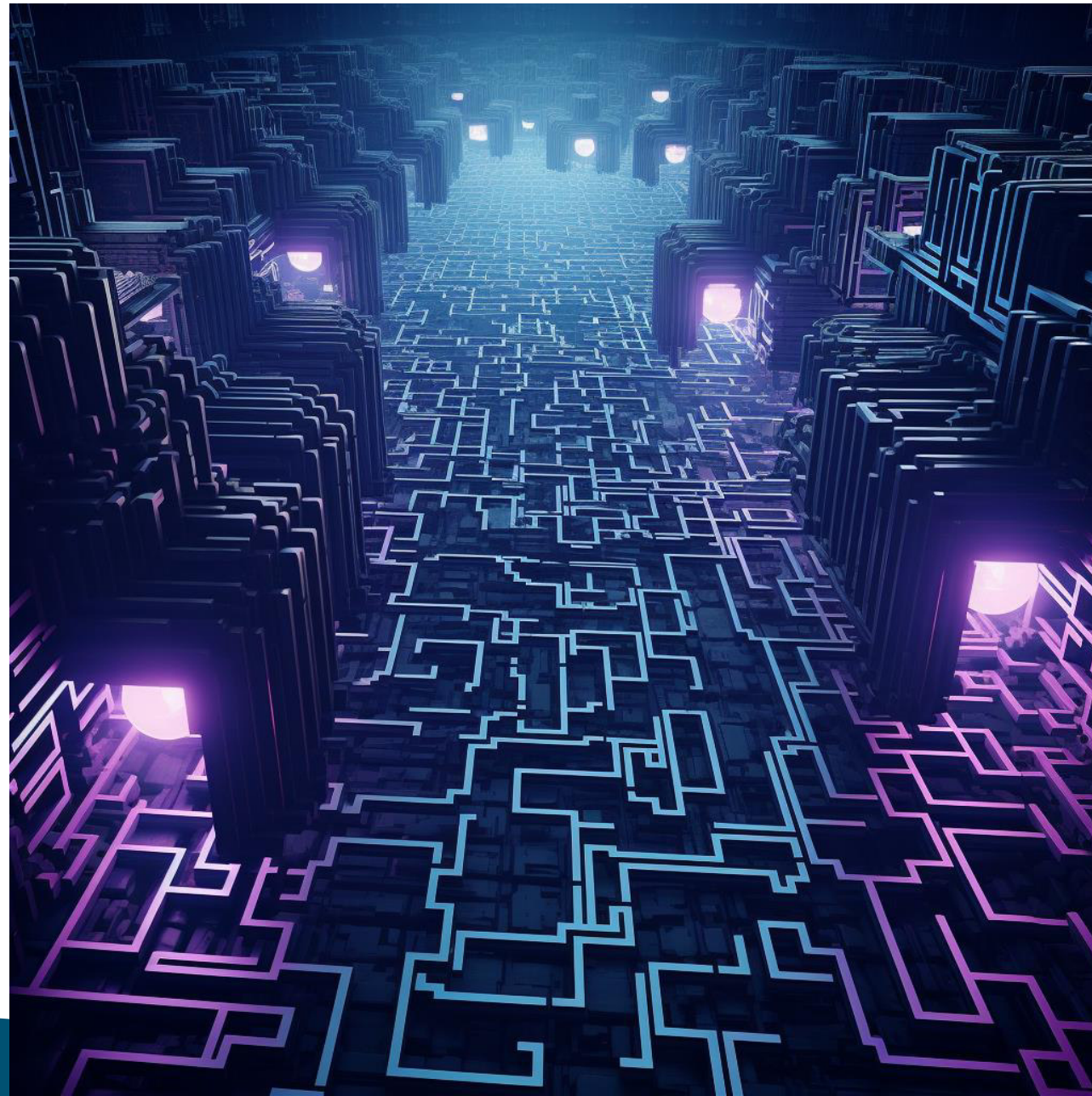
Herausforderungen

- Schutz des gesamten IT-Netzwerks
- Verwaltung von Updates
- Datensicherungen
- Sensibilisierung der MitarbeiterInnen
- Notfallmanagement
- IT Security Management

I Vorteile

Informationssicherheit

- Mitarbeiter fühlen sich als wichtiger Partner für die Informationssicherheit wertgeschätzt
- Wettbewerbsvorteile durch das gewonnene Vertrauen von Kunden und Geschäftspartnern
- Arbeiten an IT-Systemen verlaufen planbarer (Ausfallzeiten,…)



I Bekannte Cyber Angriffe

I Bekannte Cyber Angriffe

Datum	Betroffene	Land	Sicherheitsvorfall
31.08.2023	Bundesamt für Kartographie und Geodäsie	DE	Chinesische Hacker infiltrieren Netzwerk von Bundesbehörde. » Details
18.08.2023	Regierung von Mecklenburg-Vorpommern	DE	Hacker attackieren Regierungsorganisationen. » Details
16.08.2023	Jodel	DE	Daten von Nutzern von Social-Media-App bei Cyberangriff erlangt. » Details
11.08.2023	Münchner Verlagsgruppe	DE	Ransomware-Angriff legt IT-Infrastruktur lahm. » Details
11.08.2023	S-Bahn Hannover	DE	Webseite von Verkehrsbetrieben fällt nach Cyberangriff aus. » Details
07.08.2023	EcoReporter	DE	Unternehmen erneut Ziel von Cyberkriminellen. » Details
03.08.2023	Trinkwasserverband Stader Land	DE	Ransomwaregruppe LockBit greift Trinkwasserverband an. » Details
01.08.2023	EcoReporter	DE	Inhalte von Finanzmagazin nach Cyberangriff nicht zugänglich. » Details
22.07.2023	Forteil GmbH	DE	Schwachstelle in der Schufa-App Bonify erlaubt Zugriff auf fremde Bonitätsdaten. » Details

https://www.dsgvo-portal.de/sicherheitsvorfall-datenbank/

I Bekannte Cyber Angriffe

Cyberkriminelle legen Rathäuser lahm

Staatsanwaltschaft ermittelt: Hacker-Angriff auf elf Kommunen im Kreis Neu-Ulm

Stand: 24.11.2023, 15:08 Uhr
Von Peter Köpple

Teilen:

Ein Hackerangriff hat die Computersysteme in insgesamt elf Gemeindeverwaltungen im Kreis Neu-Ulm lahmgelegt. "Die Auswirkungen sind immens", sagt der Roggenburger Bürgermeister.

Dateien seien umbenannt und verschlüsselt worden. Die Art der Verschlüsselung deutete auf einen Angriff hin. Das bestätigten sowohl das "Bayerische Landeskriminalamt" als auch das "Landesamt für Sicherheit in der Informationstechnik". Die Cyberkriminellen fordern ein Lösegeld. Der Verbandsvorsitzende Stölzle im SWR: "Wir haben eine Textdatei gefunden, die zur Kontaktaufnahme auffordert, um Lösegeldverhandlungen anzugehen." Dies werde man jedoch nicht tun.

"Wir haben zum Beispiel keinen Zugriff mehr auf die Meldeamtsdaten", berichtet Mathias Stölzle, Bürgermeister von Roggenburg und zugleich Vorsitzender des Zweckverbands gemeindliche Datenverarbeitung im Landkreis Neu-Ulm. Seit Dienstagabend sind Anmeldungen, Ummeldungen und das Beantragen von Pässen nicht mehr möglich. Außerdem funktioniert nach Angaben von Stölzle das gesamte Rechnungswesen nicht mehr. Man habe keinen Zugriff mehr auf Haushaltsplanungen, Kassensysteme und Bezahlvorgänge. Zudem sei noch die Friedhofsverwaltung lahmgelegt.

https://www.swr.de/swraktuell/baden-wuerttemberg/ulm/hackerangriff-cyberangriff-neu-ulm-elf-kommunen-roggenburg-100.html

I Bekannte Cyber Angriffe

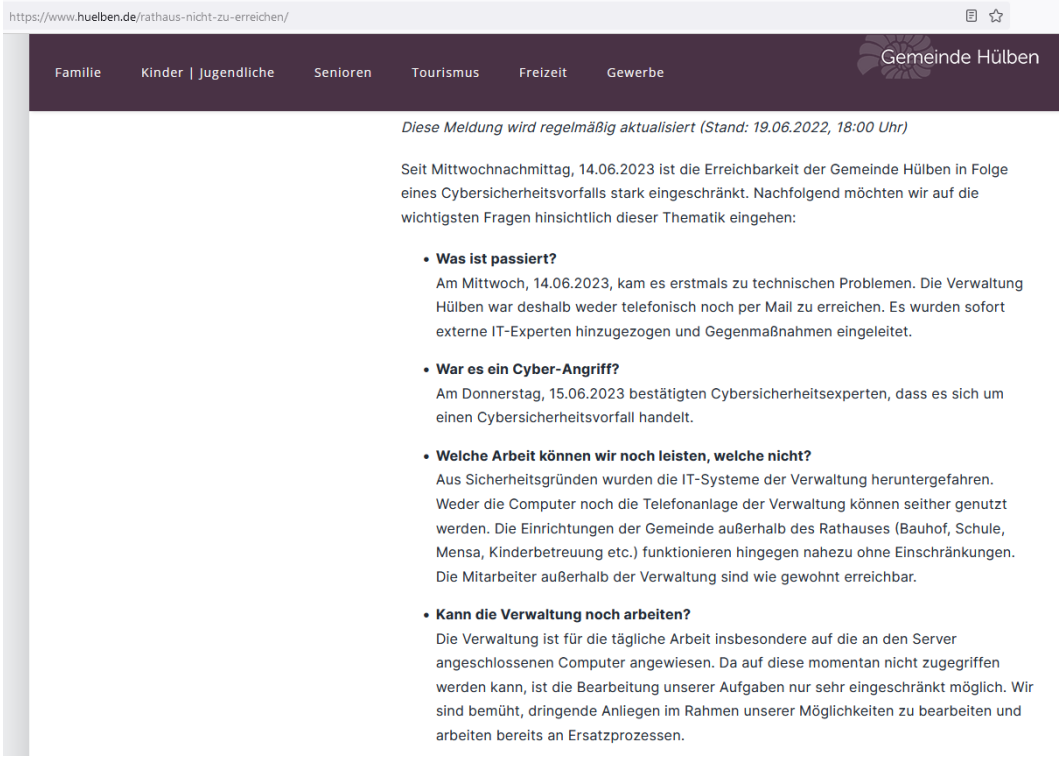
Landratsamt Ludwigsburg startet am Montag wieder in den Teilbetrieb

Das Landratsamt Ludwigsburg wird nach dem Sicherheitsvorfall ab Montag, 15.05.23 wieder in den Teilbetrieb starten. Zunächst werden die vorab definierten priorisierten Bereiche wieder an das Netz genommen. Folgende Dienstleistungen können ab Montag wieder angeboten werden: KFZ-Zulassung und Führerscheinstelle, Asylleistungen, Leistungsgewährung des Jobcenters, Grundsicherung, Teile des Jugendamts, Wohngeld, die Eingliederungshilfe und die Kreiskasse.

https://www.landkreis-ludwigsburg.de/de/landratsamt-landkreis/aktuelles/pressemitteilungen/detail/landratsamt-ludwigsburg-startet-am-montag-wieder-in-den-teilbetrieb/

https://www.alzey.de/de/aktuelles/meldungen/2023/Rathaus-offline20230831.php

I Bekannte Cyber Angriffe



https://www.huelben.de/rathaus-nicht-zu-erreichen/

Familie | Kinder | Jugendliche | Senioren | Tourismus | Freizeit | Gewerbe | Gemeinde Hülben

Diese Meldung wird regelmäßig aktualisiert (Stand: 19.06.2022, 18:00 Uhr)

Seit Mittwochnachmittag, 14.06.2023 ist die Erreichbarkeit der Gemeinde Hülben in Folge eines Cybersicherheitsvorfalls stark eingeschränkt. Nachfolgend möchten wir auf die wichtigsten Fragen hinsichtlich dieser Thematik eingehen:

- **Was ist passiert?**
  Am Mittwoch, 14.06.2023, kam es erstmals zu technischen Problemen. Die Verwaltung Hülben war deshalb weder telefonisch noch per Mail zu erreichen. Es wurden sofort externe IT-Experten hinzugezogen und Gegenmaßnahmen eingeleitet.
- **War es ein Cyber-Angriff?**
  Am Donnerstag, 15.06.2023 bestätigten Cybersicherheitsexperten, dass es sich um einen Cybersicherheitsvorfall handelt.
- **Welche Arbeit können wir noch leisten, welche nicht?**
  Aus Sicherheitsgründen wurden die IT-Systeme der Verwaltung heruntergefahren. Weder die Computer noch die Telefonanlage der Verwaltung können seither genutzt werden. Die Einrichtungen der Gemeinde außerhalb des Rathauses (Bauhof, Schule, Mensa, Kinderbetreuung etc.) funktionieren hingegen nahezu ohne Einschränkungen. Die Mitarbeiter außerhalb der Verwaltung sind wie gewohnt erreichbar.
- **Kann die Verwaltung noch arbeiten?**
  Die Verwaltung ist für die tägliche Arbeit insbesondere auf die an den Server angeschlossenen Computer angewiesen. Da auf diese momentan nicht zugegriffen werden kann, ist die Bearbeitung unserer Aufgaben nur sehr eingeschränkt möglich. Wir sind bemüht, dringende Anliegen im Rahmen unserer Möglichkeiten zu bearbeiten und arbeiten bereits an Ersatzprozessen.

https://www.huelben.de/rathaus-nicht-zu-erreichen/

Cyber-Angriff auf die VG-Verwaltung

Im Laufe der Woche sind Auffälligkeiten auf dem Citrix-Netscaler-System der VG Wörrstadt, die möglicherweise in Zusammenhang mit einer Cyber-Attacke stehen, bekannt geworden.

Umgehend nach Bekanntwerden des Vorfalls sind sämtliche Sicherheitsvorkehrungen getroffen und das kommunale RLP-Netzwerk vorsorglich vom Netzwerk der Verbandsgemeinde Wörrstadt getrennt worden. Einige Fachanwendungen der Verwaltung sind daher zum aktuellen Zeitpunkt nicht funktionsfähig.

Davon betroffen sind unter anderem das **Bürgerbüro**, das **Standesamt**, die **Bußgeldstelle**, und die **Personalabteilung,** weshalb sämtliche **Termine zunächst bis einschließlich Montag, 4. September 2023 storniert** werden müssen.

Die Mitarbeiter der Informationstechnik stehen seit Bekanntwerden des Vorfalls in engem Austausch mit den zuständigen Behörden, IT-Forensikern und Experten der Zentralen Anlaufstelle für Cyberkriminalität (kurz: ZAC) vom LKA. Bislang gibt es keine Hinweise

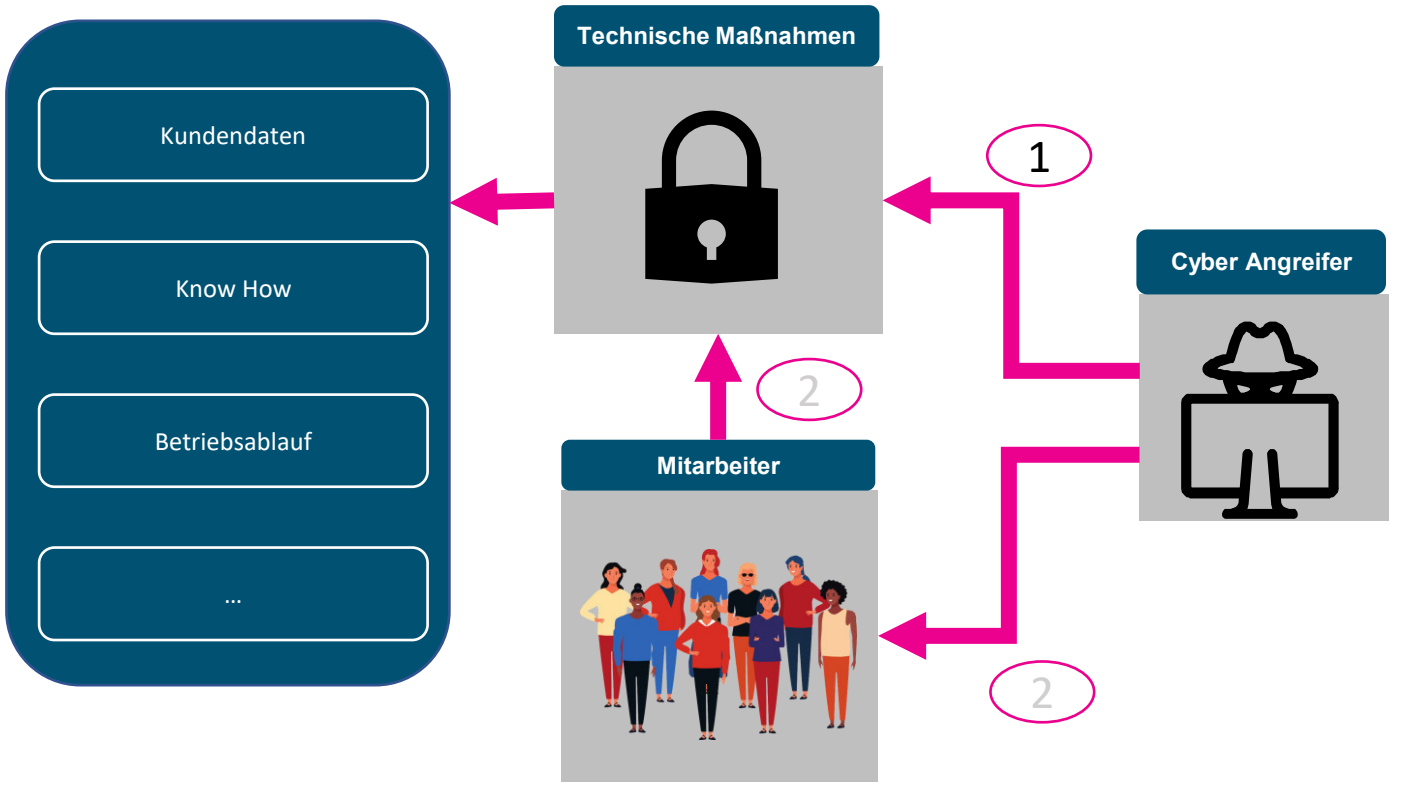
https://www.vgwoerrstadt.de/index.php?object=tx,3629.5.1&ModID=7&FID=3629.818.1

II Angriffsziele

Beschreibung

- Schritt 1
  - Der Cyber Angreifer prüft die Technische Maßnahmen des Unternehmens, ob Schwachstellen für das Eindringen in die IT-Systeme vorhanden und ausgenutzt werden können
- Schritt 2
  - Das Ziel ist weiterhin das Eindringen in die IT-Systeme
  - Der Angreifer startet den Versuch Mitarbeiter zu manipulieren, um die technischen Maßnahmen auszuhebeln bzw. abzuschwächen
  - Dies geschieht z.B. durch den Versand von E-Mails mit Malware oder E-Mails zum Erhalt von Login-Daten der Mitarbeiter

Technische Maßnahmen & MitarbeiterInnen



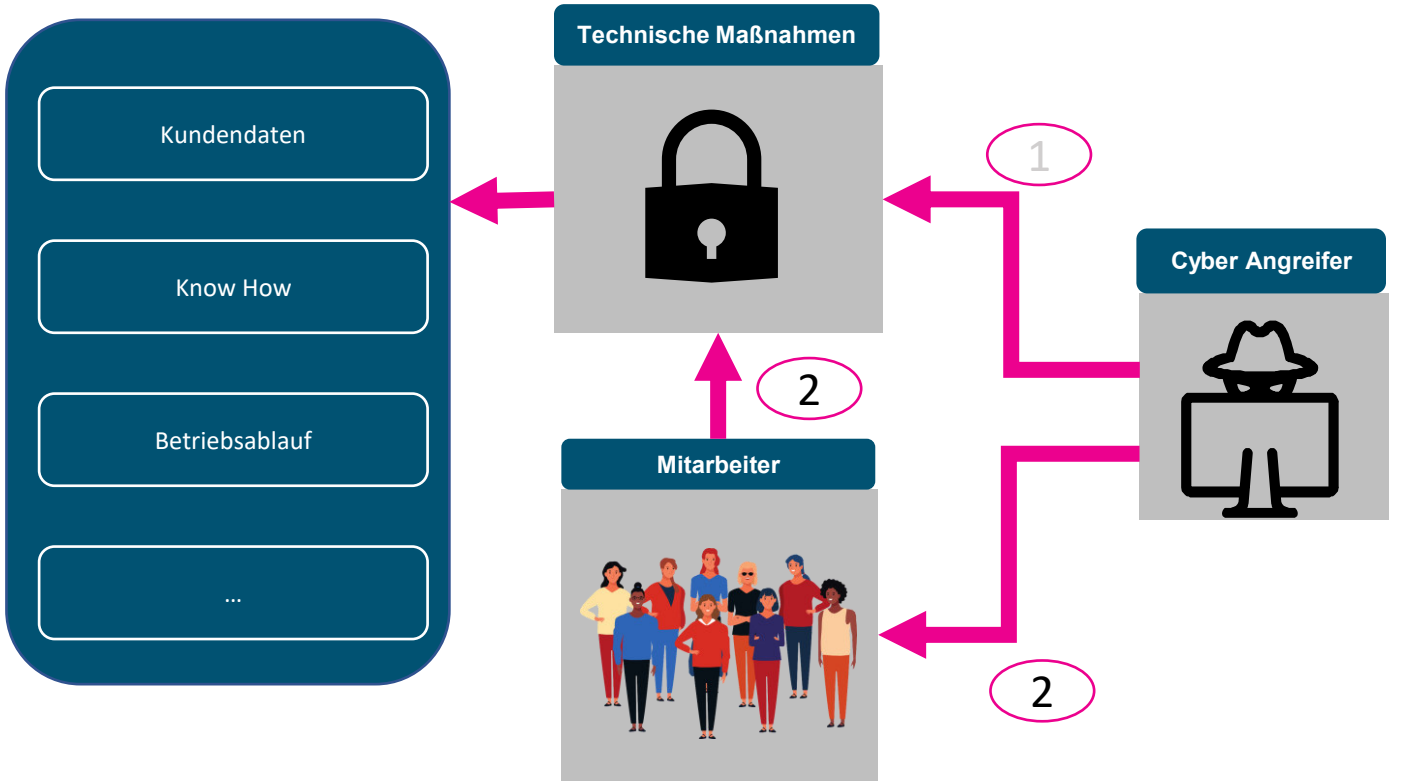
II Angriffsziele

Beschreibung

- Schritt 1
  - Der Cyber Angreifer prüft die Technische Maßnahmen des Unternehmens, ob Schwachstellen für das Eindringen in die IT-Systeme vorhanden und ausgenutzt werden können

- Schritt 2
  - Das Ziel ist weiterhin das Eindringen in die IT-Systeme
  - Der Angreifer startet den Versuch Mitarbeiter zu manipulieren, um die technischen Maßnahmen auszuhebeln bzw. abzuschwächen
  - Dies geschieht z.B. durch den Versand von E-Mails mit Malware oder E-Mails zum Erhalt von Login-Daten der Mitarbeiter

Technische Maßnahmen & MitarbeiterInnen

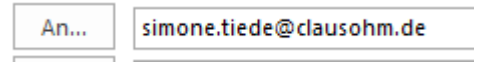


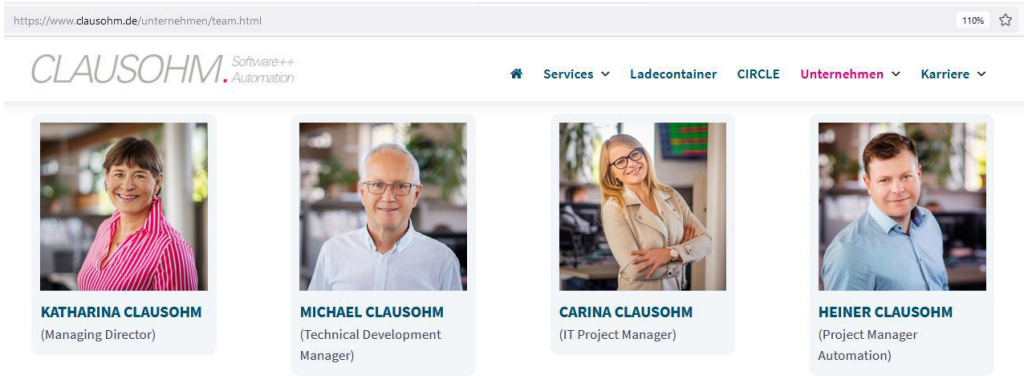
III Angriffsziele MitarbeiterInnen

Aufbau Phishing E-Mail Kampagne – Schritt 1

Vorbereitung → Köder versenden → Kommunikation → Daten auswerten / Angriff durchführen

- Aufgaben
  - Namen von Mitarbeitern sammeln
  - E-Mail-Adressen ermitteln
  - Informationen auswerten





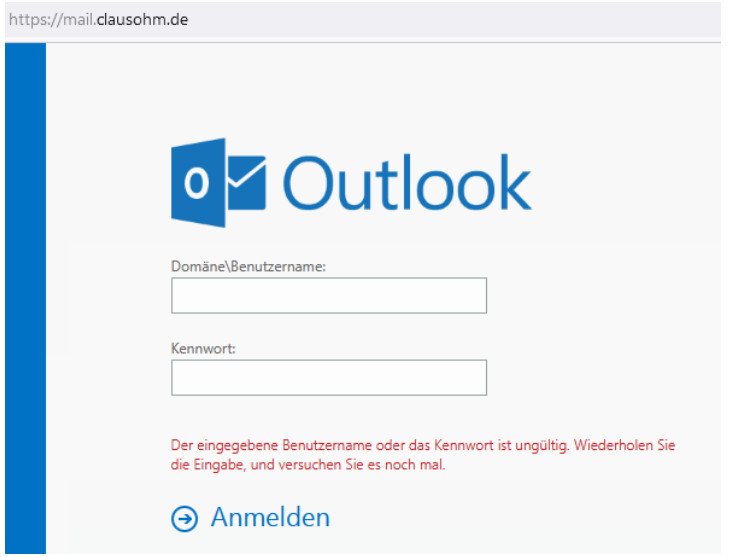
III Angriffsziele MitarbeiterInnen

Aufbau Phishing E-Mail Kampagne – Schritt 2

Vorbereitung → Köder versenden → Kommunikation → Daten auswerten / Angriff durchführen

- Aufgaben
  - Angriffsmöglichkeiten suchen
  - Auflisten von aus dem Internet erreichbaren (Sub-) Domains
  - Sichtung von Websites mit Loginmöglichkeiten

dispatcher.wzv-ms.clausohm.de	49.12.243.150
dradis.clausohm.de	5.75.246.139
gophish.clausohm.de	49.12.189.86
im.clausohm.de	82.193.231.69
karriere.clausohm.de	213.133.104.12
labor.apotheke.clausohm.de	49.12.244.47
nc.clausohm.de	82.193.231.69
new.clausohm.de	213.133.104.12
piwik.clausohm.de	213.133.104.12
wissensdatenbank.thuenen-institut.clausohm.de	162.55.43.43
www.clausohm.de	213.133.104.12

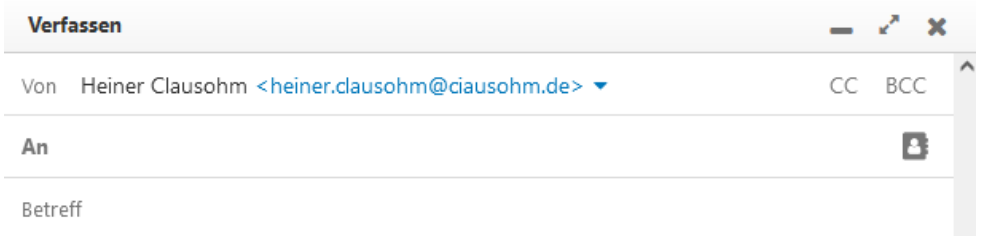


III Angriffsziele MitarbeiterInnen

Aufbau Phishing E-Mail Kampagne – Schritt 3

Vorbereitung → Köder versenden → Kommunikation → Daten auswerten / Angriff durchführen

- **Aufgaben:**
  - Erstellung einer Fake-Domain zum Erstellen einer Fake-Website
    - statt z.B. clausohm.de → clausohrn.de oder ciausohm.de
  - Erstellung Fake-Absendeadresse für die E-Mail
    - Mailversand als IT-Support
    - Mailversand als Geschäftsführer
  - Erstellung Fake-Mail
    - Inhalt erstellen

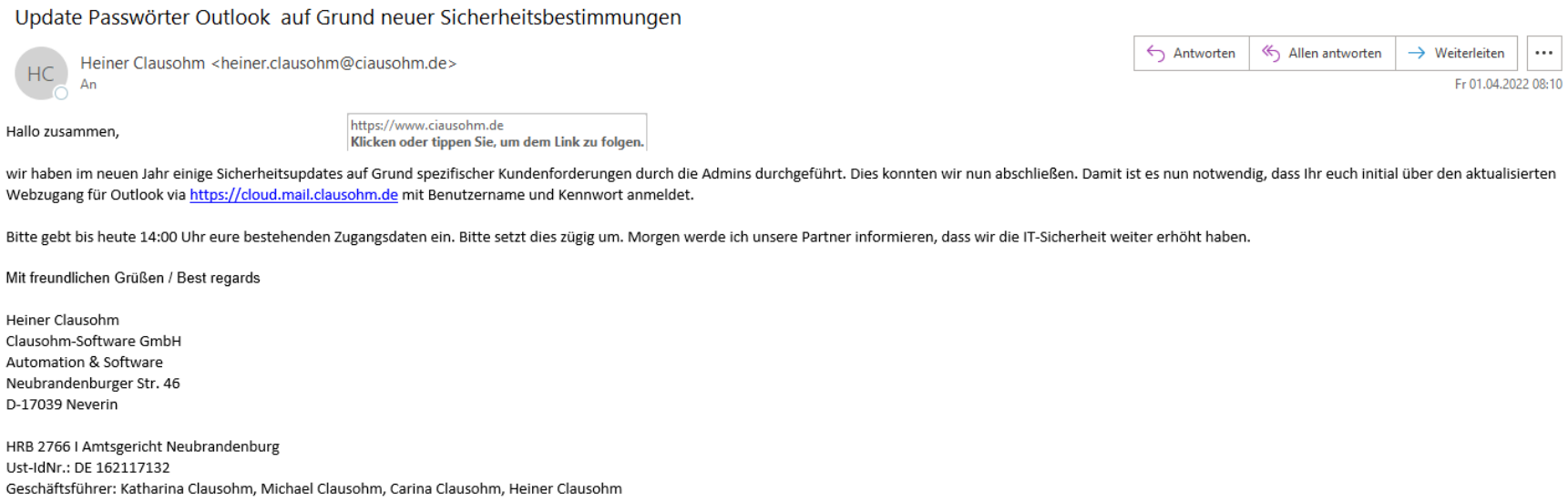


III Angriffsziele MitarbeiterInnen

Aufbau Phishing E-Mail Kampagne – Schritt 4

Vorbereitung → **Köder versenden** → Kommunikation → Daten auswerten / Angriff durchführen

- Versand der E-Mail



Update Passwörter Outlook auf Grund neuer Sicherheitsbestimmungen

HC Heiner Clausohm <heiner.clausohm@ciausohm.de>
An

Antworten | Allen antworten | Weiterleiten | ...
Fr 01.04.2022 08:10

Hallo zusammen,

https://www.ciausohm.de
Klicken oder tippen Sie, um dem Link zu folgen.

wir haben im neuen Jahr einige Sicherheitsupdates auf Grund spezifischer Kundenforderungen durch die Admins durchgeführt. Dies konnten wir nun abschließen. Damit ist es nun notwendig, dass Ihr euch initial über den aktualisierten Webzugang für Outlook via https://cloud.mail.clausohm.de mit Benutzername und Kennwort anmeldet.

Bitte gebt bis heute 14:00 Uhr eure bestehenden Zugangsdaten ein. Bitte setzt dies zügig um. Morgen werde ich unsere Partner informieren, dass wir die IT-Sicherheit weiter erhöht haben.

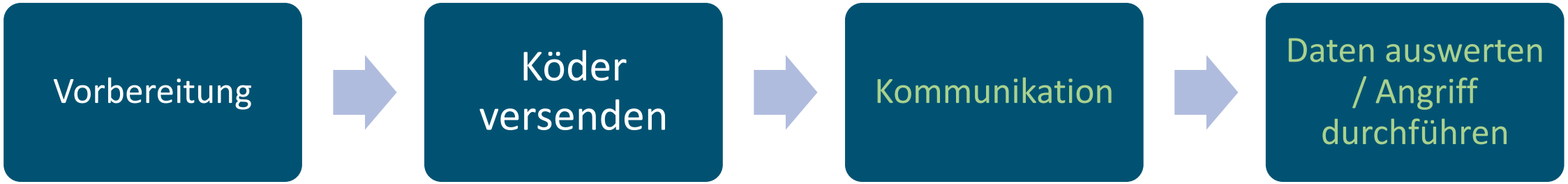
Mit freundlichen Grüßen / Best regards

Heiner Clausohm
Clausohm-Software GmbH
Automation & Software
Neubrandenburger Str. 46
D-17039 Neverin

HRB 2766 I Amtsgericht Neubrandenburg
Ust-IdNr.: DE 162117132
Geschäftsführer: Katharina Clausohm, Michael Clausohm, Carina Clausohm, Heiner Clausohm

III Angriffsziele MitarbeiterInnen

Aufbau Phishing E-Mail Kampagne – Schritt 5



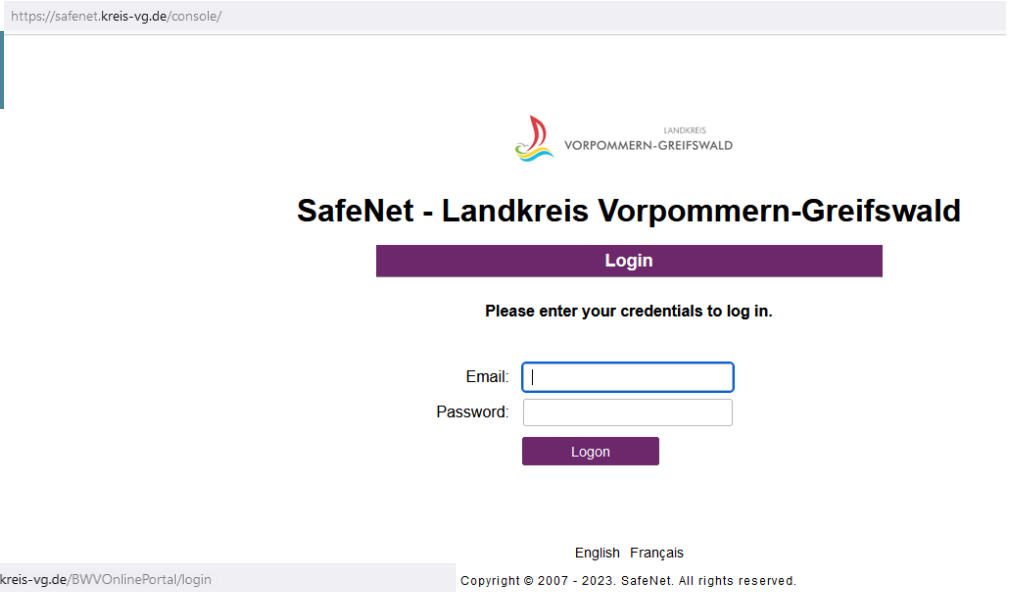
- **Kommunikation**
  - Mitarbeiter können auf die E-Mail antworten
  - Es wird ein Gespräch aufgebaut mit dem Ziel, Zugangsdaten direkt zu erhalten oder Software als Dateianhang zuzusenden

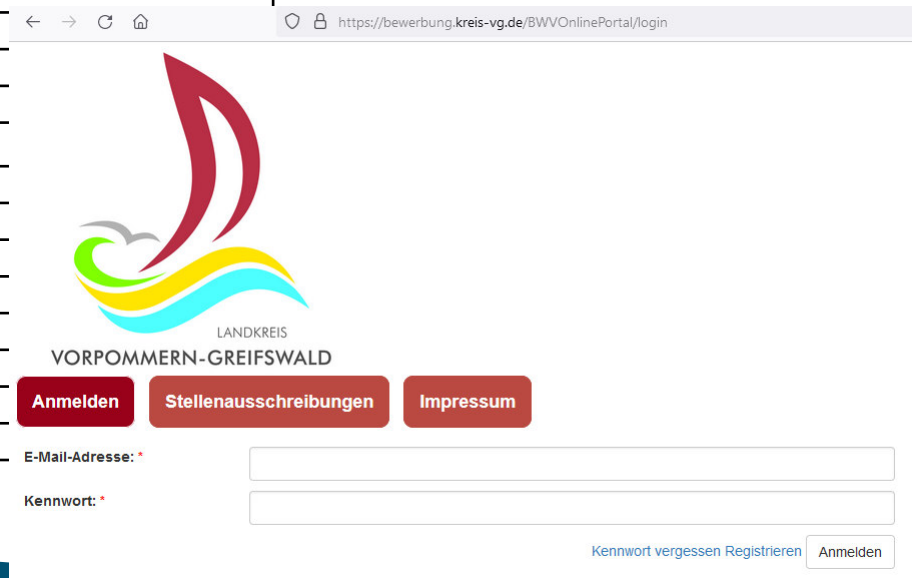
- **Daten auswerten / Angriff durchführen**
  - Eingegeben Daten über Fake-Website werden direkt auf der Original-Website des Unternehmens eingegeben und Daten entwendet bzw. eine weitere Kommunikation aus dem übernommen Account aufgebaut

III Angriffsziele MitarbeiterInnen

Informationsbeschaffung Landkreis Vorpommern Greifswald

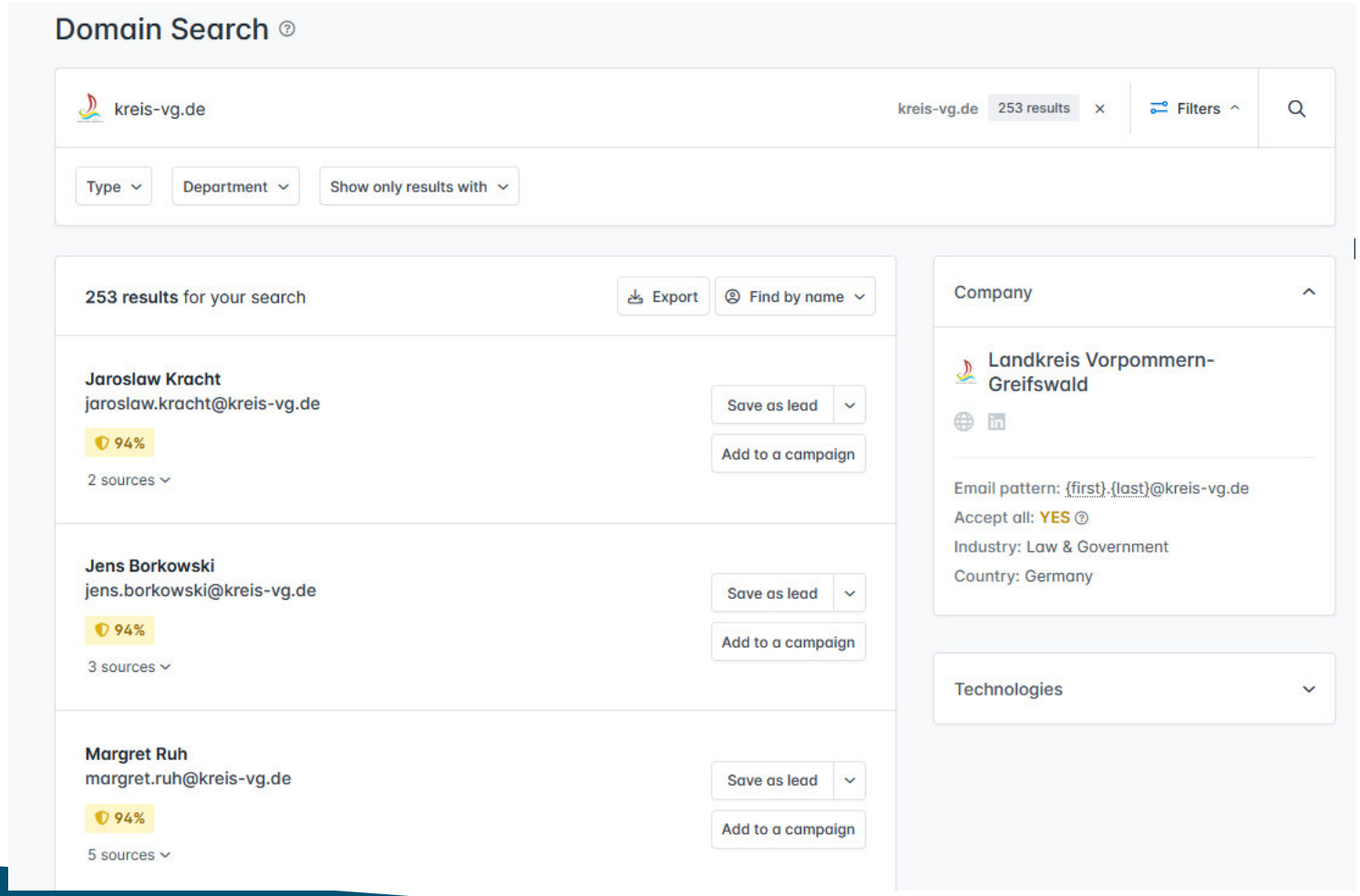
Domain/Subdomain	IP	Offene Ports
www/kreis-vg.de	213.178.85.190	80, 443
bewerbung.kreis-vg.de	185.152.106.14	80, 443
cag.kreis-vg.de	185.152.106.15	80, 443
www/corona.kreis-vg.de	213.178.85.190	80, 443
exp.kreis-vg.de	185.152.106.16	???
ikfz.kreis-vg.de	91.102.137.224	80, 442
owi.kreis-vg.de	185.152.106.14	80, 443
mail.kreis-vg.de	185.152.106.14	80, 443
mail2.kreis-vg.de	62.153.208.3	-
atlas.kreis-vg.de	138.201.31.201	via IP: 22, 25, 80, 143, 443, 465, 993
bshgw.kreis-vg.de	185.152.105.71	443
vg-expe.kreis-vg.de	62.157.133.174	-
crl.kreis-vg.de		80
ums.kreis-vg.de	185.152.106.14	80, 443
safenet.kreis-vg.de	185.152.106.14	80, 443
https://tourer.kreis-vg.de/tourer/		
http://td.kreis-vg.de/		
rbbt.kreis-vg.de		
logodata.kreis-vg.de		
dhkcall.kreis-vg.de		
caching-guetzkow.kreis-vg.de		
http://lenris.kreis-vg.de/		
https://geoportal-vg.de/geoportal/		





III Angriffsziele MitarbeiterInnen

Informationsbeschaffung Landkreis Vorpommern Greifswald



III Angriffsziele MitarbeiterInnen

Informationsbeschaffung Landkreis Vorpommern Greifswald

Update Passwörter auf Grund neuer Sicherheitsbestimmungen

IT-Support <it-support@kreisvg.de>

An

Hallo zusammen,

wir mussten einige Sicherheitsupdates auf Grund neuer Anforderungen durch die Admins durchführen. Dies konnten wir nun abschließen. Damit ist es nun notwendig, dass Ihr euch initial über den aktualisierten Webzugang zum SafeNet unter https://safenet.kreisvg.de anmeldet.

Bitte gebt bis heute 14:00 Uhr eure bestehenden Zugangsdaten ein. Bitte setzt dies zügig um.
Ansonsten müssen wir die Zugänge sperren

Mit freundlichen Grüßen / Best regards

IT-Support

Landkreis Vorpommern-Greifswald

Feldstraße 85 a
17489 Greifswald

Telefon: +49 (0)3834 8760-9995
Fax: +49 (0)3834 8760 9000

IV Angriffsziele MitarbeiterInnen

Aufbau Angriff auf das Passwort

elektro-smith.de

Elektro Smith

Ihr Spezialist für Elektroinstallationen

Startseite | Unsere Leistungen | Über Uns | Kontakt

Willkommen bei Elektro Smith

Ihr Spezialist für Elektroinstallationen

Unsere Leistungen

- **Elektroinstallationen:** Wir Übernehmen die Planung und Installation von Elektroanlagen für Neubauten und Renovierungen.
- **Beleuchtungslösungen:** Wir bieten maßgeschneiderte Beleuchtungskonzepte für Wohn- und Geschäftsräume.
- **Sicherheitstechnik:** Unser Angebot umfasst die Installation von Alarmanlagen, Videoüberwachung und Zutrittskontrollsystemen.
- **Smart-Home-Integration:** Wir machen Ihr Zuhause intelligent – von der Fernsteuerung bis zur Automatisierung.
- **Netzwerk- und Kommunikationstechnik:** Wir sorgen für eine zuverlässige Vernetzung Ihrer GerÃ¤te und Systeme.
- **Photovoltaik-Anlagen:** Nachhaltige Energiegewinnung durch die Installation von Solaranlagen.
- **Elektromobilität-Ladestationen:** Wir installieren Ladestationen für Elektrofahrzeuge, um umweltfreundliche Mobilität zu fördern.

Über John Smith

John Smith (E-Mail: john.smith@elektro-smith.de), liebevoll als **"Smithy"** von seinen Freunden bezeichnet, wurde am **6. Oktober 1987** in Musterstadt Stadt geboren. Seine leidenschaftliche Hingabe gilt jedoch nicht nur seinem Geburtsort, sondern vor allem seiner Rolle als **Geschäftsführer von Elektro Smith**.

Mit einem ausgeprägten Sinn für Innovation und QualitÃ¤t hat John es geschafft, Elektro Smith zu einem angesehenen Namen in der Branche zu machen. Sein Engagement für exzellenten Kundenservice und seine Beharrlichkeit bei der Umsetzung herausragender Elektroinstallationen haben das Unternehmen geprägt.

Abseits des Elektriker-Alltags ist John ein **leidenschaftlicher Fußballfan** und bekennender AnhÃ¤nger von **Borussia Dortmund**. An Wochenenden kann man ihn oft in schwarz-gelben Farben jubeln sehen, während er sein Team enthusiastisch anfeuert.

Das Familienleben ist ein weiterer wichtiger Eckpfeiler von Johns Identität. Er teilt sein Leben mit seiner wundervollen **Frau Lisa** (geb. am **12. Juni 1989**). Die beiden sind stolze Eltern ihres Sohnes **Paul**, der am **20. März 2006 geboren** wurde. In ihrem Zuhause dreht sich alles um Zusammenhalt, Liebe und die Freude an gemeinsamen Momenten.

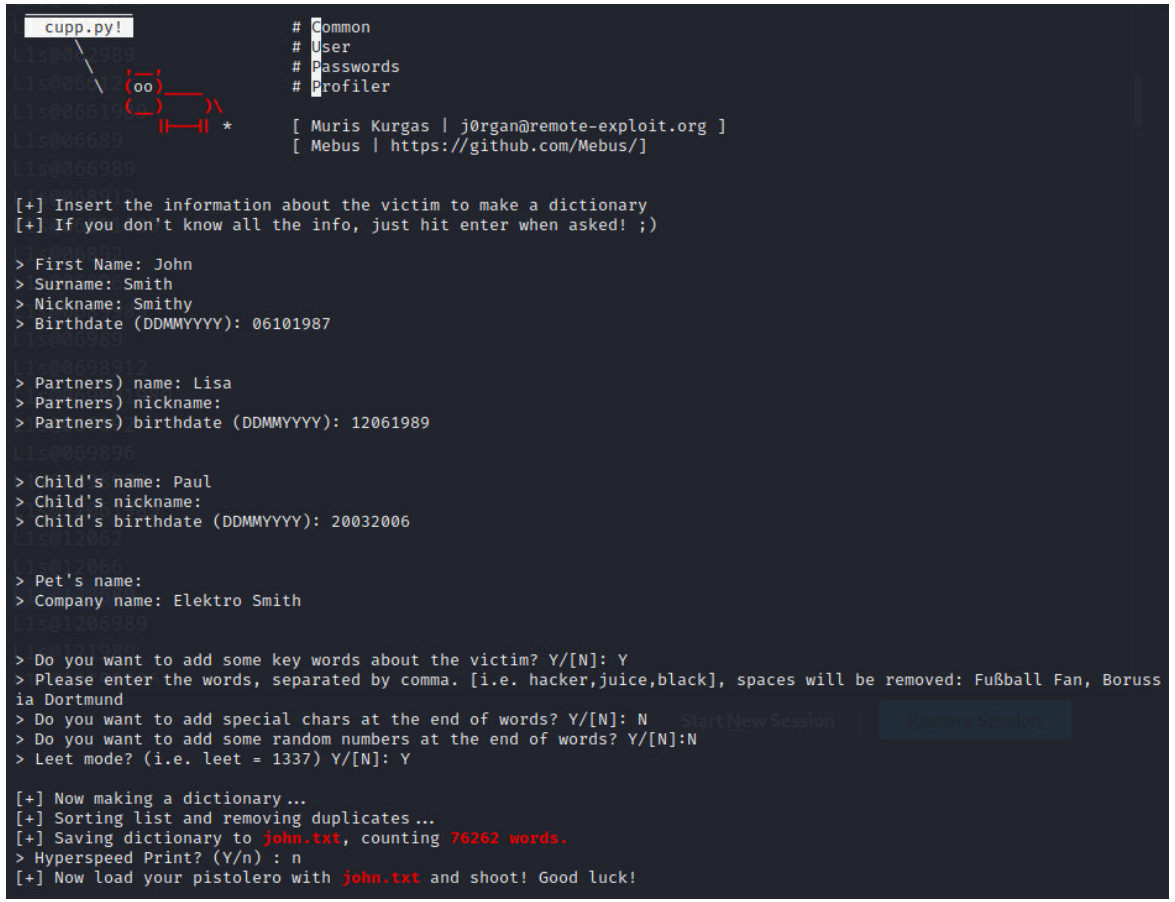
Die Familie von John und Lisa ist von einer warmen und einladenden Atmosphäre erfüllt, die sich auch auf die Arbeit von Elektro Smith überträgt.

- Datensammlung zu **John Smith** bspw. über Webseite, Social Media etc.

- **Elektriker** von Beruf
- E-Mail: **john.smith@elektro-smith.de**
- Wird häufig **Smithy** genannt
- Geboren am **06.10.1987**
- Ist Chef der Firma **Elektro Smith**
- Verheiratet, **Ehefrau** heißt **Lisa**, Geburtsdatum **12.06.1989**
- Hat einen **Sohn** namens **Paul**, geboren am **20.03.2006**
- Ist ein großer **Fußball Fan** von **Borussia Dortmund**

IV Angriffsziele MitarbeiterInnen

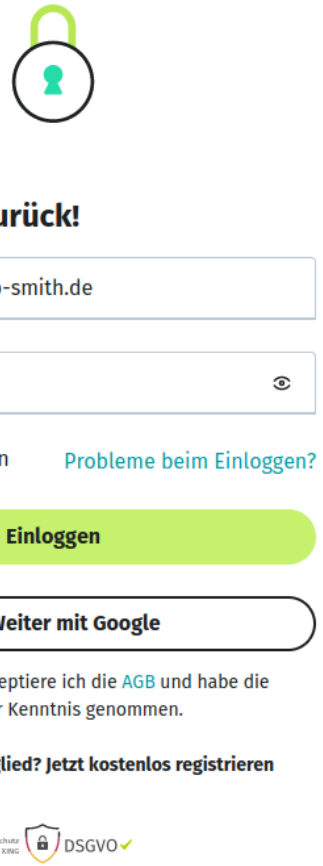
Aufbau Angriff auf das Passwort – Erstellung Passwortliste

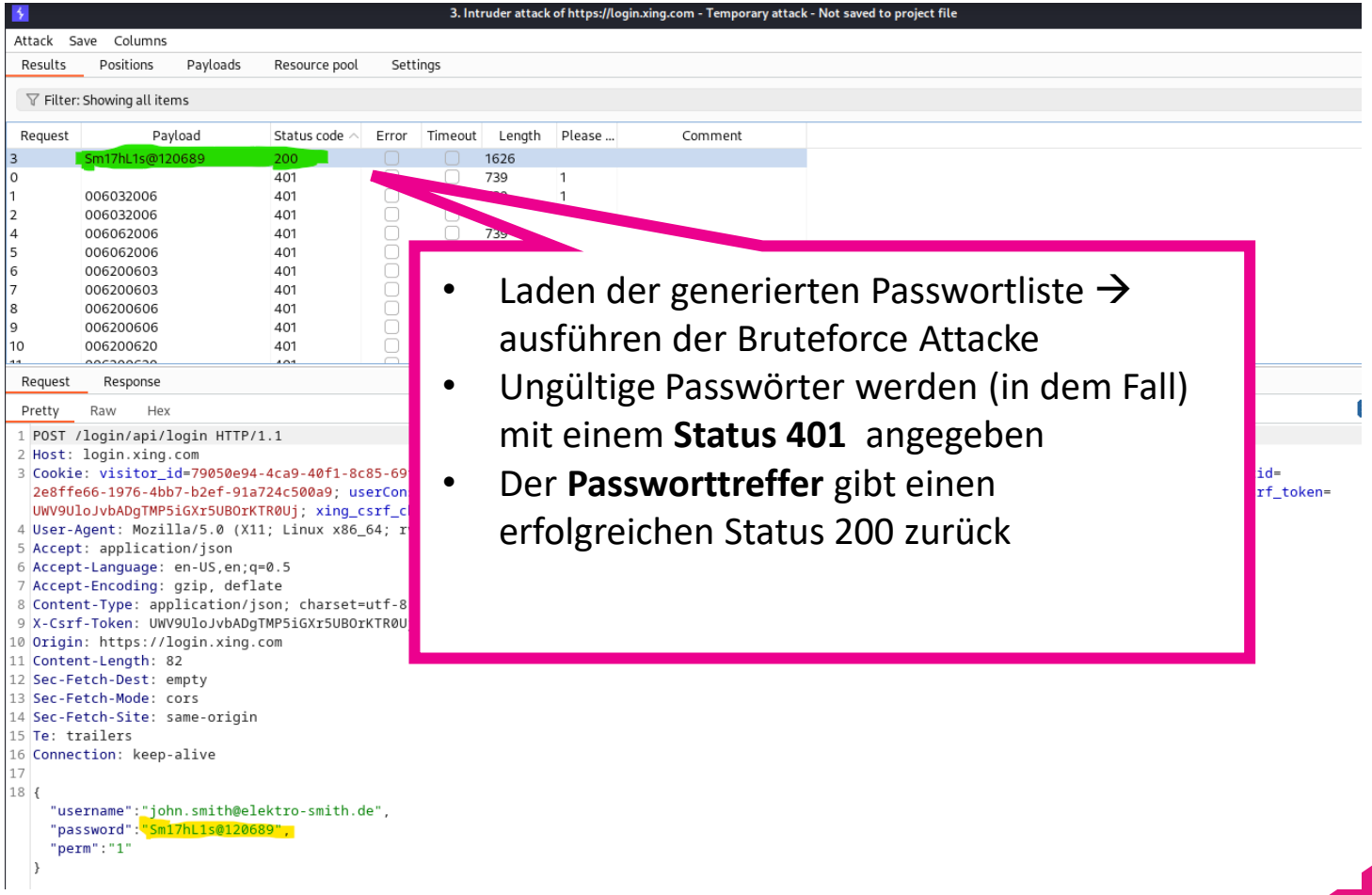


- Mit den gesammelten Daten können Passwort-Profiler wie CUPP mögliche Passwort-Kombinationen erstellen
- Diese generierten Wortlisten können für einen Bruteforce Angriff verwendet werden

IV Angriffsziele MitarbeiterInnen

Aufbau Angriff auf das Passwort – Durchführung Brute-Force Angriff

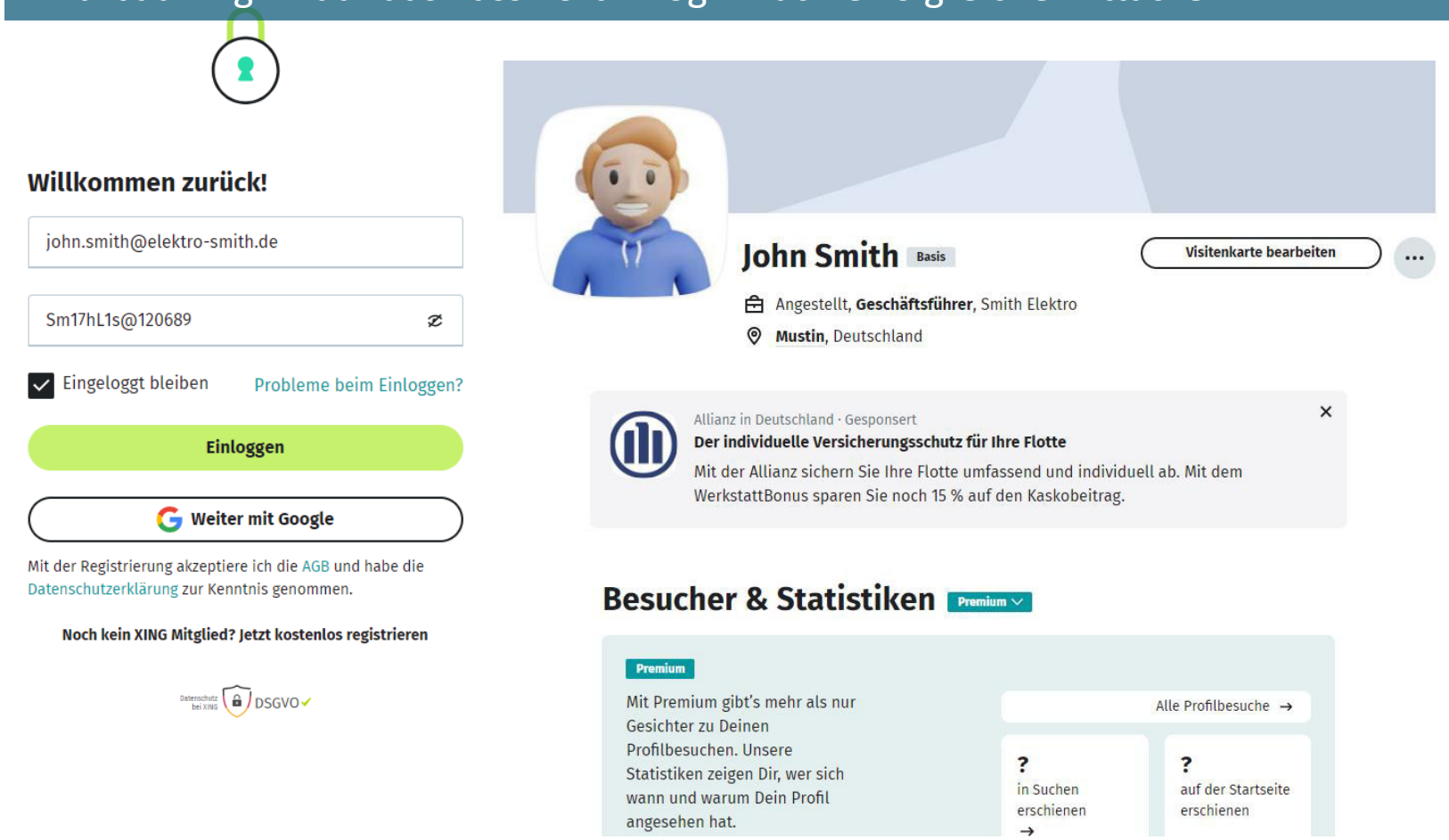




- Laden der generierten Passwortliste → ausführen der Bruteforce Attacke
- Ungültige Passwörter werden (in dem Fall) mit einem **Status 401** angegeben
- Der **Passworttreffer** gibt einen erfolgreichen Status 200 zurück

IV Angriffsziele MitarbeiterInnen

Aufbau Angriff auf das Passwort – Login nach erfolgreicher Attacke



- Das verwendete Passwort passt zur vorangegangenen Vermutung

  → **Sm17hL1s@120689**

- Anhand der gesammelten Daten konnte so das Passwort von John Smith ermittelt werden

- Passwörter daher nie in Verbindung mit Personenbezogenen Daten verwenden

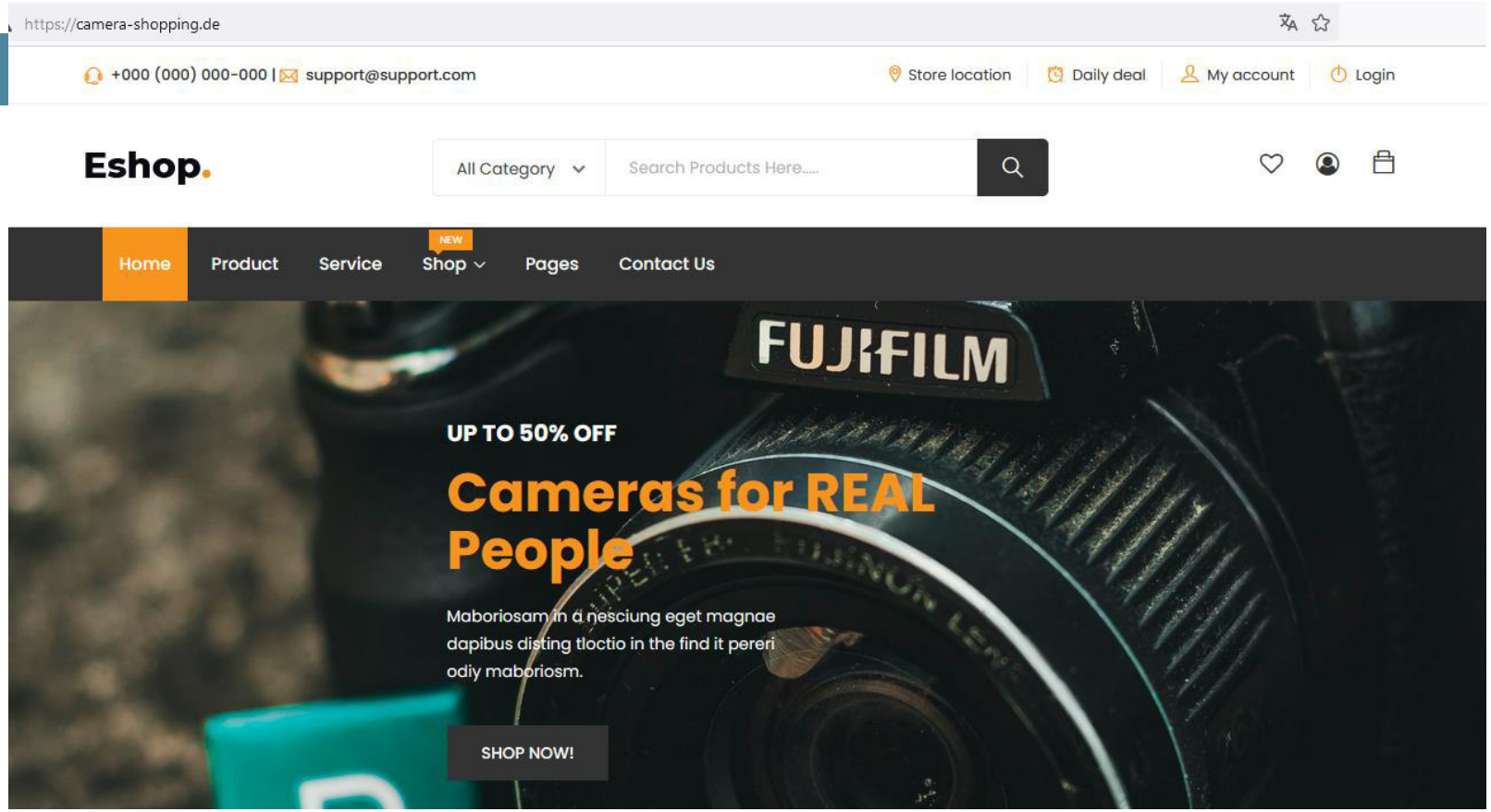
V BadUSB Stick - Rubber Ducky ???

- Praktizierte Social-Engineering-Methode
  → simuliert zufällig verlorenen USB-Stick
- Datenträger – meist im Rahmen von Tailgating-Aktionen – bewusst so platzieren, dass sie für Mitarbeiter sichtbar sind.
- Werden aufgrund von Neugier geöffnet
  → Malware gelangt so auf den Computer
- Wird auch als Baiting bezeichnet
  → dem Finder wird versprochen, etwas mit dem Datenträger zu erhalten, wie beispielsweise eine Beförderung

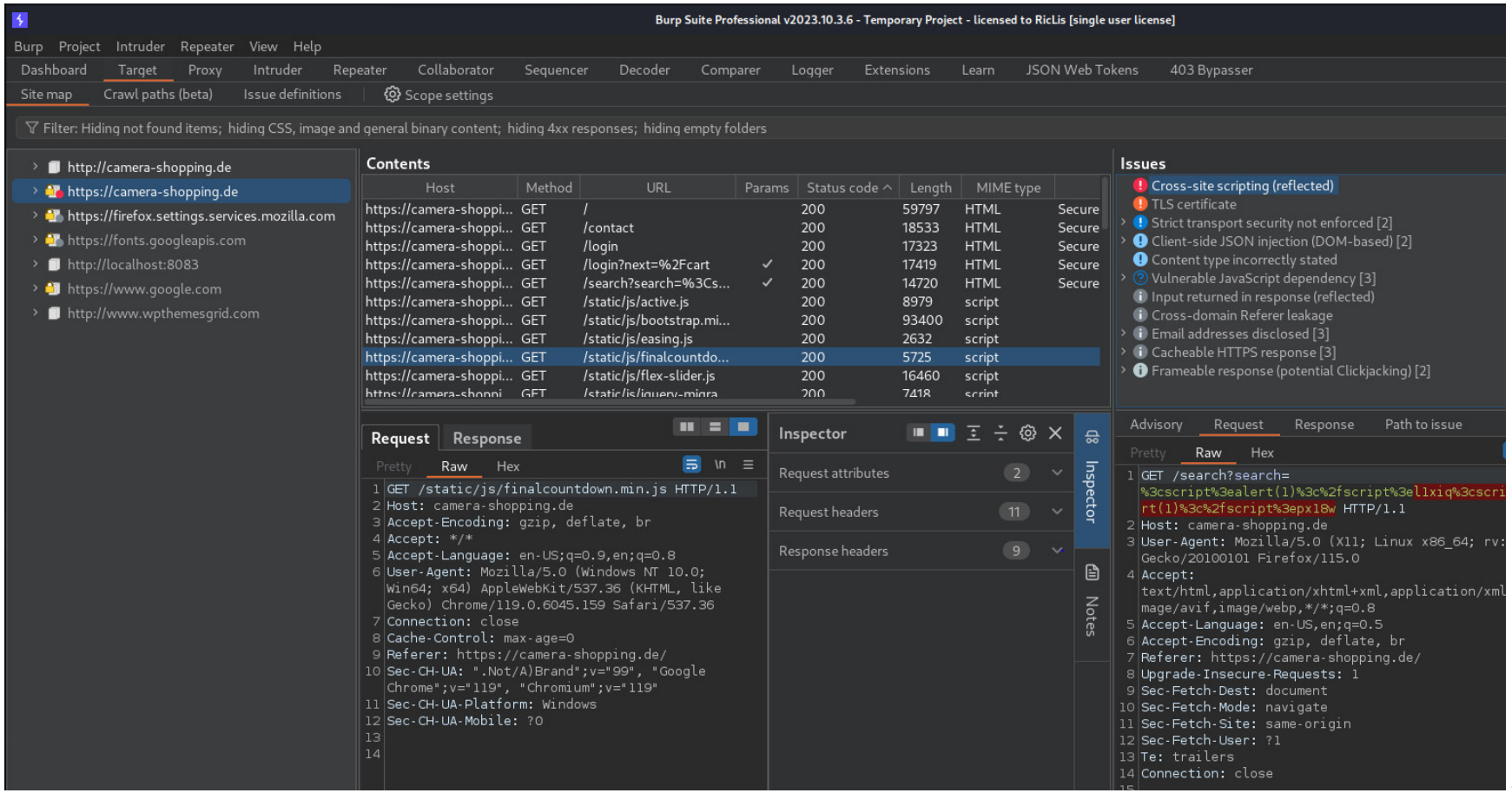
VI Angriffe gegen Webanwendungen

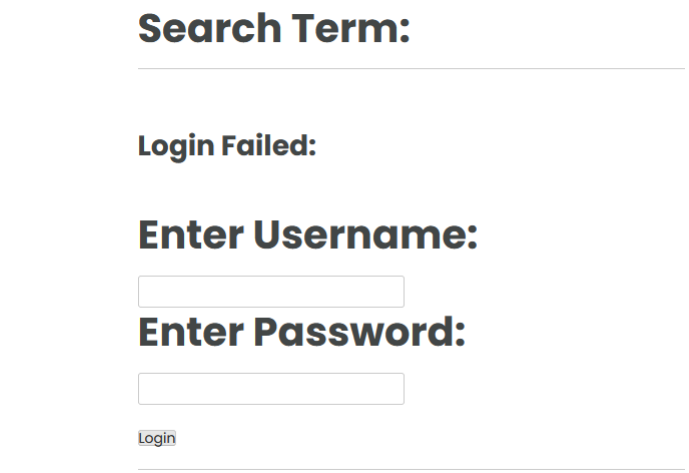
Webshop

- Cyber Angriff auf den Fake Webshop camera-shopping.de



VI Angriffe gegen Webanwendungen

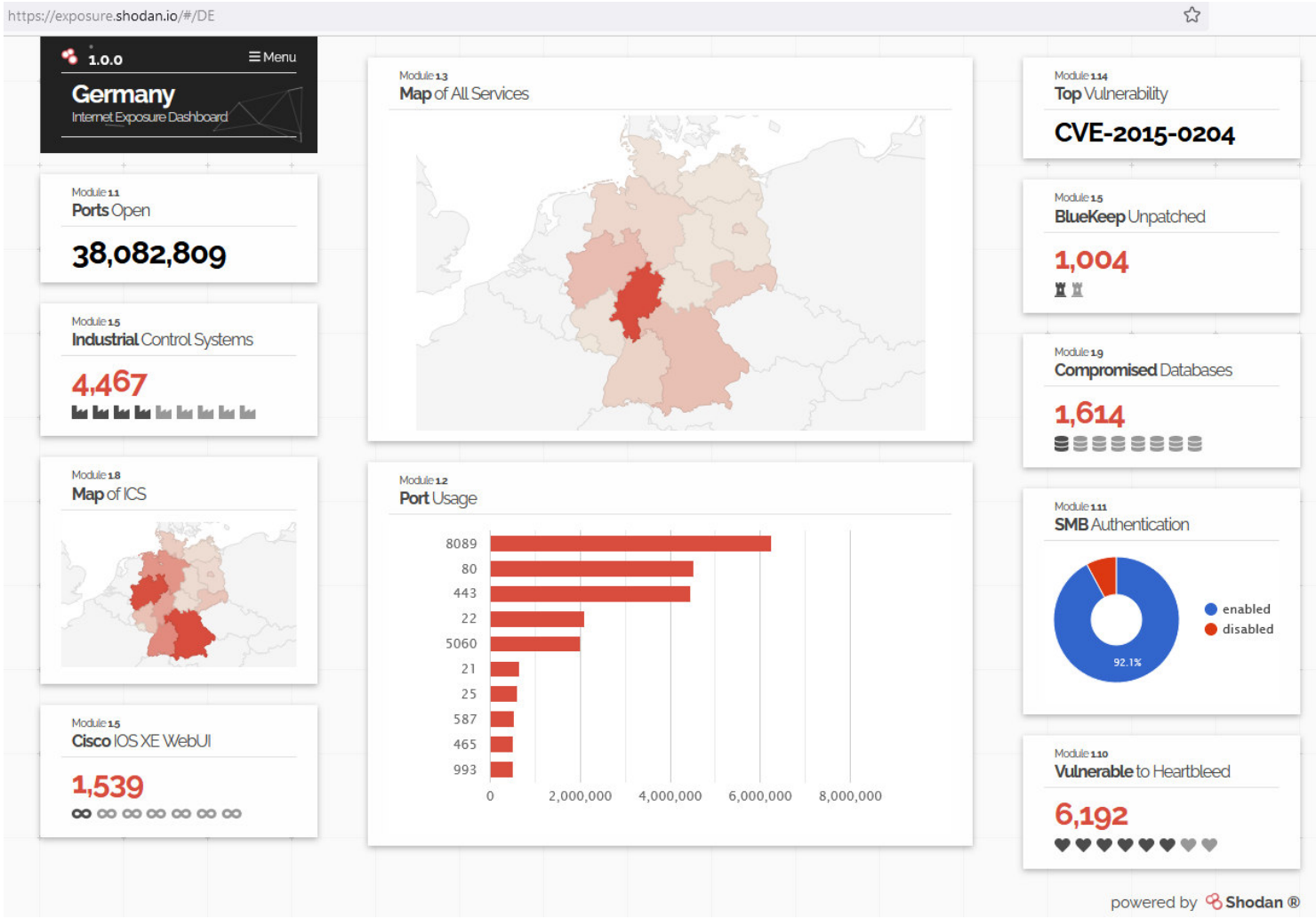




- XSS Schwachstelle ermöglicht das Ausführen von Code in der Webanwendung

```
<hr>
<form>
  <h3>Login Failed:</h3>
  <br>Enter Username:
  <br> <input type="text" id="user" name="user">
  <br> Enter Password:
  <br> <input type="password" name= "pass">
  <br><button onclick="gehAuf()">Login</button><br>
<script>
function gehAuf() {
window.open("//www.cyber24security.de/magazin/magazinartikel/so-starten-die-meisten-angriffe.html",
"_blank", "toolbar=no,scrollbars=no,top=100,left=100,width=400,height=400");
}
</script>
</form>
<hr>
```

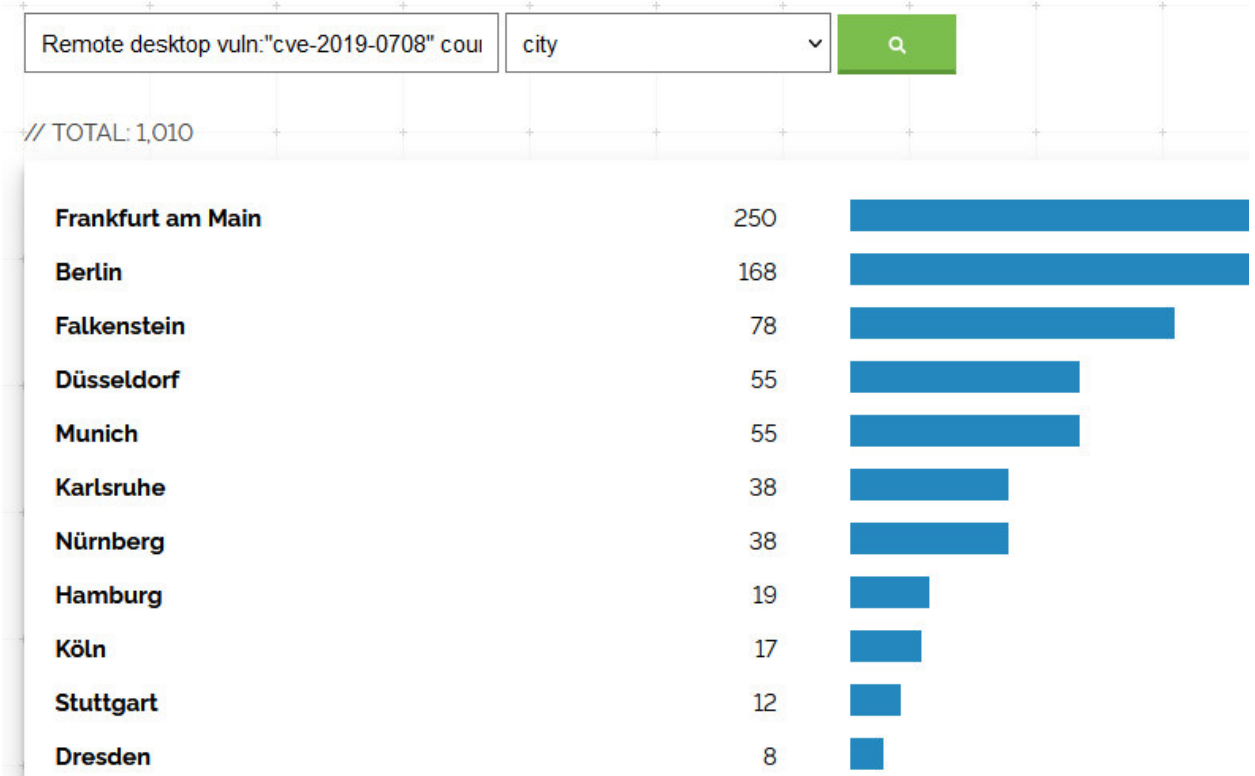
VI Angriffe gegen Webanwendungen



VI Angriffe gegen Webanwendungen

Schwachstelle Bluekeep

- Suche nach der Schwachstelle



BlueKeep

Aus dem Englischen übersetzt - BlueKeep ist eine Sicherheitslücke, die in Microsofts Remote Desktop Protocol-Implementierung entdeckt wurde, die die Möglichkeit der Remote-Code-Ausführung ermöglicht.
Wikipedia (Englisch)

VI Angriffe gegen Webanwendungen

Schwachstelle Bluekeep

- Suche nach der Schwachstelle

Achtung: Bilder wurden entfernt

Vielen Dank.

Neverin

Clausohm-Software GmbH
Automation & Software
Neubrandenburger Str. 46
D-17039 Neverin

Kontakt:
Simone Tiede
Tel: +49 39608 2690-00
simone.tiede@clausohm.de

Berlin

Clausohm-Software GmbH
Software
Bundesallee 89
D-12161 Berlin

Kontakt:
René Backasch
Tel: +49 30 897592-20
rene.backasch@clausohm.de

Aachen

Clausohm-Software GmbH
Intelligence & Automation
Philipsstraße 8
D-52068 Aachen

Kontakt:
Robin Wertz
Tel: +49 241 9278819-0
achim.merzbach@clausohm.de

Radosław Chinalski

Hacking Departement Akademie der angewandten Wissenschaften Wałcz

AKADEMIA
NAUK STOSOWANYCH
W WAŁCZU

The potential of The University of Applied Sciences in Walcz in raising awareness of cyber threats

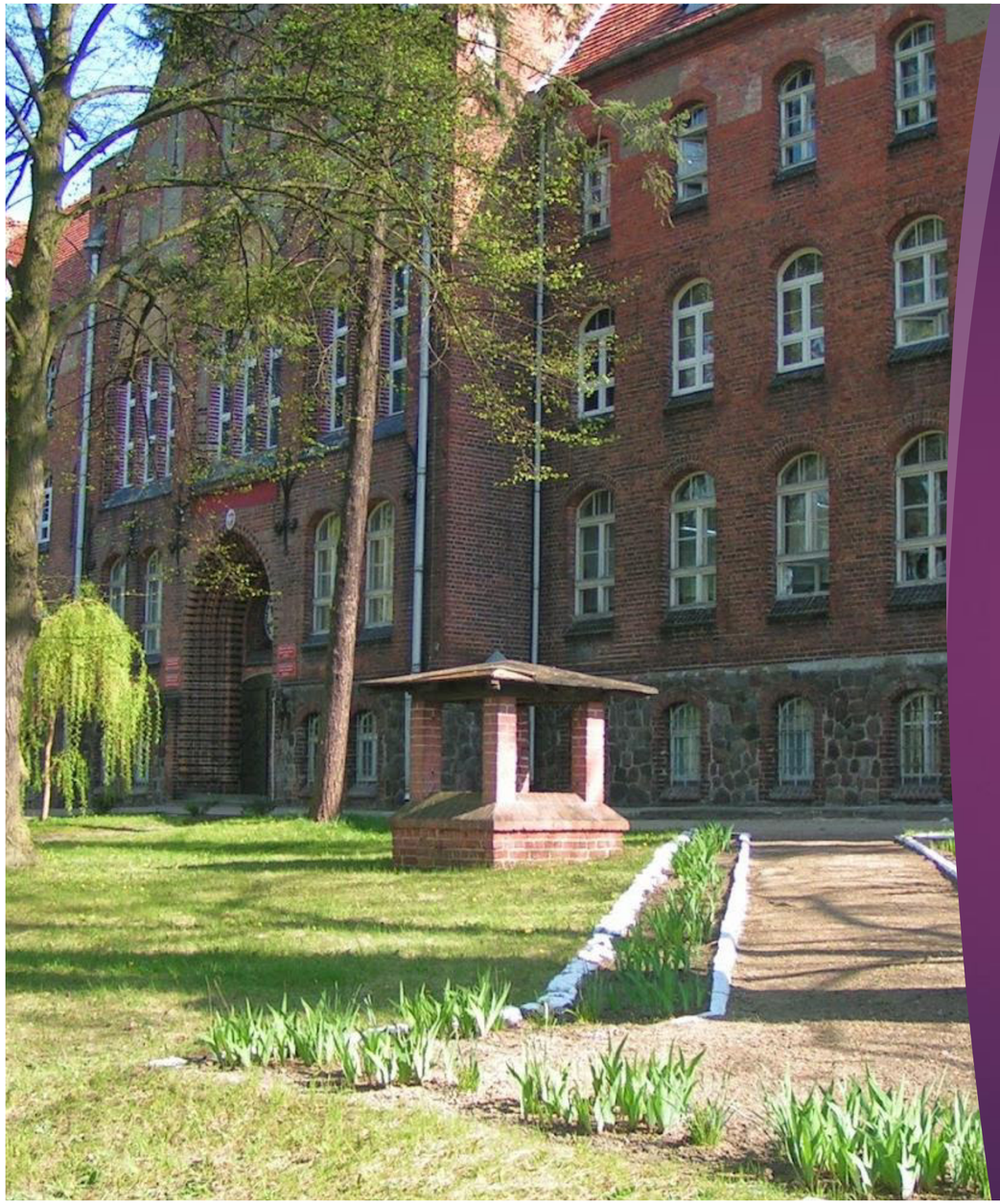
IT Security and Digital Skills – From Training to Daily Business

Col. (Ret) Police RADOSŁAW CHINALSKI

Col. (Ret) Police Radosław Chinalski

- From 1991 to 2012, 21 years of service in the Police in the communications and IT department and the criminal department.
- In 2005, one of the co-founders of the department for combating cybercrime in the Police.
- OSINT expert running the IntegracjaWiedzy business.
- Security Awareness Expert at ChangePro sp. z o. o.
- Since 2020, he has been an OSINT lecturer at ANS in Wałcz.

- Wałcz (German: Deutsch Krone) - a city in north-western Poland, in the West Pomeranian Voivodeship, the seat of the Wałcz district and the rural commune of Wałcz.
- In 2021, Wałcz had 24,802 inhabitants and was the eighth city in the West Pomeranian Voivodeship in terms of population.
- The 100th Communications Battalion, 104th Security Battalion, 1st Regional Logistics Base are stationed in Wałcz, and the 107th Military Hospital is also located in Wałcz.



The University of Applied Sciences in Walcz

AKADEMIA NAUK STOSOWANYCH W WAŁCZU

- The University of Applied Sciences in Walcz (ANS) was established on **July 1, 2004** and runs a study in the fields of Economic, Administration, Enterprise Management and IT.
- Has many years of experience in projects financed from EU funds. In the last 5 years, 8 projects with a total value of over EUR 8.2 million have been implemented.

The University of Applied Sciences in Walcz Institute of Engineering and Technical Sciences

- The mission of the Institute of Engineering and Technical Sciences is the education of high-performance engineers, with access to knowledge and technical functionalities within the framework of production engineering, within the framework of the four available data.

Faculties offered:

- ✓Management and production engineering
- ✓Industry Engineering 4.0
- ✓Information technology

The Faculty of Informatics

- ✓Network Administrator
- ✓Cybersecurity
- ✓Computer forensics

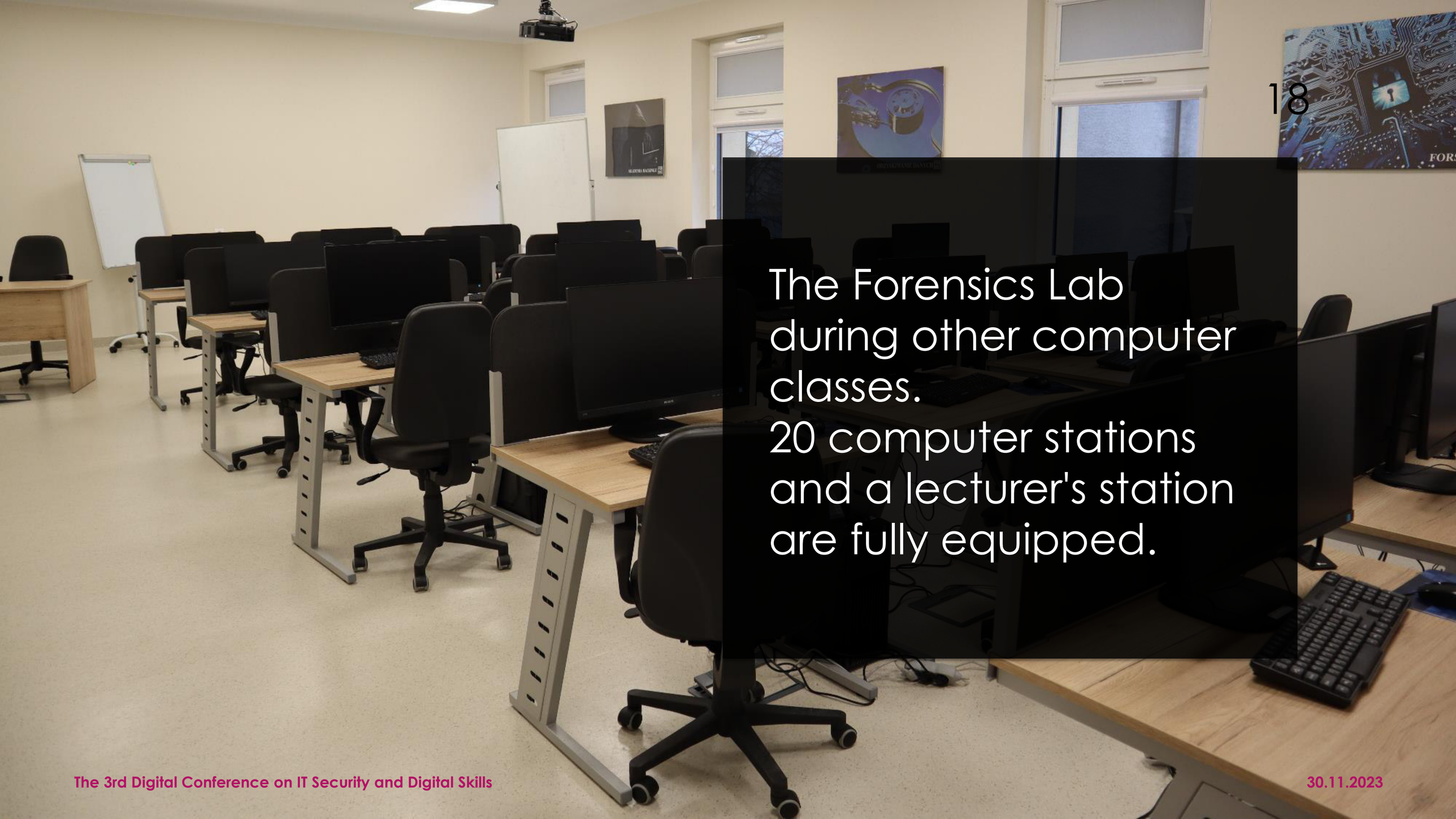
AKADEMIA
NAUK STOSOWANYCH
W WAŁCZU

Computer Laboratories

THE UNIVERSITY OF APPLIED SCIENCES

Forensics Lab

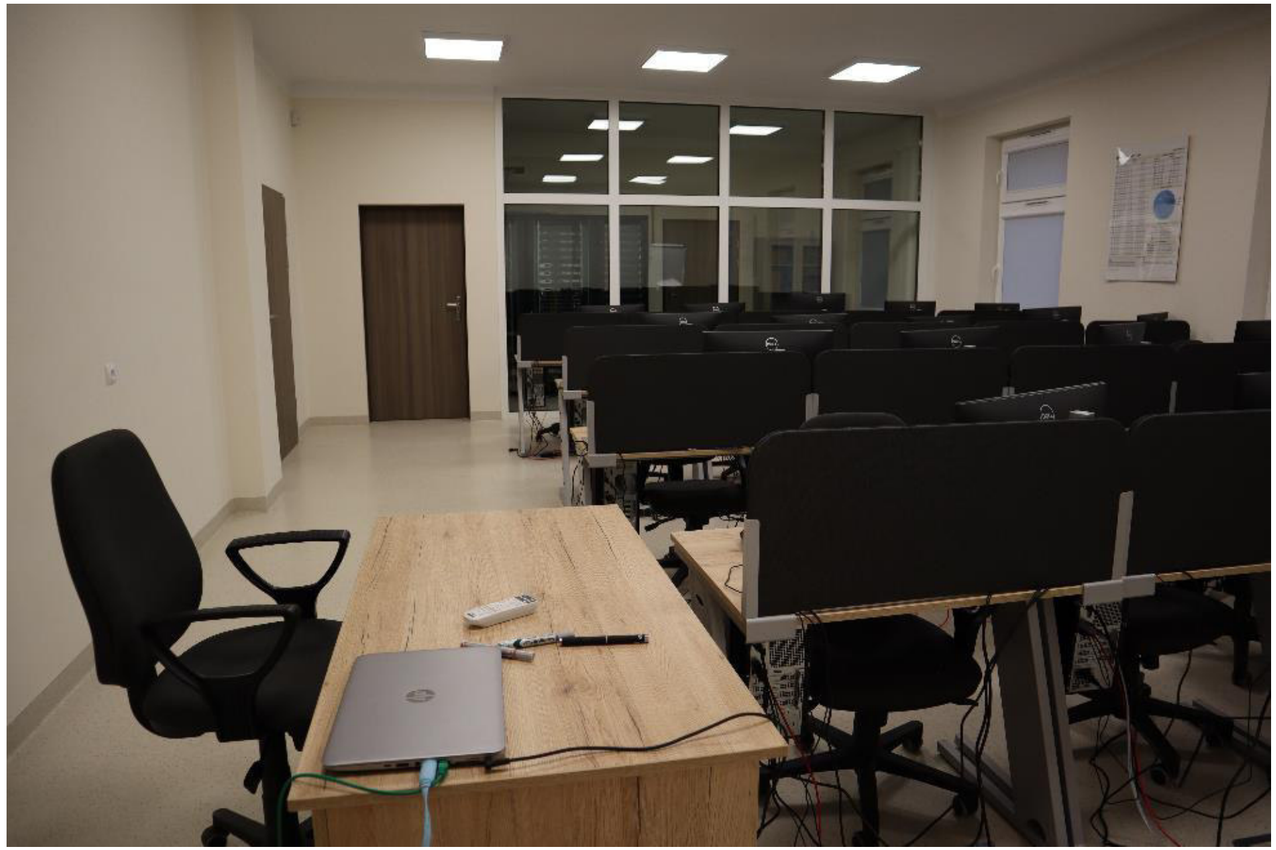
- The laboratories are equipped with state-of-the-art, fully professional equipment. This equipment allows for capturing and analysing data from all available media.
- You can see the WriteProtect™-PORTABLE devices in the picture, which ensure a fast and safe (read-only) write blocking to suspicious PCIe M.2, SATA and USB3.0 drives.

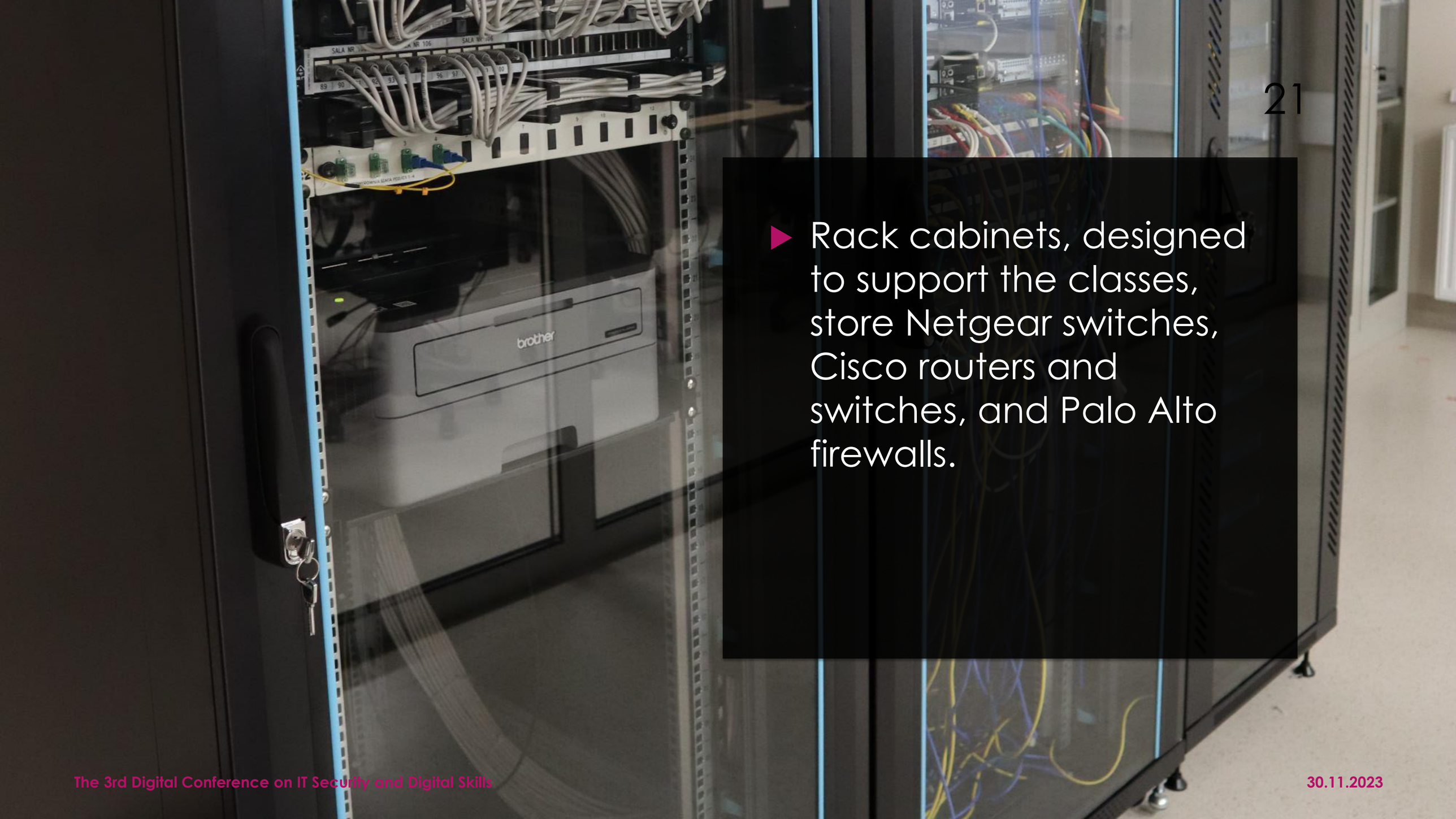


The Forensics Lab during other computer classes.
20 computer stations and a lecturer's station are fully equipped.

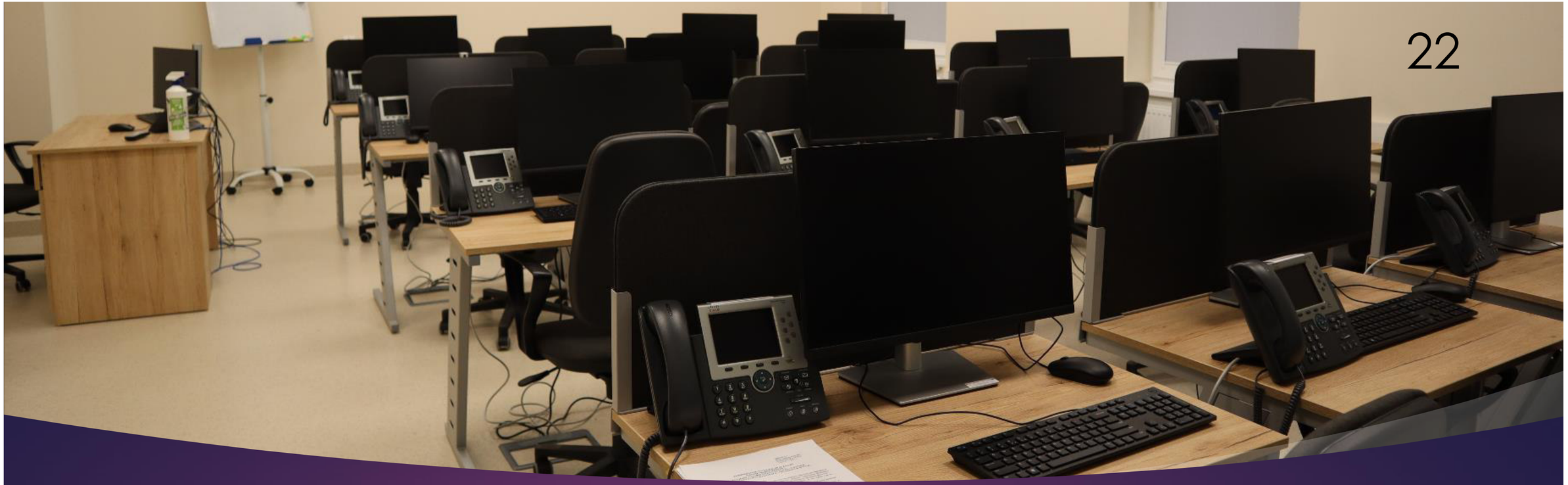
Laboratory of advanced network technologies and network operating systems

The lab uses its own access to network infrastructure, available in an adjacent glass-walled room.
Access to the equipment is possible through the use of cabling and floor outlets.

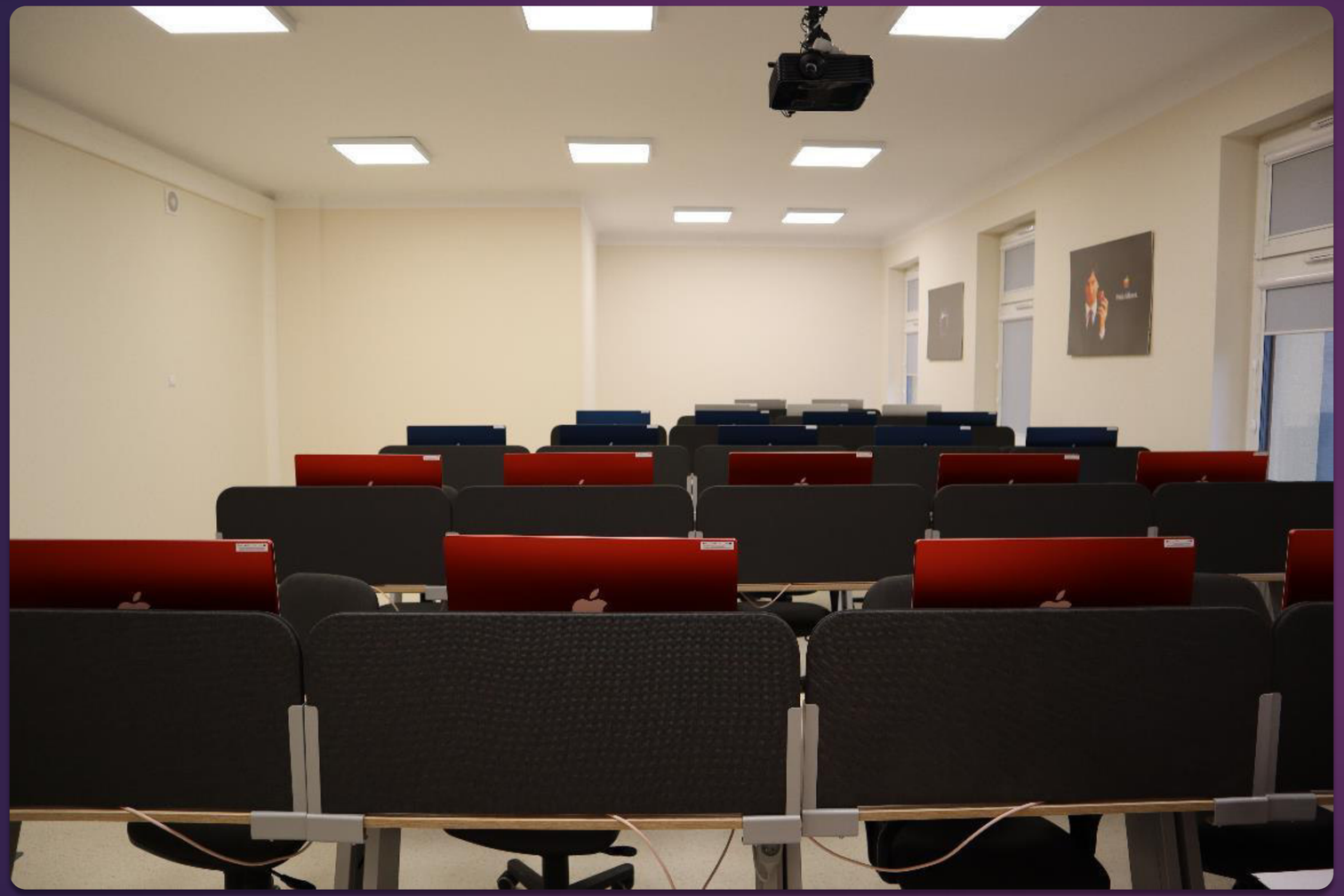




- Rack cabinets, designed to support the classes, store Netgear switches, Cisco routers and switches, and Palo Alto firewalls.



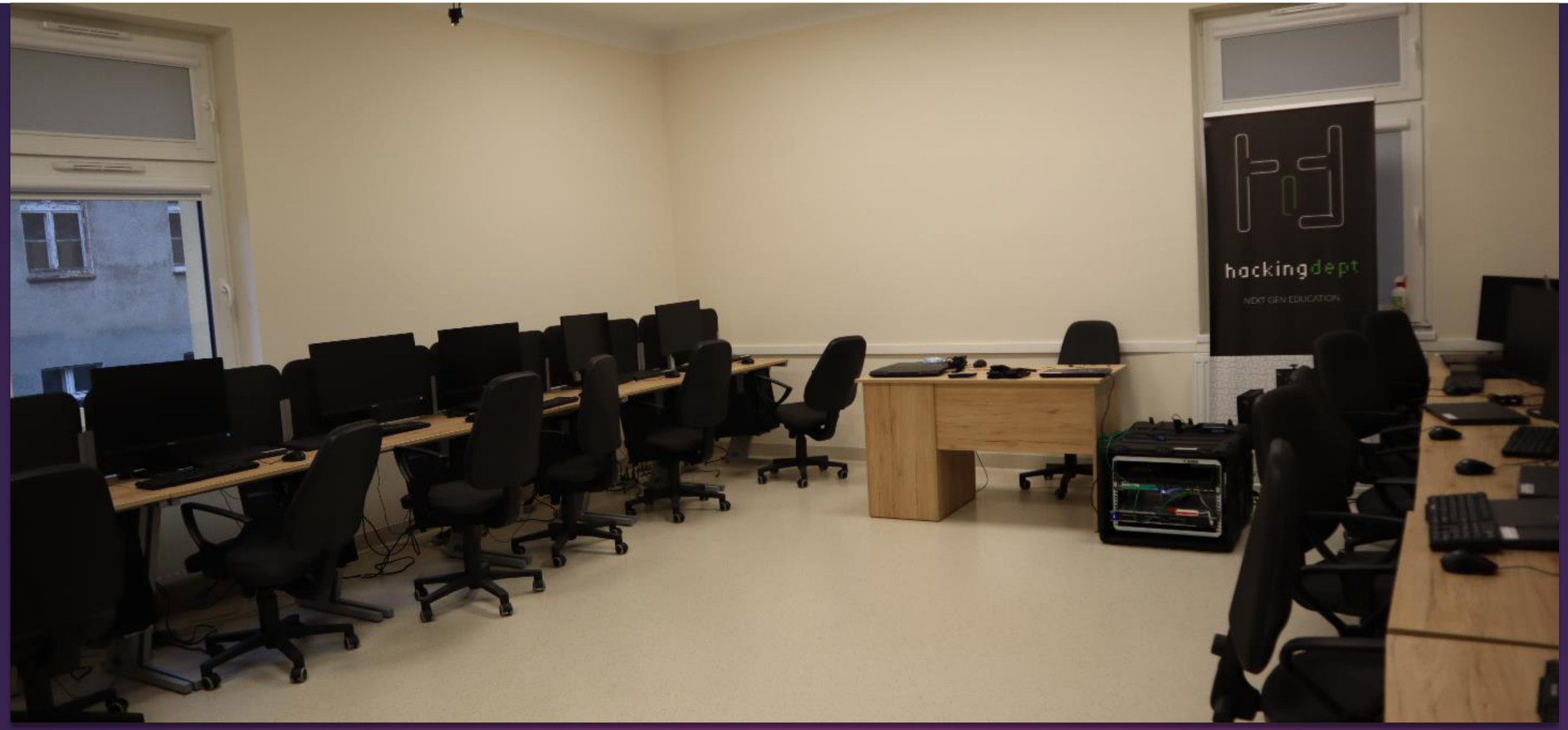
- A separate VoIP equipment lab is available within the lab
- In the back of the studio there is a dedicated server room



UNIX Systems Lab

Workstations with iMACs

- The lab is equipped with 24 student workstations, with iMAC computers, and one lecturer workstation with another iMAC (25 in total).



Cybersecurity Lab

ADDRESSES TODAY'S CYBER THREATS

- HackindDept is a hybrid of a cyber training ground and an e-learning platform in the field of offensive IT security and computer forensics. The platform is a combination of the world of hackers and their practical knowledge with the world of real IT problems.
- https://present.cloud.hackingdept.com/

#StayCyberSafe

#StayCyberSafe – increase the competitiveness of SME's, local governments and NGO's from the South Baltic area by increasing the cyber security trustiness and competences

THE INTERREG SOUTH BALTIC PROGRAMME 2021-2027

#StayCyberSafe

- The Interreg South Baltic Programme 2021-2027 is a multilateral cross-border cooperation programme between the coastal regions of five EU Member States: **Germany, Denmark, Sweden, Lithuania, and Poland**, implemented in the framework of the Interreg policy of the European Union funded by the European Regional Development Fund (ERDF)

#StayCyberSafe

AKADEMIA NAUK STOSOWANYCH W WAŁCZU

WISSENSCHAFTS + TECHNOLOGIEPARK NORD° OST WITENO

BLUE SCIENCE PARK KARLSKRONA

KLAIPĖDA CHAMBER OF COMMERCE, INDUSTRY AND CRAFTS

#StayCyberSafe

- #StayCyberSafe seeks to support SME's, local and regional self-governments and NGO's in the South Baltic Sea region (Poland, Germany, Denmark, Sweden and Lithuania) in the development of actions to improve cybersecurity.
- The project aims at simple and comparable methods of raising awareness and examining the same level of cybersecurity for the entire South Baltic region. As part of the work on the project, the need to achieve the following goals was defined:
  - (1) Building cross-border cybersecurity culture (CSC) in South Baltic region.
  - (2) Creating international cybersecurity tools and #StayCyberSafe certification processes.
  - (3) Jointly developing the marketing and capitalization strategy for #StayCyberSafe certification processes.

#StayCyberSafe

- The project idea is increase of cyber security in the South Baltic area and build up a trustful digital cooperation environment. The main project will develop certification in the field of cybersecurity quality and create a trustworthy and recognizable brand #StayCyberSafe on the international market.
- The certification system will be based on:
  - 1. online security awareness training strengthening human firewall and
  - 2. online tool to detect IT security vulnerabilities and risks (tool for data leaks).

AKADEMIA
NAUK STOSOWANYCH
W WAŁCZU

IT Security and Digital Skills – From Training to Daily Business

Dziękuję za uwagę ☺

Col. (Ret) Police RADOSŁAW CHINALSKI

Darinka Kriegel

Studiengangkoordinatorin Digitalisierung und Strukturwandel
Hochschule Neubrandenburg

Netzwerken & Imbiss

Ellen Grull

Aus und- Weiterbildung IHK Neubrandenburg

„Die für alle Ausbildungsberufe identisch formulierten Inhalte sollen sicherstellen, dass Auszubildende künftig berufsübergreifend innerhalb einer modernen und zukunftsgewandten Ausbildung Kompetenzen erwerben können, die sie als angehende Fachkräfte von morgen in einer sich verändernden Arbeitswelt benötigen, um dauerhaft beschäftigungsfähig zu

DIE QUALIFIZIERENDEN VIER

Digitalisierte Arbeitswelt
Der bewusste Umgang mit digitalen Medien und Daten, kommunikative und soziale Kompetenzen bei der kollaborativen Zusammenarbeit im virtuellen Raum, Methoden des selbstgesteuerten Lernens sowie
liche Vielfalt und
Wertschätzung fließen
lle Ausbildungsordnungen

Sicherheit und Gesundheit bei der Arbeit
Der richtige Umgang mit möglichen arbeitsspezifischen Gefahrenquellen, die Beachtung ergonomischer Arbeitsweisen sowie das Wissen um Maßnahmen zur Vermeidung von psychischen und physischen Belastungen stellt künftig eine grundlegende Voraussetzung für sicheres Handeln am

Organisation des Ausbildungsbetriebes, Berufsbildung sowie Arbeits- und Tarifrecht
Das Wissen um den Aufbau und die Organisation des eigenen Ausbildungsbetriebes, die zentralen Bestandteile des Ausbildungsvertrages sowie die Möglichkeiten des beruflichen Aufstiegs und der beruflichen Weiterentwicklung sind künftig
indestinhalt jeder
ordnung.

Umweltschutz und Nachhaltigkeit
Umweltschutz und Nachhaltigkeit
Das Thema Nachhaltigkeit gewinnt gesamtgesellschaftlich immer mehr an Bedeutung. Dabei zählt die Verbesserung nachhaltigen Handelns unter Berücksichtigung ökonomischer, ökologischer und sozialer Aspekte im eigenen Arbeitsumfeld zu den künftigen Mindestinhalten

Einleitung Standardberufsbildposit

Digitalisierte Arbeitswelt
Der bewusste Umgang mit digitalen Medien und Daten, kommunikative und soziale Kompetenzen bei der kollaborativen Zusammenarbeit im virtuellen Raum, Methoden des selbstgesteuerten Lernens sowie gesellschaftliche Vielfalt und gegenseitige Wertschätzung fließen alle Ausbildungsordnungen

Sicherheit und Gesundheit bei der Arbeit
Der richtige Umgang mit möglichen arbeitsspezifischen Gefahrenquellen, die Beachtung ergonomischer Arbeitsweisen sowie das Wissen um Maßnahmen zur Vermeidung von psychischen und physischen Belastungen stellt künftig eine grundlegende Voraussetzung für sicheres Handeln am eigenen Arbeitsplatz dar.

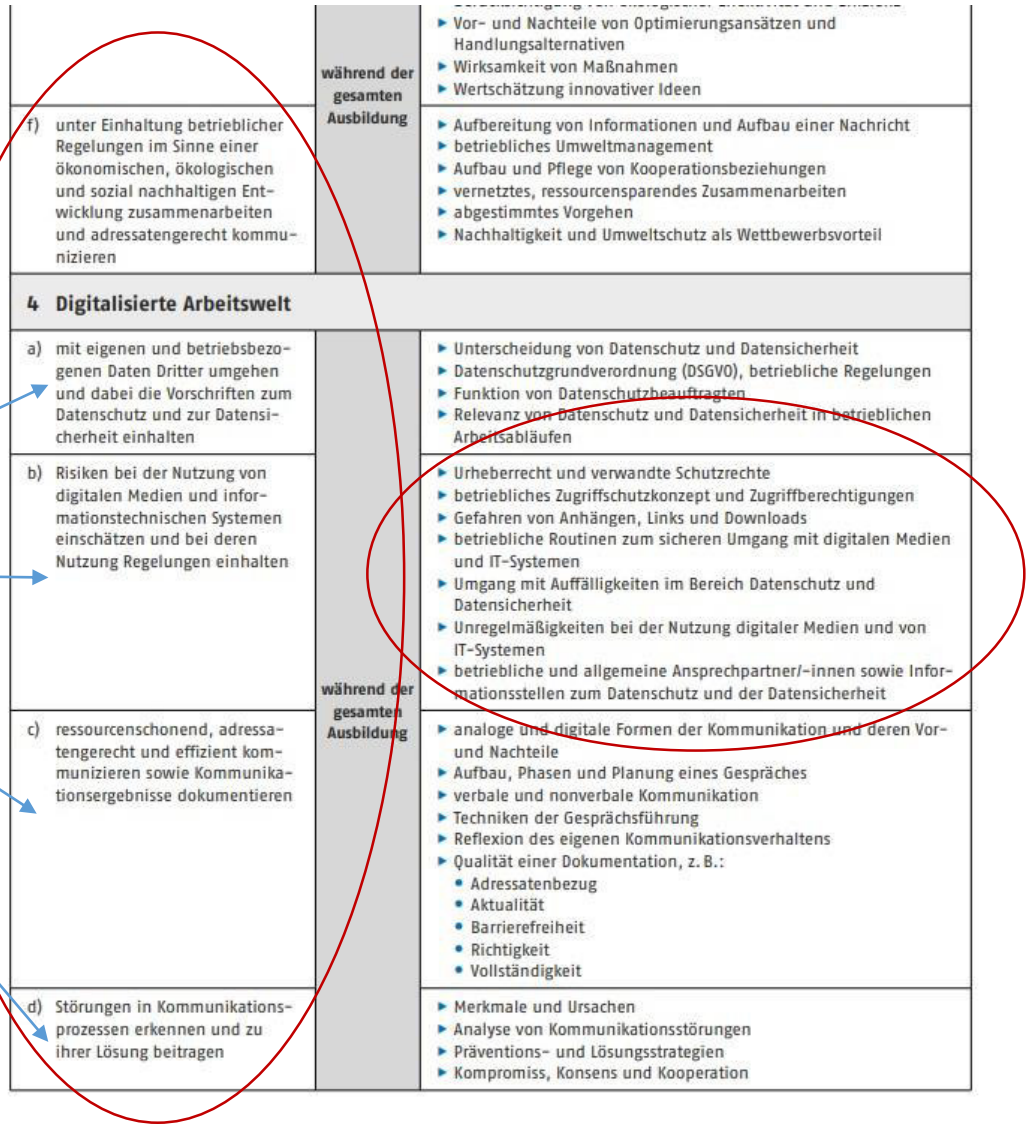
Organisation des Ausbildungsbetriebes, Berufsbildung sowie Arbeits- und Tarifrecht
Das Wissen um den Aufbau und die Organisation des eigenen Ausbildungsbetriebes, die zentralen Bestandteile des Ausbildungsvertrages sowie die Möglichkeiten des beruflichen Aufstiegs und der beruflichen Weiterentwicklung sind künftig zentraler Mindestinhalt jeder Ausbildungsordnung.

Umweltschutz und Nachhaltigkeit
Umweltschutz und Nachhaltigkeit
Das Thema Nachhaltigkeit gewinnt gesamtgesellschaftlich immer mehr an Bedeutung. Dabei zählt die Verbesserung nachhaltigen Handelns unter Berücksichtigung ökonomischer, ökologischer und sozialer Aspekte im eigenen Arbeitsumfeld zu den künftigen Mindestinhalten für alle Ausbildungsberufe

Einleitung Standardberufsbildposit

Berufsbildpositionen mit Erläuterungen und Beispielen zur Umsetzung

Einbinden in betrieblichen Ausbildungsplan!



	während der gesamten Ausbildung	▸ Vor- und Nachteile von Optimierungsansätzen und Handlungsalternativen ▸ Wirksamkeit von Maßnahmen ▸ Wertschätzung innovativer Ideen
f) unter Einhaltung betrieblicher Regelungen im Sinne einer ökonomischen, ökologischen und sozial nachhaltigen Entwicklung zusammenarbeiten und adressatengerecht kommunizieren	während der gesamten Ausbildung	▸ Aufbereitung von Informationen und Aufbau einer Nachricht ▸ betriebliches Umweltmanagement ▸ Aufbau und Pflege von Kooperationsbeziehungen ▸ vernetztes, ressourcensparendes Zusammenarbeiten ▸ abgestimmtes Vorgehen ▸ Nachhaltigkeit und Umweltschutz als Wettbewerbsvorteil
4 Digitalisierte Arbeitswelt		
a) mit eigenen und betriebsbezogenen Daten Dritter umgehen und dabei die Vorschriften zum Datenschutz und zur Datensicherheit einhalten	während der gesamten Ausbildung	▸ Unterscheidung von Datenschutz und Datensicherheit ▸ Datenschutzgrundverordnung (DSGVO), betriebliche Regelungen ▸ Funktion von Datenschutzbeauftragten ▸ Relevanz von Datenschutz und Datensicherheit in betrieblichen Arbeitsabläufen
b) Risiken bei der Nutzung von digitalen Medien und informationstechnischen Systemen einschätzen und bei deren Nutzung Regelungen einhalten	während der gesamten Ausbildung	▸ Urheberrecht und verwandte Schutzrechte ▸ betriebliches Zugriffschutzkonzept und Zugriffberechtigungen ▸ Gefahren von Anhängen, Links und Downloads ▸ betriebliche Routinen zum sicheren Umgang mit digitalen Medien und IT-Systemen ▸ Umgang mit Auffälligkeiten im Bereich Datenschutz und Datensicherheit ▸ Unregelmäßigkeiten bei der Nutzung digitaler Medien und von IT-Systemen ▸ betriebliche und allgemeine Ansprechpartner/-innen sowie Informationsstellen zum Datenschutz und der Datensicherheit
c) ressourcenschonend, adressatengerecht und effizient kommunizieren sowie Kommunikationsergebnisse dokumentieren	während der gesamten Ausbildung	▸ analoge und digitale Formen der Kommunikation und deren Vor- und Nachteile ▸ Aufbau, Phasen und Planung eines Gespräches ▸ verbale und nonverbale Kommunikation ▸ Techniken der Gesprächsführung ▸ Reflexion des eigenen Kommunikationsverhaltens ▸ Qualität einer Dokumentation, z. B.: • Adressatenbezug • Aktualität • Barrierefreiheit • Richtigkeit • Vollständigkeit
d) Störungen in Kommunikationsprozessen erkennen und zu ihrer Lösung beitragen	während der gesamten Ausbildung	▸ Merkmale und Ursachen ▸ Analyse von Kommunikationsstörungen ▸ Präventions- und Lösungsstrategien ▸ Kompromiss, Konsens und Kooperation

Danis Kotliarov, Kai Düwell, Roberto Krämer

Weber Maschinenbau GmbH Neubrandenburg

Präsentation über IT-Sicherheit & Digitale Kompetenzen

<Grundlagen für die sichere digitale Zukunft>

Auszubildener von Weber
Danis Kotliarov

AGENDA

- Wer bin ich
- Firma Weber Maschinenbau
- Was ist Cyber-Sicherheit?
- Gefahren und Schutz dagegen
- Wie Weber sich schützt

WER BIN ICH?

AZUBI FACHINFORMATIKER FÜR ANWENDUNGSENTWICKLUNG

- Danis Kotliarov
- Ukrainer
- 20 Jahre alt
- 1. Lehrjahr

INFORMATIONEN

WEBER IN WORT UND ZAHL

- Gegründet 1981 in Breidenbach – Weiterhin in Familienbesitz
- Lösungsanbieter – vom Slicen über Automatisierung bis Verpackung, alles aus einer Hand
- Produktion an 6 deutschen Standorten
- Rund 1.800 Mitarbeiter an 23 Standorten weltweit
- 100% Made in Germany

WAS IST CYBER-SICHERHEIT?

Schutz von:

- Computersystemen
- empfindlichen Daten
- Programmen

WELCHE GEFAHREN GIBT ES?

DIE HÄUFIGSTEN ARTEN VON CYBERANGRIFFEN

PHISHING

MALWARE

RANSOMWARE

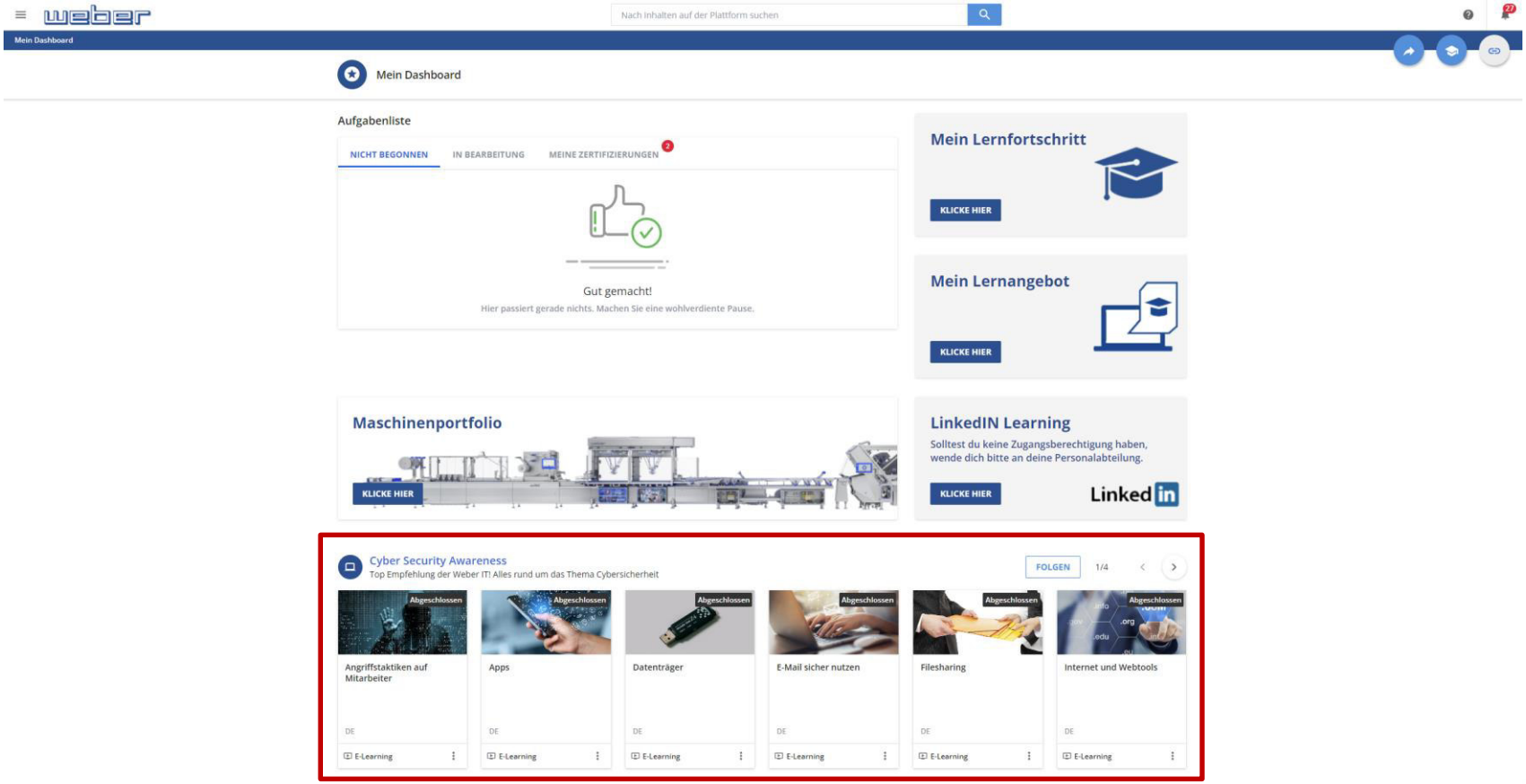
SCHUTZ

Regelmäßige Updates

Sicherheitssoftware

Authentifizierungsmethoden

gesunder Menschenverstand


Nach Inhalten auf der Plattform suchen
Mein Dashboard
Mein Dashboard
Aufgabenliste
NICHT BEGONNEN
IN BEARBEITUNG
MEINE ZERTIFIZIERUNGEN
Gut gemacht!
Hier passiert gerade nichts. Machen Sie eine wohlverdiente Pause.
Mein Lernfortschritt
KLICKE HIER
Mein Lernangebot
KLICKE HIER
Maschinenportfolio
KLICKE HIER
LinkedIN Learning
Solltest du keine Zugangsberechtigung haben, wende dich bitte an deine Personalabteilung.
KLICKE HIER
Cyber Security Awareness
Top Empfehlung der Weber IT! Alles rund um das Thema Cybersicherheit
FOLGEN
1/4
Abgeschlossen
Angriffstaktiken auf Mitarbeiter
Apps
Datenträger
E-Mail sicher nutzen
Filesharing
Internet und Webtools
DE
E-Learning

Cyber Security Awareness

Top Empfehlung der Weber IT! Alles rund um das Thema Cybersicherheit

FOLGEN 1/4

Angriffstaktiken auf Mitarbeiter

DE

E-Learning

Apps

DE

E-Learning

Datenträger

DE

E-Learning

E-Mail sicher nutzen

DE

E-Learning

Filesharing

DE

E-Learning

Internet und Webtools

DE

E-Learning

Cyber Security Awareness

Top Empfehlung der Weber IT! Alles rund um das Thema Cybersicherheit

FOLGEN 2/4

Kollaborationstools

DE

E-Learning

Messenger Dienste

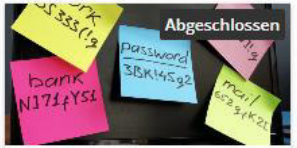
DE

E-Learning

Mobilgeräte sicher nutzen

DE

E-Learning



Passwörter

DE

E-Learning

Postfächer

DE

E-Learning

Präventive Maßnahmen am Arbeitsplatz

DE

E-Learning

WILLKOMMEN ZUM MODUL

Passwörter

V39z5k0y[*(7!JE]

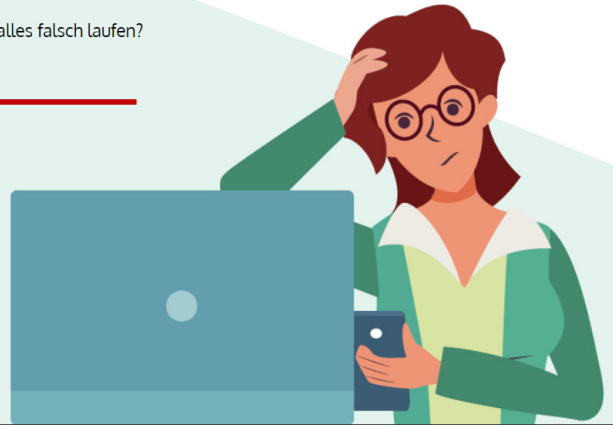
5Wer_Kennt_Ein_Besonders_Sicheres_Passwort?6

*****s?kl@aPE_Ä

Start

Was kann beim unvorsichtigen Gebrauch von Passwörtern alles falsch laufen?
Warum ist es so wichtig, Passwörter korrekt zu nutzen?
Wie wählen Sie sichere Passwörter aus?

Klicken Sie auf das Lautsprecher-Symbol oben rechts, um den Ton zu aktivieren.



Clara versucht sich in ihr E-Mail-Konto einzuloggen, aber ihr wird der Zugriff verwehrt

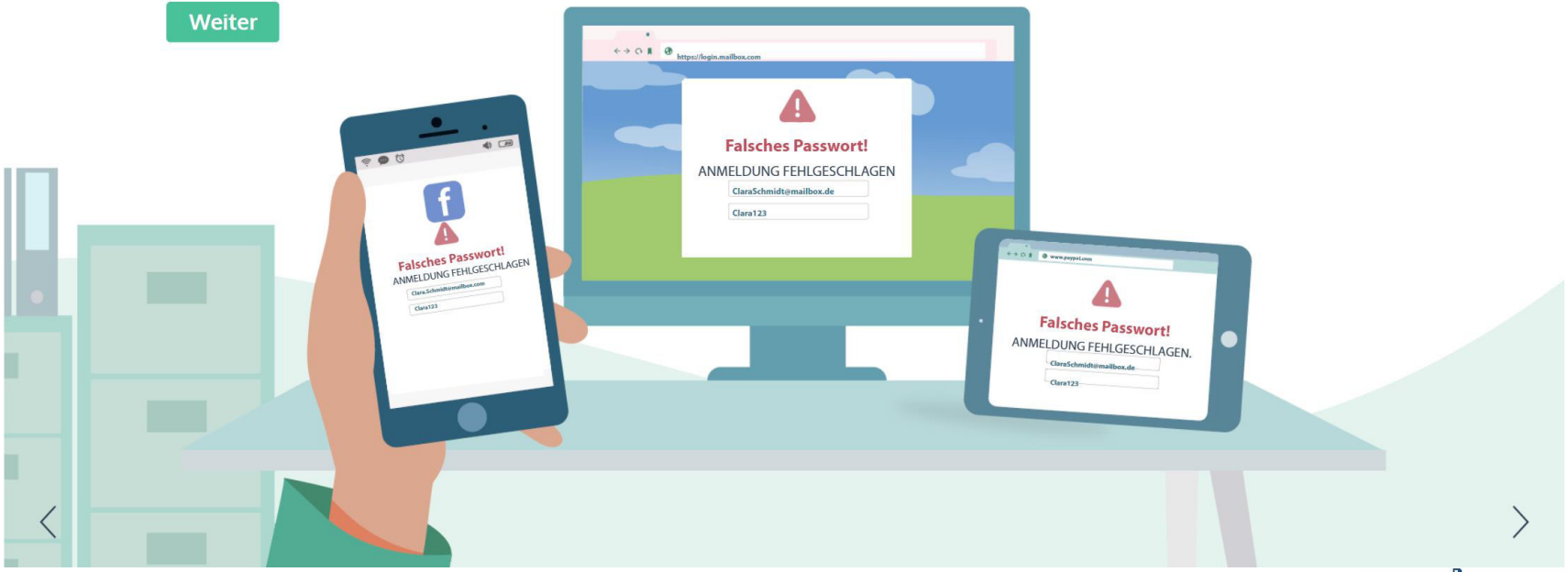
Plötzlich erscheint eine Warnmeldung. Clara wundert sich; sie benutzt ihr Lieblingspasswort „Clara123" schon seit Jahren und ist sich sicher, dass sie es in letzter Zeit nicht geändert hat.

Weiter

Clara hat auch keinen Zugriff auf ihre anderen Konten

Clara versucht, ihr Passwort für ihre sozialen Netzwerke, ihr privates und berufliches E-Mail-Konto und ihr Online-Banking einzugeben. Es erscheint überall die gleiche Nachricht.

Weiter



Die Gefahren des Kontrollverlusts über Passwörter

- [ ] FINANZIELLE SCHÄDEN FÜR SIE

  Cyberkriminelle können Überweisungen zu Ihren Lasten tätigen oder in Ihrem Namen Waren oder Dienstleistungen bestellen.

- [ ] SCHÄDEN FÜR IHR UNTERNEHMEN

  Cyberkriminelle können Firmengeheimnisse stehlen, Zahlungen tätigen oder wichtige Daten löschen.

- [ ] MISSBRAUCH IHRER IDENTITÄT

  Cyberkriminelle können Ihre Identität nutzen, um etwa Ihr privates Umfeld (Freundinnen und Freunde/Famile) anzugehen oder Sie öffentlich bloßzustellen.

Absenden

Wie erlangen Cyberkriminelle Zugriff auf Ihre Passwörter?

Es existieren verschiedene Angriffstaktiken.

PHISHING

„Abfischen" von Passwörtern über präparierte E-Mails, Nachrichten oder Anrufe.

- z. B. Abfrage des Passworts über eine gefälschte Anmelde-Maske.

BRUTE FORCE

Automatisierter Angriff auf die Anmeldemaske selbst, bei der schwache Passwörter mit „roher Gewalt" geknackt werden.

- z. B. systematisches Durchtesten von Wörter-/ und Zeichen-kombinationen mit Hilfe passender Wortlisten.

MALWARE

Schadprogramme, die sich unbemerkt auf dem Rechner des Opfers im Hintergrund installieren.

- z. B. Protokollierung der Tastatureingaben durch sog. "Key Logger".

SPIDERING

Gezielte Informationsbeschaffung über die Zielperson oder das Unternehmen, um ein naheliegendes Passwort zu erraten.

- z. B. schauen sich Cyberkriminelle Ihr Profil in den sozialen Medien an, sehen, dass Ihr Hund "Rex" heißt – und probieren dies dann als Passwort aus.

Weiter

Passwortsicherheit

Woran erkennt man starke und schwache Passwörter?

Schwache Passwörter

- ✗ Beinhalten persönliche Daten (z. B. Geburtsjahr).
- ✗ Enthalten Wiederholungs- oder Tastaturmuster.
- ✗ Beinhalten ein alleinstehendes Wort aus Lexikon oder Duden, wie z. B. "Baumhaus734".

Starke Passwörter

- ✓ **Sind möglichst lang, mindestens 16 Zeichen.**
  Dies ist der mit Abstand wichtigste Faktor bei der Sicherheit eines Passwortes.
- ✓ Beinhalten Groß- und Kleinbuchstaben.
- ✓ Enthalten Zahlen und Sonderzeichen.

Wie funktioniert ein Passwortmanager?

Weiter

Sie müssen sich **nur ein einziges, sicheres Master-Passwort merken**.
Der Passwortmanager merkt sich alle anderen Passwörter für Sie. Ihre Passwörter werden durch eine starke Verschlüsselung geschützt...

Außerdem hilft Ihnen ein Passwortmanager dabei, **starke und sichere Passwörter** für Ihre Dienste zu erstellen.
Sie sollten aber unbedingt einstellen, dass neu generierte Passwörter mindestens 16 Zeichen lang sind.

Vorsicht: auf Ihr Master-Passwort müssen Sie **ganz besonders gut achtgeben**!

Zwei-Faktor-Authentifizierung (2FA)

Für Konten mit sensiblen Daten sollten Sie eine **Zwei-Faktor-Authentifizierung** nutzen. Dabei müssen Sie Ihre Identität auf zwei unterschiedlichen und unabhängigen Endgeräten bestätigen, bevor Sie Zugriff auf die Daten erhalten. Dies erhöht die Sicherheit deutlich.

Weiter

1

PASSWORT-EINGABE AUF GERÄT 1

Melden Sie sich in Ihrem Konto mit Ihrem Benutzernamen und Passwort an.

2

BESTÄTIGUNG AUF GERÄT 2

Sie erhalten z. B. auf Ihrem Smartphone eine SMS oder Push-Nachricht. Diese müssen Sie bestätigen oder den dort enthaltenen Code eingeben.

3

DATEN-ZUGRIFF AUF GERÄT 1

Nach Eingabe erhalten Sie den Zugriff auf Ihr Konto. Man kennt das Prinzip auch vom TAN-Verfahren beim Onlinebanking.

Checkliste – Diese vier Schritte sollten Sie heute noch umsetzen

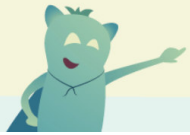
1. **Starke Passwörter**
   Nutzen Sie starke Passwörter (z. B. weBoo89tZo$%pPz6), evtl. mit Hilfe eines Passwortgenerators.

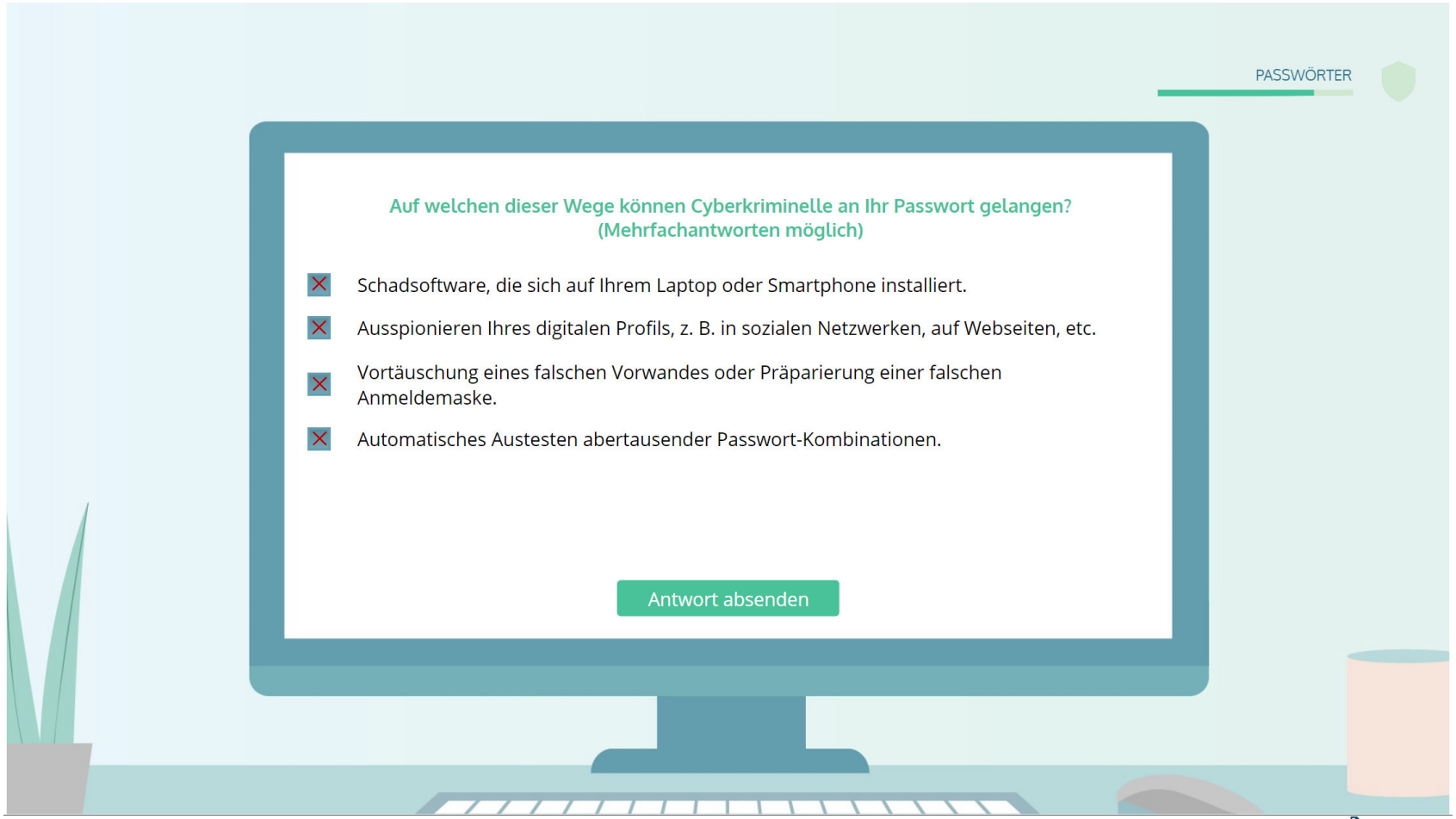
2. **Passwortmanager nutzen**
   Ein Passwortmanager hilft Ihnen, den Überblick zu behalten. So müssen Sie die Passwörter nicht aufschreiben und unsicher verwahren.

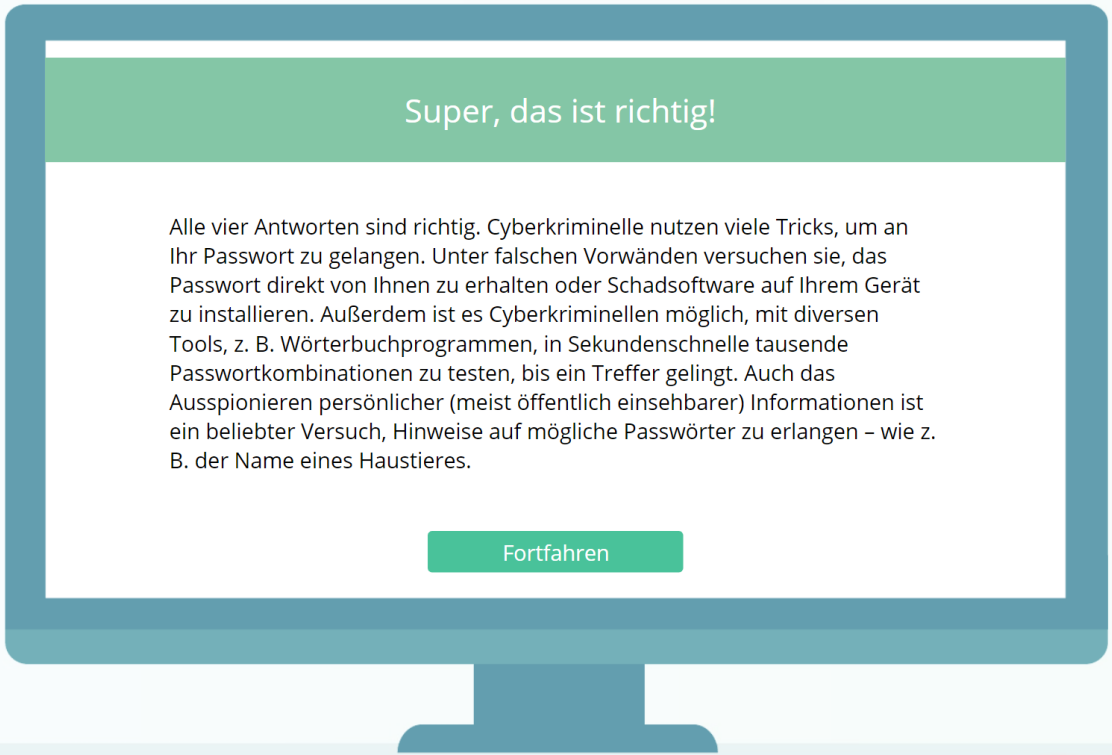
3. **Ein Passwort pro Account**
   Verwenden Sie Ihre Passwörter nicht mehrfach. Achtung: lieber lange und selten gewechselte Passwörter, als kurze und häufig gewechselte.

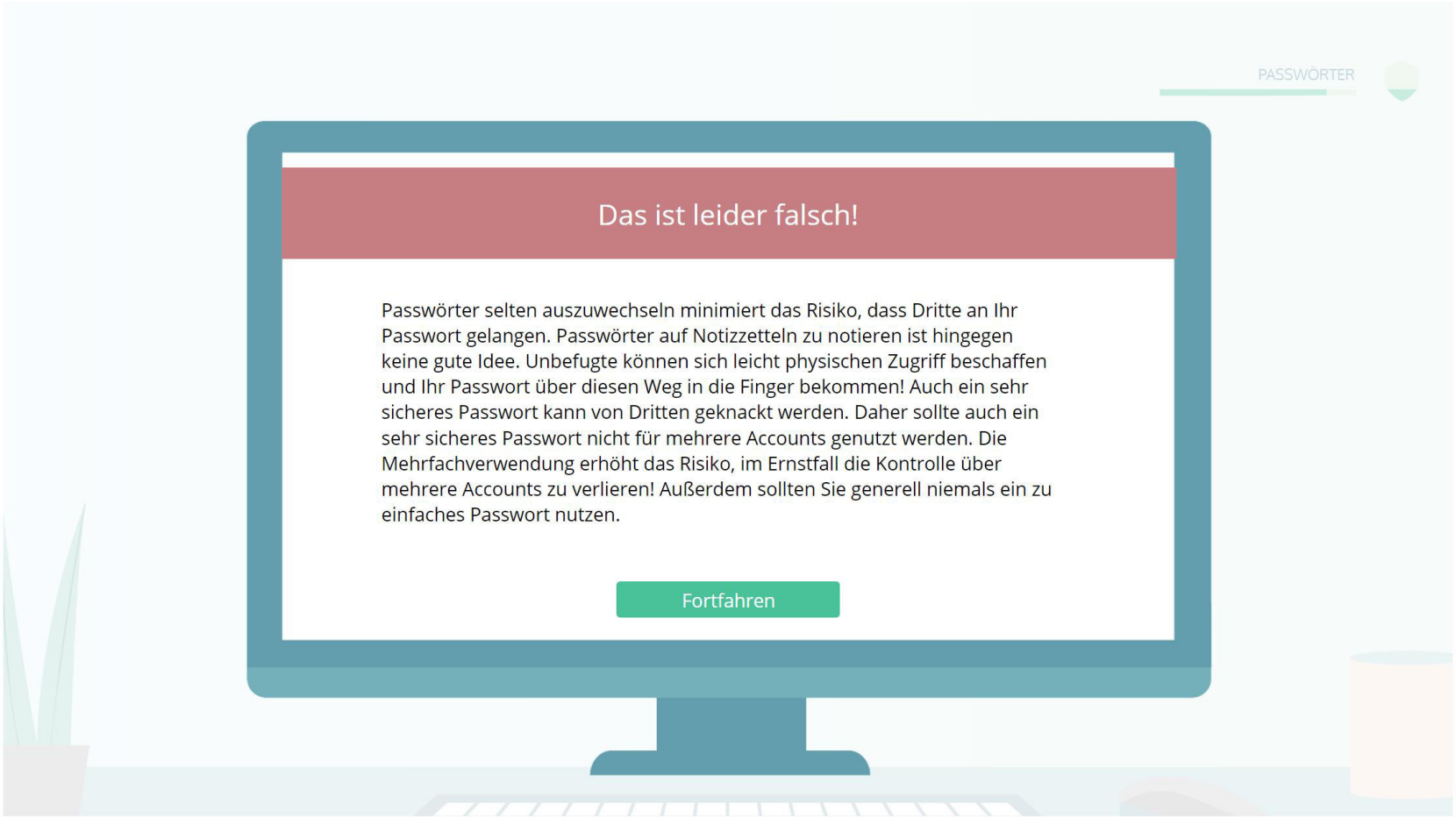
4. **2FA für sensible Konten nutzen**
   Für besonders sensible Konten/Postfächer etc. sollten Sie eine Zwei-Faktor-Authentifizierung nutzen.

Weiter




Auf welchen dieser Wege können Cyberkriminelle an Ihr Passwort gelangen?
(Mehrfachantworten möglich)
Schadsoftware, die sich auf Ihrem Laptop oder Smartphone installiert.
Ausspionieren Ihres digitalen Profils, z. B. in sozialen Netzwerken, auf Webseiten, etc.
Vortäuschung eines falschen Vorwandes oder Präparierung einer falschen Anmeldemaske.
Automatisches Austesten abertausender Passwort-Kombinationen.
Antwort absenden


Super, das ist richtig!
Alle vier Antworten sind richtig. Cyberkriminelle nutzen viele Tricks, um an Ihr Passwort zu gelangen. Unter falschen Vorwänden versuchen sie, das Passwort direkt von Ihnen zu erhalten oder Schadsoftware auf Ihrem Gerät zu installieren. Außerdem ist es Cyberkriminellen möglich, mit diversen Tools, z. B. Wörterbuchprogrammen, in Sekundenschnelle tausende Passwortkombinationen zu testen, bis ein Treffer gelingt. Auch das Ausspionieren persönlicher (meist öffentlich einsehbarer) Informationen ist ein beliebter Versuch, Hinweise auf mögliche Passwörter zu erlangen – wie z. B. der Name eines Haustieres.
Fortfahren


PASSWÖRTER
Das ist leider falsch!
Passwörter selten auszuwechseln minimiert das Risiko, dass Dritte an Ihr Passwort gelangen. Passwörter auf Notizzetteln zu notieren ist hingegen keine gute Idee. Unbefugte können sich leicht physischen Zugriff beschaffen und Ihr Passwort über diesen Weg in die Finger bekommen! Auch ein sehr sicheres Passwort kann von Dritten geknackt werden. Daher sollte auch ein sehr sicheres Passwort nicht für mehrere Accounts genutzt werden. Die Mehrfachverwendung erhöht das Risiko, im Ernstfall die Kontrolle über mehrere Accounts zu verlieren! Außerdem sollten Sie generell niemals ein zu einfaches Passwort nutzen.
Fortfahren

GRATULATION!
Sie haben 75 % erreicht.
Sie sind schon ein richtiger Cyberprofi! Sie haben dieses Modul erfolgreich bestanden.
Modul schließen
Modul wiederholen

Vielen Dank für Ihre Aufmerksamkeit!

Tom Güldner

Lehrstuhl Medienbildung und Medienpädagogik
Universität Greifswald

DigiDIALOG

DIGITALISIERUNG IM DIALOG

Prof. Dr. Ines Sura
Tom Güldner

Sicherheit durch Medienkompetenz

UNIVERSITÄT GREIFSWALD
Wissen lockt. Seit 1456

WAS IST DIGIDIALOG?

SMARTE.LAND.REGIONEN

2022-2023

Alle Bürger:innen VG

Digitalitätsbezogen Kompetenzen

kostenlos

Was ist DigiDialog

Imagefilm	01
Medienkompetenz	02
Blick in die Veranstaltungen	03
Wie ist es gelaufen?	04
Ausblick	05

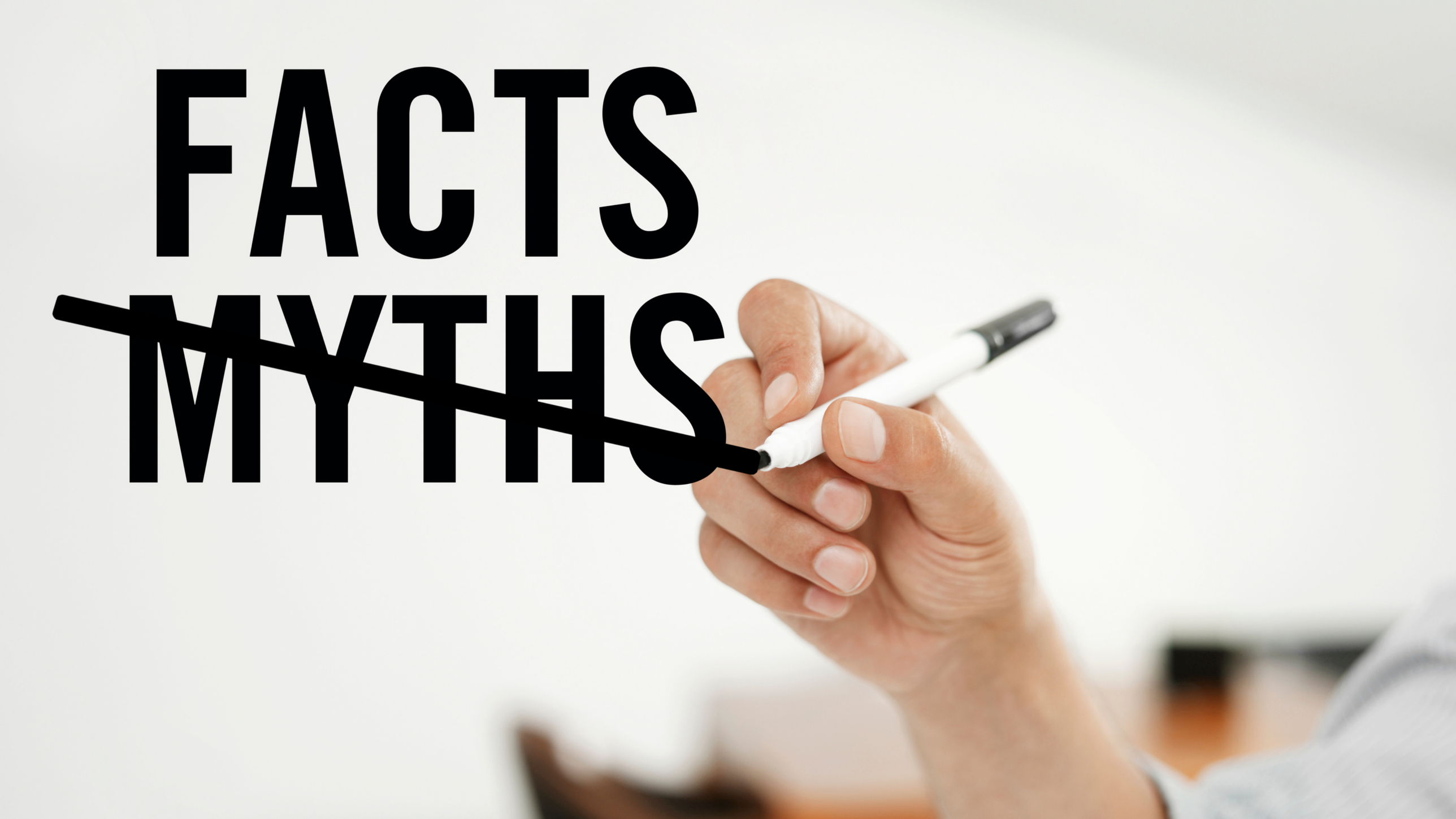
DigiDIALOG
DIGITALISIERUNG IM DIALOG

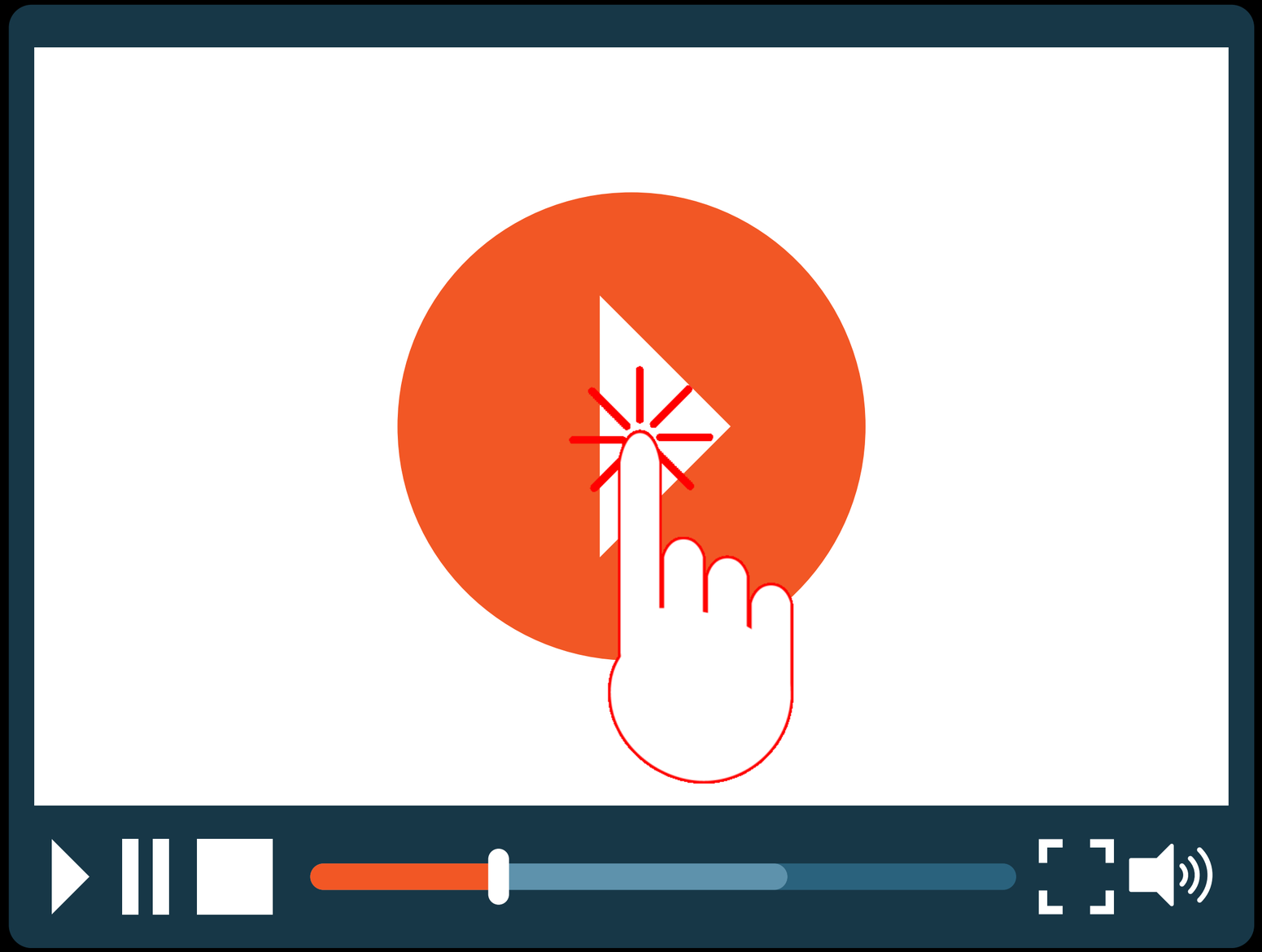
MEDIA
LITERACY

Was haben wir umgesetzt?

Kahoot Urheberrecht

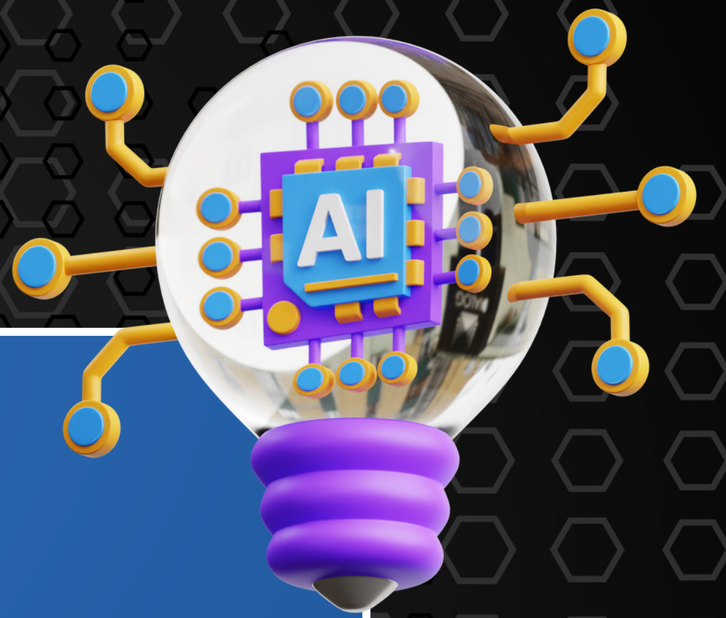
PODCAST


FACTS
MYTHS



Hilfe zur Selbsthilfe

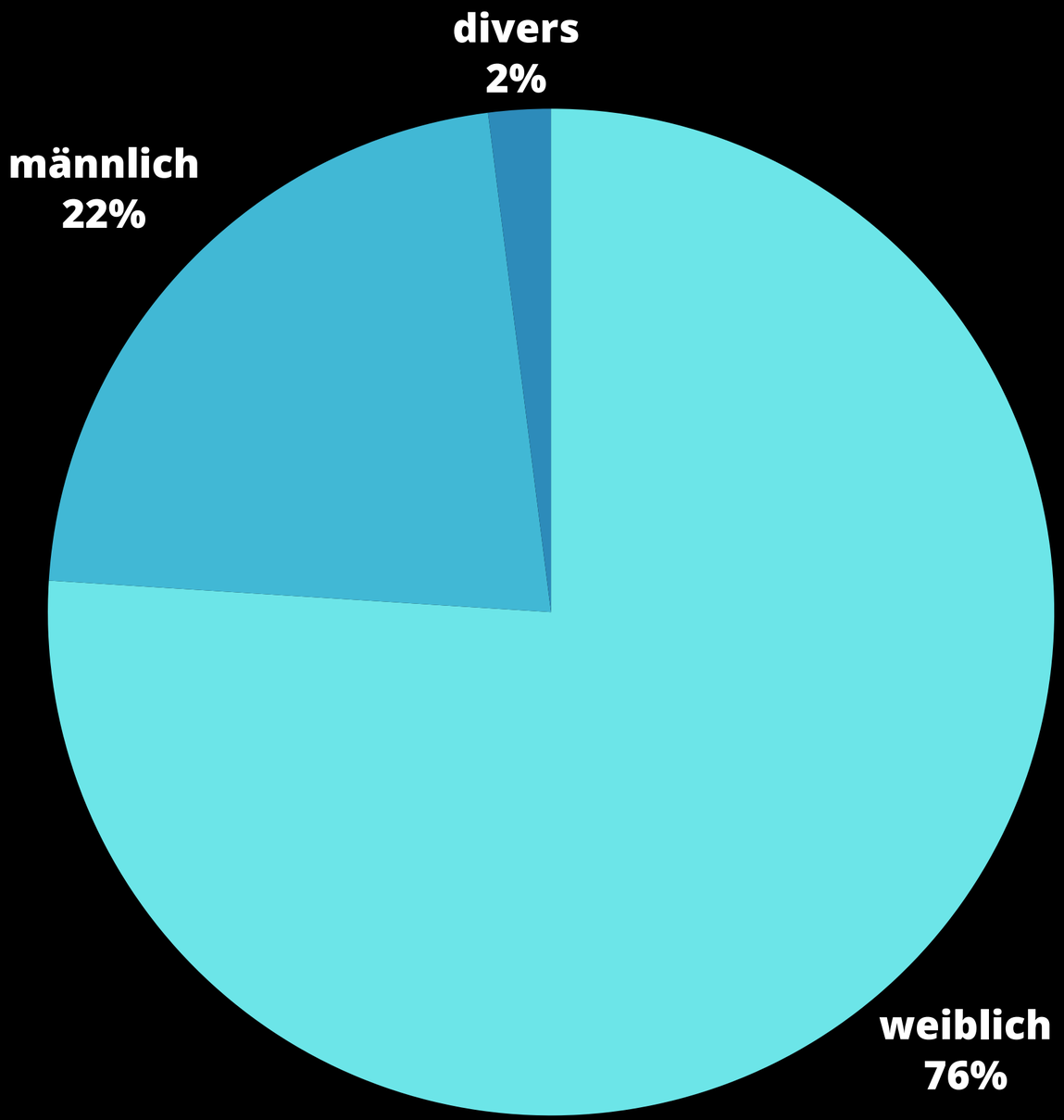
Wie ist es gelaufen?



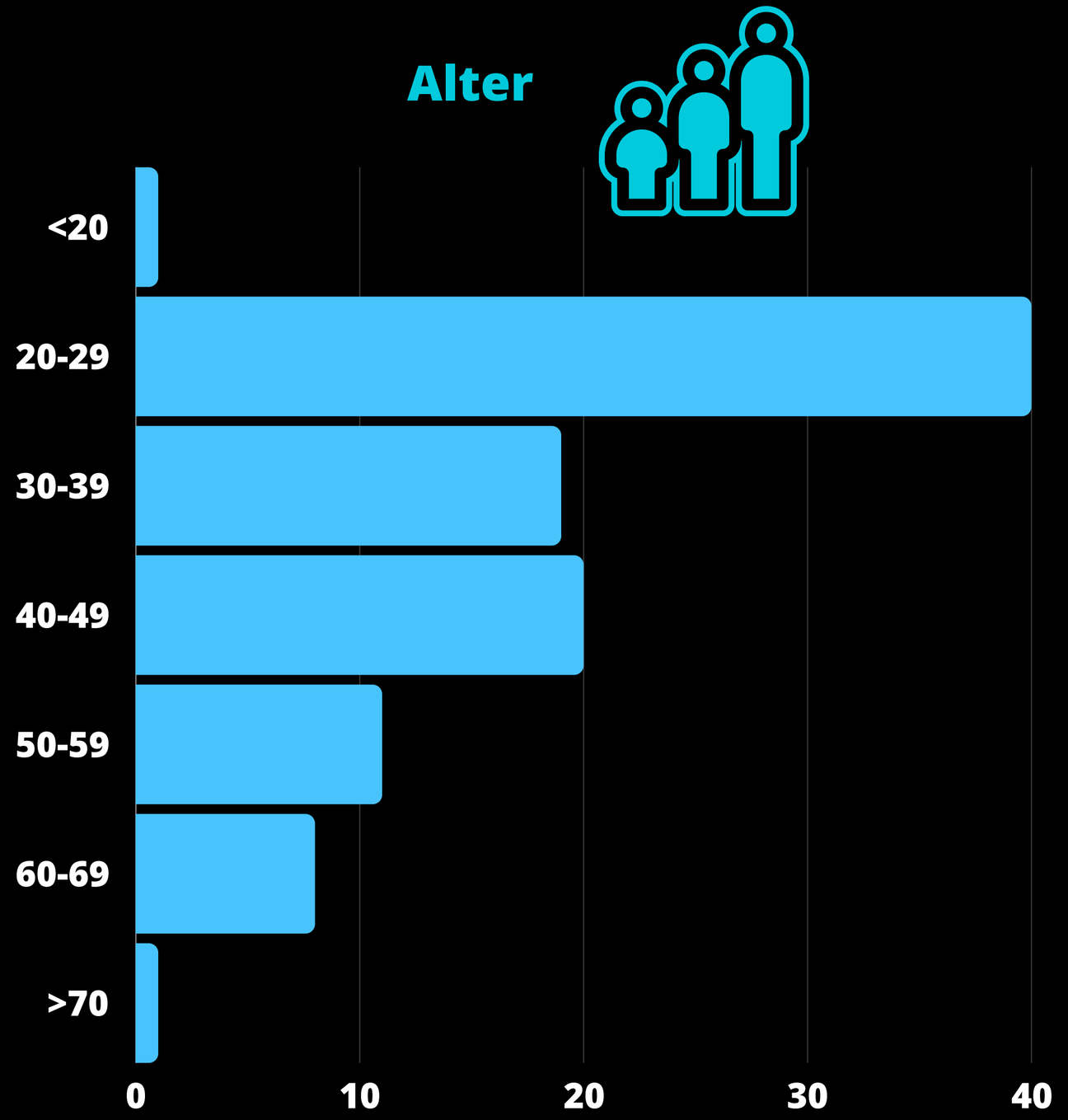
01 Quantitativ: Fragebogen (n=104) & Beobachtungsprotokoll

02 Qualitativ: Interviews mit Teilnehmer:innen (n=17)

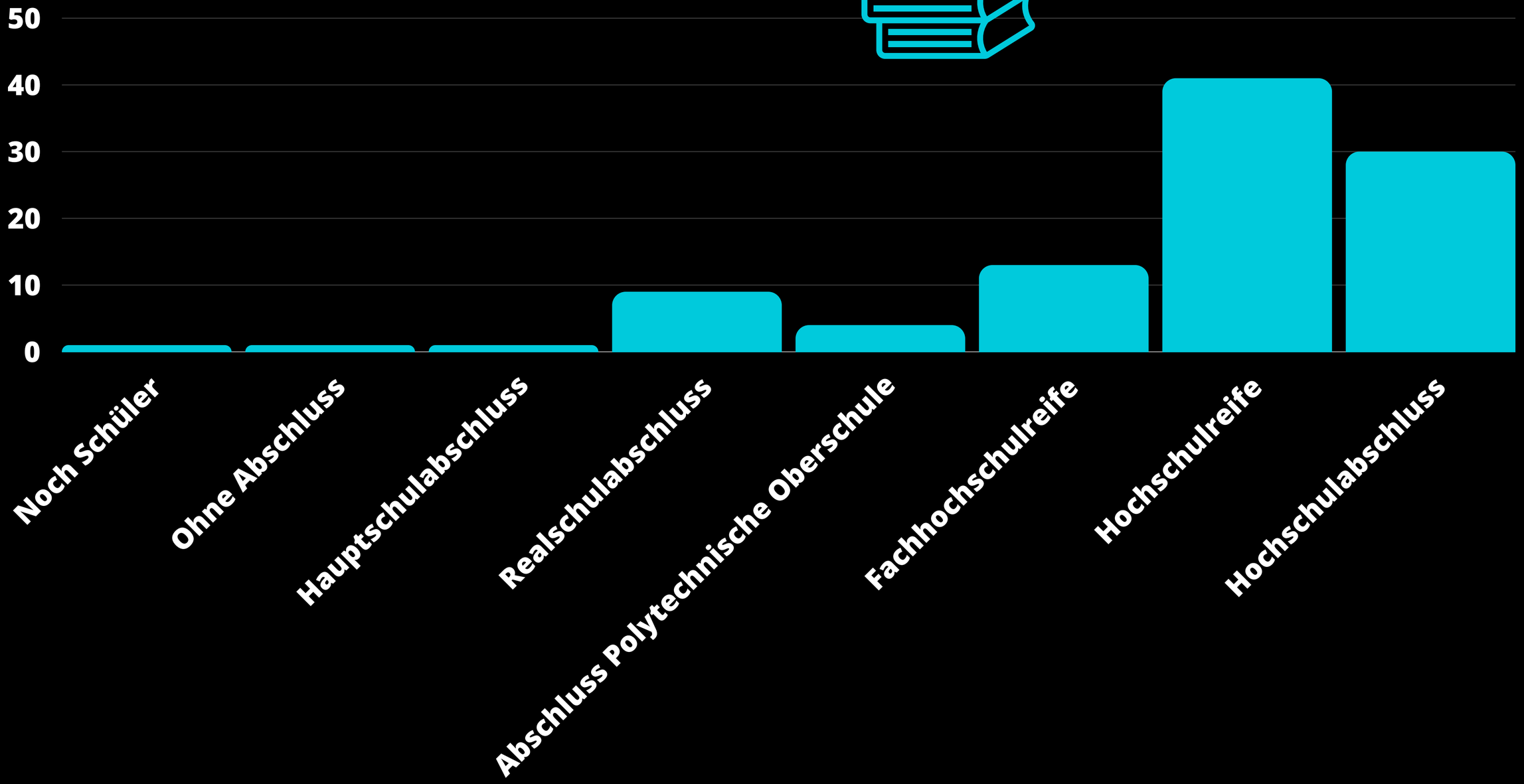
Identifikation



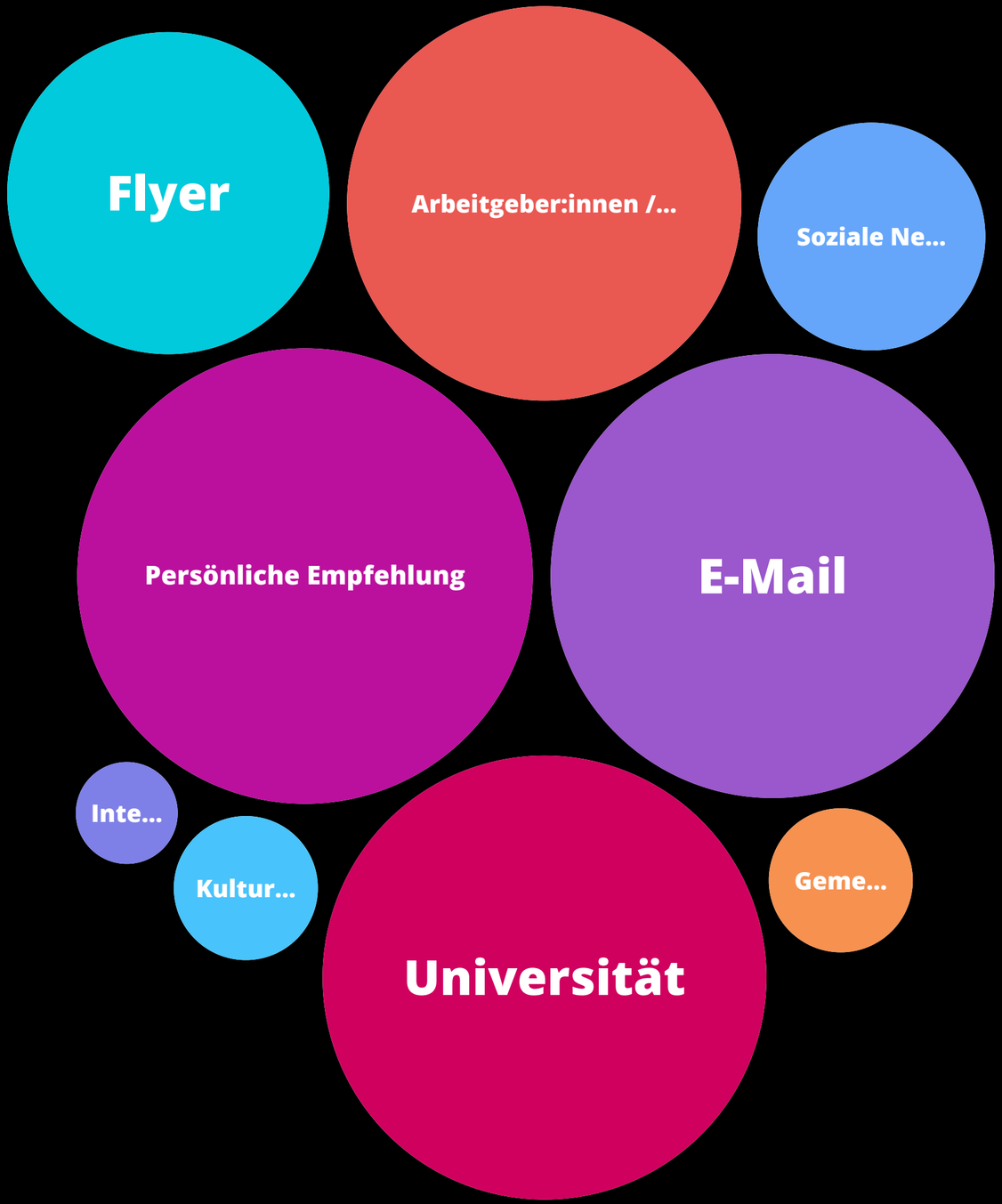
Alter



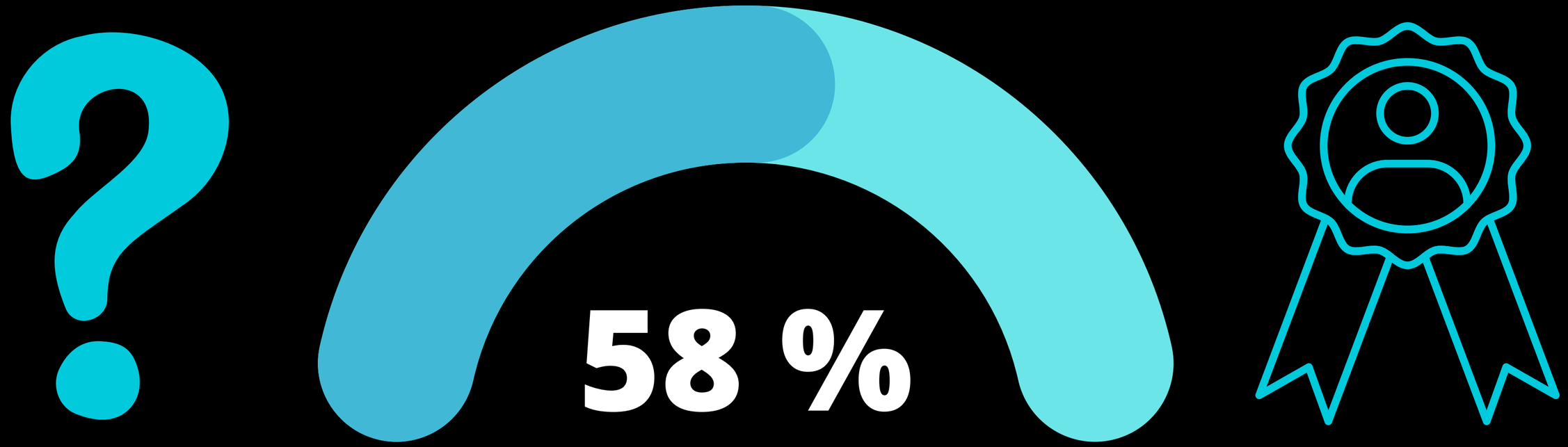
Formale Bildung



Wie sind Teilnehmer:innen auf die DigiDialoge aufmerksam geworden?



Wie schätzen die Teilnehmer:innen Ihre digitale Kompetenz ein?



Offenheit

Skepsis

An dieser Veranstaltung gefiel mir besonders...

VIELFALT

FRAGEN

INTERAKTIV

DIVERSE APPS

PRAXIS

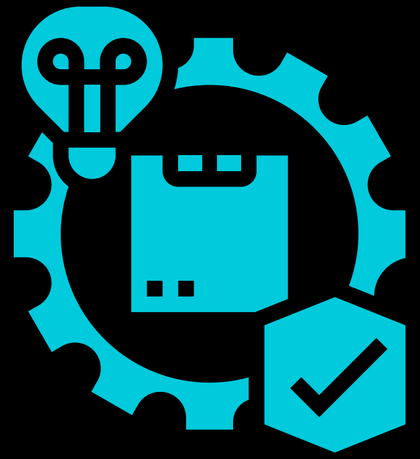
ATMOS-SPHÄRE

KREATIV

SELBER MACHEN

Weitere Tipps für eine gelungene Veranstaltung

- Stärker für Zielgruppen schärfen
- Mehr bewerben
- Anfahrt angeben



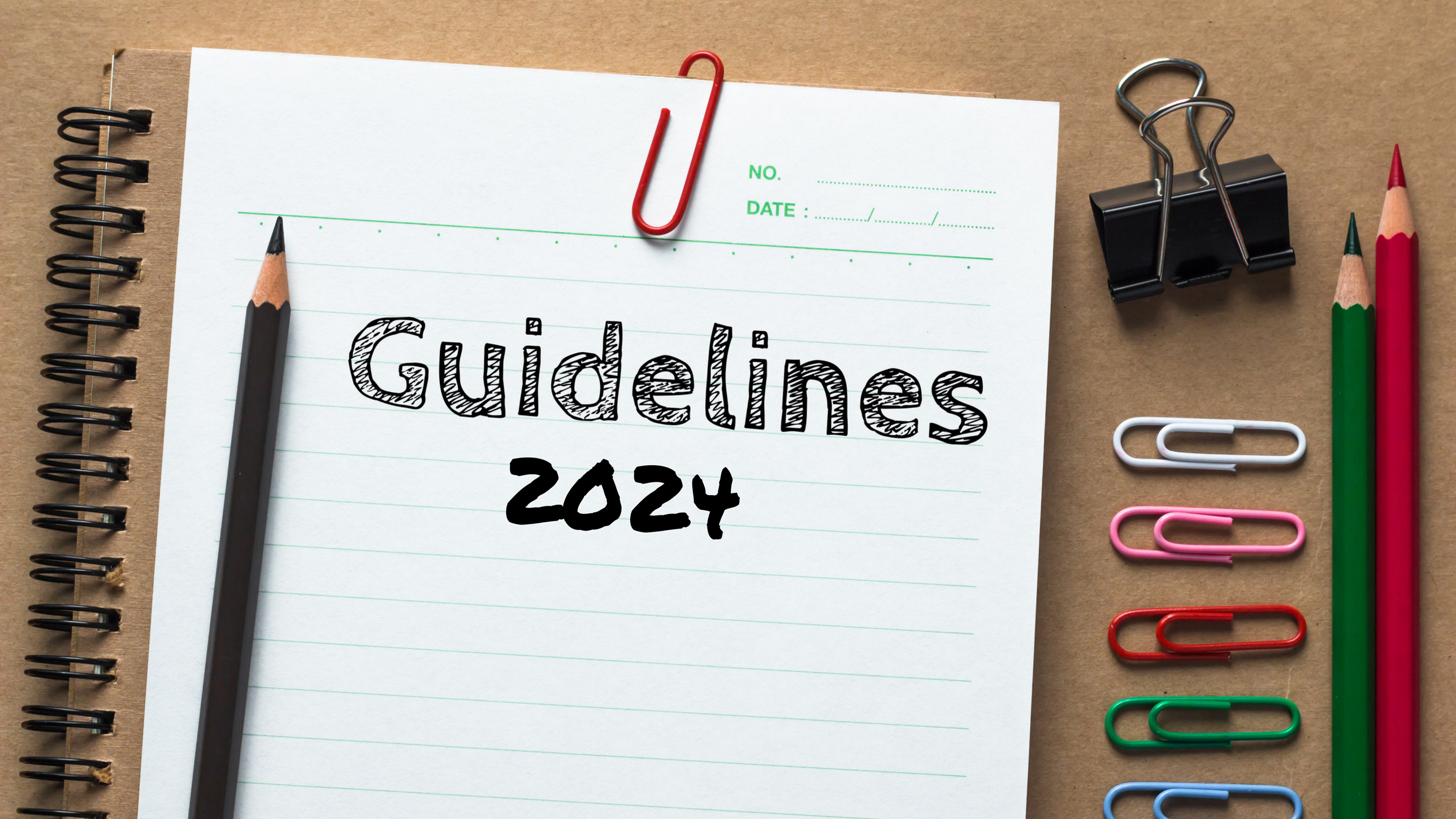
- Kurze Vorstellungsrunde
- Aufbauend vertiefende Module
- Häufiger stattfinden lassen
- Klare Struktur und Führung
- Kekse & Getränke bereitstellen

DO'S

- Praxisnah / Selber machen
- Offene Atmossphäre
- Klare Struktur

DON'TS

- Zu viel Theorie
- Keinerlei Anleitung
- Technik nicht vorab testen


NO.
DATE : ...../...../.....
Guidelines
2024

Tom Güldner

Institut für Erziehungswissenschaft

Lehrstuhl für Medienpädagogik und Medienbildung

Tom.Gueldner@uni-greifswald.de

Ausblick

Jennifer Billowie
Digitales Innovationszentrum Greifswald (WITENO)

Monique Wittassek
Landkreis Vorpommern-Greifswald /
Smarte.Land.Regionen

Feedback

Wie hat Ihnen die Veranstaltung gefallen?

Nehmen Sie teil!

https://tweedback.de/zuxx

Kofinanziert von der Europäischen Union

MV tut gut.

WITENO

digitales MV

Gefördert durch:
Bundesministerium für Ernährung und Landwirtschaft
aufgrund eines Beschlusses des Deutschen Bundestages

LANDKREIS VORPOMMERN-GREIFSWALD

digitales MV | Digitales Innovationszentrum Greifswald
Kofinanziert von der Europäischen Union
MV tut gut.

Verpassen Sie keine unserer Events in Ihrer Region!