G&R CYBERSECURITY

Mögliche Cyberattacke: Stadt Potsdam nimmt Server der Verwaltung vom Netz

Nach Malware-Infektion: Katastrophenfall im Landkreis Anhalt-Bitterfeld

KEINE E-MAILS, FRANKFURT.DE OFFLINE

„Emotet“ legt Stadt-Computer lahm

Stadtwerke Wismar: Ermittlungen nach Cyberattacke laufen

Hackerangriff auf Verwaltungen in Wesel und Witten

Brandenburg fährt die Server runter

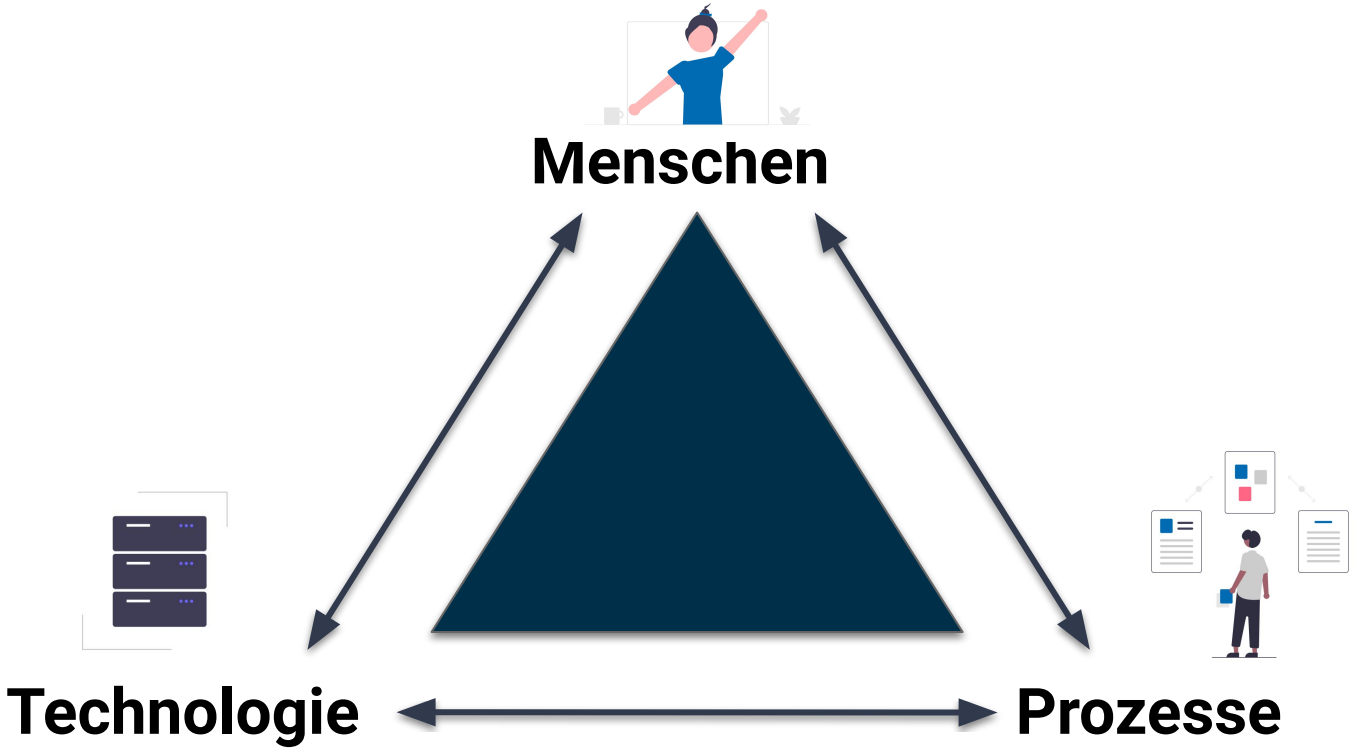
CYBERANGRIFF

Hackerangriff in Mecklenburg-Vorpommern legt Kommunalverwaltungen seit Tagen lahm

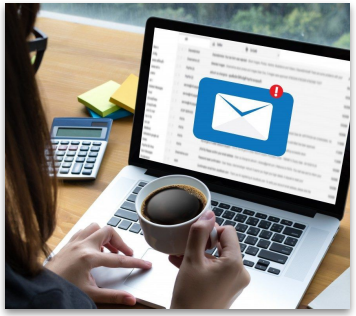
SCHWERIN UND LUDWIGSLUST-PARCHIM

Probleme nach Cyberangriff dauern an – Sicherheitslücke bisher nicht gefunden

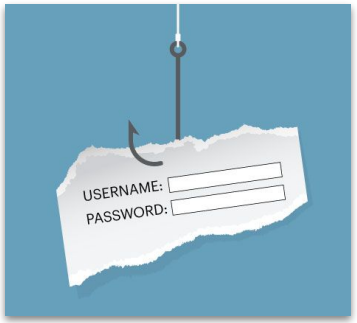
Was ist Cyber-Security?



Beispiel: Ransomware



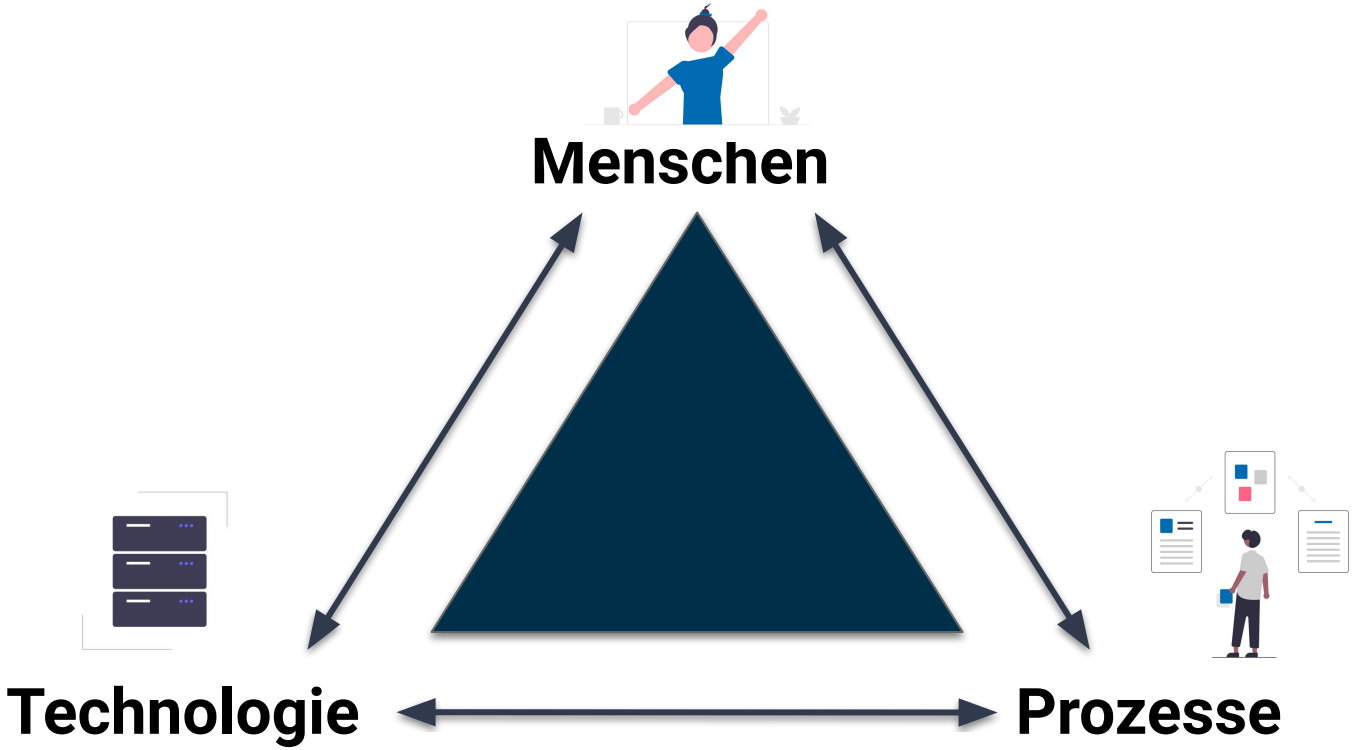
Mitarbeiter fällt auf Phishing herein



Erbeutung der Zugangsdaten

Trojaner im Hintergrund aktiv

Was ist Cyber-Security?



Was machen wir?

Technologie

- GAP-Analysen
- Penetration Tests
- Digitale Forensik

Menschen

- Schulungen
- Workshops
- Phishing Kampagnen

Prozesse

- Beratung
- Notfallkonzepte
- Incident Response

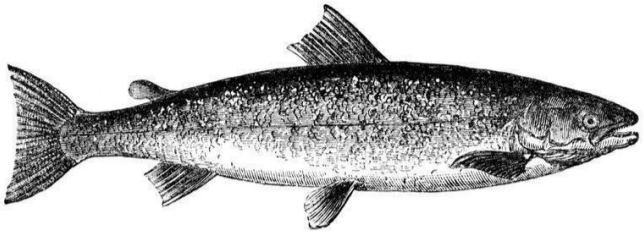
Probleme für die Gesundheitsbranche

- Vernetzung fast aller Systemen
- Wenige Sicherheitsstandards
- Unterschiedliches Bewusstsein
- Fehlende Strategie für Notfälle
- Professionalisierung von Kriminellen

Ransomware “Wannacry” befällt die Deutsche Bahn im Jahr 2017

Lösung?

Security by optimism and prayer



Expert

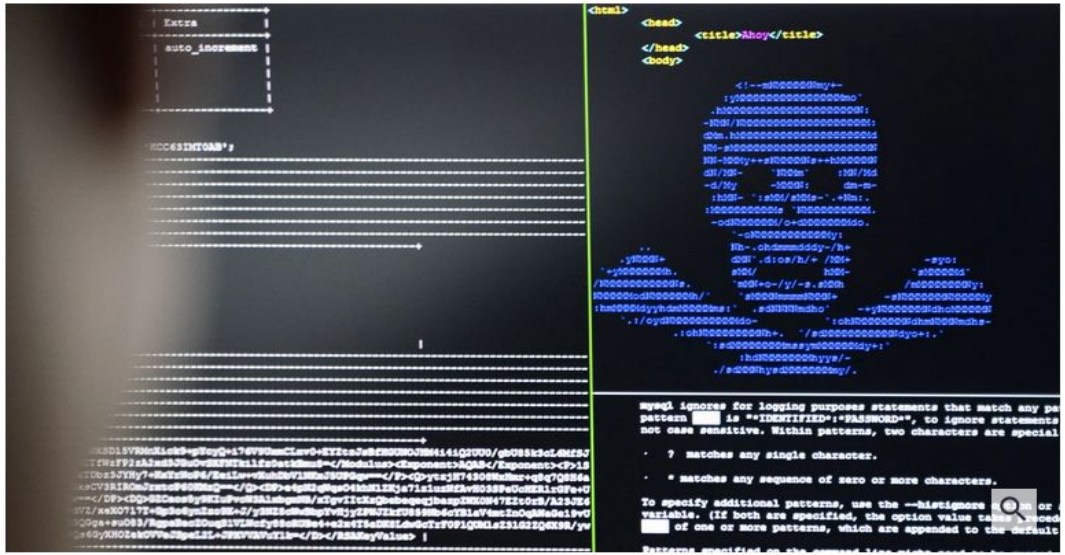
Hoping Nobody Hacks You

Cyberversicherung

Hackerangriffe bei Firmen

Versicherer werden immer vorsichtiger

16. Januar 2024, 15:57 Uhr | Lesezeit: 1 min | Kommentare



Strategie

Strategischer Ansatz

Die richtigen Fragen zu stellen

- Wo stehen wir heute?
- Wo wollen wir hin?
- Was heißt gute Sicherheit?
- Was muss getan werden?

Die richtigen Lösungen finden

Vorgehensmodell

Information Security Management ISO 27001 Certified

ISIS 12
Informationssicherheit für den Mittelstand

IHK München und Oberbayern

DWA

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Verfassungsschutz

BSI
IT Grundschutz
100-x | 200-x

Informationen aus den Interviews

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

GAP Fragenkatalog

Vorgehensweise

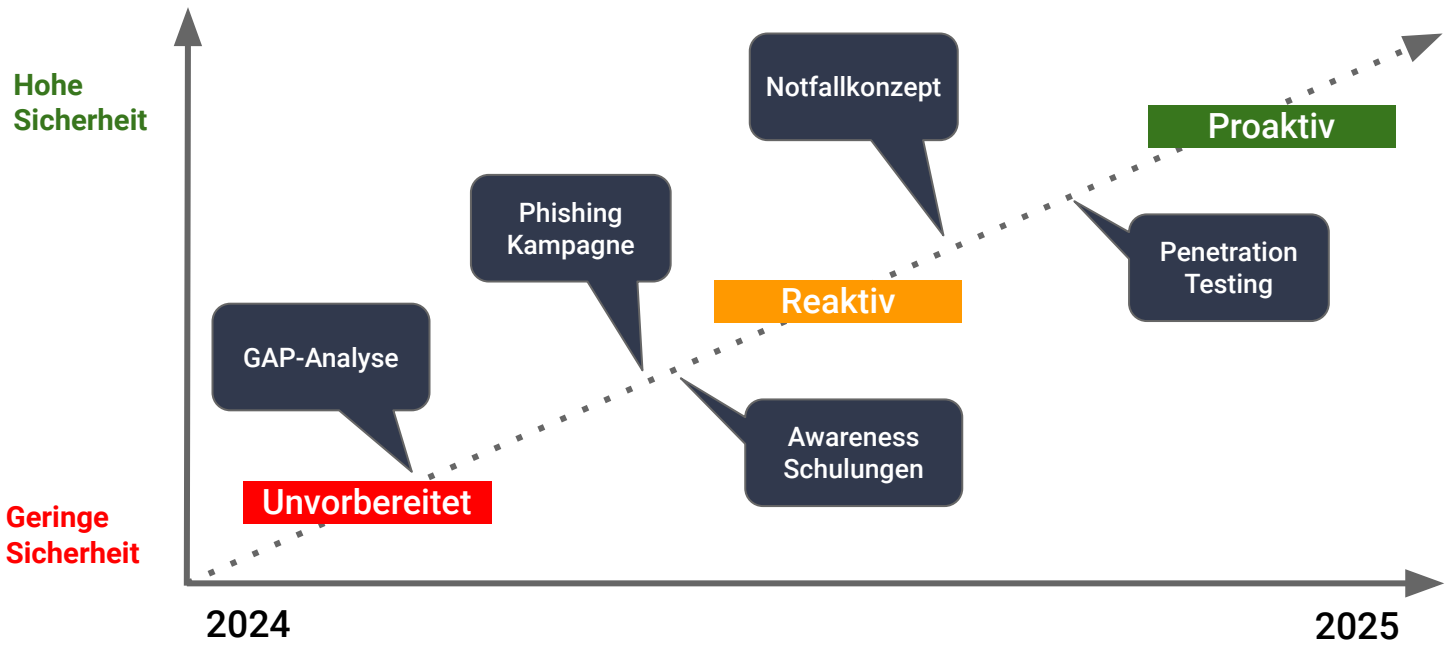
Bericht GAP-Analyse

- Liste an Schwachstellen
- Checkliste von Maßnahmen
- Handlungsempfehlungen

→ **Cybersecurity Strategie**

ID	Risiko	Name
1	Kritisch	Veraltete Office Lizenzen
2	Kritisch	Unzureichende Passwortsicherheit und Authentifizierung
3	Kritisch	Fehlender Notfallplan
4	Kritisch	Fehlendes Notfallhandbuch
5	Kritisch	Mangelendes Sicherheitsbewusstsein
6	Kritisch	Unzureichende Netzwerksicherheit
7	Kritisch	Fehlende Penetrationstests
8	Kritisch	Offene Serverraum Türen
9	Hoch	Offene Büro Türen
10	Hoch	Entsperrte Computer
11	Hoch	Fehlende Netzwerksegmentierung
12	Hoch	Unzureichende Daten Verschlüsselung
13	Hoch	Unzureichende Server-Festplatten Verschlüsselung
14	Hoch	Unzureichende Verschlüsselung aller Backups
15	Medium	Mangelnde Auflistung kritischer Daten
16	Medium	Fehlende Klassifizierung der Daten
17	Medium	Veraltete Passwortrichtlinen

Beispiel einer Cybersecurity Strategie



Inhalt

Sicherheitstests

- Schwachstellen Analysen
- Penetration Tests
- Phishing Kampagnen

Was ist ein Penetrationstest?

- Sicherheitsüberprüfung der IT-Infrastruktur
- Extern & intern
- **Ziel:** Schwachstellen Erkennen

Perimeter-Sicherheit

Schwachstellen

Diese Schwachstellen wurden bei den Tests festgestellt:

Schweregrad	Name
Kritisch	End of Life (EOL) von Betriebssystemen
Kritisch	Prüfung auf Discard-Dienst
Kritisch	MS15-034 HTTP.sys Sicherheitslücke bei der Remote-Codeausführung (Active Check)
Kritisch	Firebird Standard-Zugangsdaten (Firebird Protokoll)
Kritisch	jQuery End of Life (EOL)
Kritisch	Microsoft SQL Server End of Life (EOL)
Kritisch	VMSA-2017-0006: VMware ESXi-Updates beheben kritische und mäßige Sicherheitsprobleme (Remote-Check)
Kritisch	Schwachstelle der Microsoft Windows Remotedesktopdienste bei Remotecodeausführung (Bluekeep) - (Remote Active)
Hoch	SSL/TLS: Kompromittierte Zertifikate
Hoch	Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Sicherheitslücke
Hoch	OpenStage SIP-Standard-Zugangsdaten (HTTP)
Hoch	Anonymer FTP Login enthält Hash für Root-Zugang
Hoch	Microsoft Windows SMB Server - Mehrere Sicherheitslücken - Remote (4013389)
Hoch	SSL/TLS: Anfällige Cipher Suites für HTTPS
Medium	Anonyme FTP-Anmeldung
Medium	MQTT-Broker erfordert keine Authentifizierung
Medium	SSL/TLS: Server-Zertifikat / Zertifikat in Kette mit RSA-Schlüsseln kleiner als 2048 Bit

Kritische Schwachstellen

7.1 End of Life (EOL) von Betriebssystemen

Kritisch

CVSS:2/AV:N/AC:L/Au:N/C:C/I:C/A:C (Score: 10)

7.1.1 Betroffen

IP	Port	Hostname
192.168.110.50	general/tcp	
192.168.104.5	general/tcp	
10.211.54.30	general/tcp	
10.211.54.14	general/tcp	
10.211.54.33	general/tcp	
10.211.54.32	general/tcp	
192.168.101.101	general/tcp	
192.168.101.12	general/tcp	

Kritische Schwachstellen

Kritische Schwachstellen

8.3 OpenStage SIP-Standard-Zugangsdaten (HTTP)

Hoch

CVSS:2/AV:N/AC:L/Au:N/C:P/I:P/A:P (Score: 7.5)

8.3.1 Betroffen

IP	Port	Hostname
10.211.54.157	443/tcp	

8.3.2 Beschreibung

Das Remote OpenStage SIP Webinterface verwendet Standard-Zugangsdaten. Es war möglich, sich mit dem Benutzer Admin und dem Standardpasswort ‘123456’ anzumelden.

Kritische Schwachstellen

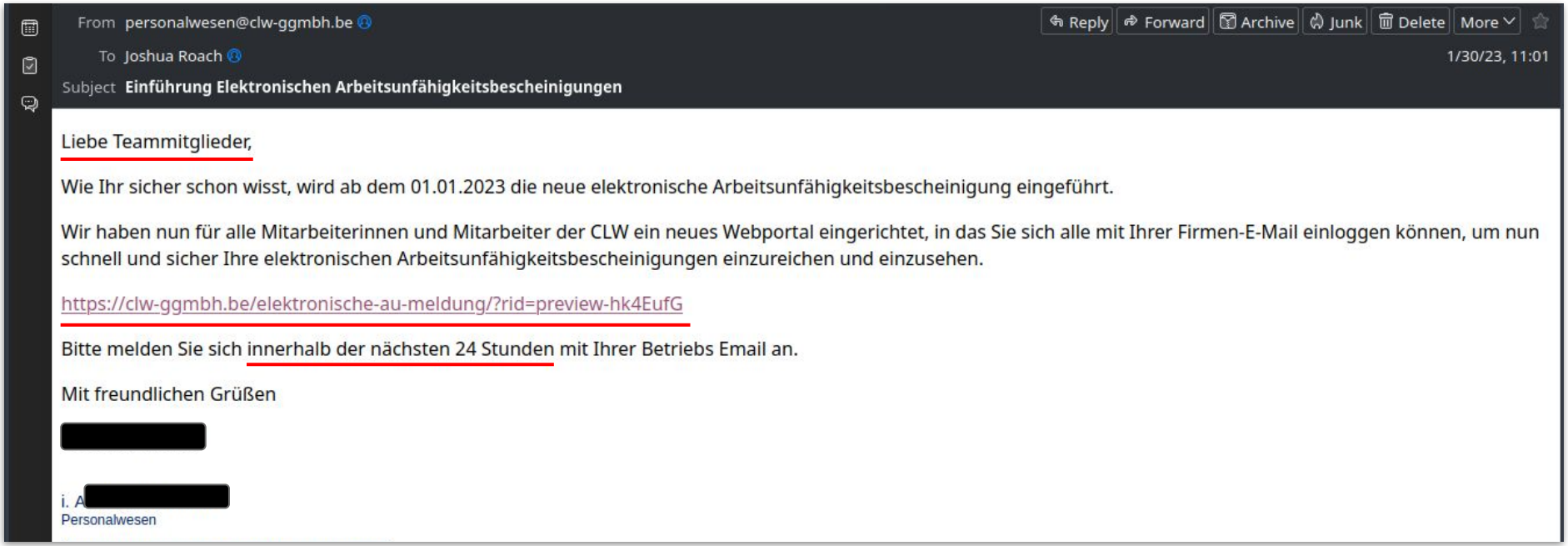
Phishing Tests

Was ist ein Phishing Test?

- Simulierte “böse” E-Mails
- Testet die Reaktion der Mitarbeiter
- **Ziel:** Sensibilisierung &

  Messung des Sicherheitsbewusstseins

Wie sieht eine Phishing E-Mail aus?



From personalwesen@clw-ggmbh.be
To Joshua Roach
Subject **Einführung Elektronischen Arbeitsunfähigkeitsbescheinigungen**

Reply | Forward | Archive | Junk | Delete | More

1/30/23, 11:01

Liebe Teammitglieder,

Wie Ihr sicher schon wisst, wird ab dem 01.01.2023 die neue elektronische Arbeitsunfähigkeitsbescheinigung eingeführt.

Wir haben nun für alle Mitarbeiterinnen und Mitarbeiter der CLW ein neues Webportal eingerichtet, in das Sie sich alle mit Ihrer Firmen-E-Mail einloggen können, um nun schnell und sicher Ihre elektronischen Arbeitsunfähigkeitsbescheinigungen einzureichen und einzusehen.

https://clw-ggmbh.be/elektronische-au-meldung/?rid=preview-hk4EufG

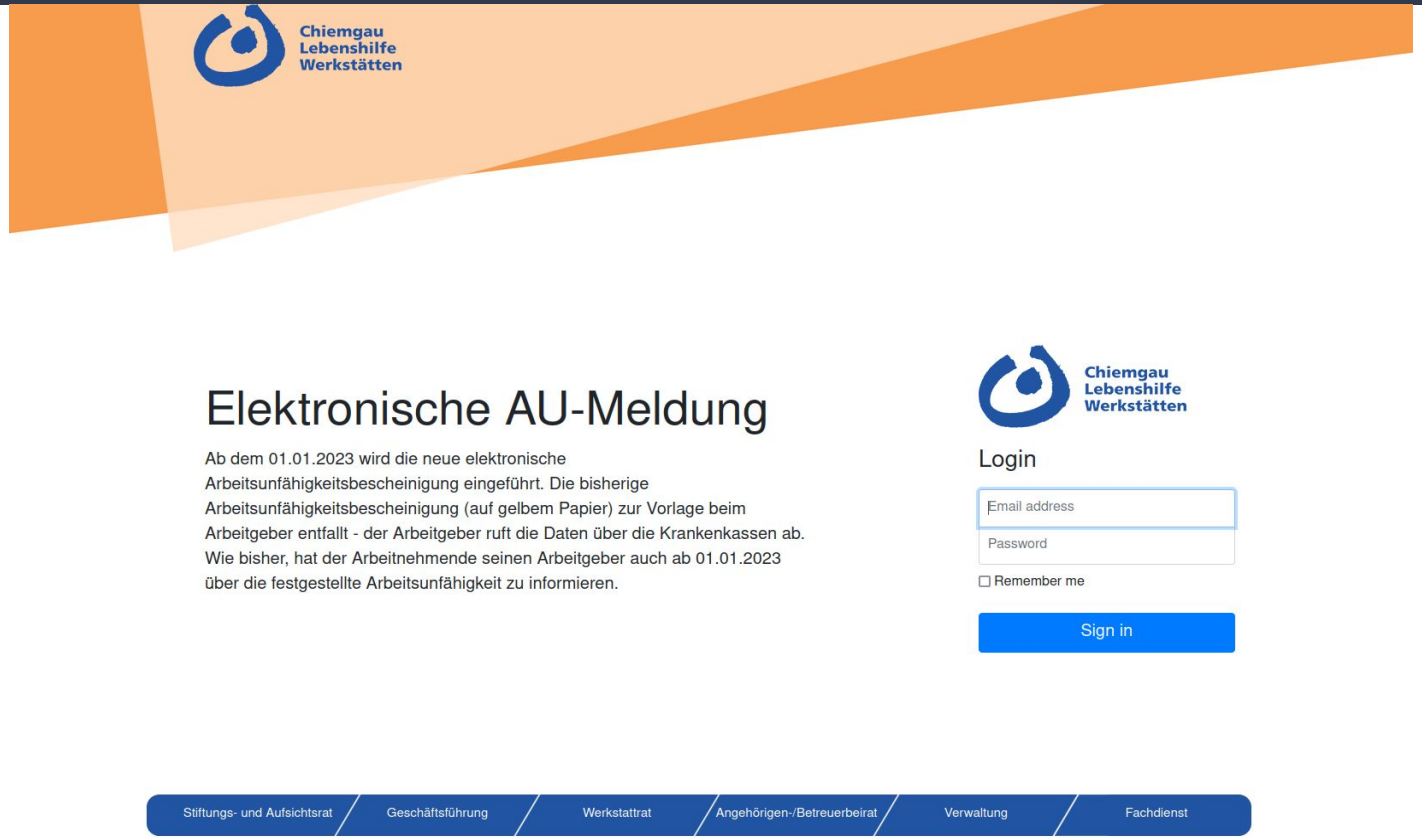
Bitte melden Sie sich innerhalb der nächsten 24 Stunden mit Ihrer Betriebs Email an.

Mit freundlichen Grüßen

[redacted]

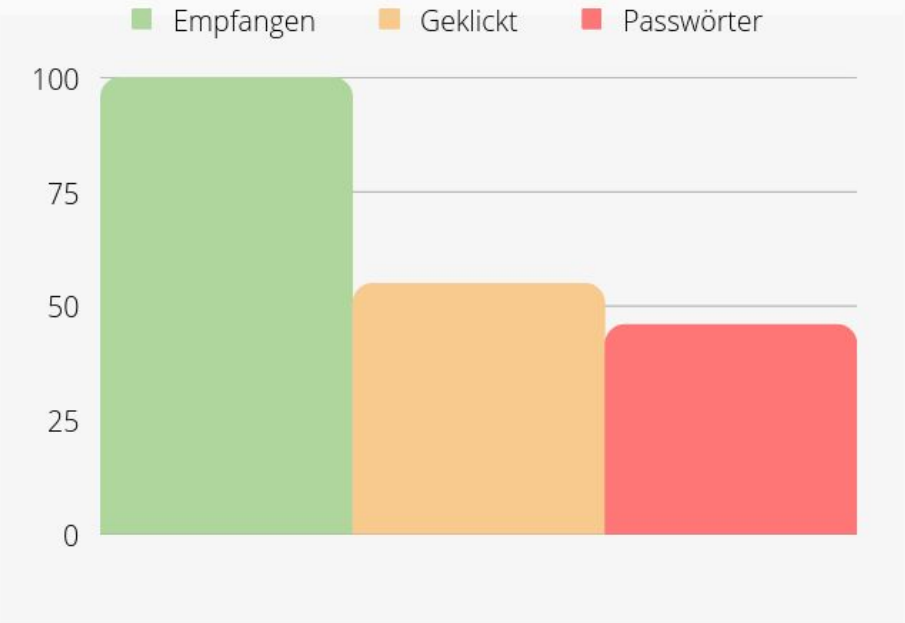
i. A [redacted]
Personalwesen

Link geklickt?



Ergebnis?

CLW PHISHING KAMPAGNE 2023

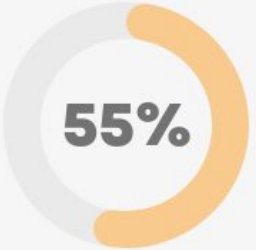


Passwörter

46% der Mitarbeiter gaben uns Ihre E-Mail und Passwort.

Link geklickt

55% der Mitarbeiter klickten auf den Link



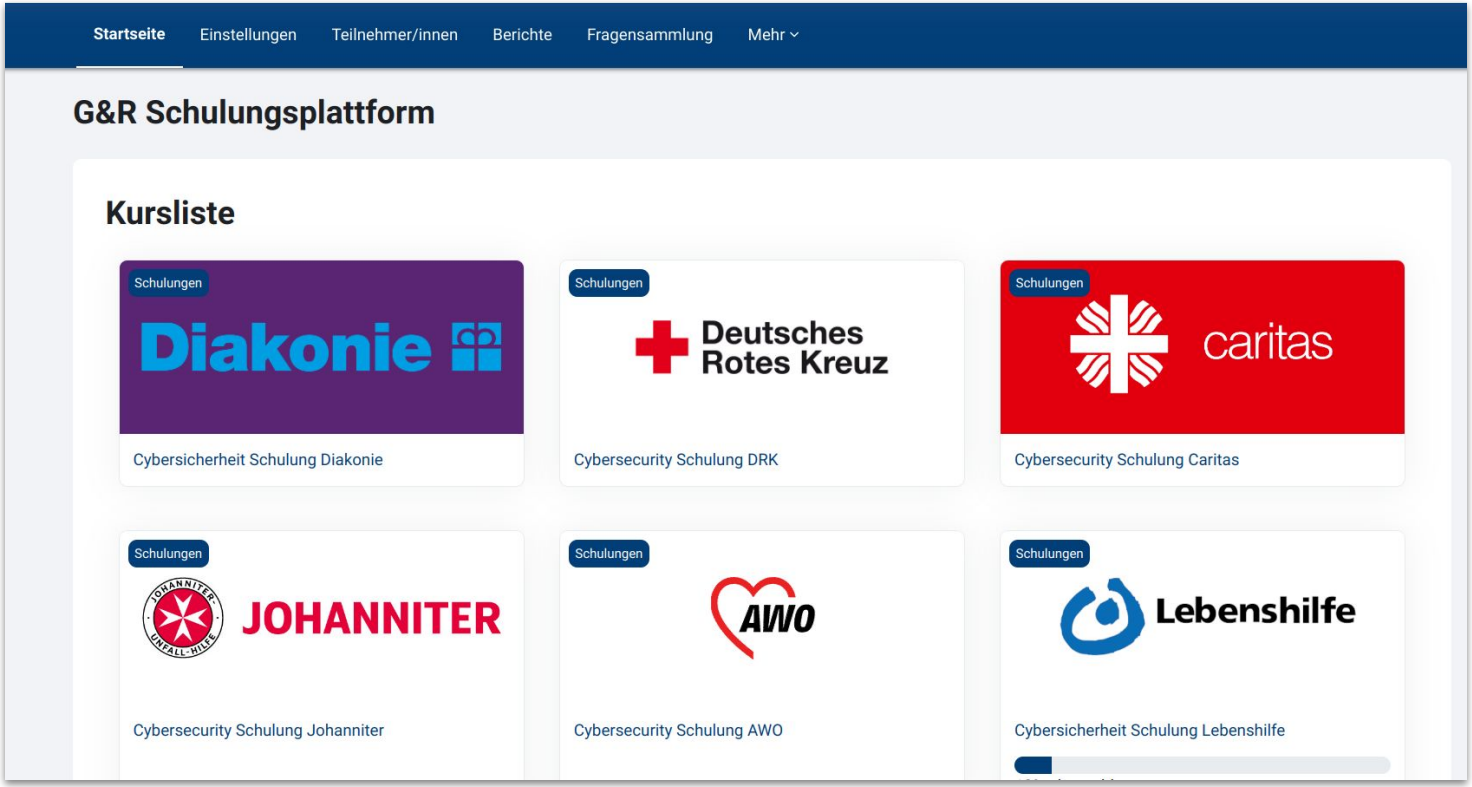
Awareness Schulungen

Awareness Schulungen

- Wissensvermittlung
- Bedrohungen erkennen
- Gruppenleiter und Verwaltung zielgruppengenau ansprechen

→ **Menschliche Firewall!**

Schulungsplattform

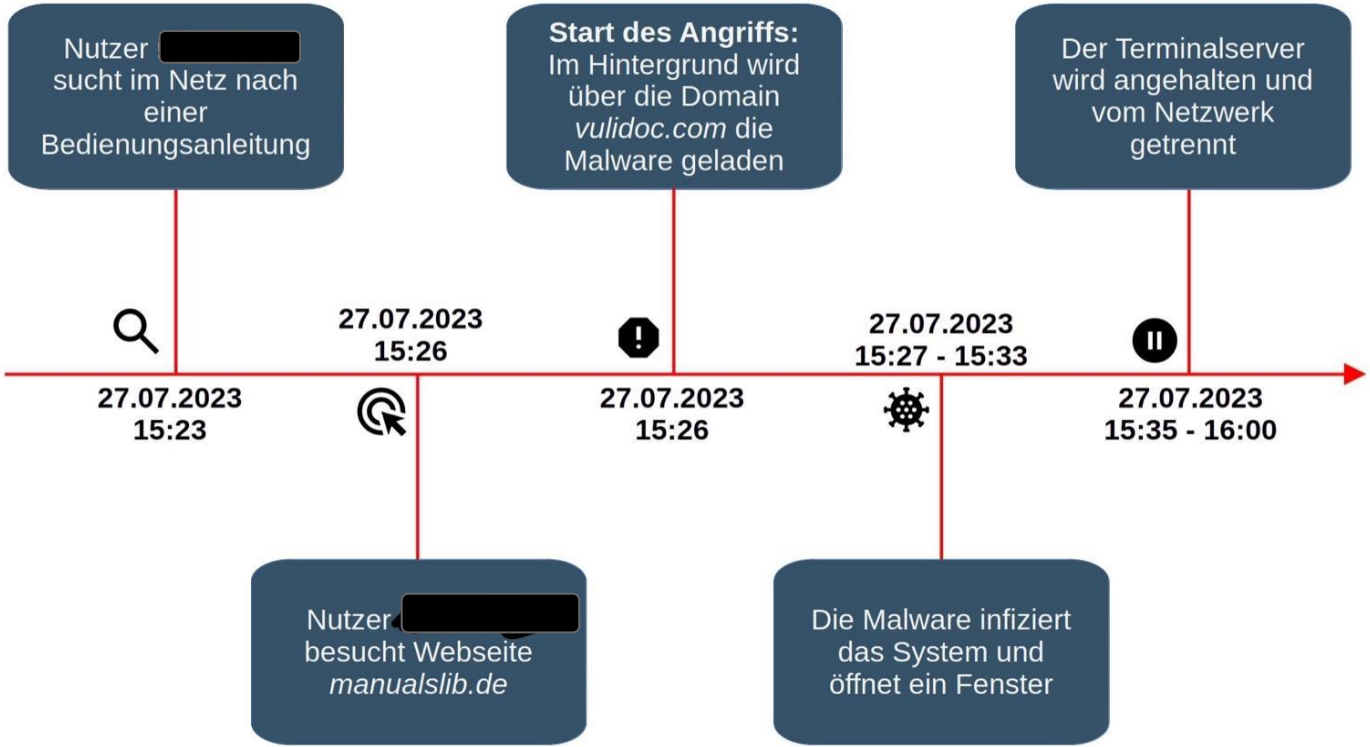


Notfall Reaktion

Notfall Reaktion

- Vorfall oder Notfall?
- Wurden Daten gestohlen?
- Wen sollte ich kontaktieren?

Notfall Reaktion



Notfallkonzept

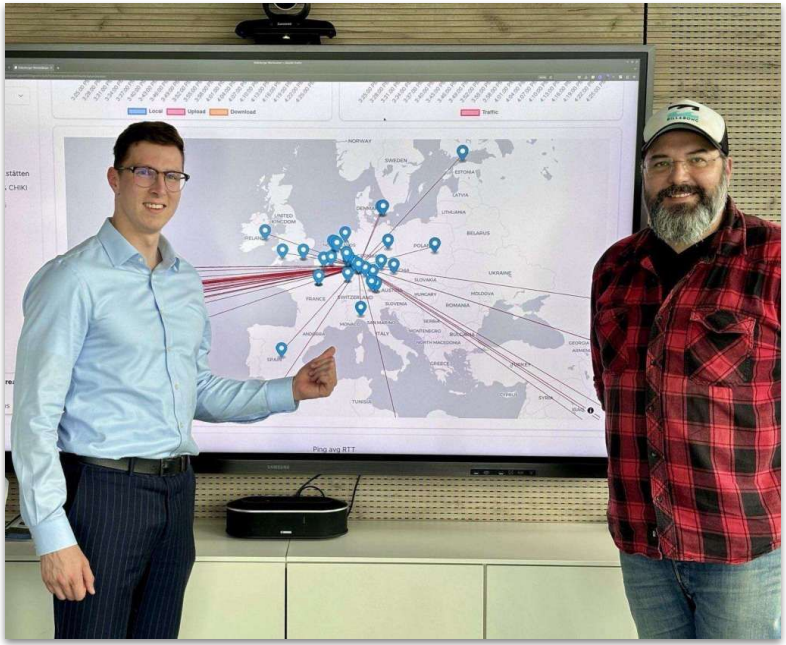
- Reaktionsteam (intern / extern)
- Geprüftes Backup Konzept
- Inventarisierung der IT
- Notfallplan für die Belegschaft
- Notfallhandbuch für die Geschäftsleitung

KI Anwendungen

KI für die Cyberabwehr

- Mustererkennung
- Training auf Angriffsmuster
- Erkennung von Anomalien
- Echtzeit-Überwachung
- Automatische Berichterstattung

→ **Lösung durch künstliche Intelligenz**



Fazit und Ausblick

- Gemeinsam Stark!
- Digitalisierung gestalten
- Innovationen entfesseln
- KI für die Verteidigung nutzen

Vielen Dank für Ihre Aufmerksamkeit

Poster Angebote

Joshua Roach - Geschäftsführer

E-Mail: j.roach@gr-sec.com

Tel: +49-89-61465283

Website: https://gr-sec.de

LinkedIn: https://linkedin.com/in/joshuaroach