Version 1.0 (Internal)
Sirnach, 12. März 2026

CRYPTRON SECURITY

«HACKED IN 60 SECONDS...»

PROTECTION FOR YOUR BUSINESS – SWISS ETHICAL HACKING

Agenda

- **Intro**
- Einblick in die Welt der Cyberangriffe (Fakten & Zahlen)
- Websicherheit, Injection Schwachstellen und OWASP Top 10
- Demo (Live Hacking)
- Gegenmassnahmen und Best Practices
- Fragen & Diskussionen

CRYPTRON SECURITY

CRYPTRON Security GmbH mit Sitz in der Schweiz ist ein IT-Sicherheitsberatungsunternehmen, das sich auf **unabhängige Audits**, **Penetrationstests** und **umfassende Risikoanalysen** aller Aspekte der Informationssicherheit spezialisiert hat.

CRYPTRON SECURITY

About me

Stefan Mettler, (42)

- Founder & Geschäftsführer von CRYPTRON Security GmbH
- Mehr als 20 Jahre Praxiserfahrung im Bereich der Informationssicherheit & Risk Management
- Referent & Speaker an internationalen Security Konferenzen
- Dozent in der Grund-, und Erwachsenenbildung (Fachbereich Applikationsentwicklung)
- Studium an der Hochschule Luzern, CISSP und diverse Security Zertifizierungen

Praxiserfahrung in diversen Fachgebieten

- CISO-Mandate, Information Security Officer, Datenschutzbeauftragter, Risiko Manager
- Penetration Tester & Senior Information Security Consultant
- Security Research im Bereich von Microsoft Windows, Apple macOS, Linux und UNIX (Oracle Solaris, IBM AIX, HP-UX, AS400)
- Expertenwissen im Bereich Mobile-, und Web Application Security (Fokus OWASP)
- Durchführung von Forensik, Malware Analyse, Reverse Engineering, Exploit Development
- Durchführung von Protokollanalysen in TCP, VoIP, DECT, MIFARE, RFID, SCADA, IoT, etc.

CRYPTRON SECURITY

CRYPTRON Security – Who we are

- Erfahrenes **White-Hat Hacking Team** von IT-Sicherheits-experten und Consultants
- Durchführung von **Security Audits & Penetrationstests pro Jahr**
- CRYPTRON Security verfügt über ein **Research Labor in der Schweiz** für Forschung & Entwicklung (R & D)
- Agile und **global operierende IT-Sicherheitsfirma** mit **zertifizierten Beratern** in unterschiedlichen Security Disziplinen
- Fokus auf **Open Source**

CRYPTRON SECURITY

CRYPTRON Security Portfolio

CRYPTRON SECURITY

PREVENTIVE SERVICES

- SECURITY REVIEW
- SOURCE CODE REVIEW
- THREAT MODELING
- CLOUD SECURITY CHECK
- THREAT HUNTING

- PENETRATION TESTING & RED TEAMING
- AUDITS & RISK ASSESSMENTS
- PHISHING SIMULATION & SOCIAL ENGINEERING

PROAKTIVE SERVICES

- VULNERABILITY SCANNING (AUTOBAHN)
- DDoS BENCHMARK SERVICE
- IT FORENSIC & SECURITY INCIDENT RESPONSE SERVICE

Information Security Officer as a Service (Rent a CISO)

ISMS Framework (ISO/IEC 27001), Data Privacy (GDPR), NIS2, NIST 800-53 Standard

Enterprise Risk Management (ISO 31000), Risk Analyses

Cybersecurity Awareness Training, Keynote Speaker

CRYPTRON Security employees are certified experts

CRYPTRON SECURITY

CRYPTRON
SECURITY

Agenda

- Intro
- **Einblicke in die Welt der Cyberangriffe (Fakten & Zahlen)**
- Websicherheit, Injection Schwachstellen und OWASP Top 10
- Demo (Live Hacking)
- Gegenmassnahmen und Best Practices
- Fragen & Diskussionen

CRYPTRON SECURITY

Forbes

INNOVATION > CYBERSECURITY

Just 60 Seconds From Attacked To Hacked — The Speed Of Cybercrime

By Davey Winder, Senior Contributor. ⓘ Davey Winder is a veteran cybersecur... Follow Author

Published Apr 25, 2025, 08:58am EDT, Updated Apr 25, 2025, 12:33pm EDT

CRYPTRON SECURITY

Einblick in die Welt der Cyberangriffe

Nach drei Jahren intensiver Forschung hat ein internationales Forscherteam der Universität Oxford den ersten „**World Cybercrime Index**“ zusammengestellt, der die wichtigsten Cybercrime-Hotspots der Welt laufend identifiziert.

Source: ox.ac.uk (WCI-Score April 2024)

CYBERCRIME INDEX

Ranking countries by cybercrime threat level

Ranking	Country	WCI score
1	Russia	58.39
2	Ukraine	36.44
3	China	27.86
4	United States	25.01
5	Nigeria	21.28
6	Romania	14.83
7	North Korea	10.61
8	United Kingdom	9.01
9	Brazil	8.93
10	India	6.13

Ranking	Country	WCI score
11	Iran	4.78
12	Belarus	3.87
13	Ghana	3.58
14	South Africa	2.58
15	Moldova	2.57
16	Israel	2.51
17	Poland	2.22
18	Germany	2.17
19	Netherlands	1.92
20	Latvia	1.68

CRYPTRON SECURITY

Einblick in die Welt der Cyberangriffe

Erfolgreiche **Ransomware** Angriffe auf staatliche Organisationen und Unternehmen weltweit gemessen von **Januar 2025 bis Februar 2026.**

Weltweite Ransomware-Vorfälle primär in den USA sowie Europa inkl. Schweiz.

Source: CRYPTRON Research Labs (siehe Grafik)

CRYPTRON SECURITY

Einblick in die Welt der Cyberangriffe

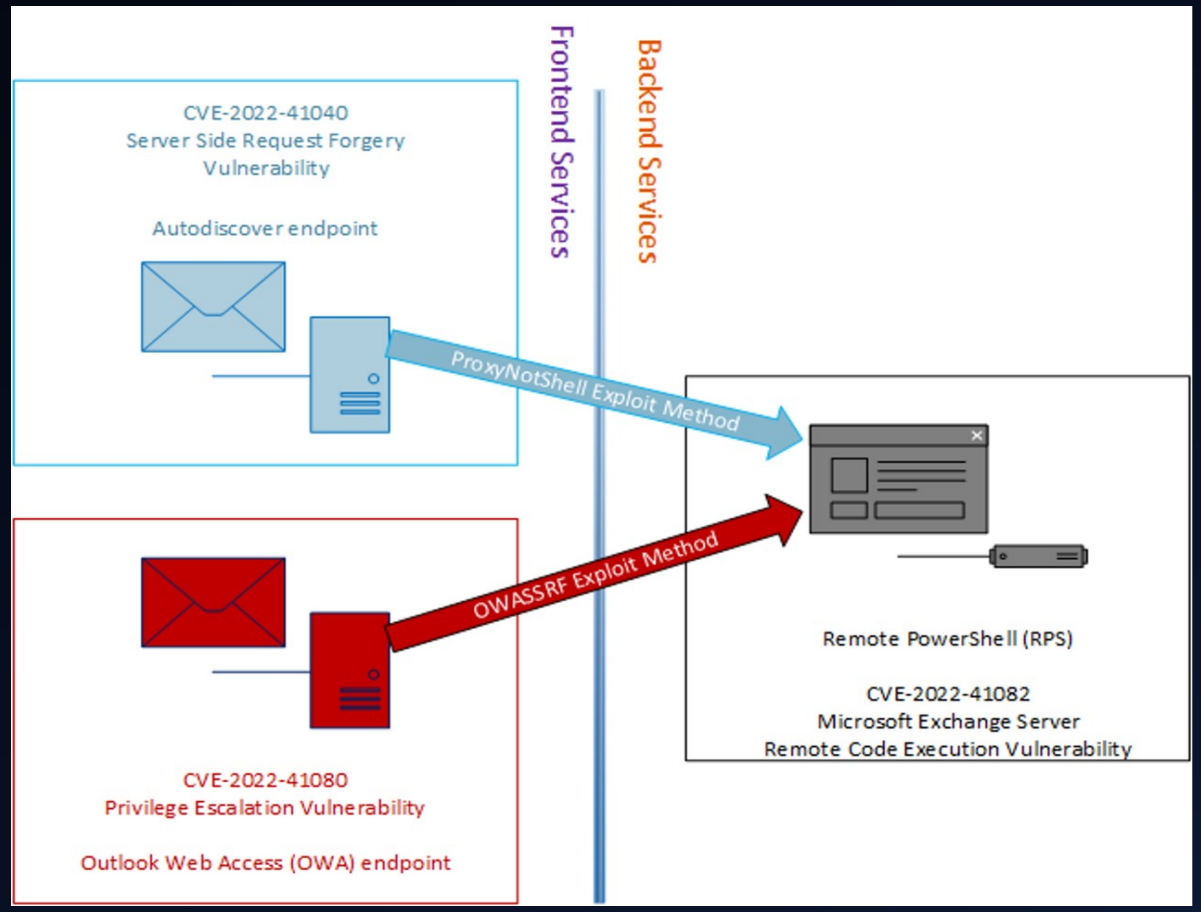
Fokus Medien-Organisationen

Data Breach und Abzug von personenbezogenen Daten und sensiblen Informationen bei einem Medienunternehmen in der Schweiz

Stichwort Quellenschutz (Journalismus)

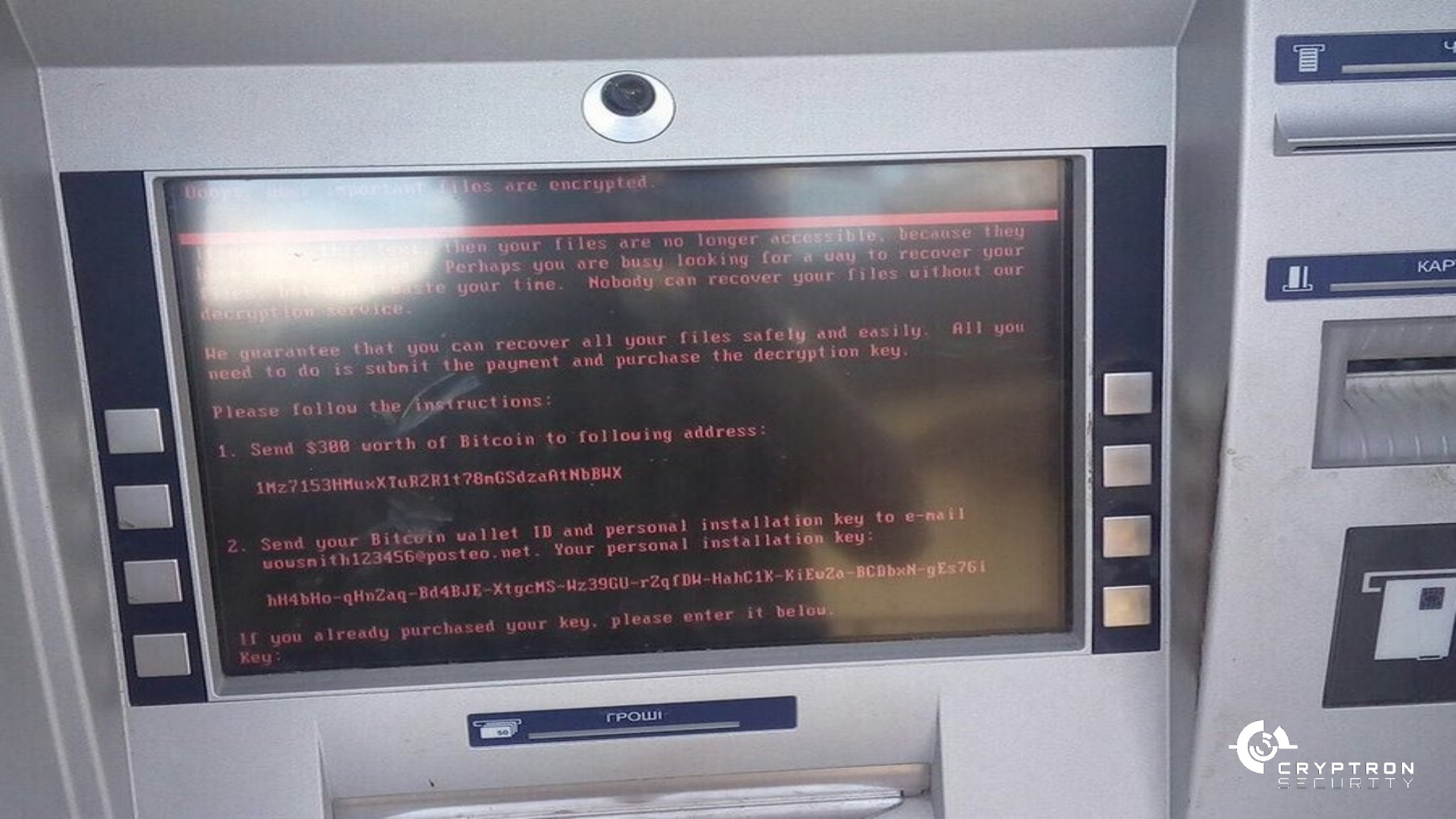
Cyberangriff auf Microsoft Exchange Server

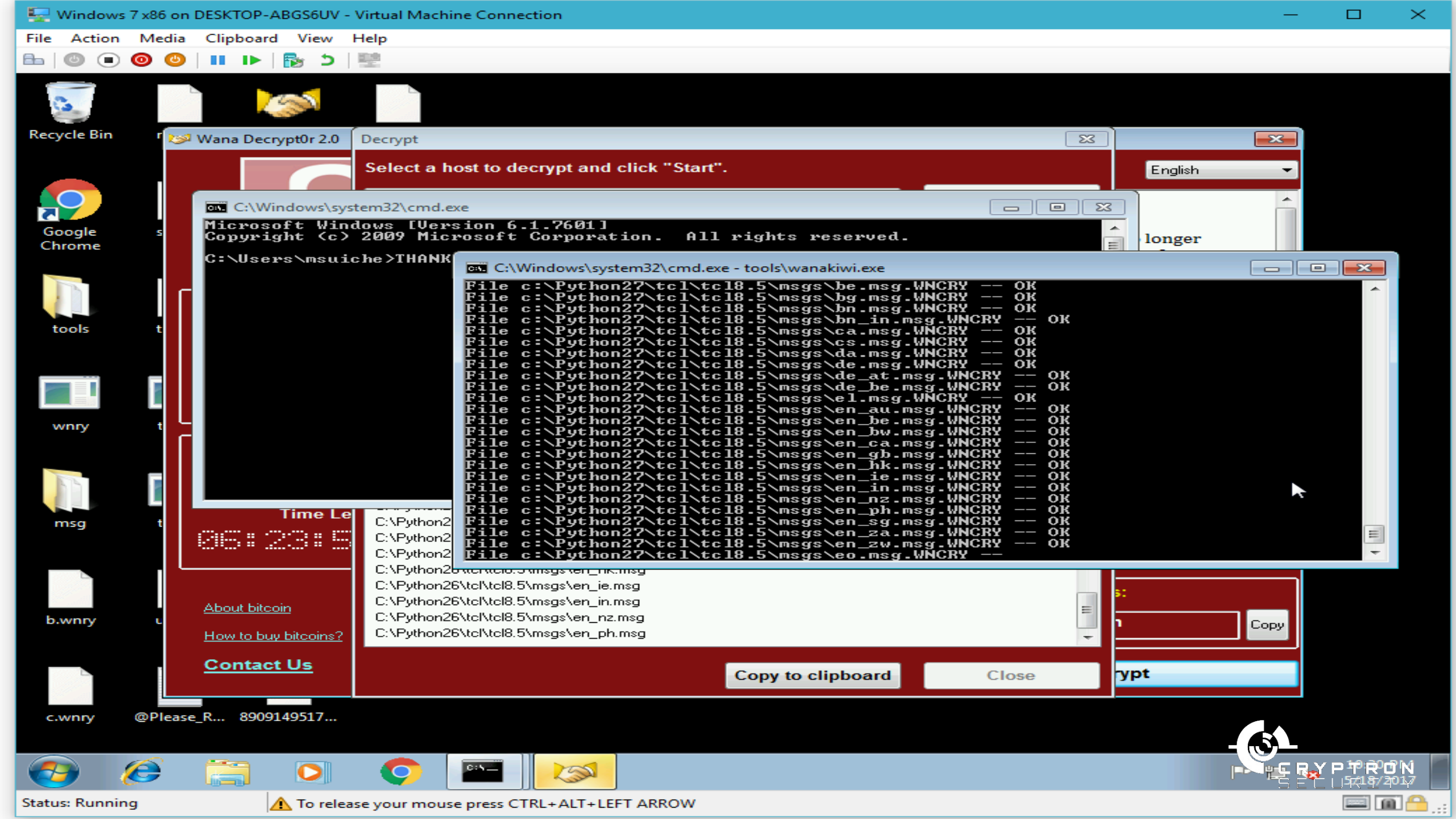
- CVE-2022-41082 (RCE)
- CVE-2022-41040 (SSRF)
- CVE-2021-27065 (Proxylogon)
- Kombination dieser Exploits

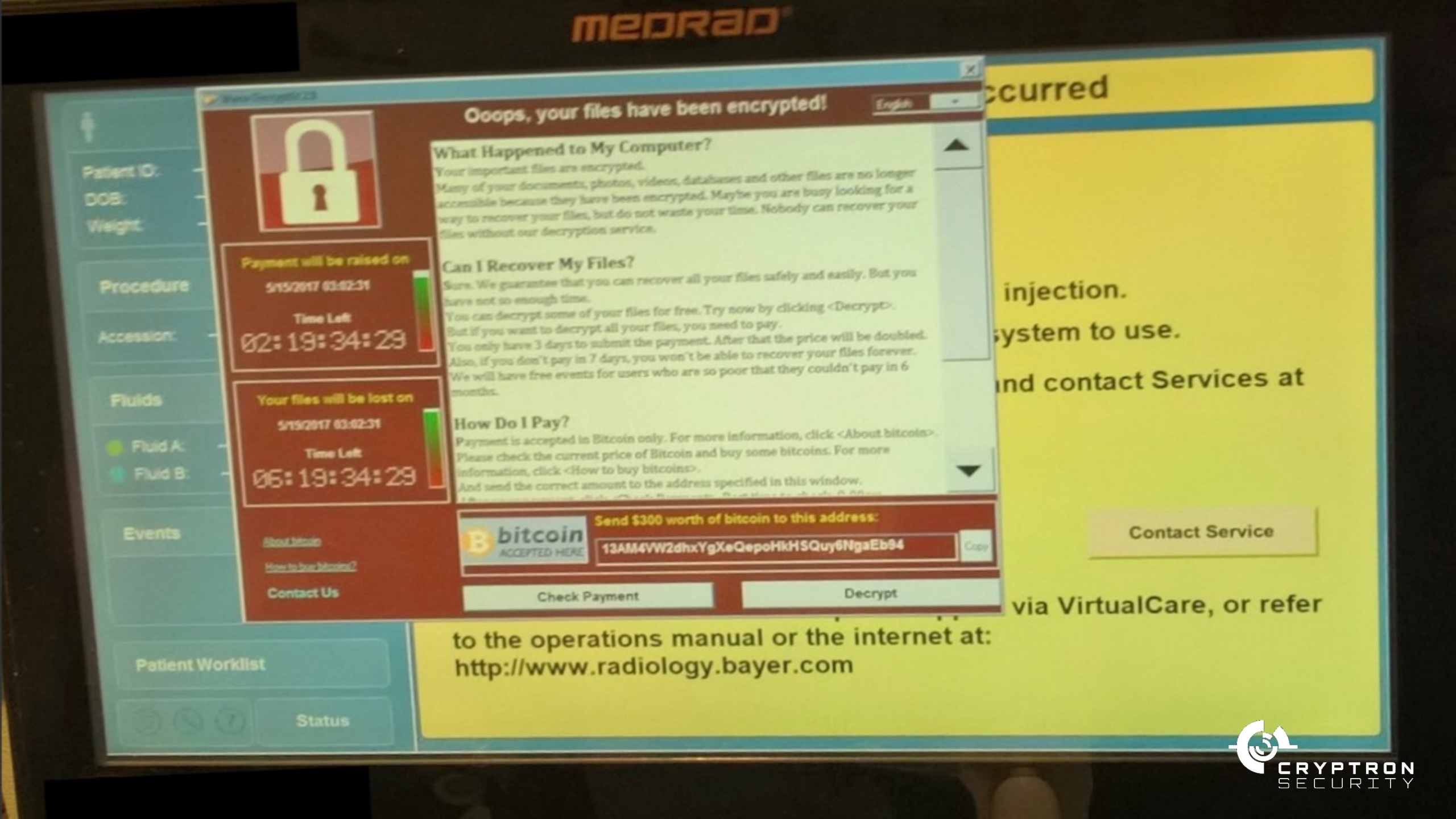


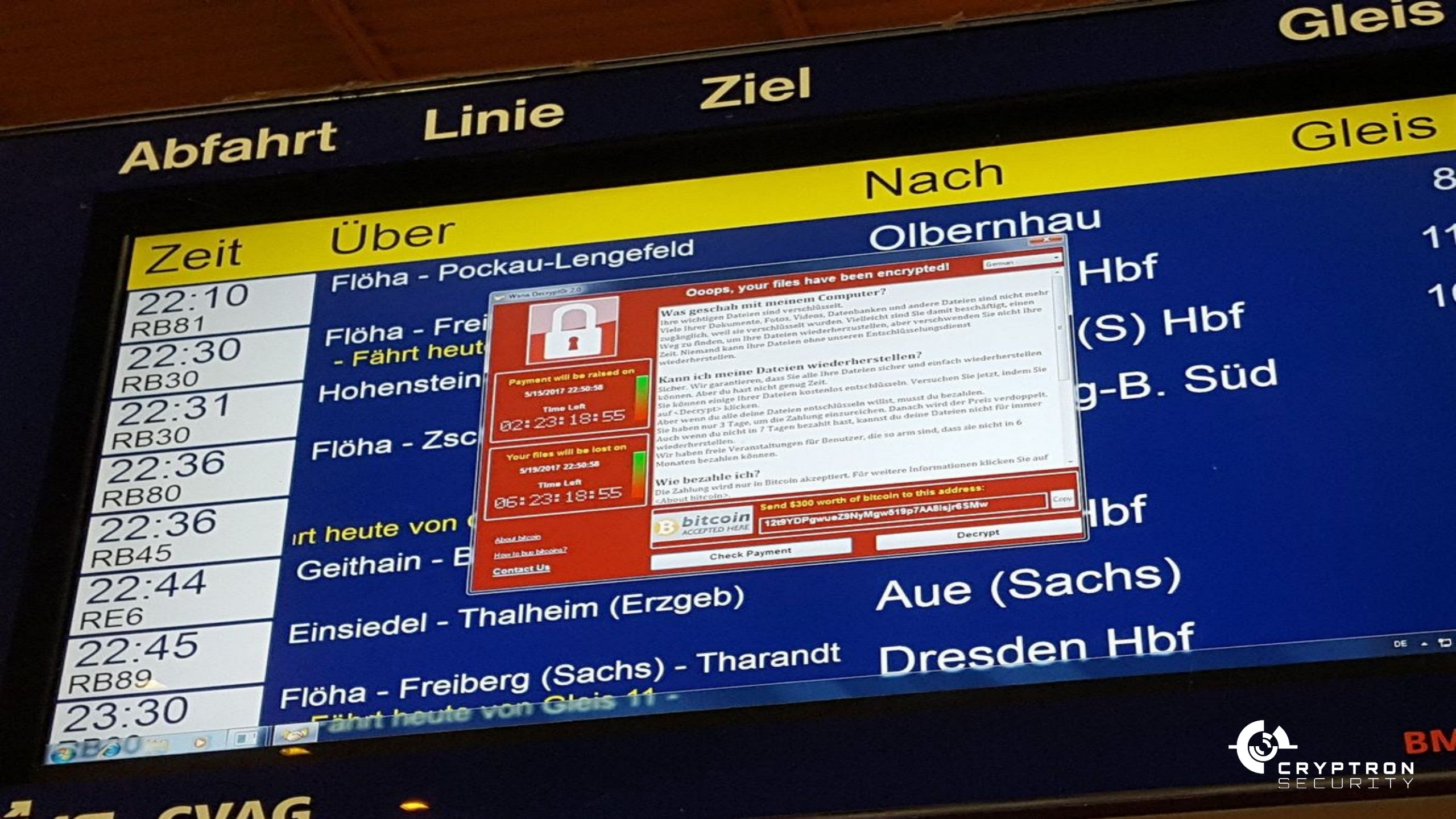
CRYPTRON SECURITY


CRYPTRON
SECURITY


Your important files are encrypted.
Then your files are no longer accessible, because they
Perhaps you are busy looking for a way to recover your
waste your time. Nobody can recover your files without our
decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wousmith123456@posteo.net. Your personal installation key:
hH4bHo-qHnZaq-Bd4BJE-XtgcMS-Wz39GU-rZqfDW-HahC1K-KiEuZa-BCBbxN-gEs76i
If you already purchased your key, please enter it below.
Key:
ГРОШІ
CRYPTRON
SECURITY


Windows 7 x86 on DESKTOP-ABGS6UV - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Google Chrome
tools
wnry
msg
b.wnry
c.wnry
@Please_R...
8909149517...
Wana Decrypt0r 2.0
Decrypt
Select a host to decrypt and click "Start".
English
longer
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\msuiche>THANK
C:\Windows\system32\cmd.exe - tools\wanakiwi.exe
File c:\Python27\tcl\tcl8.5\msgs\be.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\bg.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\bn.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\bn_in.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\ca.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\cs.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\da.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\de.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\de_at.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\de_be.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\el.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_au.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_be.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_bw.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_ca.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_gb.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_hk.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_ie.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_in.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_nz.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_ph.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_sg.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_za.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_zw.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\eo.msg.WNCRY --
Time Le
About bitcoin
How to buy bitcoins?
Contact Us
C:\Python26\tcl\tcl8.5\msgs\en_ie.msg
C:\Python26\tcl\tcl8.5\msgs\en_in.msg
C:\Python26\tcl\tcl8.5\msgs\en_nz.msg
C:\Python26\tcl\tcl8.5\msgs\en_ph.msg
Copy to clipboard
Close
Copy
ypt
CRYPTRON
SECURITY
Status: Running
To release your mouse press CTRL+ALT+LEFT ARROW


MEDRAD
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
Payment will be raised on
5/15/2017 03:02:31
Time Left
02:19:34:29
Your files will be lost on
5/19/2017 03:02:31
Time Left
06:19:34:29
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
Check Payment
Decrypt
ccurred
injection.
system to use.
nd contact Services at
Contact Service
via VirtualCare, or refer
to the operations manual or the internet at:
http://www.radiology.bayer.com
Patient ID:
DOB:
Weight:
Procedure
Accession:
Fluids
Fluid A:
Fluid B:
Events
Patient Worklist
Status
CRYPTRON
SECURITY


Abfahrt
Linie
Ziel
Gleis
Zeit
Über
Nach
Gleis
22:10 RB81 Flöha - Pockau-Lengefeld Olbernhau
22:30 RB30 Flöha - Frei - Fährt heut Hohenstein Hbf
22:31 RB30 Flöha - Zsc (S) Hbf
22:36 RB80 g-B. Süd
22:36 RB45 Geithain - B Hbf
22:44 RE6 Einsiedel - Thalheim (Erzgeb) Aue (Sachs)
22:45 RB89 Flöha - Freiberg (Sachs) - Tharandt Dresden Hbf
23:30
Fährt heute von Gleis 11 -
Ooops, your files have been encrypted!
Was geschah mit meinem Computer?
Kann ich meine Dateien wiederherstellen?
Wie bezahle ich?
Payment will be raised on
5/15/2017 22:50:58
Time Left
02:23:18:55
Your files will be lost on
5/19/2017 22:50:58
Time Left
06:23:18:55
About bitcoin
How to buy bitcoins?
Contact Us
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
CRYPTRON
SECURITY

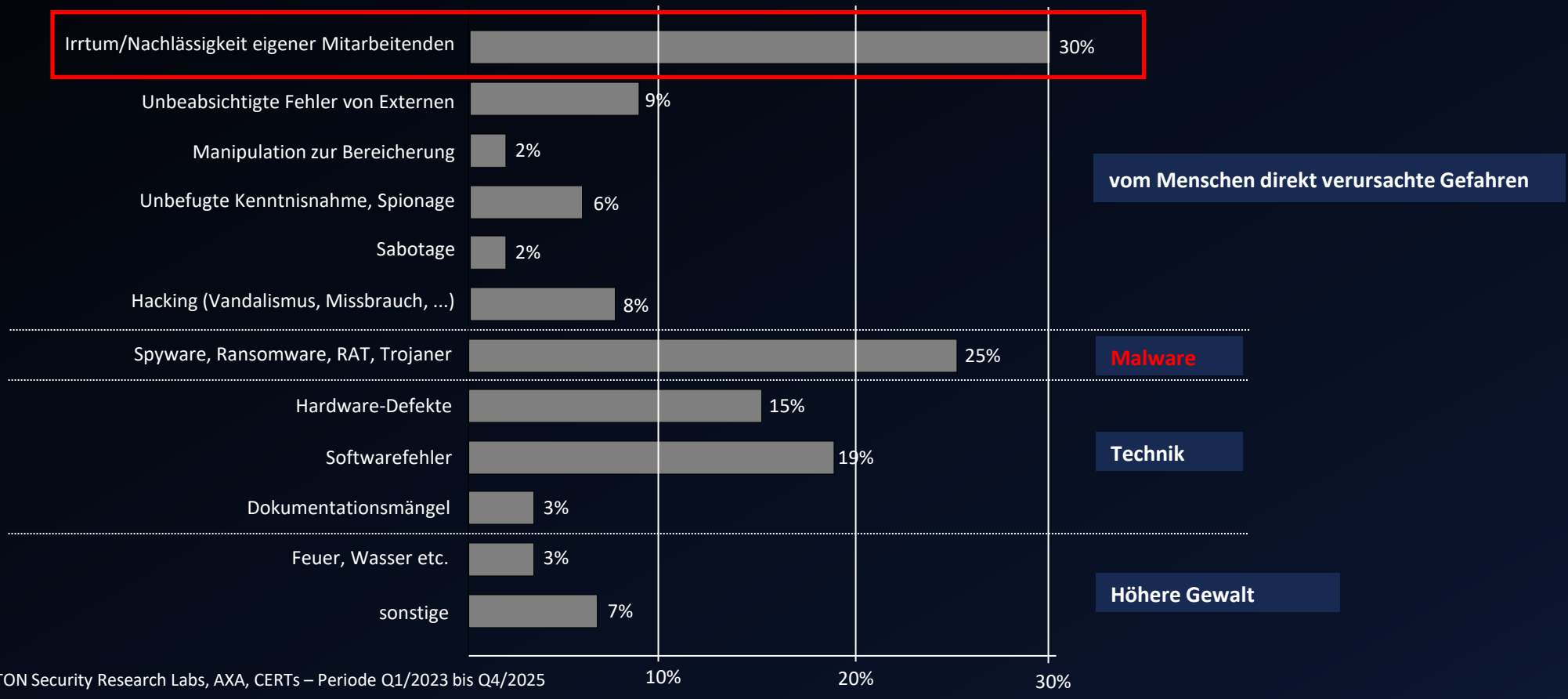

0x0006926F 0xFFF34A56
CRYPTRON
SECURITY

Zahlen und Fakten

- **Beispiele für Cyber-, und Wirtschaftskriminalität**
  - Fraud / Betrug
  - Falschbilanzierungen
  - Geldwäsche mit Kryptowährungen im Darknet
  - Insiderhandel - Aktienhandel an der Börse mit Insider Know-How
  - Industriespionage durch Hacking und Social Engineering
  - Korruption
  - Produktepiraterie
  - Steuerstraftaten
  - Subventionsbetrug
  - Unterschlagung
  - Untreue
  - **Cyber Crime, Phishing, Ransomware, «CFO» Fraud, Social Engineering, DDoS, APTs, Deepfakes, etc.**

CRYPTRON SECURITY

Zahlen und Fakten



Quelle: CRYPTON Security Research Labs, AXA, CERTs – Periode Q1/2023 bis Q4/2025

CRYPTRON SECURITY

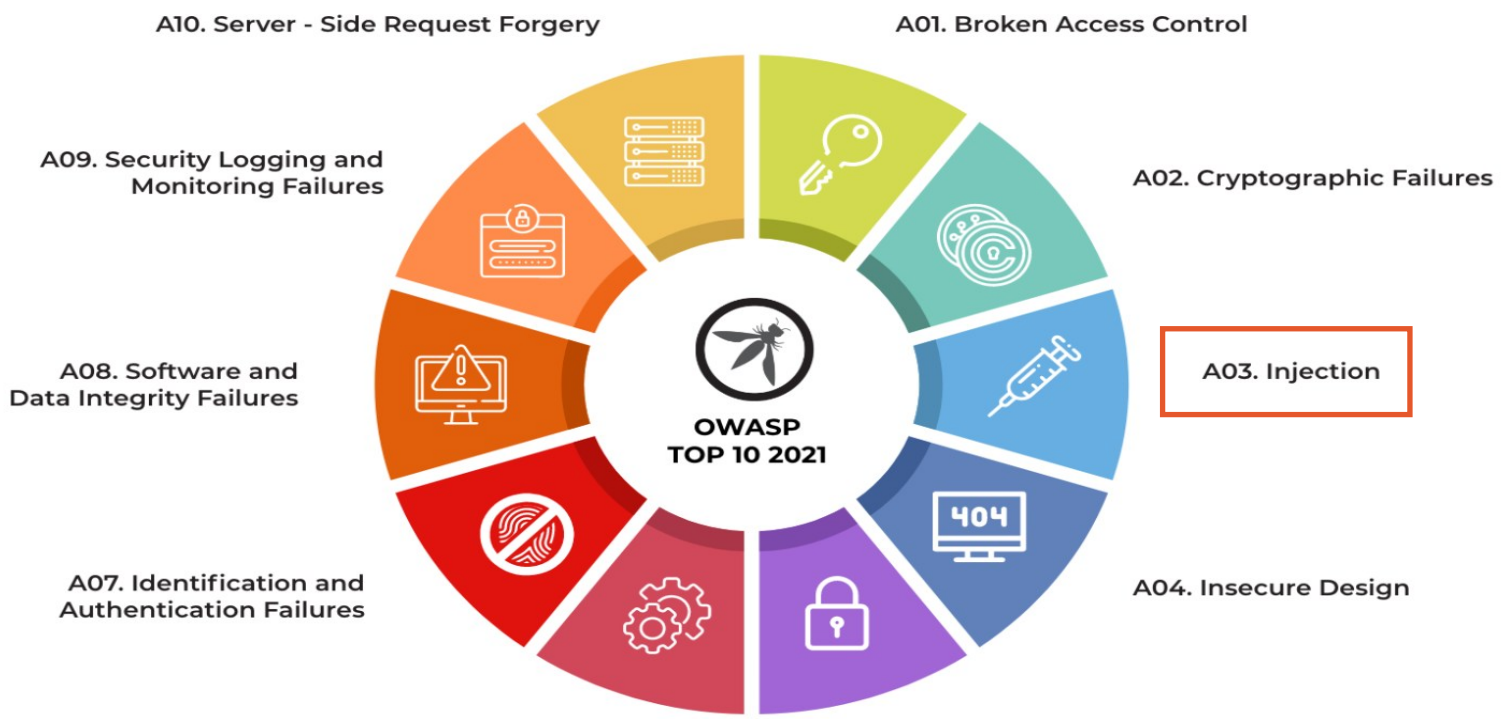
CRYPTRON SECURITY

Agenda

- Intro
- Einblicke in die Welt der Cyberangriffe (Fakten & Zahlen)
- **Websicherheit, Injection Schwachstellen und OWASP Top 10**
- Demo (Live Hacking)
- Gegenmassnahmen und Best Practices
- Fragen & Diskussionen

CRYPTRON SECURITY

OWASP Top 10 – Erläuterung



CRYPTRON SECURITY

YOU HAVE BEEN HACKED !

CRYPTRON SECURITY

Agenda

- Intro
- Einblicke in die Welt der Cyberangriffe (Fakten & Zahlen)
- Websicherheit, Injection Schwachstellen und OWASP Top 10
- Demo (Live Hacking)
- **Gegenmassnahmen und Best Practices**
- Fragen & Diskussionen

CRYPTRON SECURITY

Gegenmassnahmen & Best Practices

- Regelmässige Durchführung von **Sicherheitsaudits, Assessments oder Penetrationstests**
- **Hinweis:** *Sicherheitsprüfbericht aus Revisions- oder Compliance-Gründen (FINMA, Rundschreiben 2023/1 „Operationelle Risiken und Widerstandsfähigkeit 2023/1- Banken“)*
- **Cybersecurity Monitoring (SIEM) oder 7/24 Überwachung** der Infrastruktur durch Partner
- **Konfiguration-, oder Code-Reviews** von kritischen Plattformen oder Applikationen durch externe Sicherheitsexperten
- **Informationen klassifizieren** mit Labels wie Public, Intern, Vertraulich (Microsoft Pureview)
- **Server Härtung (Hardening)** (CIS-Benchmarks, STIGS)
- **Awareness-Schulungen** zur regelmässigen Sensibilisierung von Mitarbeitenden, Kader und Management
- **Einführung ISMS – Information Security Managementsystem - ISO 27001:2022**

CRYPTRON SECURITY


CRYPTRON
SECURITY

Kontakt

CRYPTRON SECURITY GMBH

Châtelstrasse 5, CH-8355 Aadorf, Switzerland

Office: +41 52 366 80 87

Website: https://www.cryptron.ch

E-Mail: info@cryptron.ch

Enterprise Support: blueteam@cryptron.ch (nur für Unternehmen)