
POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM MANNHEIM

Struktur

BKA

LKA BaWü
Abt. 510 / ZAC

Staatsanwaltschaften
Mannheim (Cybercrime)
Heidelberg

KI 5

D 5.1

D 5.2

DA

MMF

Cyber crime

Forensik

Daten analyse

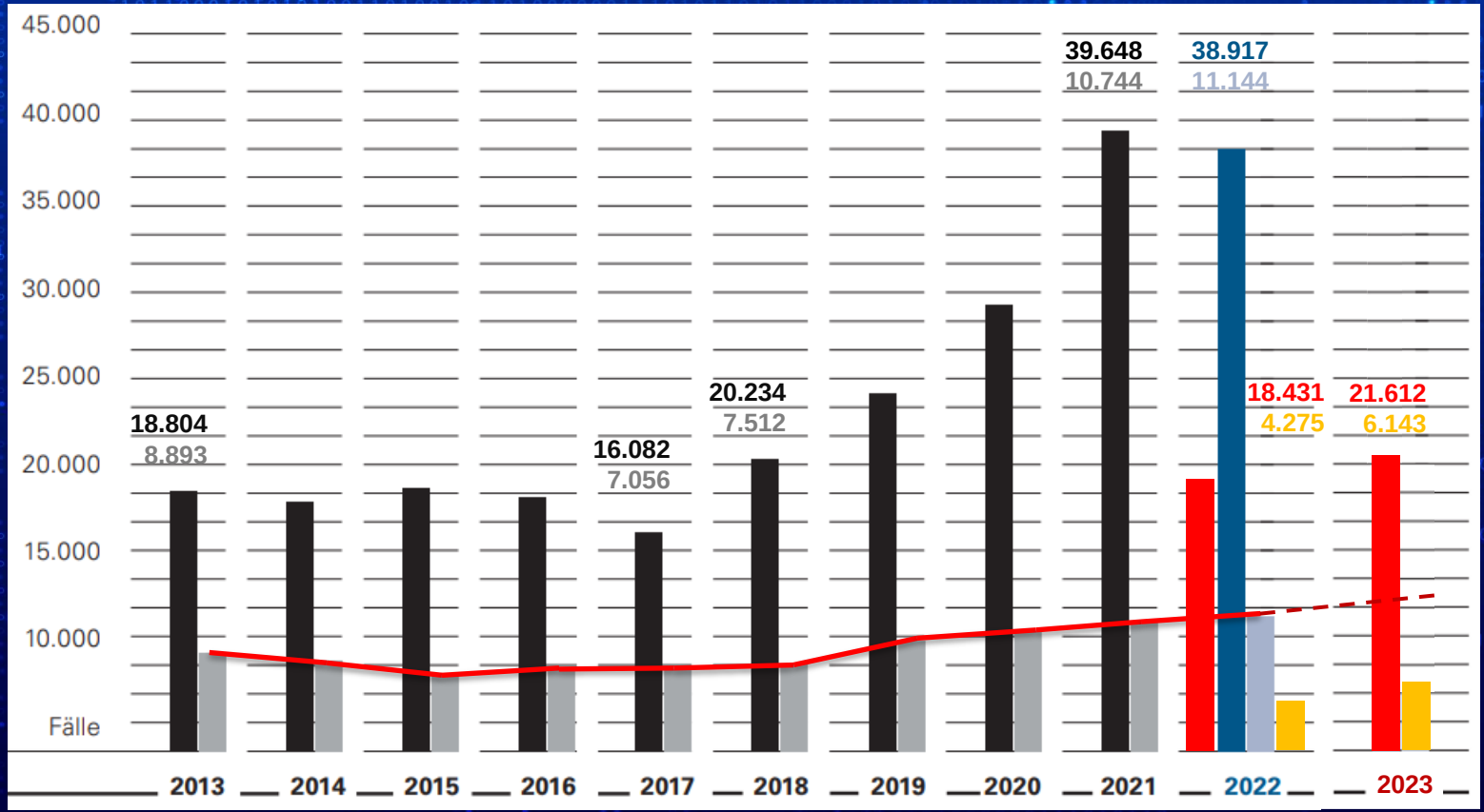
Multi media forensik


Erpressung
Beleidigung
Betrug
Tatmittel Internet und/
oder IT-Geräte
Verbreitung porno-
grafischer Inhalte
Rauschgiftdelikte
Fälschung
beweiserheblicher Daten, Täuschung im Rechtsverkehr
Ausspähen, Abfangen
von Daten, einschließlich Vorbereitungs-
handlungen und Datenhehlerei
Cybercrime
Datenveränderung, Computersabotage
Computerbetrug

Aufgabenfelder Cybercrime

- Ausspähen von Daten
- Abfangen von Daten
- Datenveränderung
- Computersabotage
- Computerbetrug
- Fälschung beweiserheblicher Daten
- (digitale) Erpressung
- Geldwäsche
- Internetermittlungen
- Hacking
- Ransomware
- DDOS-Angriff / Bot-Netze
- CEO-Fraud / BEC
- Identitätsdiebstahl
- Phishing / Smishing
- Sextortion
- SPAM
- OSINT

Fallzahlen Baden-Württemberg



Cyberstraftaten 2023

9 Fälle Ransomware + 3

2 DDoS-Angriffe + 2

47 BEC / CEO-Fraud + 31

168 Phishing + 34 /

224 Angriff aufs online-Banking & Betrug

108 Geldwäsche + 31

„Highlights“ - Ransomware -

- 2 börsennotierte Unternehmen
- Autohaus
- Spedition
- Stadtverwaltung
- Universität
- Architekturbüro
- Möbelhaus
- Elektronikhändler

„Highlights“ - Ransomware -

```
root     /vmfs/volumes# ls
 bb.xlsx.basta     'IDA Freeware 7.6.desktop.basta'   readme.txt
 bcc                kk.txt.basta                      ssd1.pcap.basta
 d1e                ll.txt.basta                      sss.jpeg.basta
 dd.docx.basta      logo.png.basta                    testing.elf.basta
 debugf.py.basta    pp.elf.basta
 ff.doc.basta       pp.txt.basta
root(    :/vmfs/volumes# cat readme.txt
Your data are stolen and encrypted
The data will be published on TOR website if you do not pay the ransom
You can contact us and decrypt one file for free on this TOR site
(you should download and install TOR browser first https://torproject.org)
https://aazsbsgya565vlu2c6bzy6yfiebkcbtvvcytvolt33s77xypi7nypxyd.onion/

Your company id for log in: 01e

root(    :/vmfs/volumes#
ENCRYPTION
Done time: 14.5620 seconds, encrypted: 0.0016 gb
```

„Highlights“ - Ransomware -

Q: www.uptycs.com

Fall 1 - „Ransomware“ Black Basta

Börsennotiertes weltweit operierendes Unternehmen

„nur“ 13.000 Clients betroffen

„Patient Zero“ Laptop eines kanadischen Mitarbeiters

Täter beschafften sich sog. „golden Tickets“

enormer Personalaufwand

neue Domain aufgesetzt

„Highlights“ - Ransomware-

Fall 2 - „Ransomware“ unbekannt

regionales Speditionsunternehmen

unbekannter Einfallsvektor

ein Backup gelöscht und 2 virtuelle Server verschlüsselt

nach 3 Tagen wieder voll handlungsfähig

funktionierende Backups

BusinessEmailCompromise

1. man-in-the-middle-Attacken (MITM)

2. kompromittierte EMail-Server „hacking“
   Office 365 • Exchange-Server • 1 & 1 / IONOS • […]

3. look-a-like-Emailadressen

BusinessEmailCompromise -

Social Engineering / Hacking

Email mit gefälschter Rechnung (Bankverbindung)

Ausführung der Überweisung

Zahlungserinnerung / Mahnung

interne Prüfung / Kommunikation mit Geschäftspartner

Kontakt mit der Hausbank

Anzeige bei der Polizei

BusinessEmailCompromise

look-a-like-Emailadresse

vbkraichgau.**de**	Vergeben
vbkraichgau.**com**	✓ Noch frei!
vbkraichgau.**eu**	✓ Noch frei!
vbkraichgau.**net**	✓ Noch frei!
vbkraichgau.**org**	✓ Noch frei!
vbkraichgau.**info**	✓ Noch frei!

volksbank-sinsheim.**de**	✓ Noch frei!
volksbank-sinsheim.**com**	✓ Noch frei!
volksbank-sinsheim.**eu**	✓ Noch frei!
volksbank-sinsheim.**net**	✓ Noch frei!
volksbank-sinsheim.**org**	✓ Noch frei!
volksbank-sinsheim.**info**	✓ Noch frei!

BusinessEmailCompromise

look-a-like-Emailadresse Bsp. Finanzbuchhaltung (FIBU)

Recherche mit „FIBU“

BusinessEmailCompromise

Unsere Empfehlungen

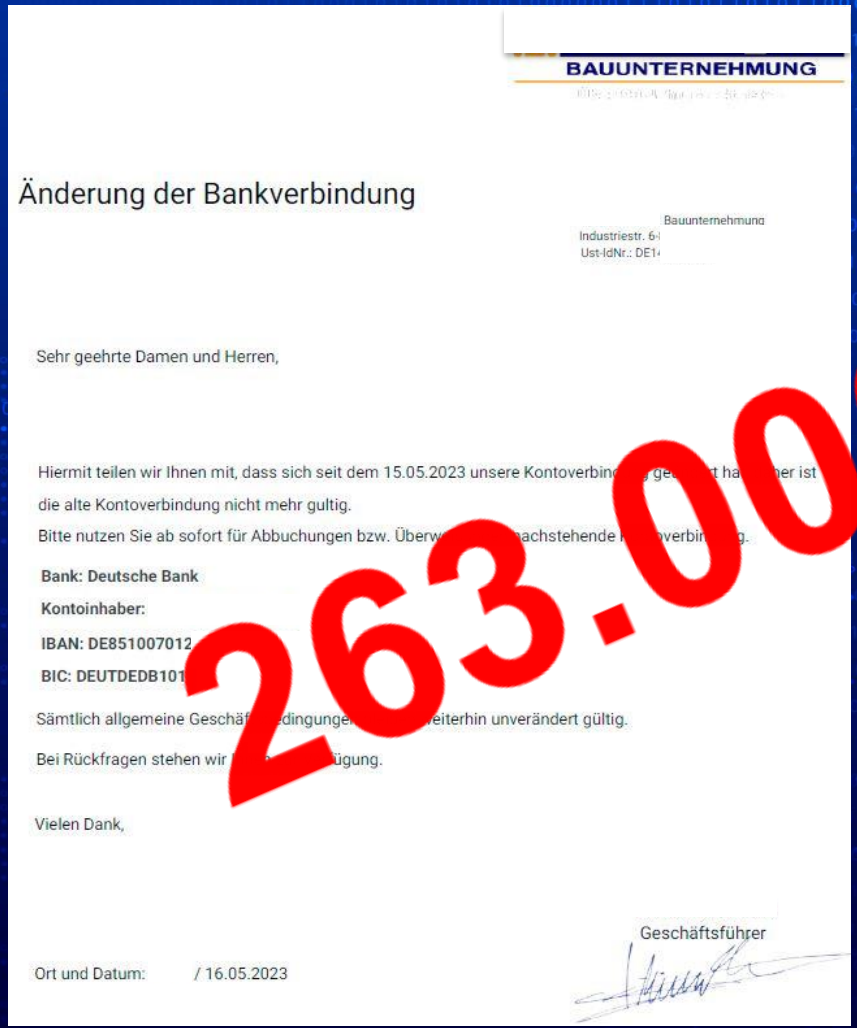
fibu-buchhaltung.**de**	Vergeben
fibu-buchhaltung.**com**	Vergeben
fibu-buchhaltung.**eu**	✓ Noch frei!
fibu-buchhaltung.**net**	✓ Noch frei!
fibu-buchhaltung.**org**	✓ Noch frei!
fibu-buchhaltung.**info**	✓ Noch frei!

Städte & Regionen

fibu-buchhaltung.**berlin**	✓ Noch frei!
fibu-buchhaltung.**bayern**	✓ Noch frei!
fibu-buchhaltung.**hamburg**	✓ Noch frei!
fibu-buchhaltung.**nrw**	✓ Noch frei!
fibu-buchhaltung.**koeln**	✓ Noch frei!

Weitere Domains anzeigen

Q: www.ionos.de/domaincheckresult & www.checkdomain.de



BAUUNTERNEHMUNG

Änderung der Bankverbindung

Bauunternehmung
Industriestr. 6
Ust-IdNr.: DE1

Sehr geehrte Damen und Herren,

Hiermit teilen wir Ihnen mit, dass sich seit dem 15.05.2023 unsere Kontoverbin g ge t ha her ist die alte Kontoverbindung nicht mehr gultig.
Bitte nutzen Sie ab sofort für Abbuchungen bzw. Überw achstehende K overbin g.

Bank: Deutsche Bank
Kontoinhaber:
IBAN: DE851007012
BIC: DEUTDEDB101

Sämtlich allgemeine Geschäf dingunge eiterhin unverändert gültig.

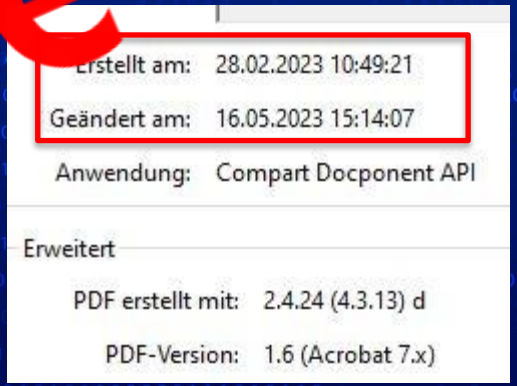
Bei Rückfragen stehen wir ügung.

Vielen Dank,

Geschäftsführer

Ort und Datum: / 16.05.2023

263.000 €



„Highlights“ - Betrug -

Fall - Angriff aufs online Banking

unbekannter Zeitpunkt Zugangsdaten ausgespäht

10. Januar 2023 neues Endgerät wird registriert & Zusendung des Aktivierungscodes

21. Februar 2023 neues Endgerät wird aktiviert

22. Mai 2023 Löschung des berechtigten Endgeräts & Änderung der persönlichen Daten

23. Mai 2023 Limiterhöhung auf 1 Mio Euro

23. Mai 2023 Überweisung von 1 Mio Euro auf ein Konto in der Schweiz

25. Mai 2023 Überweisung von 300.000 Euro auf ein dt. Konto

Prävention


R
CYBER
HYGIENE
C


CRIME
ALLOWED
ALARM
ALERT
DENIED
VIRUS
BUG
SPAM
IDENTITY
MALWARE
CYBER ATTACK
LOCKED
PHISHING
SECURITY
HACKED
CYBERAWARE
DENIED
TROJAN
USER DATA
PASSWORD
BUG
SPAM
CRACK
HACK
MALWARE
ALARM
ERROR
VIRUS
CRIME
ALLOWED