



**Torsten Seeberg**

Landeskriminalamt Baden-Württemberg

Zentrale Ansprechstelle Cybercrime (ZAC)

Taubenheimstraße 85 · 70372 Stuttgart

Telefon: 0711 5401 - 2444

Webseite: [lka.polizei-bw.de/zac](https://lka.polizei-bw.de/zac)



- polizeiliche Kontaktstelle für Institutionen
- 17 ZAC-Dienststellen bundesweit ([www.polizei.de/zac](http://www.polizei.de/zac))
- national und international vernetzt
- 24/365
- Beratung und Anzeigenaufnahme
- Prävention: Unterlagen, Warnmeldungen, Awareness-Vorträge, Übungen für KRITIS, Messestände





# Bedrohungslage Cybercrime



@kenji@chaos.social

@Dennis\_Kipker

...

Zwei Jahre hat die [#Caritas](#) gebraucht, um wirtschaftlich über den [#Cyberangriff](#) hinwegzukommen - und die Caritas ist kein [#Produktionsbetrieb](#):

"Durch den Angriff von Hackern auf die IT war die Caritas im Jahr 2022 in ein Minus von 23 Mio. Euro geraten."



Von br.de

5:06 nachm. · 17. Juli 2024 · 187 Mal angezeigt





# Indonesia's National Data Centre Ransomware Attack: A Digital Governance Failure?

PUBLISHED 8 AUG 2024

## Ransomware-Befall: Notstand in Costa Rica – Erpressergruppe veröffentlicht Daten

Ein Befall mit Ransomware legt Regierungsbehörden lahm. Der Präsident verkündet den Cyber-Notstand, will aber nicht zahlen – Conti leakt daraufhin die Daten.





11.02.2025 | Aktuelle Meldung | Nr. 004

# Cyberangriff auf die IT-Systeme des Sekretariats der Deutschen Bischofskonferenz



## Russische Angreifer hacken E-Mail-Konten der Microsoft-Chefetage

Russischen Hackern ist es gelungen, sich über Umwege Zugang zu der E-Mail-Kommunikation von Microsofts Führungs-Team zu verschaffen. Die Attacke wurde von Microsofts Sicherheitsabteilung erst nach knapp zwei Monaten bemerkt. Welche Manager betroffen sind, ist unklar.



Roland Quandt, 20.01.2024 11:53 Uhr



BACK-UP FEHLT

## Feuer zerstört ungesicherte Cloud der koreanischen Regierung

750.000 Beamte haben ihre Dateien in dem zerstörten Cloud-System abgelegt. Das war aber nicht an ein Back-up angeschlossen – ein fataler Fehler.

6. Oktober 2025 um 10:05 Uhr / [Oliver Nickel](#)

76

News folgen Teilen





Microsofts Digital Defense Report

## Deutschland ist Hauptziel von Cyberangriffen in der EU

Nur drei Staaten werden weltweit häufiger mit Cyberattacken bedroht als die Bundesrepublik. Häufig involviert: Hackergruppen aus Russland, China und Nordkorea. Verbraucher können sich mit einem einfachen Trick schützen.

17.10.2025, 10.01 Uhr

Die zehn Länder, die am häufigsten Ziel von Hacker-Angriffen wurden

Land	Anteil in Prozent
USA	24,8 %
Vereinigtes Königreich	5,6 %
Israel	3,5 %
Deutschland	3,3 %
Ukraine	2,8 %
Kanada	2,6 %
Japan	2,6 %
Indien	2,3 %
Vereinigte Arabische Emirate	2,0 %
Australien / Taiwan	1,8 %

(Quelle: Microsoft Digital Defense Report 2025 - Zahlen für Januar bis Juni 2025)



## Polizeiliche Kriminalstatistik Baden-Württemberg

PKS BW	2020	2021	2022	2023	2024
Computer-kriminalität	10.248	10.744	11.144	13.531	14.986
Tatmittel Internet	29.575	39.648	38.917	43.280	46.090

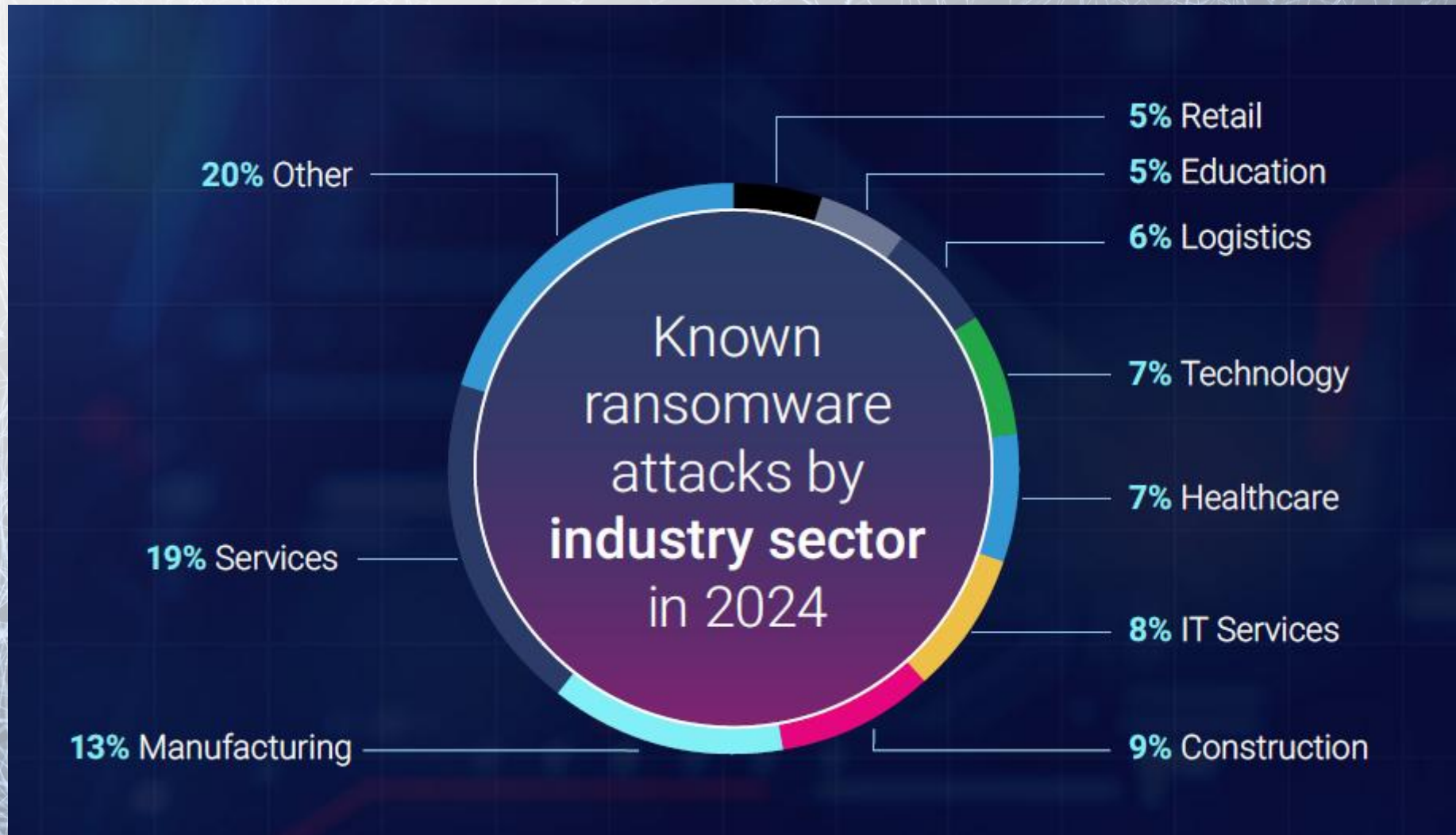




## Bedrohungslage Cybercrime

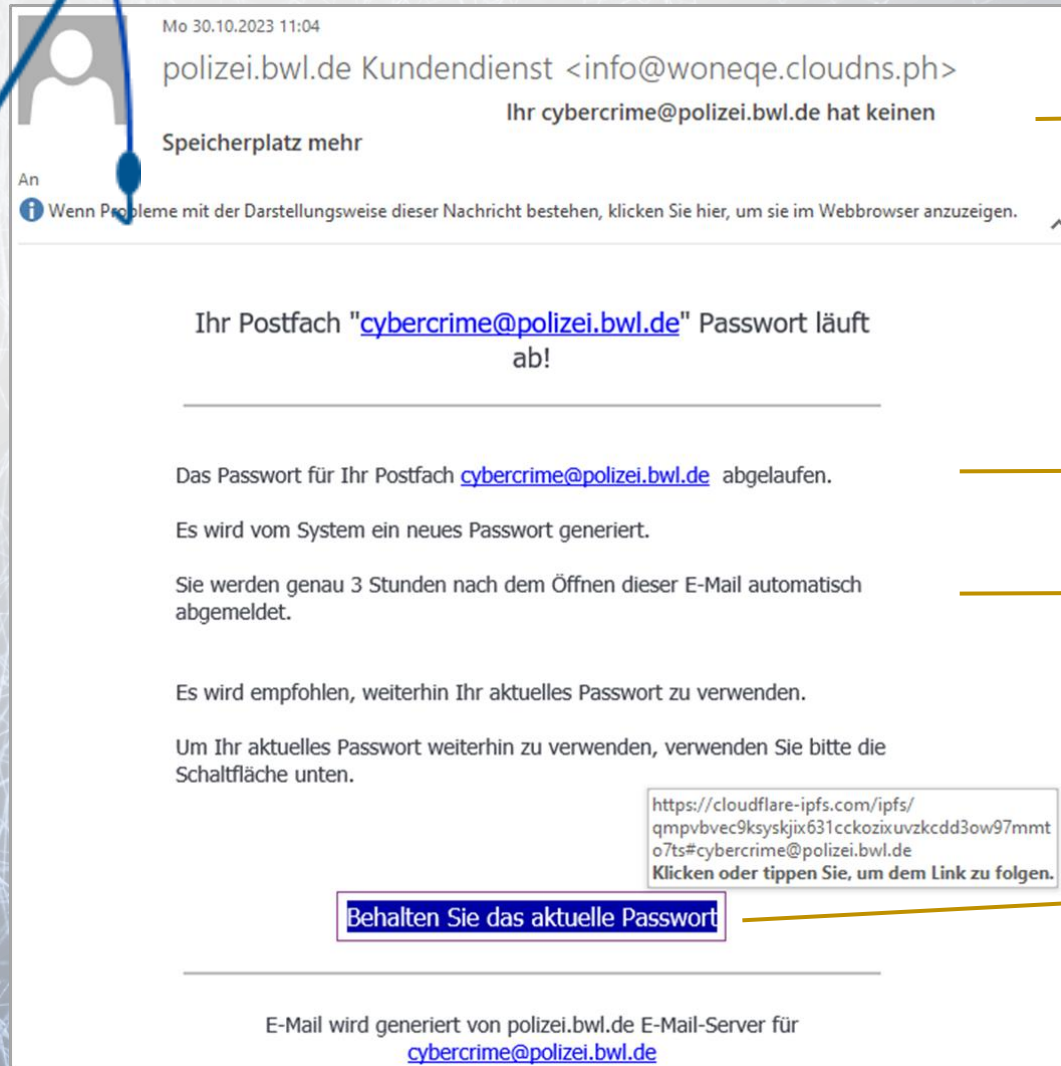








# Phishing



Plausibilitätskontrolle

persönliche Ansprache

Zeitdruck

"Mouse-over"

Folie 12





## E-Mail-Finanzbetrug





# E-Mail-Finanzbetrug

Endbetrag EUR : 3.341,66

## ZAHLUNGSBEDINGUNGEN

Zahlung bis zum 20.10.2025 ohne Abzug

Bei Zahlung bis zum 14.10.2025 2,0% Skonto vom Warenwert EUR 2.477,01 = EUR 49,54;  
ergibt Zahlungsbetrag = EUR 3.292,12

Private Rechnungsempfänger sind bei steuerpflichtigen Werkleistungen gesetzlich dazu verpflichtet,  
Rechnungen und ähnliche Belege zwei Jahre lang aufzubewahren.

Soweit nicht anders angegeben, entspricht das Lieferscheindatum dem Leistungsdatum

Bei Rückfragen zu dieser Rechnung wenden Sie sich bitte an

der

persönliche Ansprache

**FRACHTEN SIND NICHT SKONTIERBAR! Unberechtigte Abzüge werden nachgefordert.**

## Artikel-Auflistung

Artikel-Nr.	Bezeichnung	Anz. LS	Menge	Preis	Nettobetrag
B127/1	C30/37 GK16 F3 XC4/XF1/XD1/XA1	3	16,80 m³	200,90	2.619,12
			16,80 m³		

Am 09. Oktober tritt die EU Verordnung „VoP“ in Kraft.

Mit dieser Verordnung wird ein IBAN Namensabgleich durchgeführt. Bitte verwenden Sie daher verbindlich folgenden  
Empfängernamen: Heinz M

Umgehungstaktik  
Empfängerabgleich  
Kontoinhaber (VoP)

Betreiber: [REDACTED]

Persönlich haftende  
Gesellschafterin:

Sitz:  
Pfullendorf

Bankverbindung:  
IBAN: DE20 50 [REDACTED] 7 92  
BIC: BBVADEFFXXX

USt. IdNr.  
DE813056053

Betrugskonto





## E-Mail-Finanzbetrug

- Auftrag des falschen Geschäftsführers:  
vorgetäuschte Rechnung

Angeblicher Absender:  
Geschäftsführer

Adressat Rechnungsstelle

Passende  
Dokumentenbezeichnung

Rechnung vom 13/10-2025



Markus B [REDACTED].net>

An rechnungen@[REDACTED]le



Die Rechnung liegt bei; bitte zahlen Sie diese heute per Sofortüberweisung.

Viele Grüße

Markus B [REDACTED]





## E-Mail-Finanzbetrug

- Auftrag des falschen Geschäftsführers: vorgetäuschte Rechnung
- PDF-Anlage

Polnische Bankverbindung

**KOLASIŃSKI**  
SEO OPTIMALIZATION

Place of issue:  
Siemianowice Śląskie  
Date of issue: 2025-10-03

Invoice No. of: 13/10-2025

**Seller**

KAJETAN KOLASIŃSKI  
UL. POWSTAŃCÓW 18/6  
41-100 SIEMIANOWICE ŚLĄSKIE, POLAND  
VAT no: PL6443547315

**Buyer**

[REDACTED] GERMANY  
VAT no: DE815857134

Account number: PL28 1090 1186 0000 0001 6412 7024  
SWIFT/BIC number: WBKPPLPP

No	Name of goods/service	Amount	Unit	Net price	VAT	Net amount	VAT amount	Pre-tax amount
1.	SEO Audit and Website Optimization Services	1.00	piece	7000.00	0%	7000.00	0.00	7000.00
SUM: 7 000.00								

Payment method: wire transfer  
Payment date: 7 days 2025-10-10

VAT rate	Net	VAT	Pre-tax
0%	7000.00	0.00	7 000.00
Total	7000.00	0.00	7 000.00

**To pay: 7 000,00EUR**

Paid: 0.00 EUR  
Left to pay: 7 000.00 EUR  
Amount in words: seven thousand EUR 00/100

-----  
Person authorized to receive

-----  
Person authorized to issue

VAT exempt according to Article 44 and 196 of the EU VAT Directive (reverse charge).





# E-Mail-Finanzbetrug

Hbheitliche Wappen

## Betrugsdelikte:

- vermeintlich amtliche Rechnungen

[https://www.bzst.de/DE/Service/Betrug/warnung\\_betrugsversuche\\_node.html](https://www.bzst.de/DE/Service/Betrug/warnung_betrugsversuche_node.html)

Polnisches Bankkonto



Bundeszentralamt  
für Steuern

Bundeszentralamt für Steuern - An der Kuppe 1, 53225 Bonn



## RECHNUNG

Rechnungs-Datum: 17.05.2025  
Rechnungs-Nr.: FVG-298024

Produkt-Nr.	Produkt	Anzahl	Stückpreis exkl. MwSt.	Gesamt exkl. MwSt.	MwSt.
3475238	Verspätungszuschlag Steuererklärung (ZAHLUNGSZIEL 2 TAGE NACH ERHALT UNSERES SCHREIBENS) (steuerfrei)	1	390,32 €	390,32 €	-
Gesamtsumme (Netto):					390,32 €
Gesamtsumme:					390,32 €

Bitte Überweisen Sie den Betrag auf das folgende Konto

Zahlungsempfänger: Zahlstelle BZST · IBAN: PL75 1090 2835 0000 0001 6226  
2614 · BIC: WBKPPLPPXXX · Verwendungszweck: N5UJVA

Mit dem nebenstehenden Girocode können Sie die Rechnungsdaten schnell,  
bequem und sicher über Ihr Smartphone in Ihre Mobile-Banking-App  
übernehmen. Bei Fragen wenden Sie sich bitte an Ihre Bank.



Bundeszentralamt für  
Steuern  
An der Kuppe 1, 53225  
Bonn  
DE259582878

Bankverbindung  
Zahlstelle BZST  
PL75 1090 2835 0000 0001  
6226 2614  
WBKPPLPPXXX

Gerichtsstand  
HRB Bonn

Kundenservice  
Tel.: 0221-95019931  
poststelle@bzst.de-mail.de





NACH 194 JAHREN

### Cyberangriff drängt deutsches Unternehmen in die Insolvenz

Die Aachener Schumag AG ist weltweit bekannt für ihre Präzisionsteile. **Finanziell** lief es zuletzt nicht so gut. Ein **Cyberangriff** hat die Situation verschärft.

**schwäbische** 

Startseite > Regional > Region Ostalb > Aalen > **Finanzieller**

**Stadtoval**

### Finanzieller Engpass nach Cyberangriff: Hotelbetreiber insolvent

Die Scoop Aalen Hotelbetriebs GmbH ist insolvent. Sie betreibt das Hotel MAXX in Aalen. Laut Unternehmern ist ein Cyberangriff für den finanziellen Engpass verantwortlich.

Ransomware

Fasana stellt Insolvenz Antrag nach Cyberangriff

### Cloudanbieter geht durch Hackerangriff pleite

**Cyberkriminelle** haben im August 2023 die Systeme von Cloudnordic **verschlüsselt**. Nun existiert der dänische **Cloudanbieter** nicht mehr.





- Handlungsempfehlungen der Polizei gegen **Verschlüsselungsangriffe** und **E-Mail-Betrug**  
[Webseite](#)
- Cybersicherheitscheck (IHK)  
[Beratungsangebot für KMU](#)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)  
[NIS2G – Betroffenheitsprüfung](#) - fallen Sie mit Ihrem Unternehmen unter die künftigen Regularien?  
[NIS2G – Sicherheitscheck](#)  
[Basis-Empfehlungen zur Stärkung der IT-Sicherheit](#)  
[IT-Grundschutzkompendium](#)
- Warn- und Informationsdienst (CERT Bund)  
[Datenbank mit aktuellen Sicherheitslücken](#)
- Microsoft  
[Schadensverhinderung](#) + [Schadensfindung/-bewältigung](#) - Sicherheitsempfehlungen für Office365
- CISA (Cybersecurity & Infrastructure Security Agency)  
[www.cisa.gov](http://www.cisa.gov) (englisch)



Zentrale Ansprechstelle Cybercrime

# ZAC

Damit Sie im Netz niemandem ins Netz gehen

## Für Behörden und Unternehmen

© Landeskriminalamt Baden-Württemberg

0711 5401-2444

cybercrime@polizei.bwl.de

[www.LKA.POLIZEI-BW.DE/ZAC](http://www.LKA.POLIZEI-BW.DE/ZAC)