„Cybercrime – Wie kann ich mein Unternehmen schützen?“

ZENTRALE ANSPRECHSTELLE CYBERCRIME

FÜR UNTERNEHMEN UND BEHÖRDEN

Baden-Württemberg

LANDESKRIMINALAMT

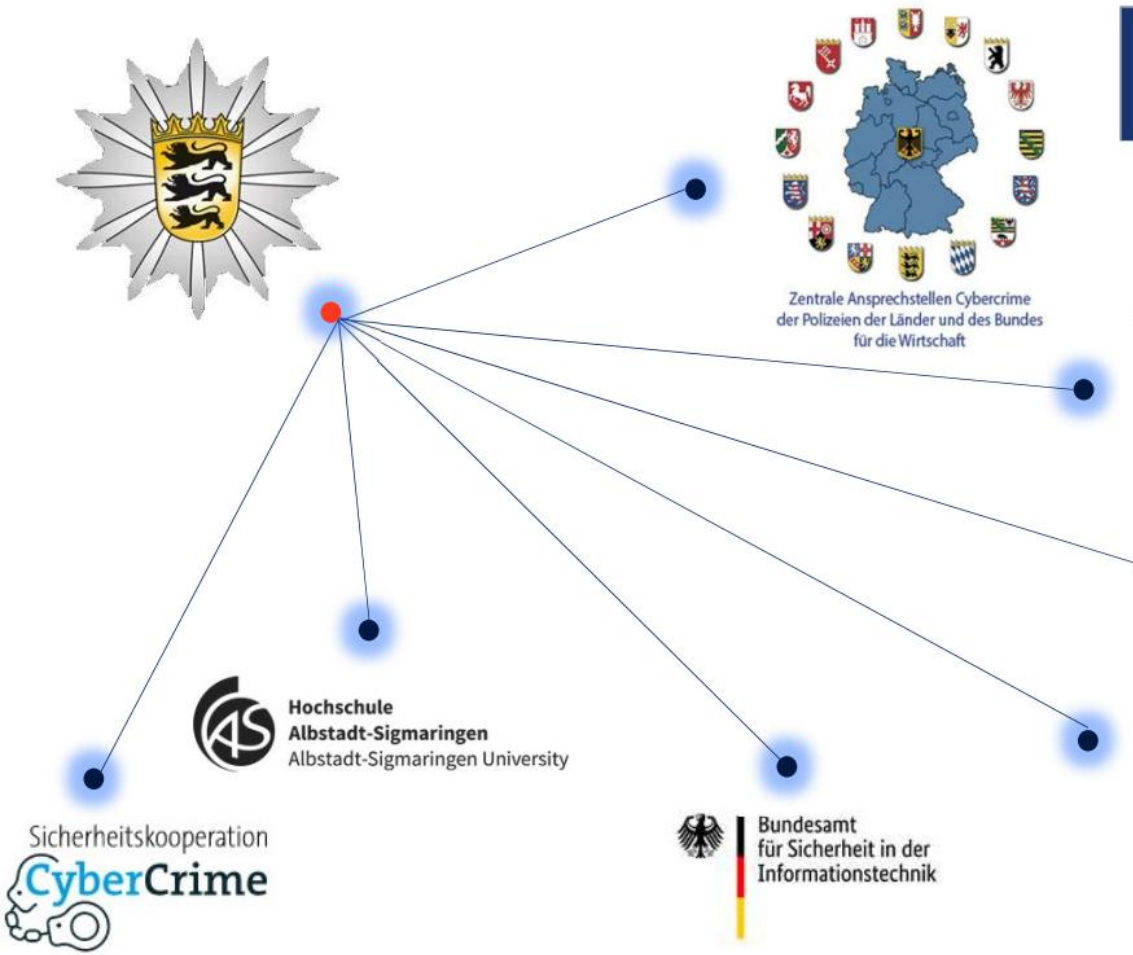
BEREIT FÜR SICHERHEIT

Zentrale **A**nsprechstelle **C**ybercrime

- polizeiliche Kontaktstelle für Institutionen in BW
- Einrichtung im Jahr 2012
- Beratung und Anzeigenaufnahme
- 17 ZAC-Dienststellen bundesweit (www.polizei.de/zac)
- national und international vernetzt

Baden-Württemberg
LANDESKRIMINALAMT

Unser Netzwerk



Baden-Württemberg
LANDESKRIMINALAMT

Aufgaben:

- Erster Angriff und Unterstützung im Schadensfall
- Koordinierung der Sachbearbeitung
- Enger Austausch mit den K5-Dienststellen (TSK)
- Austausch mit anderen Behörden
- Bundesweite Gremienarbeit
- Statistikerfassung
- Steuerung von Lage- & Warnmeldungen

Baden-Württemberg
LANDESKRIMINALAMT

Kontaktaufnahme:

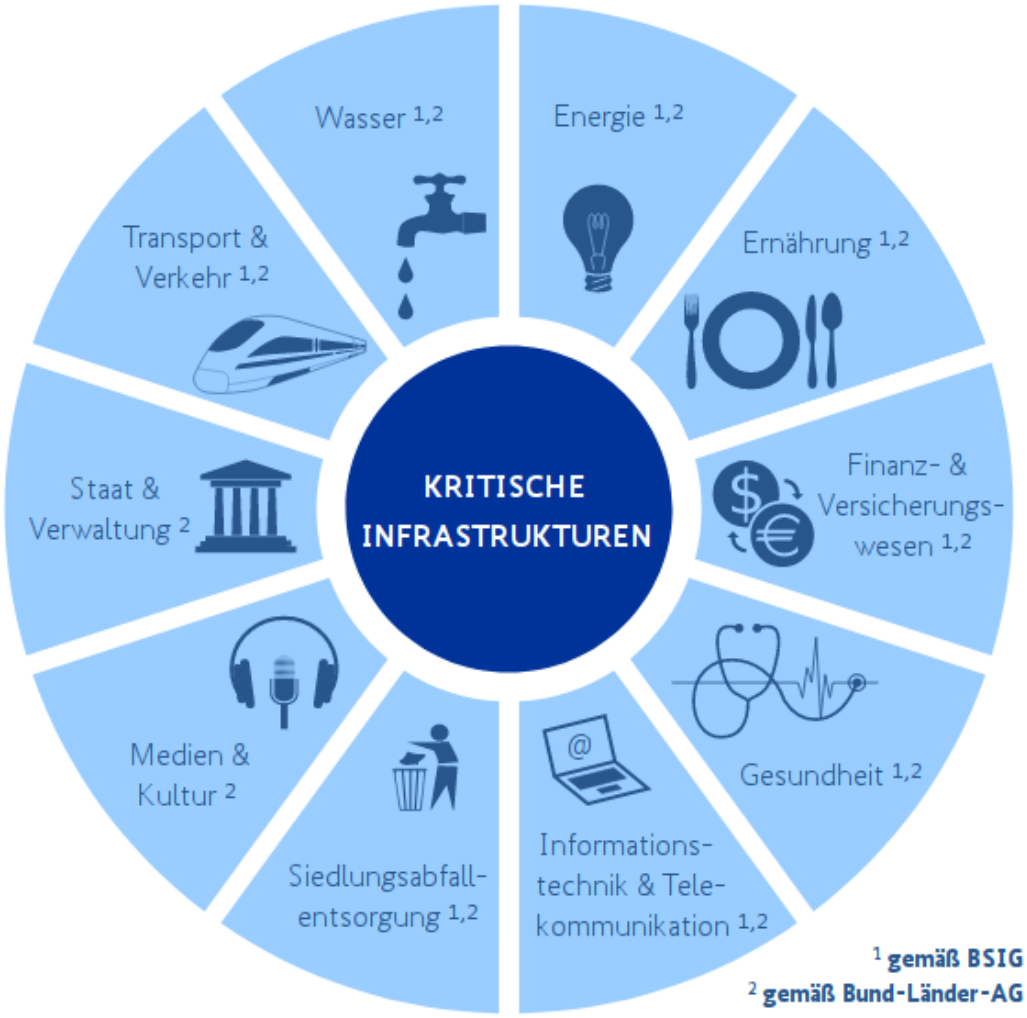
Tel.: **0711-54012444**

E-Mail: **cybercrime@polizei.bwl.de**

1. Kurzdarstellung der Lage
2. Überblick bereits entstandener oder bevorstehender Schäden sowie eventueller Versorgungsstörungen.
3. Schilderung der bisher getroffenen Maßnahmen.
4. Standort der betroffenen Systeme.
5. Erreichbarkeiten des Ansprechpartners.
6. Kontaktdaten IT-Dienstleister.
7. Autorisierung des Dienstleisters zur Kooperation mit der Polizei.

„formlos & unbürokratisch“

Baden-Württemberg
LANDESKRIMINALAMT



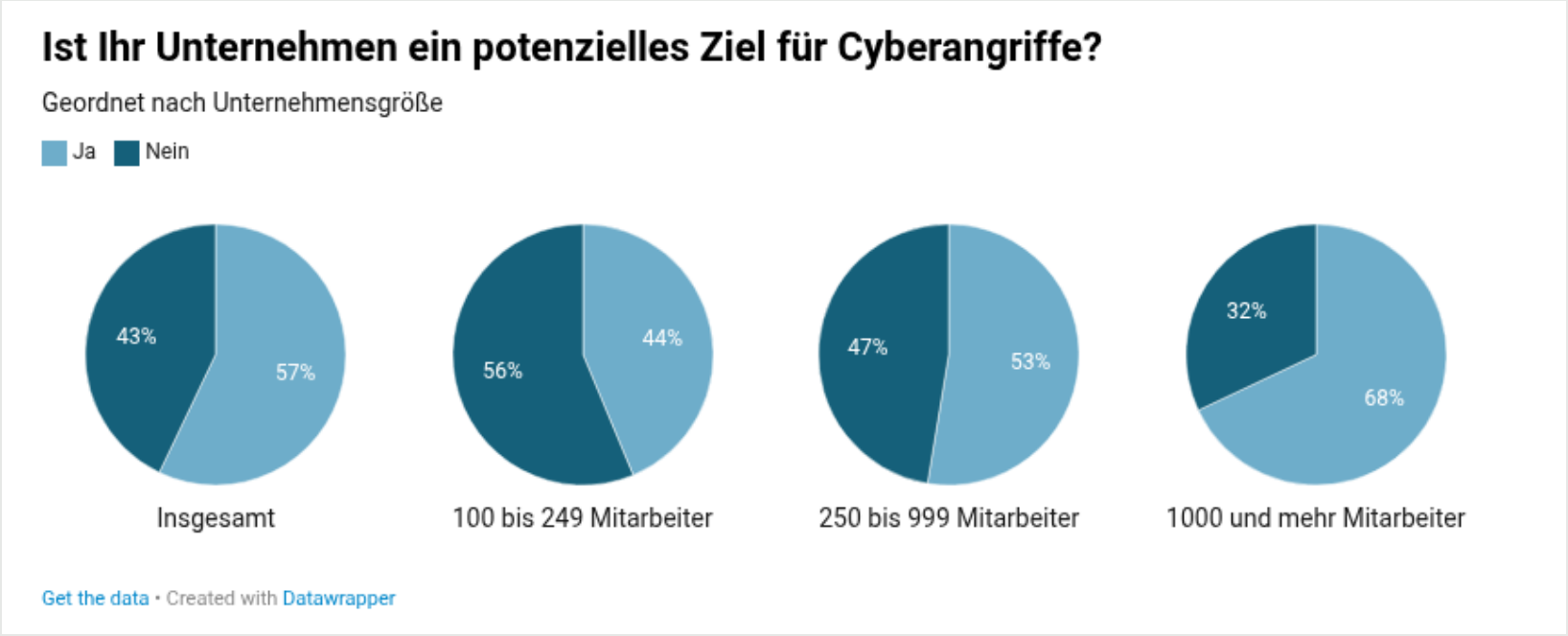
Kritische Sektoren

„Jeder ist Zielperson“

„Kleine und mittelständische Unternehmen (KMU) sind besonders attraktive Ziele für Cyberkriminelle. Das liegt vor allem daran, dass es ihnen oftmals an personeller Security-Expertise und finanziellen Mitteln fehlt, um eine ausgereifte, solide Cybersicherheit aufzubauen.“

(https://www.security-insider.de/cybersicherheit-fuer-kmu-herausforderungen-und-loesungen-a-a84466b969396788acc6f32d02d883dd/?cflt=rdt, 07.11.2024)

einerseits:
„Wir sind kein interessantes Ziel für Angreifer“



https://www.security-insider.de/cybersicherheit-in-kmus-unterschaetzte-gefahr-a-03e972d2030e6b8c0569c56446b78e6d/

… andererseits:

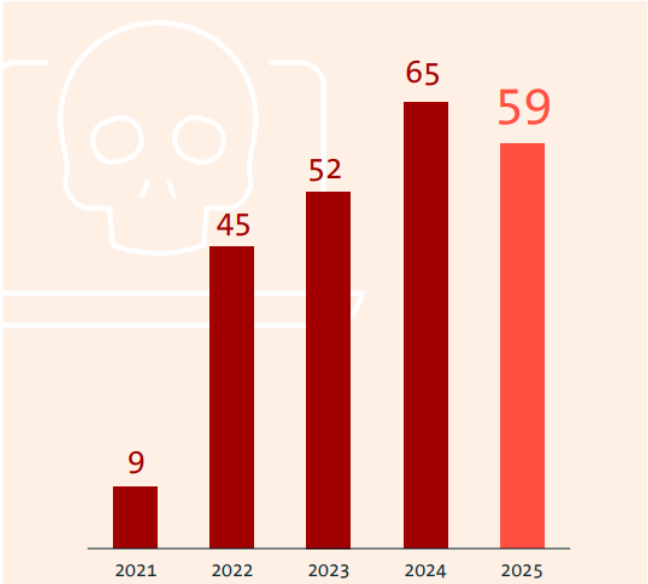
https://www.bitkom.org/sites/main/files/2025-10/bitkom-charts-cybercrime-und-der-markt-fuer-it-sicherheit-2025.pdf

Unternehmen halten Cyberattacken für existenzbedrohend – und jedes Zweite fühlt sich sehr gut vorbereitet

Inwieweit treffen die folgenden Aussagen zu?

50% (2024: 53%)
»Unser Unternehmen ist auf Cyberangriffe **sehr gut vorbereitet**.«

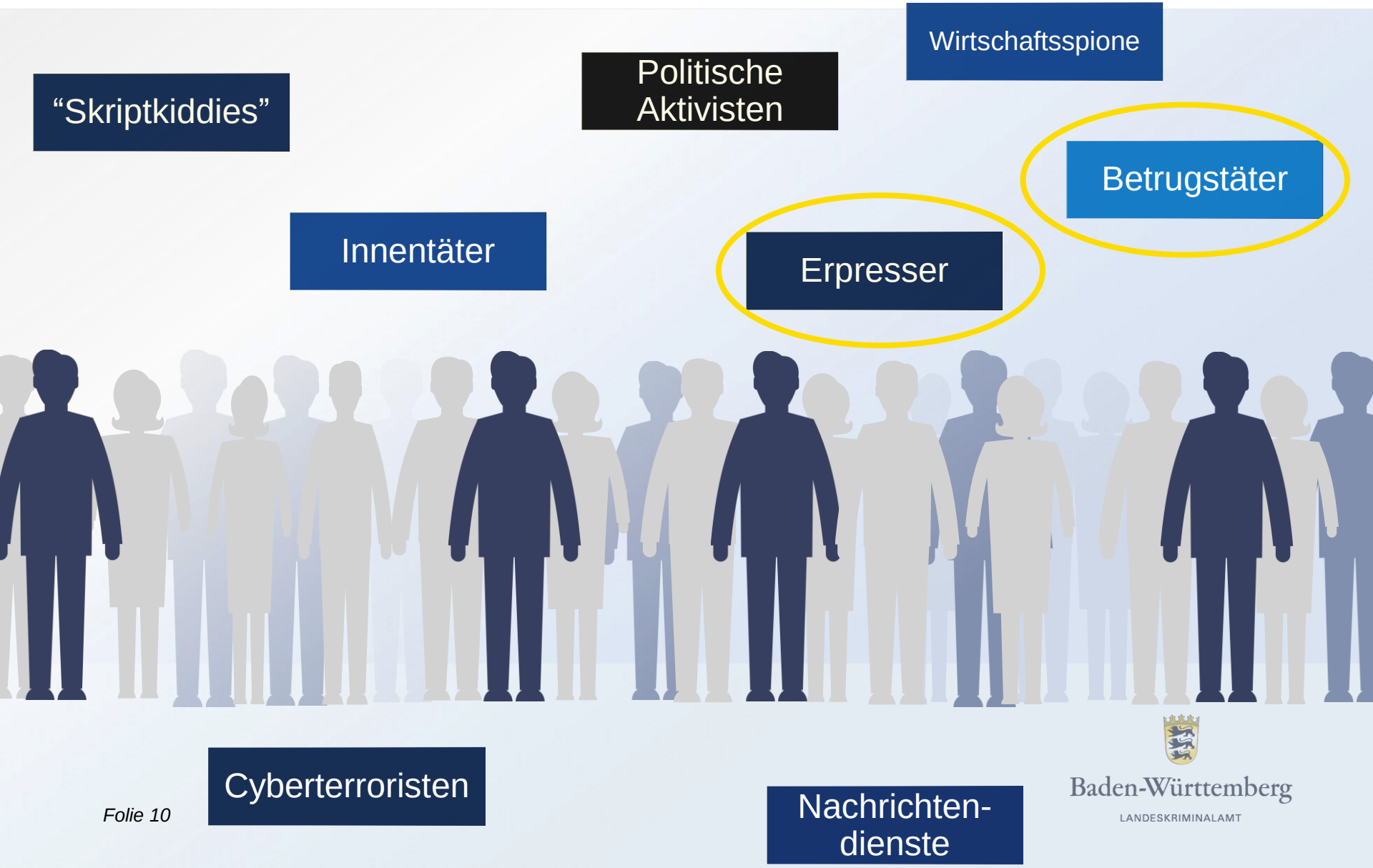
in Prozent



3 Basis: Alle Unternehmen (n=1.003) | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research 2025

bitkom

Wer sind die Täter?



Baden-Württemberg
LANDESKRIMINALAMT

Wer sind die Täter?

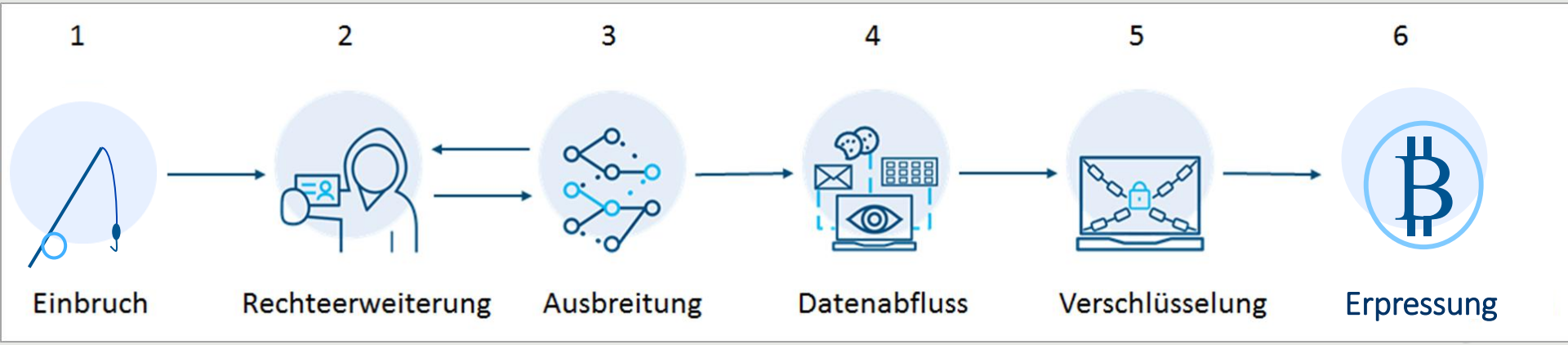
Erpresser

Betrugstäter

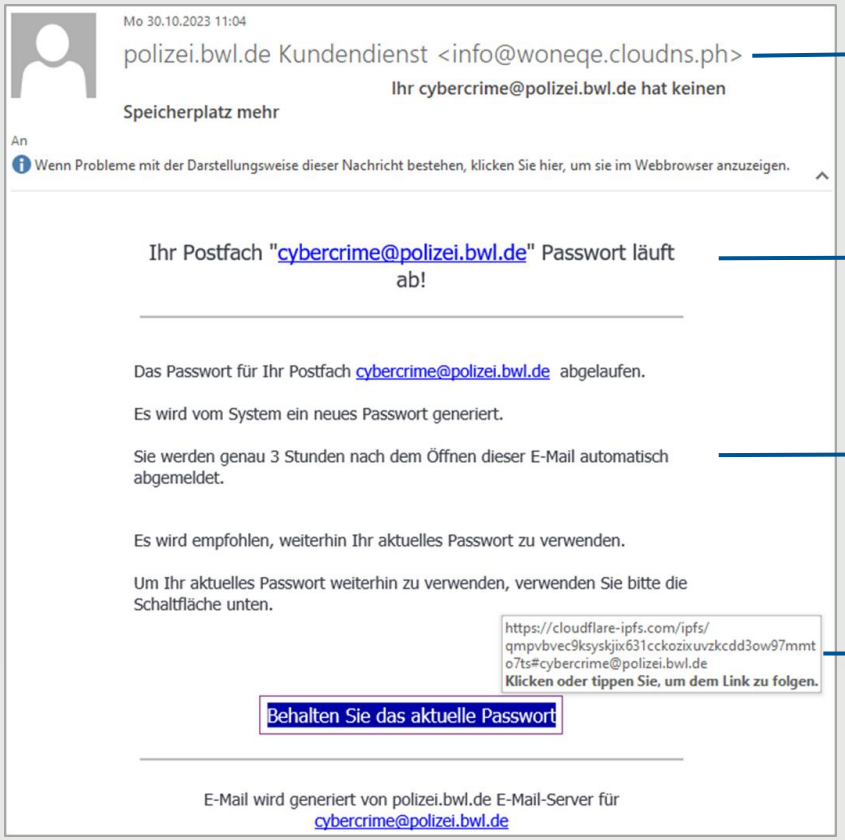
Erpresser

Phänomen „Ransomware“ (Verschlüsselungstrojaner)
Angriffsvektoren:

- „end-of-life“ Soft- & Hardware
- „Phishing“ (Fernzugriff)
- fehlerhafte Konfiguration
- Schadsoftware



„Phishing“



→ Plausibilitätskontrolle

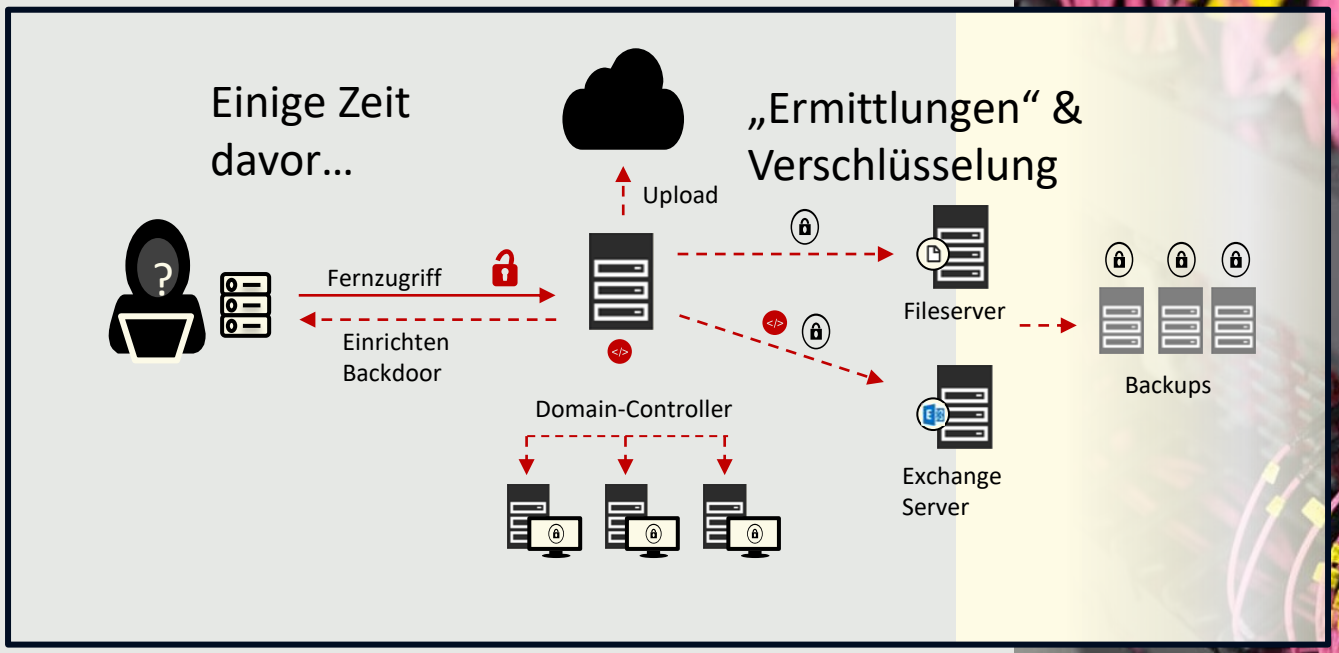
→ persönliche Ansprache

→ Zeitdruck

→ “Mouse-over“

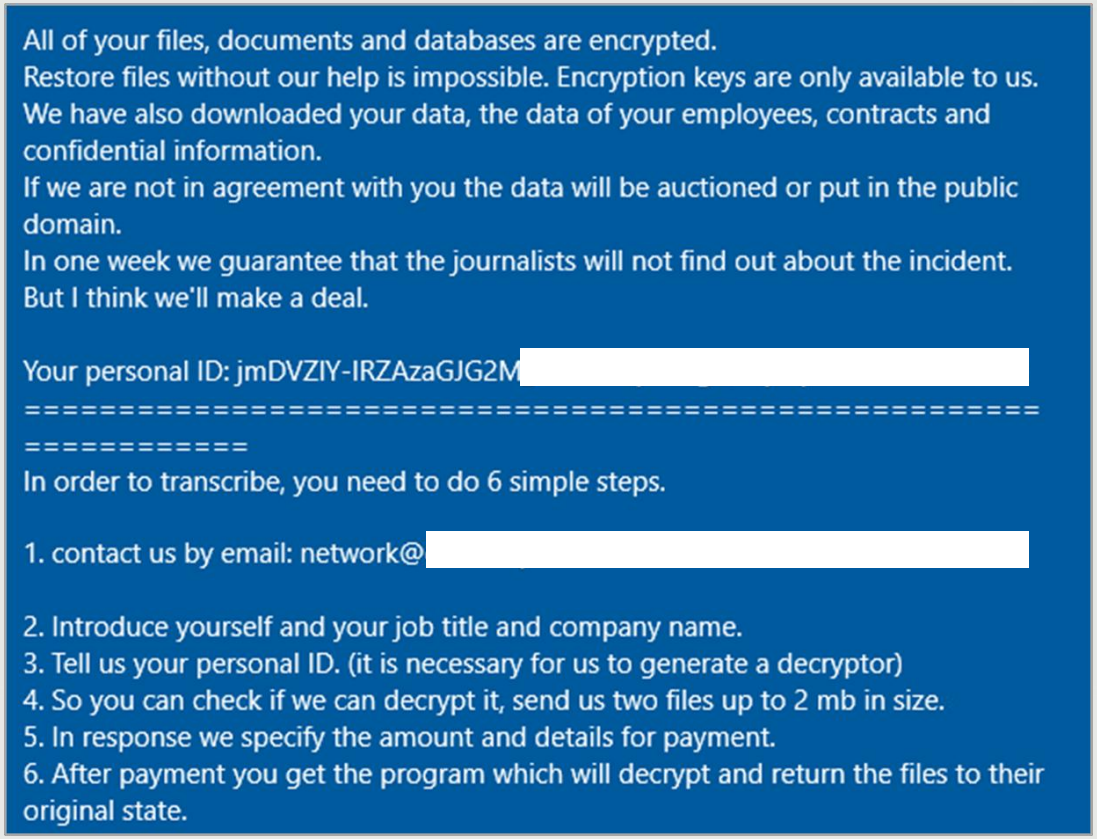
https://cloudflare-ipfs.com/ipfs/qmpvbvec9ksyskjix631cckozixuvzkcdd3ow97mmto7ts#cybercrime@polizei.bwl.de
Klicken oder tippen Sie, um dem Link zu folgen.

Vorgehensweise der Täter



Baden-Württemberg
LANDESKRIMINALAMT

Ransomware


All of your files, documents and databases are encrypted.
Restore files without our help is impossible. Encryption keys are only available to us.
We have also downloaded your data, the data of your employees, contracts and confidential information.
If we are not in agreement with you the data will be auctioned or put in the public domain.
In one week we guarantee that the journalists will not find out about the incident.
But I think we'll make a deal.

Your personal ID: jmDVZIY-IRZAzaGJG2M[redacted]
==========
==========
In order to transcribe, you need to do 6 simple steps.

1. contact us by email: network@[redacted]

2. Introduce yourself and your job title and company name.
3. Tell us your personal ID. (it is necessary for us to generate a decryptor)
4. So you can check if we can decrypt it, send us two files up to 2 mb in size.
5. In response we specify the amount and details for payment.
6. After payment you get the program which will decrypt and return the files to their original state.

„Ransom- Note“ der Tätergruppierungen

Drohung von Veröffentlichung auf „Leakboard“

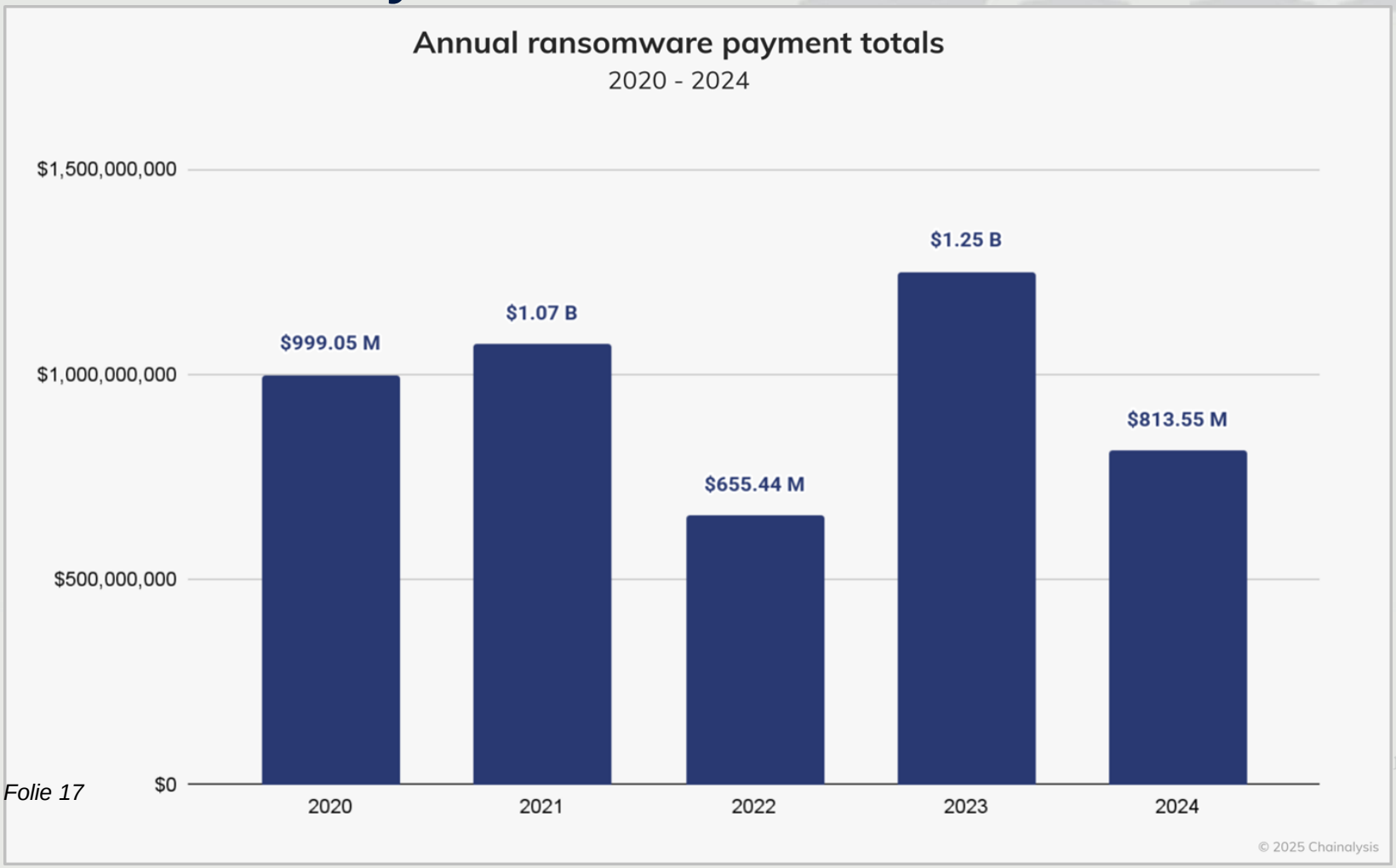
Ransomware Auswirkungen

Eigenschäden

Reputationsschäden

Fremdschäden

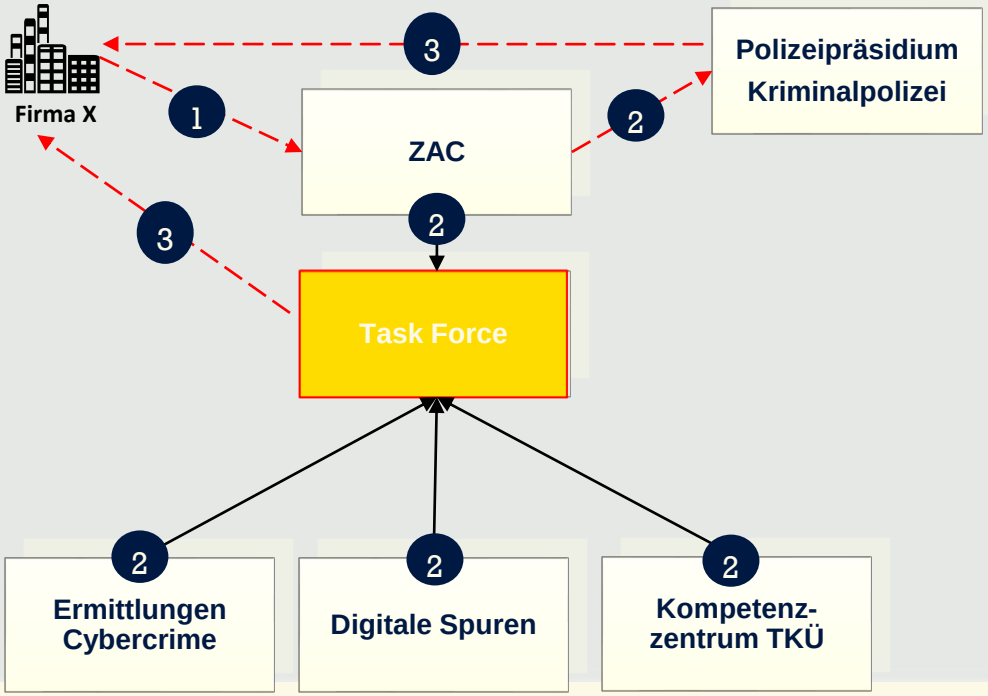
Ransomware Zahlungen laut Chainalysis



1. Vorbereitung einer Krisenorganisation (Krisenstab und operative Einheiten) mit klaren Rollen und Verantwortlichkeiten
2. Erstellung einer strukturierten Übersicht der IT-infrastruktur
3. zeitnahes Einspielen von Sicherheitsupdates (Patchmanagement)
4. Multifaktorauthentifizierung
5. insb. hinsichtlich Ransomware sicheres Backupkonzept
6. regelmäßige Schulung /Sensibilisierung der Mitarbeiter
7. Frühzeitige Einbindung der Polizei

Handlungsempfehlungen

Wie reagieren wir, wenn Sie (richtig) reagieren?

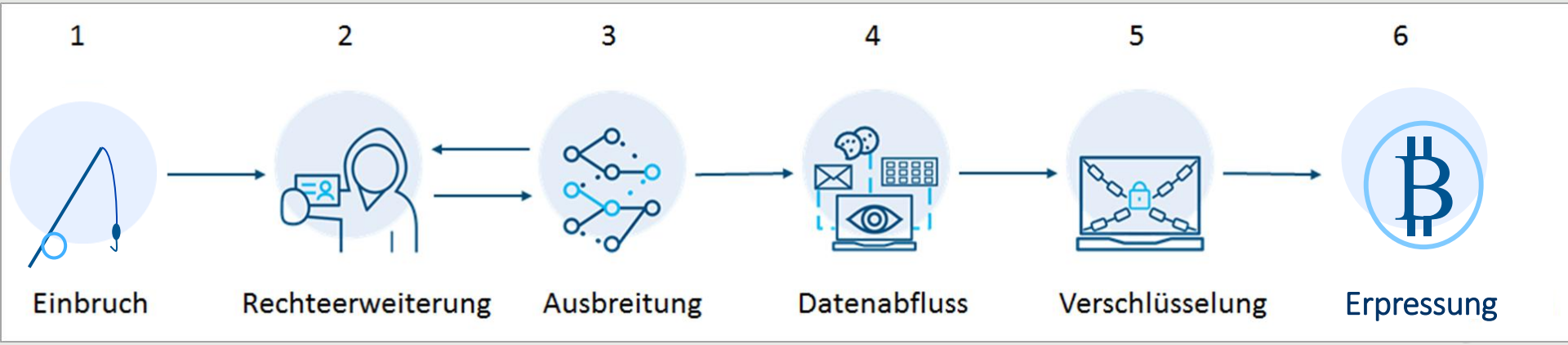


Baden-Württemberg
LANDESKRIMINALAMT

Erpresser

Phänomen „Sextortion“ (Erpressung aufgrund sexueller Grundlage)

- Spam (nicht ernst zu nehmen)
- oftmals Spoofing (eigene E-Mail; .de. ; .de-)
- §254 StGB Erpressung/ §240 StGB Nötigung (§23 StGB Versuch)



Erpresser

Dies ist die letzte Warnung.

Ich habe über eine von Ihnen besuchte Website für Erwachsene einen Trojanervirus auf Ihrem Betriebssystem installiert.
Alle persönlichen Daten sind auf meine Server kopiert worden.
Ich habe Zugriff auf Ihre persönlichen Daten, Messenger, sozialen Netzwerke, E-Mails, Chatverläufe und Kontaktlisten.

Mein Virus erlaubt es mir, Ihr System zu infiltrieren. Es handelt sich um einen Multiplattform-Virus mit einem versteckten VNC.
Es funktioniert auf iOS, Android, Windows und macOS.
Es ist verschlüsselt, so dass Ihr System es nicht erkennen kann, ich lösche seine Signaturen jeden Tag.

technische Erklärung

Beim Sammeln von Informationen über Sie habe ich festgestellt, dass Sie ein großer Fan von Websites für Erwachsene sind.
Du besuchst gerne Pornoseiten und schaust dir schmutzige Videos an, während du einen Orgasmus hast.

Ich habe bereits ein Bildschirmfoto gemacht.
Es ist eine Montage aus dem pornografischen Video, das Sie sich gerade angesehen haben, und Ihrer Selbstbefriedigung.
Ihr Gesicht ist deutlich sichtbar. Dieses Video wird Ihren Ruf für immer ruinieren.

Ich werde dieses Video an alle Ihre Kontakte und Bekannten weitergeben und es im Internet veröffentlichen.
Außerdem werde ich alle Ihre persönlichen Daten veröffentlichen (Anrufe, Korrespondenz, Besuchshistorie, Ihre persönlichen Fotos und Videos, alle Ihre Geheimnisse werden öffentlich zugänglich sein).
Ich werde alles, was ich über Ihr Gerät finden konnte, ins öffentliche Internet stellen.

Ich denke, Sie wissen, was ich meine.
Das wird eine echte Katastrophe für Sie sein.

Ich könnte dein Leben für immer ruinieren.

Drohung

Ich glaube nicht, dass Sie das wirklich wollen.

Lassen Sie uns das so lösen: Sie überweisen mir 1100 Euro (EUR) (in Bitcoin-Gegenwert zum Wechselkurs im Moment der Überweisung), und ich werde diesen ganzen Dreck sofort von meinen Servern löschen.
Danach werden wir uns gegenseitig vergessen.

Meine Bitcoin-Brieftasche für die Zahlung: [redacted]

Wenn Sie nicht wissen, wie man Geld überweist und was Bitcoin ist. Verwenden Sie Google.

Ich gebe Ihnen 2 Arbeitstage.

Forderung

Versuchen Sie nicht, sich irgendwo zu beschweren, denn es gibt keine Möglichkeit, die Brieftasche zurückzuverfolgen, und die Post, von der der Brief kam, ist ebenfalls nicht zurückverfolgbar und wird automatisch erstellt, so dass es keinen Sinn hat, mir zu schreiben.
Versuchen Sie nicht, die Polizei oder andere Sicherheitsdienste zu kontaktieren, da Ihre Daten sonst veröffentlicht werden.

Betrugstäter

Betrugsdelikte :

- Falsche Bankverbindung (Spam-E-Mails)
- erfundene Rechnungen
- geänderte Bankverbindungen von Mitarbeitern
- Falsche Geschäftsführer

Cybercrimedelikte:

- technische Kompromittierung (Strafrechtlich)
- §§202a,b,c; 263a; 269; 303a/b StGB

Betrugstäter

Angriffsvektoren:

- Spam E-Mails mit Zahlungsaufforderungen
- Gespoofte E-Mails mit Rechnungen/ Erpressungen
- E-Mail Hacking (CCieS)
- Ausspähen von Daten
- Öffentliche Ausschreibungsportale

Betrugstäter

Betrugsdelikte :
- erfundene Rechnungen

1&1 Telecom GmbH - Elgendorfer Str. 57 - 56410 Montabaur

[redacted]
70182 Stuttgart
Deutschland

Rechnungs-Nr. RE-25-[redacted]
Rechnungsdatum 02.05.2025
Lieferdatum 02.05.2025

Ihre Kundennummer 7987418
Ihr Ansprechpartner Florian Horst

Rechnungs Nr. RE-25-[redacted]

Sehr geehrte Damen und Herren,

hiermit stellen wir Ihnen die folgende Leistung in Rechnung:

Pos.	Beschreibung	Menge	Einzelpreis	Gesamtpreis
1.	**Domainverlängerung 1 Jahr [redacted]** **stuttgart.de** Domainverlängerung 1 Jahr Verlängerung bis 02.05.2026 [redacted]	1,00 Stk	21,00 EUR	21,00 EUR
	Gesamtbetrag netto			21,00 EUR
	Umsatzsteuer 19% Deutschland			3,99 EUR
	Gesamtbetrag brutto			**24,99 EUR**

Zahlungsbedingungen: Zahlung sofort nach Rechnungseingang ohne Abzüge.

Bitte überweisen Sie den Rechnungsbetrag unter Angabe der Rechnungsnummer.

Mit freundlichen Grüßen
Florian Horst

Seite 1 von 1

1&1 Telecom GmbH
Elgendorfer Str. 57
56410 Montabaur
Deutschland

Tel.: +49 (0) 721 960
E-Mail: info@1und1.de
Web: 1und1.de

Amtsgericht Montabaur
HR-Nr.: HRB 22331
USt.-ID: DE273413910
Geschäftsführung: Christian Bockelt

1&1 Telecom GmbH
IBAN:
CY53902000010000020109055595
BIC: CARDCY2L

1&1 Telecom GmbH
IBAN:
CY53902000010000020109055595
BIC: CARDCY2L

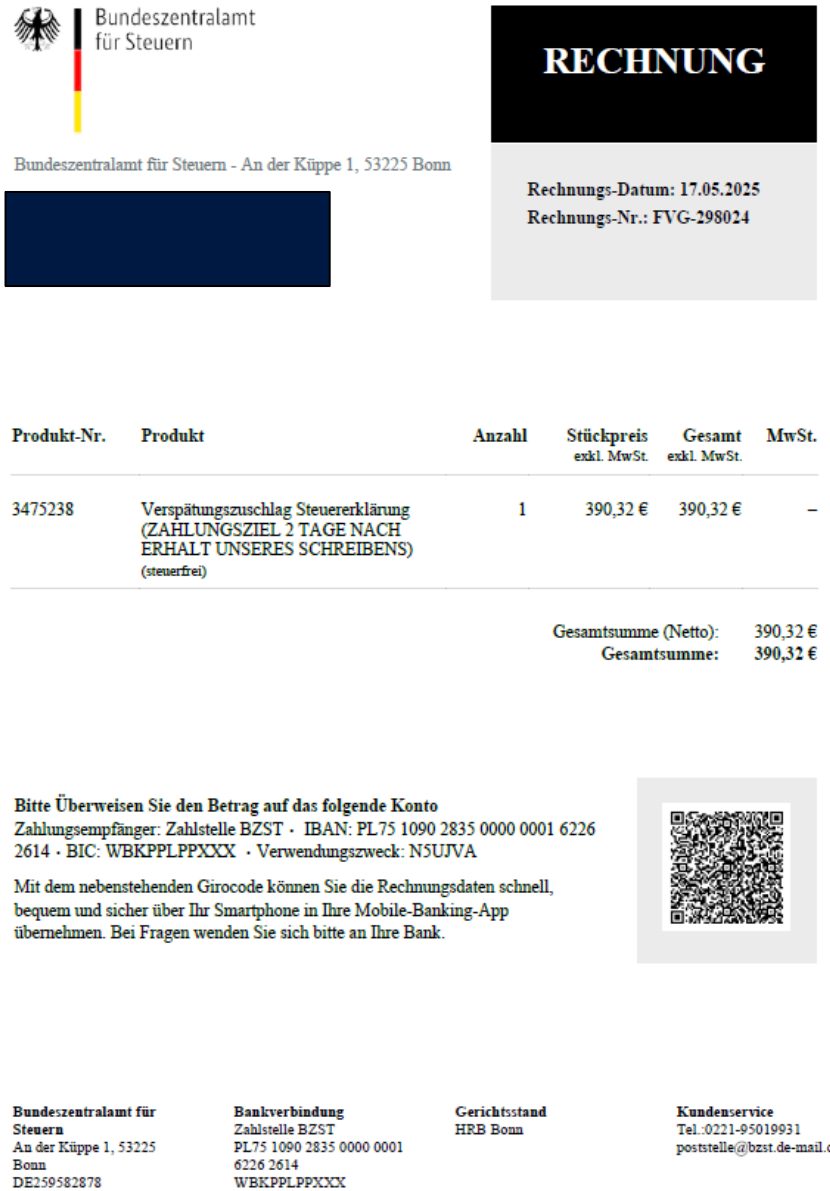
Bankkonto in Zypern

Betrugstäter

Betrugsdelikte :

- vermeintlich amtliche Rechnungen

https://www.bzst.de/DE/Service/Betrug/warnung_betrugsvers



Bundeszentralamt für Steuern

Bundeszentralamt für Steuern - An der Küppe 1, 53225 Bonn

[redacted]

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 Küppe 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

Betrugstäter

- Landeswappen NRW
- Zahlstelle Frankfurt a.M.
- Richter AG Stuttgart
- Konto Spanien

Amtsgericht

Zentrale Zahlstelle, 60313 Frankfurt am Main

Herrn/Frau/Firma/Büro
[redacted]

Datum: 09.05.2025

Rechnung

Bei Zahlung bitte **nur** das Kassenzeichen angeben!

Unser Geschäftszeichen:
24 DE 3745214/2025 / HRB 799756

Kassenzeichen: PANUPSLGD
Bankverbindung:
Empfänger: Forderungsregister
IBAN: ES25 0182 5319 7802 0827 0940
BIC: BBVAESMMXXX

Bezeichnung der Rechtsangelegenheit:
Handelsregisterbekanntmachung

0255(2429292942924 9)
04.592950035

Sehr geehrter Herr [redacted]

in dem vorgenannten Verfahren werden folgende Positionen in Rechnung gestellt:

Nr.	Bezeichnung des Ansatzes, ggfls. Nummer des Kostenverzeichnisses zum GKG, FamGKG, KostO bzw. GNotKG	Wert EUR	Ihr Anteil	Betrag EUR
	01 Eintragung mit wirtschaftlicher Bedeutung, § 58 GNotKG, § 1 HregGebV, Nr. 250 GV	2,00	1/1	1992,00

Ihre Zahlungsverpflichtung beträgt 1992,00

Rechnungsbetrag 1992,00

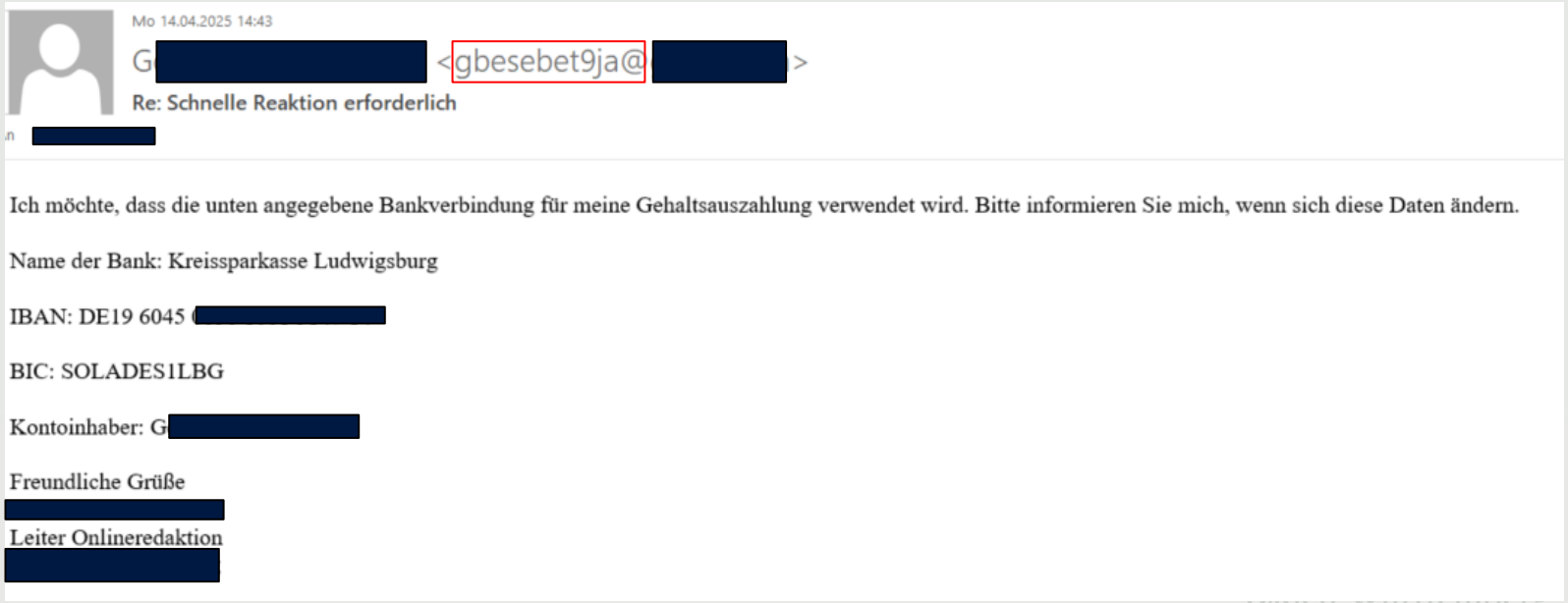
Zahlen Sie bitte unter Angabe des Kassenzeichens innerhalb von 3 Werktagen auf das oben bezeichnete Konto der Zahlstelle. Geben Sie für die Zahlung bitte als Referenz unbedingt **nur** allein das Kassenzeichen an. Ansonsten kann Ihre Zahlung zu spät gebucht werden, was eine selbstverschuldete Mahngebühr auslösen kann. Gerichtskostenmarken und Abdrucke von Gerichtskostenstemplern dürfen für die Zahlung nicht verwendet werden. Bitte beachten Sie, dass nach Ablauf der Zahlungsfrist die mit weiteren Kosten verbundene zwangsweise Einziehung des Betrages ohne vorherige Mahnung zulässig ist. Wenn Sie nicht oder zu spät zahlen, wird eine Mahngebühr in Höhe von 25,00 EURO gem. KV 1403 der Anlage zu § 4 Abs. 1 JVKostG fällig.

Hochachtungsvoll
Dr. Jörg Raupach
Richter am Amtsgericht Stuttgart

Betrugstäter

Betrugsdelikte :

- geänderte Bankverbindungen von Mitarbeitern
- Falsche Geschäftsführer



Mo 14.04.2025 14:43

G [redacted] <gbesebet9ja@[redacted]>

Re: Schnelle Reaktion erforderlich

[redacted]

Ich möchte, dass die unten angegebene Bankverbindung für meine Gehaltsauszahlung verwendet wird. Bitte informieren Sie mich, wenn sich diese Daten ändern.

Name der Bank: Kreissparkasse Ludwigsburg

IBAN: DE19 6045 [redacted]

BIC: SOLADES1LBG

Kontoinhaber: G[redacted]

Freundliche Grüße

[redacted]

Leiter Onlineredaktion

[redacted]

Betrugstäter

Öffentliche Ausschreibungsportale:

Sehr geehrte Damen und Herren,

vielen Dank für Ihre Information und die Anfrage zur Zusendung der neuen Bankverbindungsdetails. Bitte lassen Sie mir diese direkt (auf [redacted] zukommen, ich sorgen dann für eine entsprechende Einpflegung ins System. Vielen Dank bereits vorab.

Für künftige Zuschriften/Rückfragen wenden Sie sich gerne an mich und nehmen den in Kopie befindlichen Personenkreis ebenfalls in Cc. Das unten adressierte Vergabepostfach ist nach Abschluss der Vergabe des Auftrags zukünftig nicht mehr involviert. Auch hier bereits vorab vielen Dank für eine entsprechende Berücksichtigung.

Abschließend noch ein Hinweis: Wir gehen davon aus, dass der Versandweg der E-Rechnungen hiervon nicht berührt ist, da diese bereits einmal an der korrekten Stelle im Haus ankam. Nach Rücksprache mit Herrn [redacted] soll hier lediglich der Rechnungsbetrag noch angepasst und eine korrigierte Fassung versandt werden.

Mit freundlichen Grüßen

[redacted]

Betrugstäter

„Eine, tatsächlich von der Firma XXX an uns gestellte Rechnung in Höhe von 268.228,38 EUR war mit Zahlungsziel 14.09.2025 zu begleichen, weshalb die Anpassung der Kontoverbindung als zunehmend dringlich erschien.“
– Anzeige bei der ZAC

Schadenersatzpflichtig nach Art. 82 DSGVO

Machen Sie sich bewusst:

Jedes am Internet angebundene System kann über das Internet angegriffen werden!

Keine Internetanbindung = keine Angriffs- und Ausleitungsmöglichkeit über das Internet.

Der Wirtschaftsstandort steht durchgehend im Fokus von Cyberkriminellen.

Sie verantworten die Sicherheit der bei Ihnen gespeicherten Daten.

Investieren Sie Zeit, Personal und Geld in das Thema IT-Sicherheit.

Vorbereitung auf den Ernstfall:

- Erstellung Checkliste „IT-Notfall“.
- Binden Sie sich an einen IT-Vertragsdienstleister.
- Unbedingt externe Sicherheitskopien erstellen.
- E-Mail- und IT-Fernzugriffszugänge technisch absichern („Zweiter Sicherheitsfaktor“).
- Bewältigung IT-Krisenlage und Datenwiederherstellung üben.
- Im Schadensfall: Ruhe bewahren und Checkliste abarbeiten.
- „Neue“ Bankdaten erfordern die telefonische Verifizierung.
- Geld an Betrüger überwiesen? Sofortige Kontaktierung Hausbank und Polizei (ZAC).

  Grundsatz:

  Beachtung der Empfehlungen der Polizei und sonstiger Stellen.

CyberSicherheitsCheck für KMU

CyberSicherheitsCheck für KMU

→ Gegenseitige Unterstützung von Unternehmen und Polizei

- Polizei ist auf Anzeigen angewiesen (keine Anzeigepflicht)
- Ermittlungsansätze → Monitoring von Servern und Seiten
- Warnungen und Handlungsempfehlungen
- Take Down der Täterserver → Festnahme und Zerschlagung der Strukturen
- Finanzermittlung

Es floss Lösegeld – Cyber-Erpresser der Staatstheater Stuttgart gefasst

Sebastian Steegmüller 10.10.2024 - 13:27 Uhr

E-Mail-Betrug im Lörracher Rathaus: Verdächtiger wird in Lahr festgenommen

LockBit power cut: four new arrests and financial sanctions against affiliates

A developer, a Bulletproof hosting service administrator, and two other associates arrested in a series of coordinated action by France, the United

Schäden in Millionenhöhe

Mutmaßlicher Cybererpresser in Deutschland angeklagt

VANIR LOCKER

Deutsche Polizei übernimmt Tor-Seite einer Hackergruppe

BKA: Cybercrime: Festnahmen in Hessen und Rheinland-Pfalz - Erneuter Schlag gegen Underground Economy im Internet

und Computersabotage:
errt Webseite im Darknet

BILD KI GENERIERT

LANDESKRIMINALAMT

Zentrale Ansprechstelle Cybercrime

ZAC

Damit Sie im Netz niemandem ins Netz gehen

Für Behörden und Unternehmen

0711 5401-2444
cybercrime@polizei.bwl.de