PROFESSIONALITÄT
TOLERANZ
VERANTWORTUNG

POLIZEI
Sachsen

Cybercrime

Phänomene und polizeiliche Handlungsfelder

Agenda

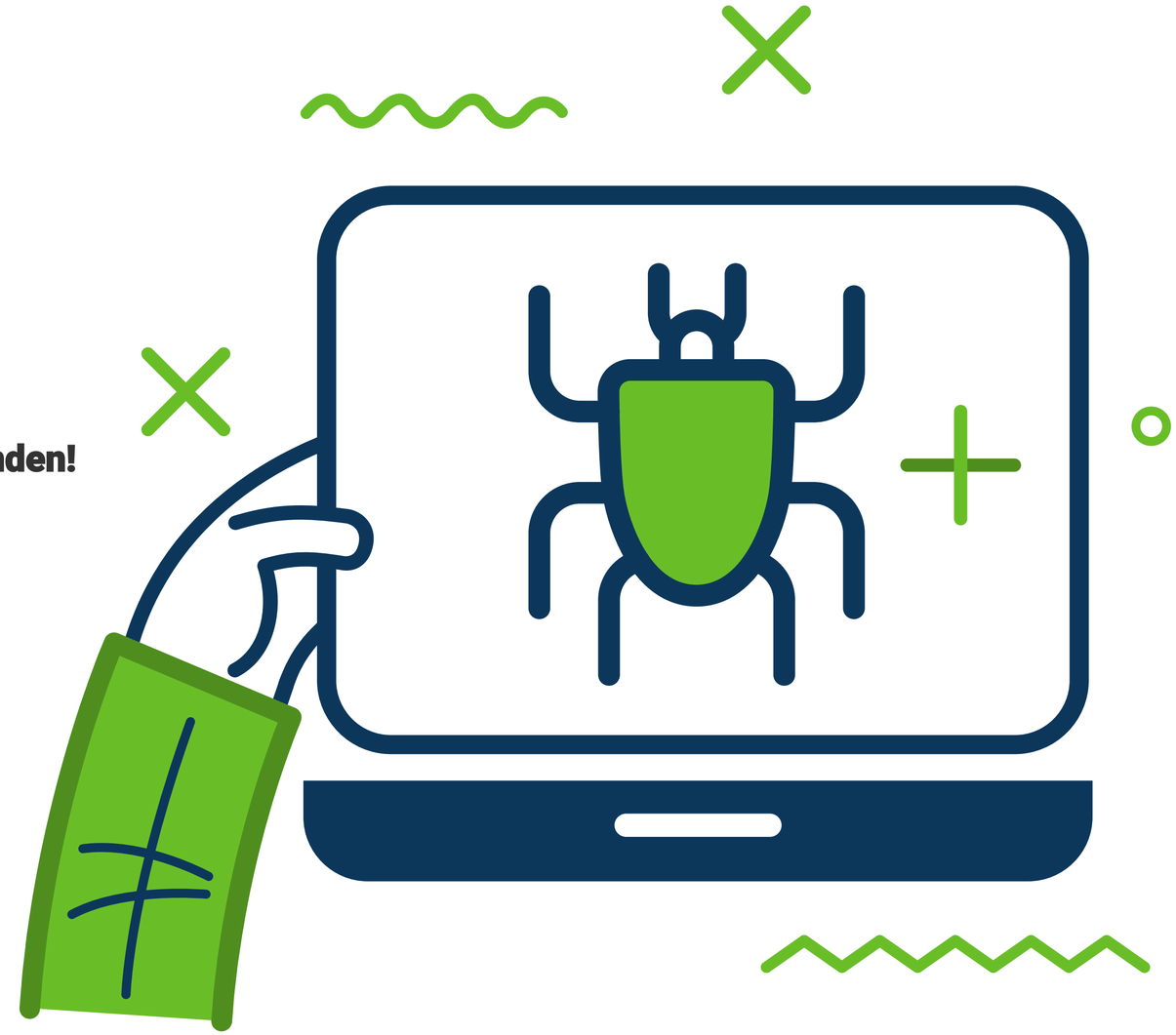
Statistik und Phänomene
Was sagt die Wirtschaft?
Was sagt die Polizei?

Aktuelle Fälle
Einfallstore der vergangenen Monate

ZAC LKA
Aufgaben und Handlungsfelder

Unterstützung finden!
Kooperationspartner und Netzwerke

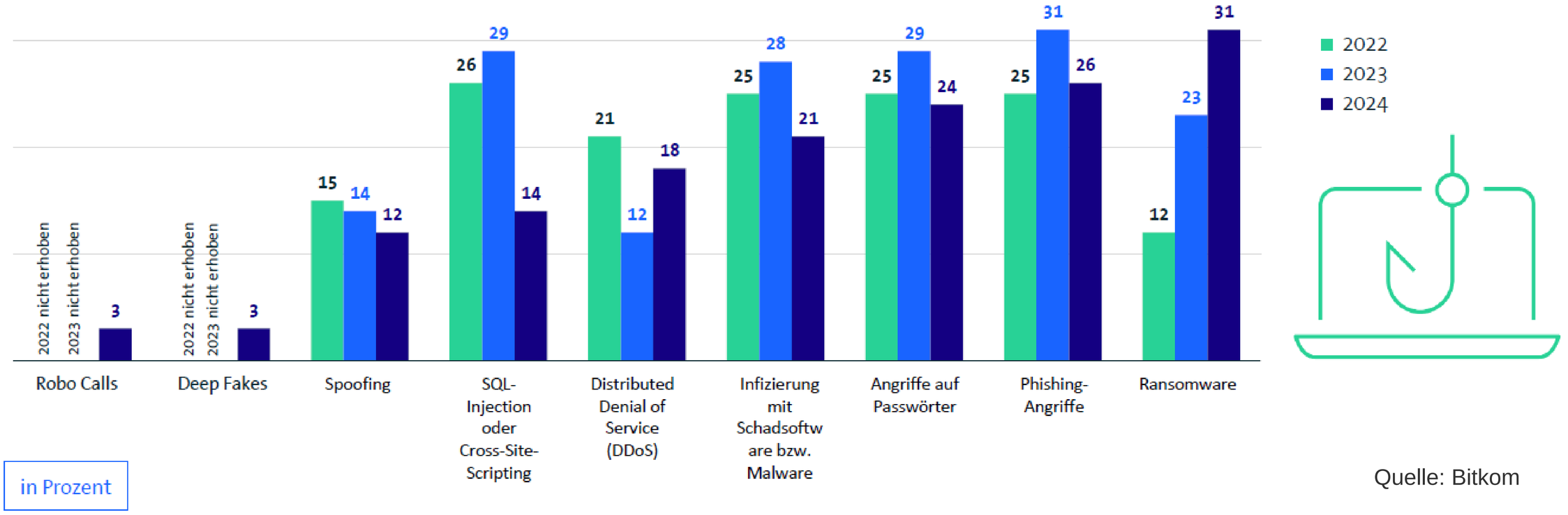
Erfolge
Wir geben Tätern ein Gesicht!



Cyber-Angriffe – Infografik Bitkom

Ransomware verursacht häufiger Schäden

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monate in Ihrem Unternehmen einen Schaden verursacht?

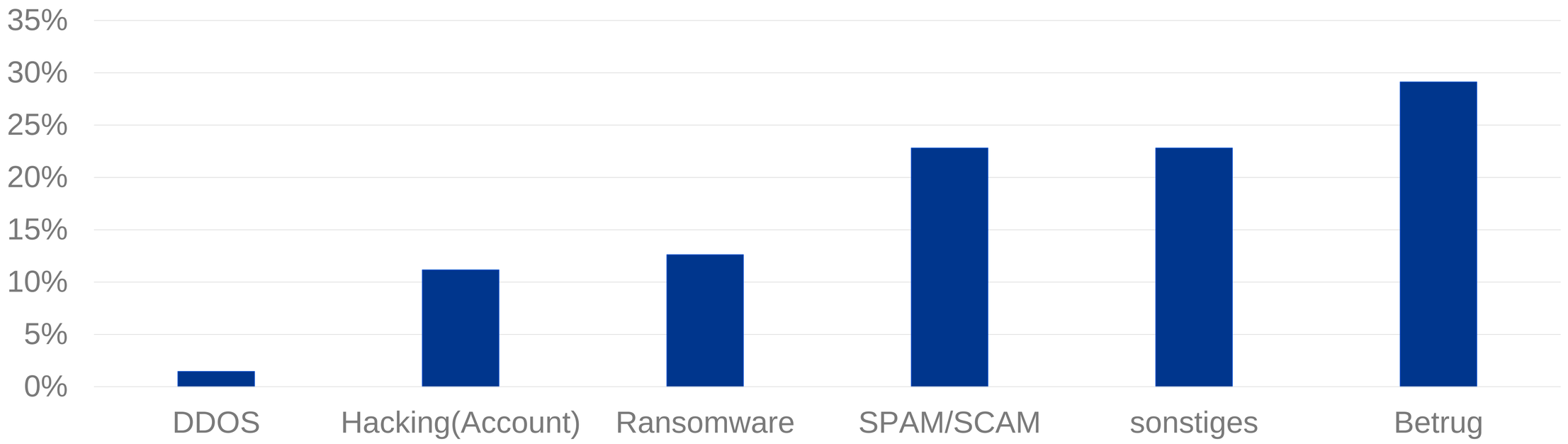


in Prozent

Quelle: Bitkom

POLIZEI Sachsen

Cyber-Angriffe 2024
Anzeigenaufkommen in der ZAC / Polizei SN



SPAM/SCAM – Phishing, Sextorsion

Sonstiges – Suizidankündigung in Foren, Verleumdung, Volksverhetzung, Schwachstellenübermittlugn durch dritte

Betrug – CEO Fraud, BeC, Fakeshop, Callcenter

Cyberangriffe in Sachsen 2024
- Eine Auswahl -

Ransomware

Vollverschlüsselung.

- Vermeintliche Freischaltung gegen Bezahlung
- Angriffswege vielfältig (Mails mit Anhängen, Drive-by-Download, Schwachstellen etc.)

Acc Hackinig

Benutzen von Zugangsdaten.

- Anmelden im Firmennetzwerk
- Schwer zu erkennen da plausible Nutzerkennung
- Zugang zu Zugangskennungen vielfältig zu erhalten (DarkWeb)

Phishing

Angeln nach Zugangsdaten

- Schwerpunkt Firmen
- Zugänge zum Firmennetzwerk
- Mitarbeiter im HomeOffice
- Bankingdaten

BEC

Benutzen gefälschter Geschäfts E-Mails

- E-Mails von scheinbaren Mitarbeitern, Lieferanten, Geschäftspartnern etc.
- Ziel: monetär
- Gut kopiert, um Vertrauenswürdigkeit herzustellen

PROFESSIONALITÄT
TOLERANZ
VERANTWORTUNG

POLIZEI Sachsen

Top 4 der Cyberangriffe in Sachsen 2024

Ransomware

Von Viktoria Hagen <Viktoria@infinitevo.com>
Antworten | Weiterleiten | Archivieren | Junk | Löschen | Mehr
Betreff **Bewerbung auf die ausgeschriebene Stelle - Viktoria Hagen** 10:26
An

Sehr geehrte Damen und Herren,

anbei erhalten Sie meine Bewerbung für Ihre ausgeschriebene Stelle. Warum ich die Stelle optimal ausfüllen kann und Ihrem Unternehmen durch meine Erfahrung im Vertrieb und der Kundenbetreuung zahlreiche Vorteile biete, entnehmen Sie bitte meinen ausführlichen und angehängten Bewerbungsunterlagen.

Ich freue mich auf ein persönliches Vorstellungsgespräch.

Mit besten Grüßen

Viktoria Hagen

Foto_Viktoria_Hagen.jpg

2 Anhänge 352 KB — Alle speichern

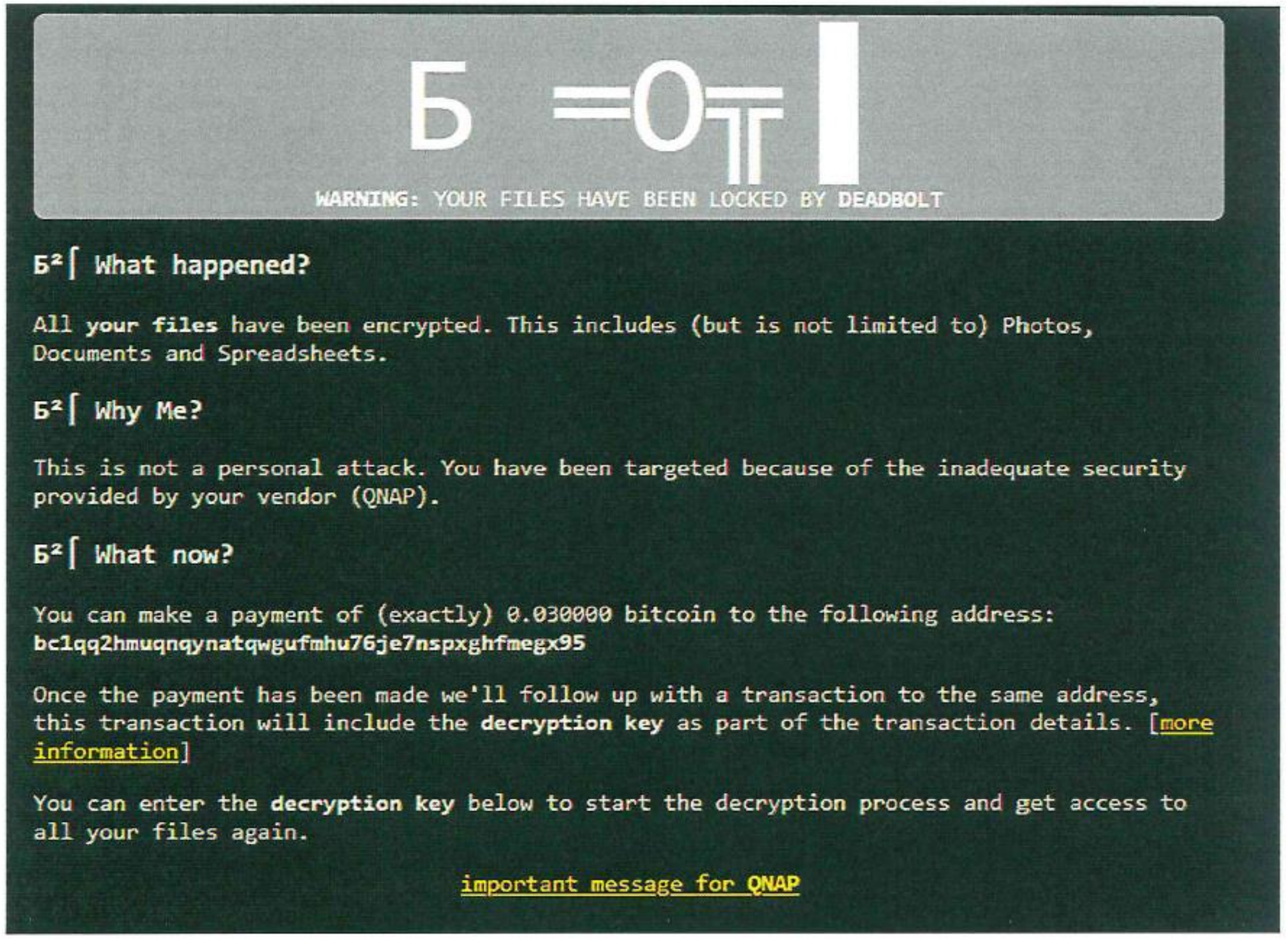
Foto_Viktoria_Hagen.jpg 61,1 KB | Viktoria Hagen - Bewerbung und Lebenslauf - 31.08.2018.zip 290 KB

PROFESSIONALITÄT
TOLERANZ
VERANTWORTUNG

POLIZEI Sachsen

Top 4 der Cyberangriffe in Sachsen 2024

Ransomware



Б =OТ▌

WARNING: YOUR FILES HAVE BEEN LOCKED BY DEADBOLT

Б²⌈ What happened?

All **your files** have been encrypted. This includes (but is not limited to) Photos, Documents and Spreadsheets.

Б²⌈ Why Me?

This is not a personal attack. You have been targeted because of the inadequate security provided by your vendor (QNAP).

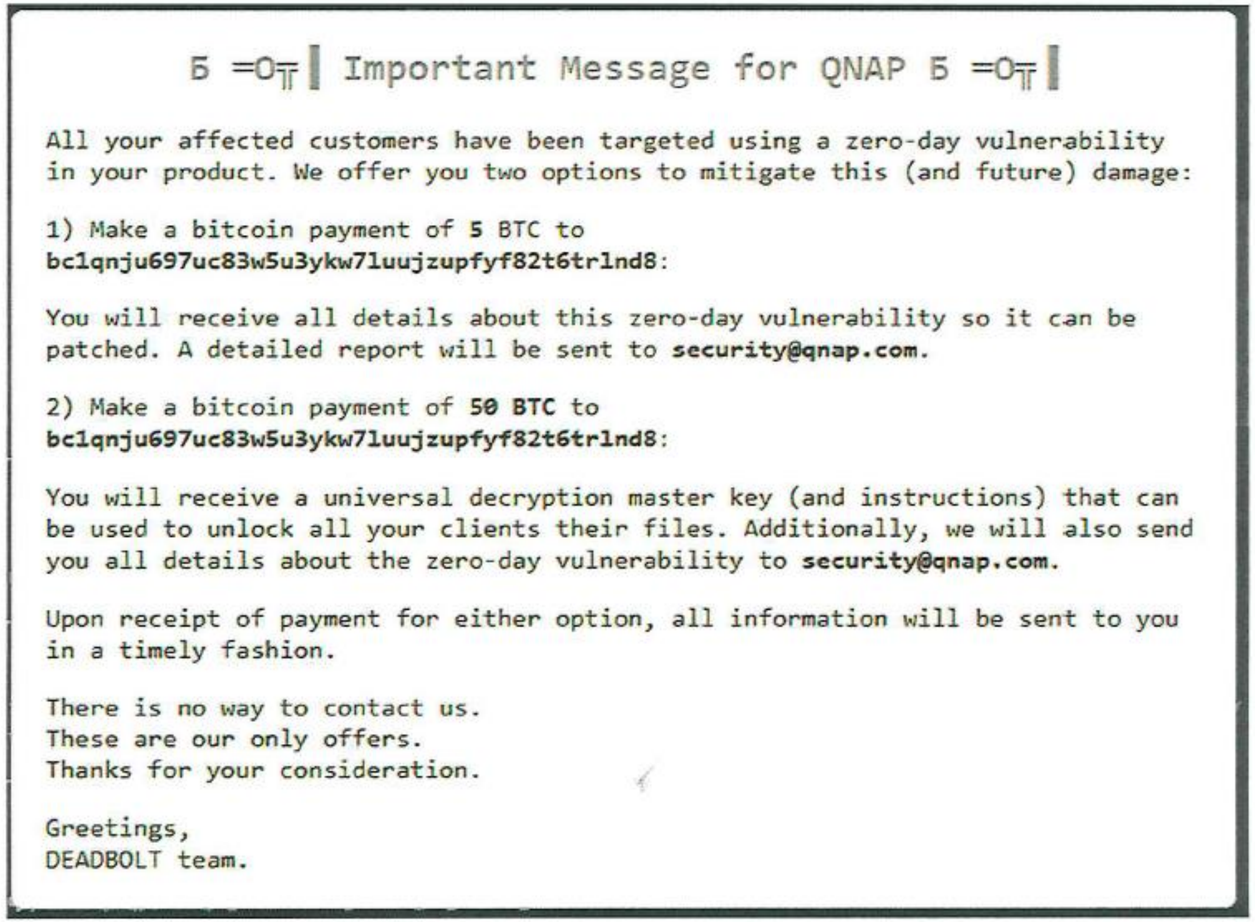
Б²⌈ What now?

You can make a payment of (exactly) 0.030000 bitcoin to the following address:
bc1qq2hmuqnqynatqwgufmhu76je7nspxghfmegx95

Once the payment has been made we'll follow up with a transaction to the same address, this transaction will include the **decryption key** as part of the transaction details. [more information]

You can enter the **decryption key** below to start the decryption process and get access to all your files again.

important message for QNAP



Б =OТ▌ Important Message for QNAP Б =OТ▌

All your affected customers have been targeted using a zero-day vulnerability in your product. We offer you two options to mitigate this (and future) damage:

1) Make a bitcoin payment of **5** BTC to
bc1qnju697uc83w5u3ykw7luujzupfyf82t6trlnd8:

You will receive all details about this zero-day vulnerability so it can be patched. A detailed report will be sent to **security@qnap.com**.

2) Make a bitcoin payment of **50 BTC** to
bc1qnju697uc83w5u3ykw7luujzupfyf82t6trlnd8:

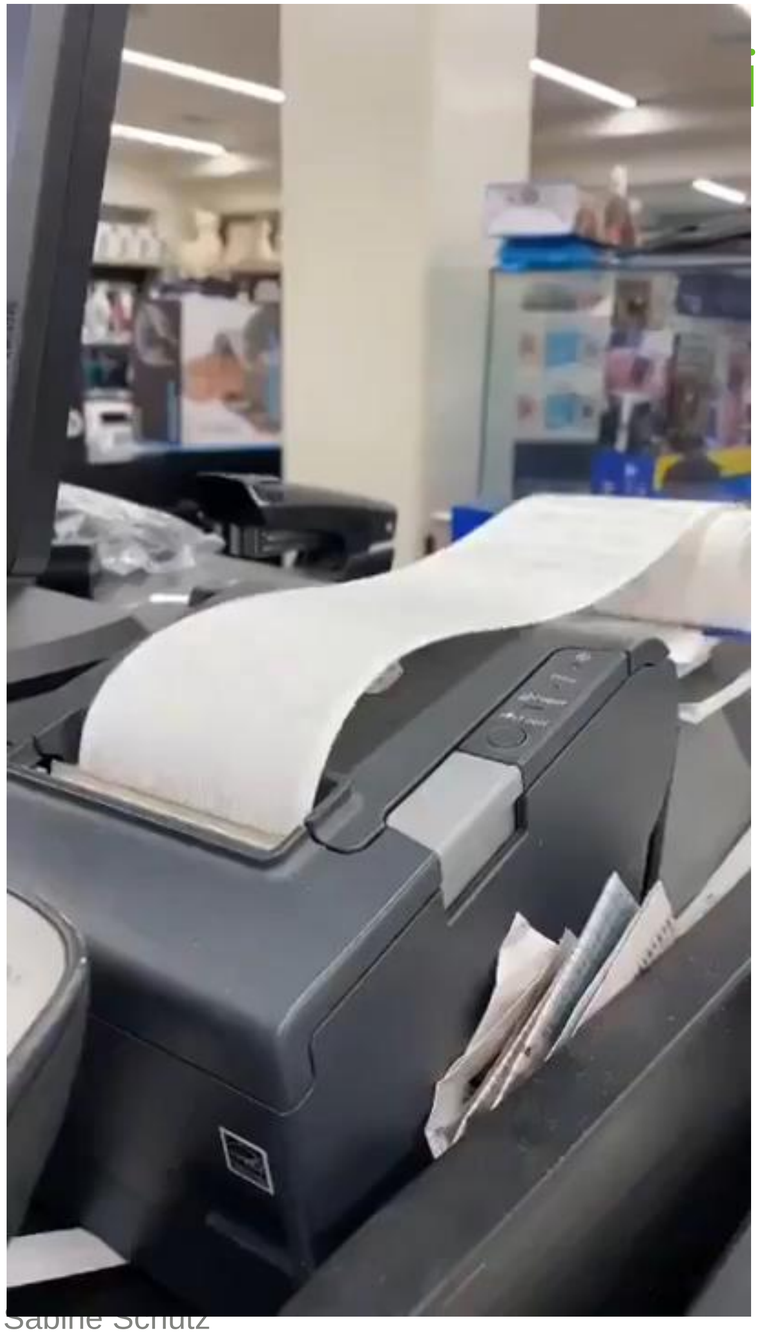
You will receive a universal decryption master key (and instructions) that can be used to unlock all your clients their files. Additionally, we will also send you all details about the zero-day vulnerability to **security@qnap.com**.

Upon receipt of payment for either option, all information will be sent to you in a timely fashion.

There is no way to contact us.
These are our only offers.
Thanks for your consideration.

Greetings,
DEADBOLT team.

Ransomware



Top 4 der Cyberangriffe in Sachsen 2024

CEO-Fraud

Von: Uwe [redacted]
Gesendet: [redacted] 11:36
An: [redacted] Anica - [redacted]-online.de>
Betreff: Dringende Anfrage

Guten Morgen,

Leider war die Mail im Spam gelandet, ich habe sie erst jetzt lesen können, sonst gern

P.S: Ich bin jetzt in einer Besprechung und kann nicht

sprechen, also antworte einfach.

Mit freundlichen Grüßen

Uwe [redacted]
Geschäftsführer

Gesendet von meinem iPhone

Top 4 der Cyberangriffe in Sachsen 2024

CEO-Fraud

[redacted] 17:31

[redacted] Uwe <uwe.[redacted]-online.de>

AW: Dringende Anfrage

Online hat das nicht geklappt, vielleicht liegt es daran das ich keine 300 Euro auf meinem Konto mehr habe. Soll ich es nochmal im Laden probieren?

Anica [redacted]

Uwe [redacted]
Geschäftsführer

Gesendet von meinem iPhone

Top 4 der Cyberangriffe in Sachsen 2024

CEO-Fraud

[redacted] 18:01
[redacted] Uwe <uwe[redacted]online.de>
AW: Dringende Anfrage
An [redacted] Anica

Ja, Sie können sie im Laden bekommen

Mit freundlichen Grüßen

Uwe [redacted]
Geschäftsführer

Gesendet von meinem iPhone

Top 4 der Cyberangriffe in Sachsen 2024

CEO-Fraud

[redacted] 18:16
[redacted] Anica <anica[redacted]
Re: Dringende Anfrage
An Uwe[redacted]
Image.jpeg
2 MB

Anica [redacted]

Top 4 der Cyberangriffe in Sachsen 2024

CEO-Fraud

[redacted] 18:42
[redacted] Uwe <uwe.[redacted]online.de>
Re: Dringende Anfrage
An [redacted], Anica

Könnten Sie mir bitte noch 3 weitere Gutscheine besorgen?

Mit freundlichen Grüßen

Uwe [redacted]
Geschäftsführer

Gesendet von meinem iPhone

Top 4 der Cyberangriffe in Sachsen 2024

CEO-Fraud

- 40.000 Euro in vier Stunden durch „Social-Engineering“

> Von: Mario[redacted]
> Gesendet: Mittwoch, 26. Februar 2025 08:09
> An[redacted] Kathrin <Kathrin[redacted]@[redacted]de>
> Betreff: Re: AW: Zahlung
>
> ZAHLUNGSINFORMATIONEN
>
> IBAN:
> PT50003502170001064943090
>
> BIC/SWIFT
> CGDIPTPLXXX
>
> Name der Bank:
> CAIXA GERAL DE DEPÓSITOS, SA
>
> Name des Empfängers:
> MATEUS FRANCELINO CORREIA
>
> Rechnungsadresse (Firmensitz)
> Beco da Verónica 1, Lisboa, Lisboa 1170-386, Portugal
>
> Referenz: INV11715
>
> 38.158,07 EUR
>
> Wenn Sie Fragen haben, werde ich per E-Mail erreichbar sein, lassen Sie
> es mich wissen, sobald die Zahlung erfolgt ist.
>
> Freundliche Grüße
> Mario[redacted]

An: [redacted]
Betreff: 250226 499260 Prüfung einer Überweisung - EILIG

Sehr geehrte Fra[redacted]

die unten angegebene Zahlung wurde als möglicher Betrug angehalten. Bitte teilen Sie uns schnellstmöglich mit, ob es sich um eine ordnungsmäßige oder betrügerische Überweisung handelt.

Transaction Type: **SCT**	dbDetect Status: **De**
Product Variant Name:	Is Manual Alert: **Dete**
Party Name: [redacted]	Payee Name: **Mateu**
Account Number: **DE29870700000649922200**	Payee Account Key:
Orderer BIC: **DEUTDE8CXXX**	Payee BIC: **CGDIPT**
	Payee Country:
	Payee Party Key:
Account Amount:	
Amount As Entered: **38,158.07 EUR**	Remittance Informati
Normalized Amount: **38,158.07 EUR**	Purpose Code:
Is Standing Order: **0**	Purpose Code Desc

Mit freundlichen Grüßen / Kind regards
[redacted]

POLIZEI Sachsen

- **Abteilung Disposition | Logistik**
- **Abteilung Fakturierung**
- **Abteilung Finanzen**

Sitz: [redacted]

Finanzbuchhaltung	Gruppenruf	[redacted]
Kathrin [redacted]	Leiterin Finanzbuchhaltung	[redacted]
Katrin [redacted]	Sachbearbeiterin	[redacted]
Uwe [redacted]	Sachbearbeiter	[redacted]
Verawaty [redacted]	Sachbearbeiterin	[redacted]

[redacted]

- **Abteilung Geschäftsführung**

[redacted]

Sekretariat	Geschäftsleitung	[redacted]
Mario [redacted]	Geschäftsführer	[redacted]

- **Abteilung Immobilien | Vermietung - Übersicht der Vermietungsobjekte**
- **Abteilung Personalmanagement**

Top 4 der Cyberangriffe in Sachsen 2024

Acc Hacking

- Unternehmen kauft Kleinwagen
- Autohaus stellt Rechnung an Unternehmen (Anhang in E-Mail)
- Ein paar Minuten später kommt die Rechnung erneut, wird nicht geprüft und bezahlt.

POLIZEI Sachsen

Von: Daniel [redacted]
Gesendet: Mittwoch, 12. März 2025 10:19
An: [redacted]t-online.de
Betreff: Re: Kaufvertrag
Anlagen: [redacted]

Guten Morgen,

vielen Dank für die Rücksendung des unterzeichneten Kaufvertrages.
Im Anhang erhalten Sie diesen von uns gegengezeichnet als Auftragsbestätigung zurück.
Ausserdem sende ich Ihnen noch die Fahrzeugrechnung zur Überweisung des Kaufpreises.

Die Kosten für den Marderschutz hatte ich Ihnen schon gesendet - das sind rund 350 Euro Brutto.
Für den Zulassungsdienst fallen 150 Euro Kosten für Zulassungsdienst und 2x Expressversand an, zudem kommen noch die Kosten für die eigentliche Zulassung - diese sind dann gleich, wie als wenn Sie das selbst vornehmen.

Für die Zulassung benötige ich folgende Unterlagen:

EVB von der Versicherung für einen LKW
Kopie Personalausweis GF
Handelsregisterauszug aktuell
Wunschkennzeichen?

POLIZEI Sachsen

[redacted]

Bitte bei Zahlung die Rechnungsnummer als Verwendungszweck angeben!

Nummer: [redacted]
Datum: 12.03.2025
Lieferdatum: 12.03.2025
Kundennummer: [redacted]

Rechnung

Seite 1 von 1

Marke:	VOLKSWAGEN-VW	Zulassung	15.01.2025	§ 29 StVZO:	Januar 2027	Km-Stand:	10
Modell:	VW CRAFTER 35 DOKA 2	FIN:	WV3ZZZSZ6S9037241	Kennzeichen:	S9037241		

Pos	Menge	Einh.	Nummer	Bezeichnung	EP	GP	M
				FAHRZEUGRECHNUNG EU-NEUWAGEN			
1	1,00	Stück	WV3ZZZSZ6S9037241	VW CRAFTER 35 DOKA 2.0 TDI 103KW/140PS	33.596,64	33.596,64	A

Eingeführtes Neufahrzeug aus Polen, es wurde noch keine deutsche Zulassungsbescheinigung Teil II erstellt.

Bei EU-Neufahrzeugen beginnt die Herstellergarantie mit dem Datum der Auslieferung durch den Vertragshändler im Ausland an die Firma OX Automobile GmbH.

Bis zur Tilgung des gesamten Kaufpreises bleibt das Fahrzeug Eigentum des Verkäufers.

Fahrzeuge	33.596,64 €	Schmierstoffe	0,00 €	durchl. Posten	0,00 €	**Summe netto**	**33.596,64 €**
Lohnkosten	0,00 €	Fremdleistung	0,00 €	Lackmaterial	0,00 €	19,00% USt. (A)	6.383,36 €
						Endbetrag	**39.980,00 €**

Der Rechnungsbetrag ist sofort ohne Abzug fällig. Bitte geben Sie als Verwendungszweck zwingend die Rechnungsnummer an, anderenfalls ist keine Zuordnung möglich!

18.56 Uhr.

Falsche Bankverbindung.

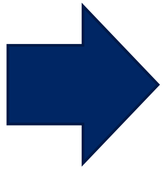
13.3.25

Bankverbindung Deutsche Bank Chemnitz
BLZ: 87070024
Kto.Nr.: 2098499
BIC: DEUTDEDBCHE
IBAN: DE49 8707 0024 0209 8499 00

Achtung! Nach 50 Kilometern die Radschrauben auf festen Sitz überprüfen lassen!

[redacted]

…ein paar Minuten später…



[redacted]

Bitte bei Zahlung die Rechnungsnummer als Verwendungszweck angeben!

Nummer: [redacted]
Datum: 12.03.2025
Lieferdatum: 12.03.2025
Kundennummer: [redacted]

Rechnung

Seite 1 von 1

Marke:	VOLKSWAGEN-VW	Zulassung:	15.01.2025	§ 29 StVZO:	Januar 2027	Km-Stand	10
Modell:	VW CRAFTER 35 DOKA 2	FIN:	WV3ZZZSZ6S9037241	Kennzeichen:	S9037241		

Pos	Menge	Einh.	Nummer	Bezeichnung	EP	GP	M
				FAHRZEUGRECHNUNG EU-NEUWAGEN			
1	1,00	Stück	WV3ZZZSZ6S9037241	VW CRAFTER 35 DOKA 2.0 TDI 103KW/140PS	33.596,64	33.596,64	A

Eingeführtes Neufahrzeug aus Polen, es wurde noch keine deutsche Zulassungsbescheinigung Teil II erstellt.

Bei EU-Neufahrzeugen beginnt die Herstellergarantie mit dem Datum der Auslieferung durch den Vertragshändler im Ausland an die Firma OX Automobile GmbH.

Bis zur Tilgung des gesamten Kaufpreises bleibt das Fahrzeug Eigentum des Verkäufers.

Fahrzeuge	33.596,64 €	Schmierstoffe	0,00 €	durchl. Posten	0,00 €	**Summe netto**	**33.596,64 €**
Lohnkosten	0,00 €	Fremdleistung	0,00 €	Lackmaterial	0,00 €	19,00% USt. (A)	6.383,36 €
						Endbetrag	**39.980,00 €**

Der Rechnungsbetrag ist sofort ohne Abzug fällig. Bitte geben Sie als Verwendungszweck zwingend die Rechnungsnummer an, anderenfalls ist keine Zuordnung möglich!

18.56 Uhr

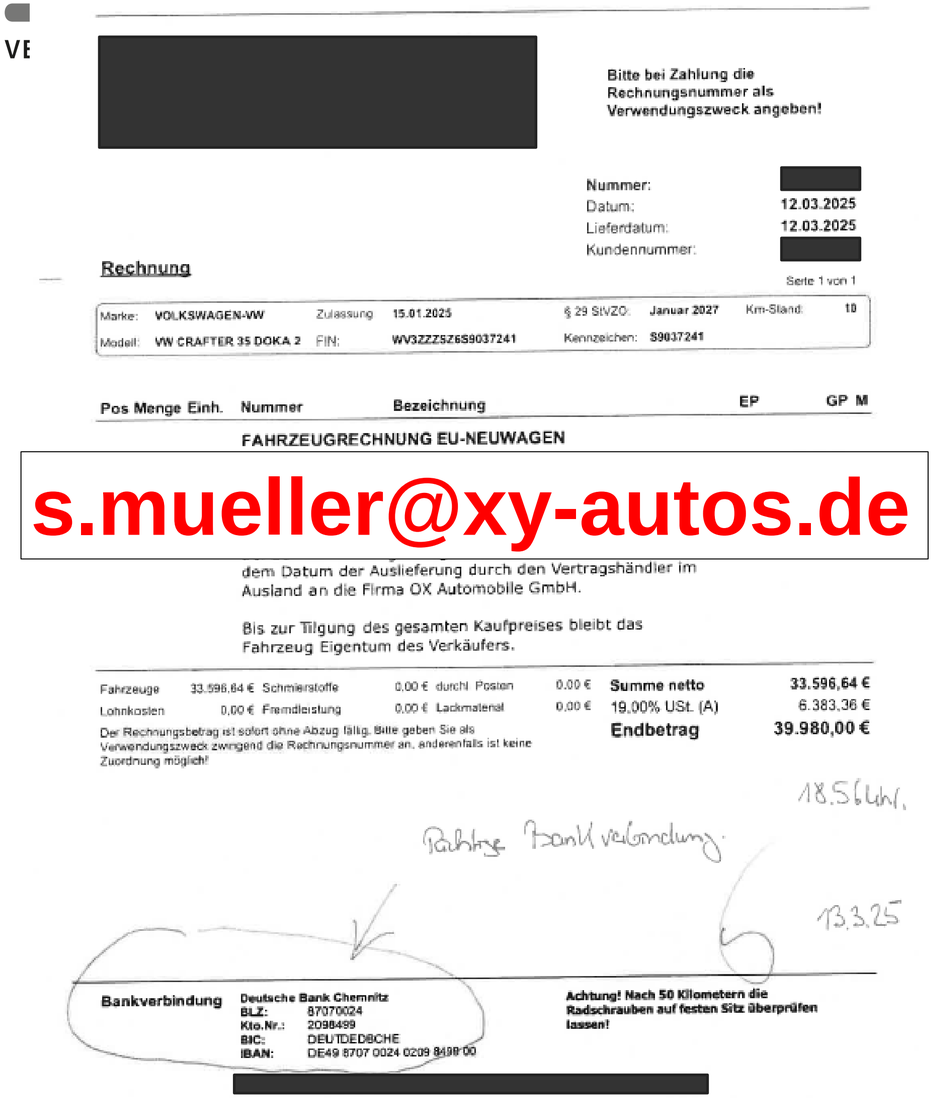
falsche Bankverbindung 13.3.25

Bankverbindung BNP Paribas
BLZ: 76030080
Kto.Nr.: 0280027913
BIC: CSDBDE71
IBAN: DE45 7603 0080 0280 0279 13

Achtung! Nach 50 Kilometern die Radschrauben auf festen Sitz überprüfen lassen!

[redacted]

POLIZEI Sachsen



Bitte bei Zahlung die Rechnungsnummer als Verwendungszweck angeben!

Nummer: [redacted]
Datum: 12.03.2025
Lieferdatum: 12.03.2025
Kundennummer: [redacted]

Rechnung

Seite 1 von 1

Marke: VOLKSWAGEN-VW Zulassung 15.01.2025 § 29 StVZO: Januar 2027 Km-Stand 10
Modell: VW CRAFTER 35 DOKA 2 FIN: WV3ZZZSZ6S9037241 Kennzeichen: S9037241

Pos Menge Einh. Nummer Bezeichnung EP GP M

FAHRZEUGRECHNUNG EU-NEUWAGEN

s.mueller@xy-autos.de

dem Datum der Auslieferung durch den Vertragshändler im Ausland an die Firma OX Automobile GmbH.

Bis zur Tilgung des gesamten Kaufpreises bleibt das Fahrzeug Eigentum des Verkäufers.

Fahrzeuge	33.596,64 €	Schmierstoffe	0,00 €	durchl. Posten	0,00 €	**Summe netto**	**33.596,64 €**
Lohnkosten	0,00 €	Fremdleistung	0,00 €	Lackmaterial	0,00 €	19,00% USt. (A)	6.383,36 €
						Endbetrag	**39.980,00 €**

Der Rechnungsbetrag ist sofort ohne Abzug fällig. Bitte geben Sie als Verwendungszweck zwingend die Rechnungsnummer an, anderenfalls ist keine Zuordnung möglich!

18.56 Uhr

Falsche Bankverbindung

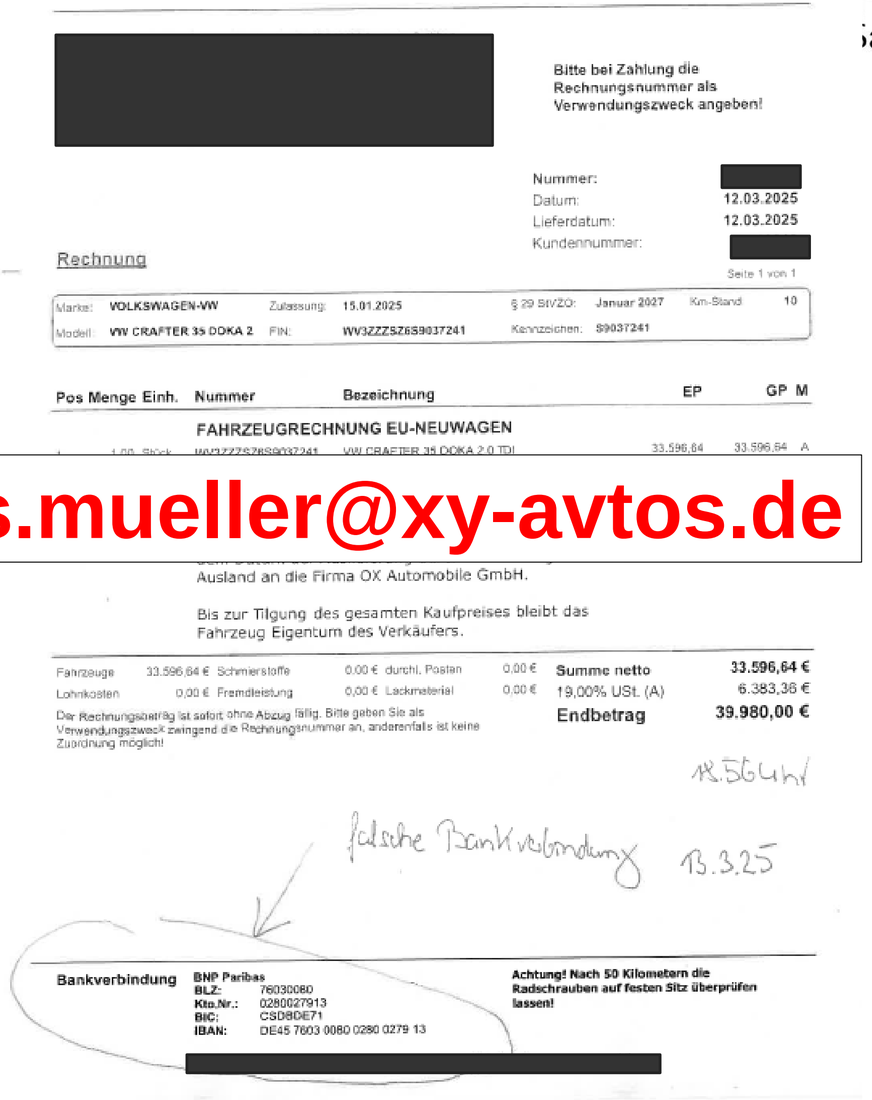
13.3.25

Bankverbindung Deutsche Bank Chemnitz
BLZ: 87070024
Kto.Nr.: 2098499
BIC: DEUTDEDBCHE
IBAN: DE49 8707 0024 0209 8499 00

[redacted]

Achtung! Nach 50 Kilometern die Radschrauben auf festen Sitz überprüfen lassen!

…ein paar Minuten später…



Bitte bei Zahlung die Rechnungsnummer als Verwendungszweck angeben!

Nummer: [redacted]
Datum: 12.03.2025
Lieferdatum: 12.03.2025
Kundennummer: [redacted]

Rechnung

Seite 1 von 1

Marke: VOLKSWAGEN-VW Zulassung: 15.01.2025 § 29 StVZO: Januar 2027 Km-Stand 10
Modell: VW CRAFTER 35 DOKA 2 FIN: WV3ZZZSZ6S9037241 Kennzeichen: S9037241

Pos Menge Einh. Nummer Bezeichnung EP GP M

FAHRZEUGRECHNUNG EU-NEUWAGEN

s.mueller@xy-avtos.de

Ausland an die Firma OX Automobile GmbH.

Bis zur Tilgung des gesamten Kaufpreises bleibt das Fahrzeug Eigentum des Verkäufers.

Fahrzeuge	33.596,64 €	Schmierstoffe	0,00 €	durchl. Posten	0,00 €	**Summe netto**	**33.596,64 €**
Lohnkosten	0,00 €	Fremdleistung	0,00 €	Lackmaterial	0,00 €	19,00% USt. (A)	6.383,36 €
						Endbetrag	**39.980,00 €**

Der Rechnungsbetrag ist sofort ohne Abzug fällig. Bitte geben Sie als Verwendungszweck zwingend die Rechnungsnummer an, anderenfalls ist keine Zuordnung möglich!

18.56 Uhr

falsche Bankverbindung

13.3.25

Bankverbindung BNP Paribas
BLZ: 76030080
Kto.Nr.: 0280027913
BIC: CSDBDE71
IBAN: DE45 7603 0080 0280 0279 13

[redacted]

Achtung! Nach 50 Kilometern die Radschrauben auf festen Sitz überprüfen lassen!

Top 4 der Cyberangriffe in Sachsen 2024

“Rip Deal”

Rip-Deal

- Unternehmenspräsentation auf Messe „Grüne Woche“
- Im Nachgang erhält GF eine Anfrage mit Vermittlung eines Kunden:
  - An 25.000 Getränkeflaschen interessiert (Warenwert ca. 628.000)
  - 30% Provision (ca. 170.000 Euro)
  - Provision soll in der Kryptowährung Tether geleistet werden
  - → Provisionsvertrag

PROFESSIONALITÄT
TOLERANZ
VERANTWORTUNG

Die Zentrale Ansprechstelle Cybercrime (ZAC) Sachsen

POLIZEI Sachsen

Strafverfolgung

Sofortmaßnahmen

- Anzeigenaufnahme telefonisch oder per Mail
- Im Einzelfall persönliches Gespräch vor Ort
- Straftaten auf informationstechnische Systeme

Vertrauensvolle Zusammenarbeit

Ansprechpartner

Informationen zum Thema Cybercrime für:

- Unternehmen
- Verbände
- Behörden

Informationen und Warnungen

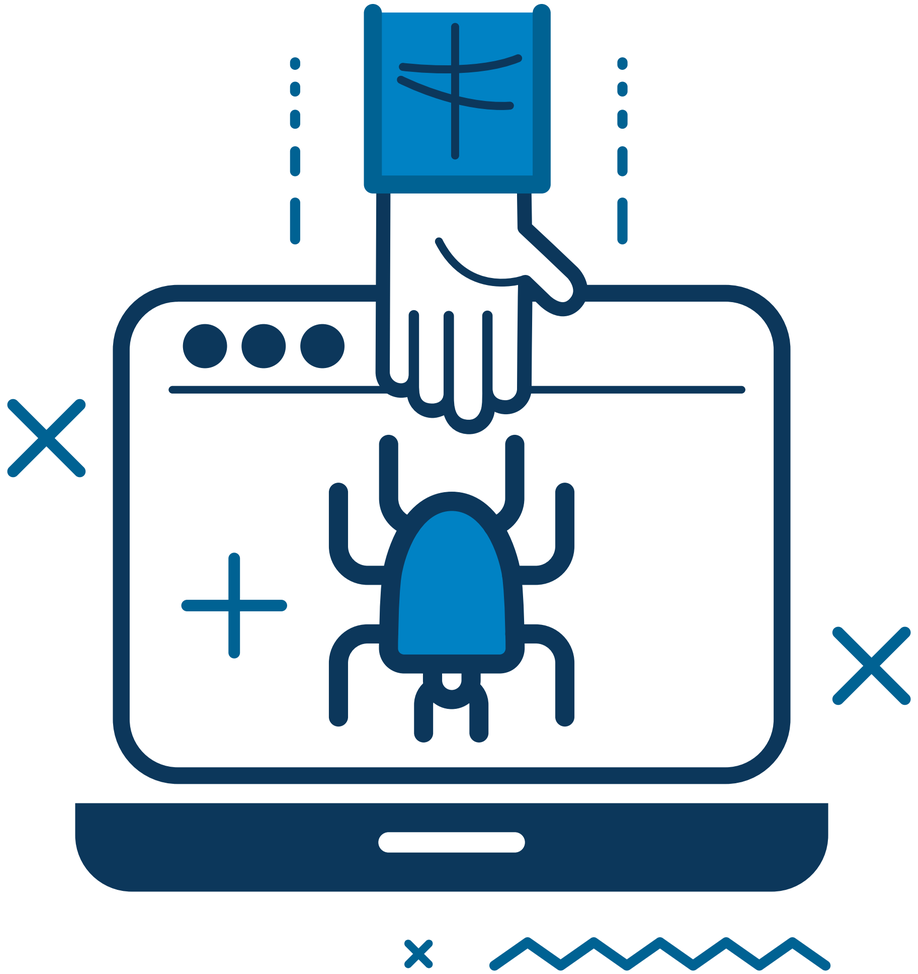
Informiert und warnt

- Aktuelle Phänomene im Bereich Cybercrime
- Awareness für Behörden, Verbände, KMU

Abgrenzung zum IT-Dienstleister

Polizei vs. IT-Dienstleister

- Keine Datensicherung von Sytemen
- Keine Wiederherstellung
- Keine sonstigen IT-Dienstleistungen

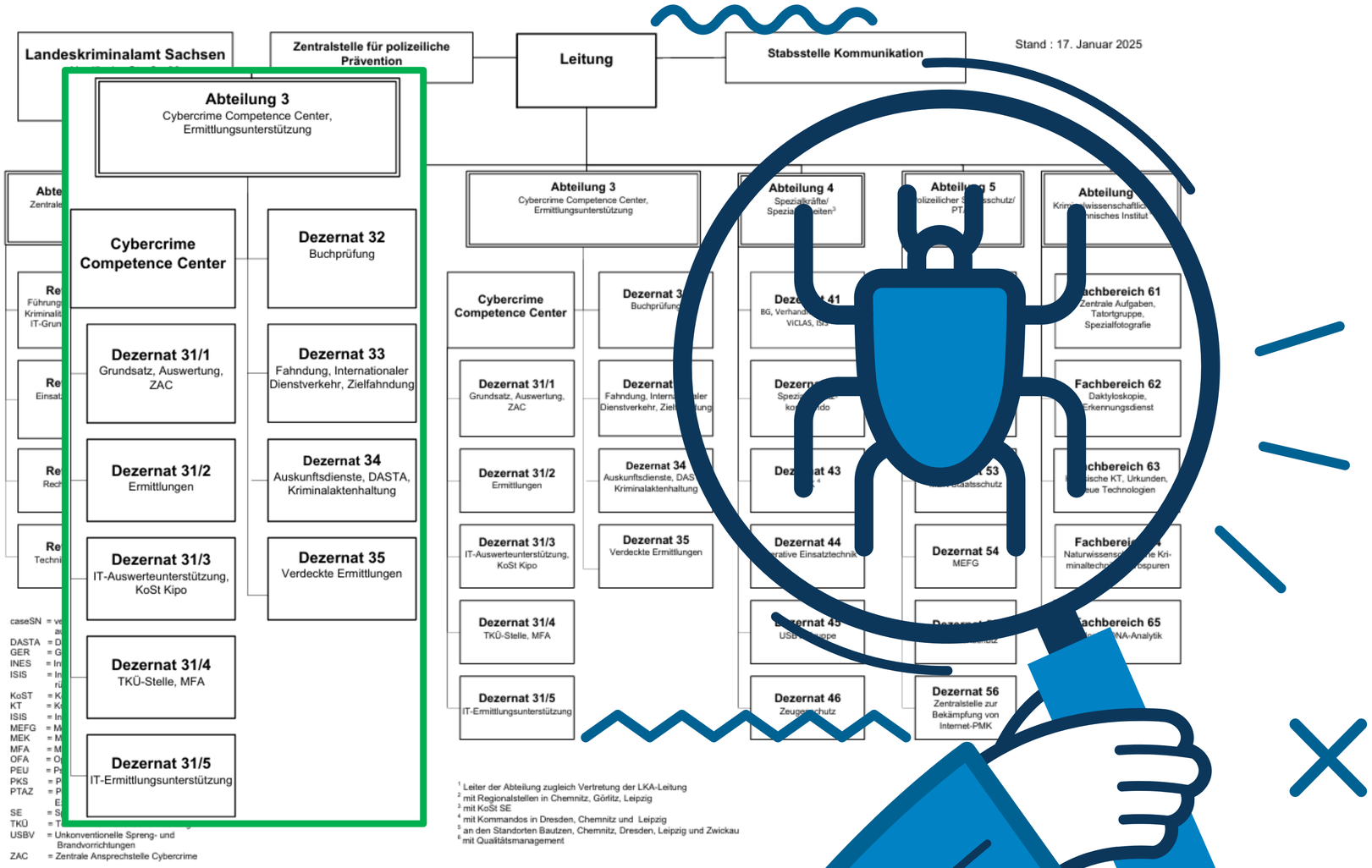


CybercrimeCompetenceCenter (SN4C) Sachsen

Insgesamt 94 Stellen

2/3 spezialisierte Kriminalbeamte

1/3 IT-Ausbildung



PROFESSIONALITÄT
TOLERANZ
VERANTWORTUNG

Incident Response – Unterstützung finden!

POLIZEI Sachsen

Awareness

Seien sie sich den Gefahren durch CC bewusst!

Setzen sie sich mit aktuellen Sicherheitsvorfällen auseinander. Denken Sie an ein gutes Backup.

Vorbereitung

Erstellen Sie Maßnahmenpläneim Falle des Falles

Klären sie grundsätziche Fragestellungen, denken sie an Informationsketten, Pressearbeit, Räumlichkeiten

Cybersicherheitsnetzwerk Sachsen

Untersützung finden bei der Digitalagentur SN

Holen Sie sich Infopläne, Checklisten und Informationen zu Ansprechpartnern.

BSI direkt

Unterstützung finden beim BSI direkt

Auch hier gibt es Hilfe zu Checklisten, Infopläne aber auch zu aktuellen Sicherheitslücken in Software.

CHECKLISTE

Sofortmaßnahmen eingeleitet ? ☐

Geschäftsführung informiert ? ☐

IT-Notfallplan beachtet ? ☐

NOTFALLKONTAKTE

Ansprechpartner IT-Sicherheit:

Geschäftsführung:

IT-Dienstleister:

BSI-Hotline:

0800-2741000

Weiterer Notfallkontakt:

www.cyber-sicherheitsnetzwerk.sachsen.de

Eine Initiative der sächsischen Handwerkskammern, sächsischen Industrie- und Handelskammern, des Landeskriminalamts Sachsen und der Digitalagentur Sachsen

IT-NOTFALLKARTE

POLIZEI Sachsen

Technisch — **Sofortmaßnahmen**

- Keine Anmeldung als Admin, wenn Netzwerk noch aktiv
- Vom Netzwerk trennen; Gerät anlassen
- Arbeiten mit dem IT-System einstellen; Weitere Maßnahmen nur nach Anweisung einleiten!

Tutorial

cyber-sicherheitsnetzwerk.sachsen.de

Organisatorisch

- Verantwortliche im Betrieb informieren
- Helfer informieren (z. B. IT-Dienstleister, ggf. Cyber-Versicherung)
- Meldepflichten beachten (Datenschutz)

Grundsätzlich wird empfohlen:
Bei Erpressungsversuch ⇨ NICHT auf Lösegeldzahlungen einlassen
Für alle Cyber-Angriffe ⇨ Strafanzeige erstatten, hat in der Regel polizeiliche Maßnahmen zur Folge

Geschäftsbetrieb wiederaufnehmen

1. Verantwortliche bestimmen — Wer? Was? Wann?

2. Check Arbeitsfähigkeit

Jede Anwendung/ Jedes IT-System überprüfen →

System 1
- ☐ Nicht betroffen
- ☐ Auslagerungsfähig auf anderes System
- ☐ Nicht arbeitsfähig, Neuaufbau nötig
- ☐ Eingeschränkt arbeitsfähig (z. B. Laptop, Handy)

System 2
- ☐ ...

3. Wiederherstellung des Datenbestands

Vorhandene saubere Backups, bzw. nicht-betroffene Daten

www.cyber-sicherheitsnetzwerk.sachsen.de

Eine Initiative der sächsischen Handwerkskammern, sächsischen Industrie- und Handelskammern, des Landeskriminalamts Sachsen und der Digitalagentur Sachsen

TLP-AMBER

PROFESSION
VERANTWOF

Einstieg ins IT-Notfallmanagement für kleinere und mittelständische Unternehmen (KMU)

POLIZEI Sachsen

1. Vorbereitung

Die nachfolgenden Aufgaben sollten Sie bearbeiten, um im Fall der Fälle geeignet auf einen IT-Notfall vorbereitet zu sein:

- Bestimmen Sie Beauftragte für die Belange der IT-Sicherheit und des Notfallmanagements.
- Stellen Sie sicher, dass Ihnen Ihre individuellen Erstmaßnahmen bei IT-Vorfällen vorliegen (u. a. Alarmierungs- und Meldewege im Unternehmen).
- Identifizieren Sie zeitkritische Geschäftsprozesse und Assets (Kronjuwelen) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, bei welcher Art von IT-Vorfällen diese unterstützen können.
- Identifizieren und kontaktieren Sie ggf. weitere IT-Dienstleister, die Sie bei der Bewältigung unterstützen können.
- Fertigen Sie eine Liste mit Ansprechpartnern und deren Erreichbarkeiten und Verfügbarkeiten.
- Legen Sie Regeln zur Kommunikation nach innen und außen fest, Stichwort: Presse- und Öffentlichkeitsarbeit.
- Implementieren Sie aktive Überwachungsmaßnahmen (Monitoring) für Ihre IT-Landschaft. Beachten Sie den Datenschutz.
- Üben Sie IT-Notfallszenarien.
- Lassen Sie Ihre IT-Infrastruktur auf Angreifbarkeit prüfen (Penetrationstests).
- Schulen und sensibilisieren Sie Ihr gesamtes Personals.
- Denken Sie an grundlegende Schutzmaßnahmen:
  - Installieren Sie regelmäßig und unverzüglich Patches und Sicherheitsupdates.
  - Setzen Sie Programme zum Schutz vor Schadsoftware ein und aktualisieren Sie diese regelmäßig.
  - Nutzen Sie Firewalls, um Ihre Netze und Rechner vor Angriffen von außen zu schützen.
  - Ändern Sie in jedem Fall Standard-Passwörter und nutzen Sie sichere Passwörter und, wenn möglich, Zwei-Faktor-Authentisierung.
  - Erstellen Sie regelmäßig Sicherheitskopien (Backups) Ihrer Daten, und testen Sie regelmäßig deren Wiederherstellung.
- Inventarisieren Sie Ihre IT-Infrastruktur (u.a. Netzplan).
- Vergeben Sie restriktive Benutzerrechte an Ihren Systemen.
- Vernetzen Sie Ihre Systeme restriktiv (Netzsegmentierung).
- Bereiten Sie Meldewege für externe Meldepflichten vor (Datenschutz, KRITIS etc.).

2. Bereitschaft

Um jederzeit einem IT-Notfall entgegnen zu können beachten Sie die nachfolgenden Punkte:

- Überprüfen Sie regelmäßig den Sicherheitsstatus Ihrer Systeme.
- Gewährleisten Sie, dass Ihr Personal den richtigen Ansprechpartner für IT-Notfälle kennt (Einsatz der IT-Notfallkarte). Bestimmen Sie einen angemessenen Erstkontakt für IT-Notfälle und gewährleisten Sie die Erreichbarkeit.

3. Bewältigung

Zur Bewältigung eines IT-Notfalls helfen Ihnen die folgenden Punkte:

- Kontaktieren Sie alle Ansprechpartner in der Organisation, die Sie zur Bewältigung brauchen.
- Befragen Sie betroffene Nutzer über Beobachtungen und Aktivitäten.
- Kontaktieren Sie IT-Dienstleister, die Ihnen bei der Bewältigung helfen können.
- Sammeln und sichern Sie Systemprotokolle, Logdateien, etc.
- Dokumentieren Sie Sachverhalte, die mit dem Notfall in Zusammenhang stehen könnten.
- Prüfen Sie Kontaktaufnahmen mit den ZACs der Polizeien, sowie freiwillige Meldungen an die ACS.
- Vermuten Sie als Urheber einen fremden Nachrichtendienst, wenden Sie sich an die Verfassungsschutzbehörden.
- Beachten Sie Meldepflichten.

4. Nachbereitung

Ein aufgetretener IT-Notfall muss auch nachbereitet werden. Hinweise geben die folgenden Punkte:

- Schließen Sie durch den IT-Notfall aufgedeckte Schwachstellen und Sicherheitslücken.
- Überwachen und Monitoren Sie Ihr Netzwerk und Ihre IT-Systeme im Nachgang besonders gründlich.
- Lessons Learned: Überprüfen Sie bestehende Regelungen, Prozesse und Maßnahmen, optimieren Sie diese gegebenenfalls.
- Halten Sie Ihre Dokumentationen zum Notfallmanagement auf dem aktuellen Stand.
- Entwickeln Sie Ihre IT-Sicherheitsarchitektur weiter.

Hinweis: Bei diesem Dokument handelt es sich um eine Kurzfassung des „Maßnahmenkatalog zum Notfallmanagement – Fokus IT-Notfälle“ welcher weitere Erläuterungen und Verweise enthält.

Stand: Mai 2021

Disclaimer: Produkt einer Arbeitsgruppe deutscher Cyber-Sicherheitsorganisationen

PROFESSIONALITÄT
TOLERANZ
VERANTWORTUNG

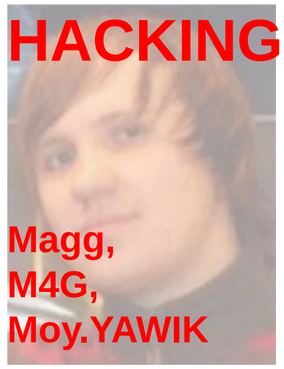
Wir geben Cybertätern ein Gesicht!

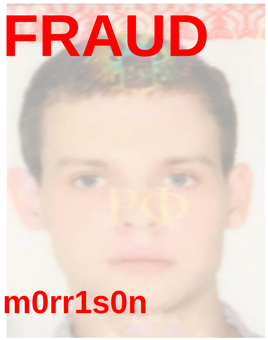
POLIZEI Sachsen

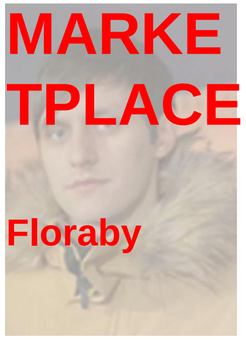
PROFESSIONALITÄT
TOLERANZ
VERANTWORTUNG

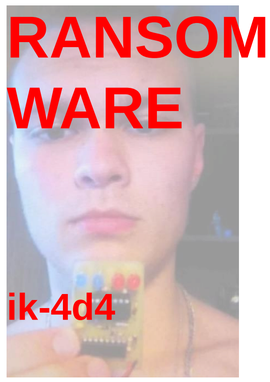
Wir geben Cybertätern ein Gesicht!

POLIZEI Sachsen

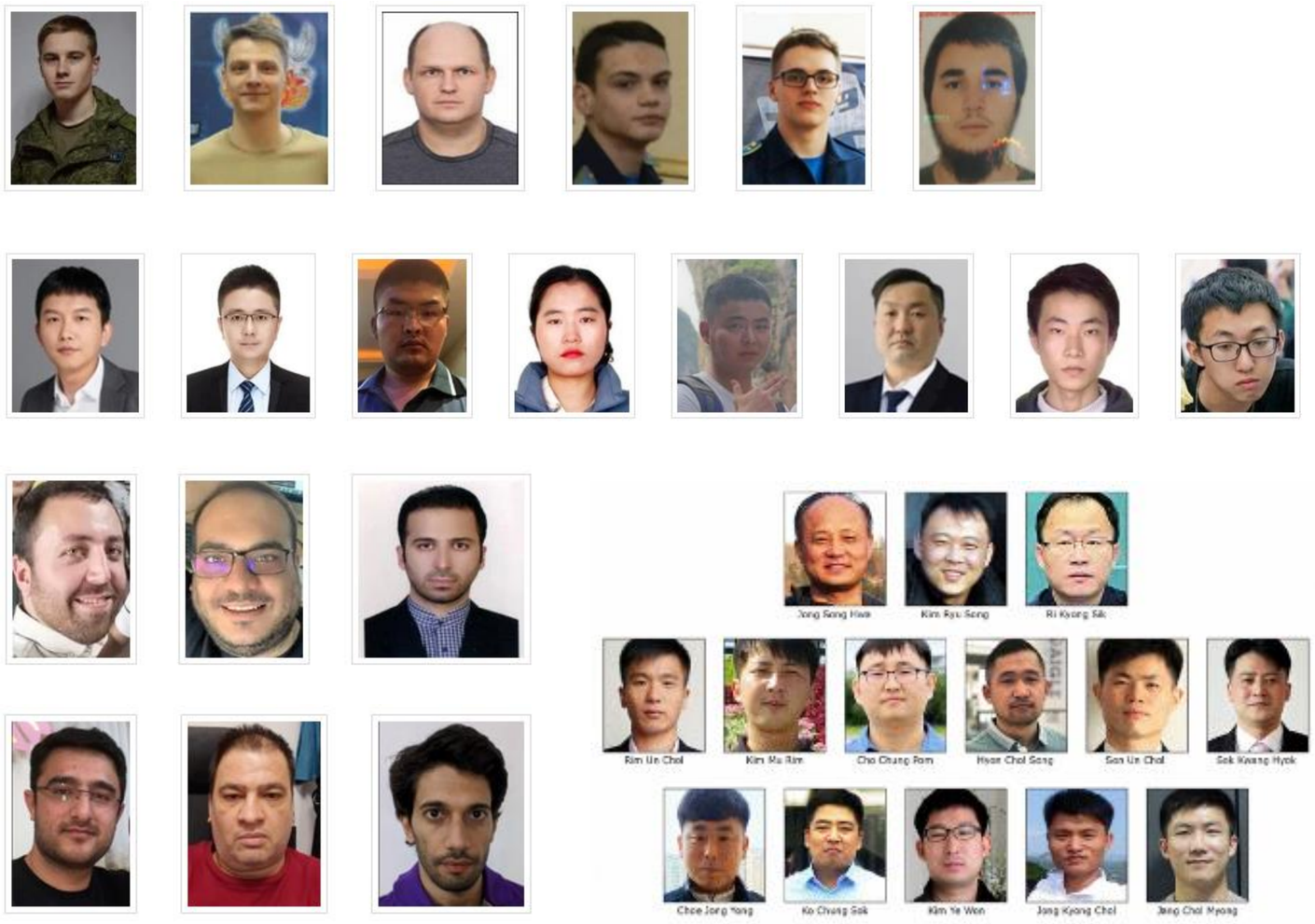








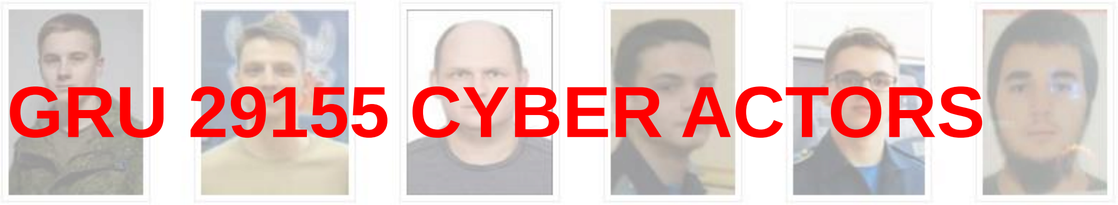
Wir geben Cybertätern ein Gesicht!



PROFESSIONALITÄT
TOLERANZ
VERANTWORTUNG

Wir geben Cybertätern ein Gesicht!

POLIZEI Sachsen



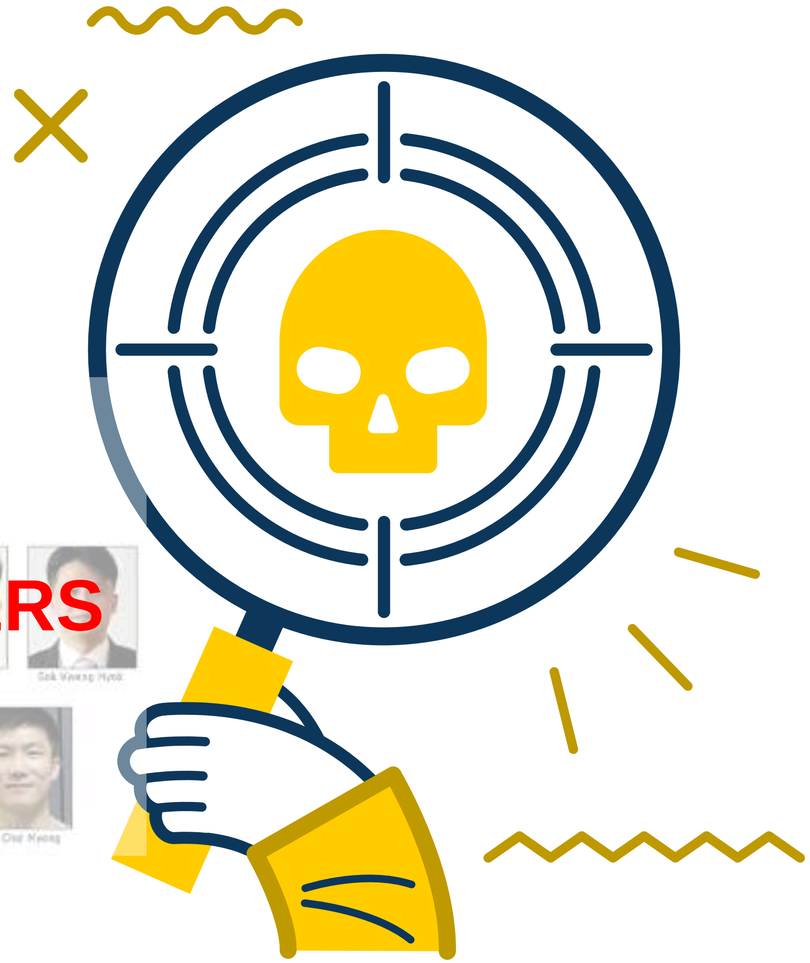
GRU 29155 CYBER ACTORS

AQUATIC PANDA CYBER ACTORS

THREE IRANIAN CYBER ACTORS

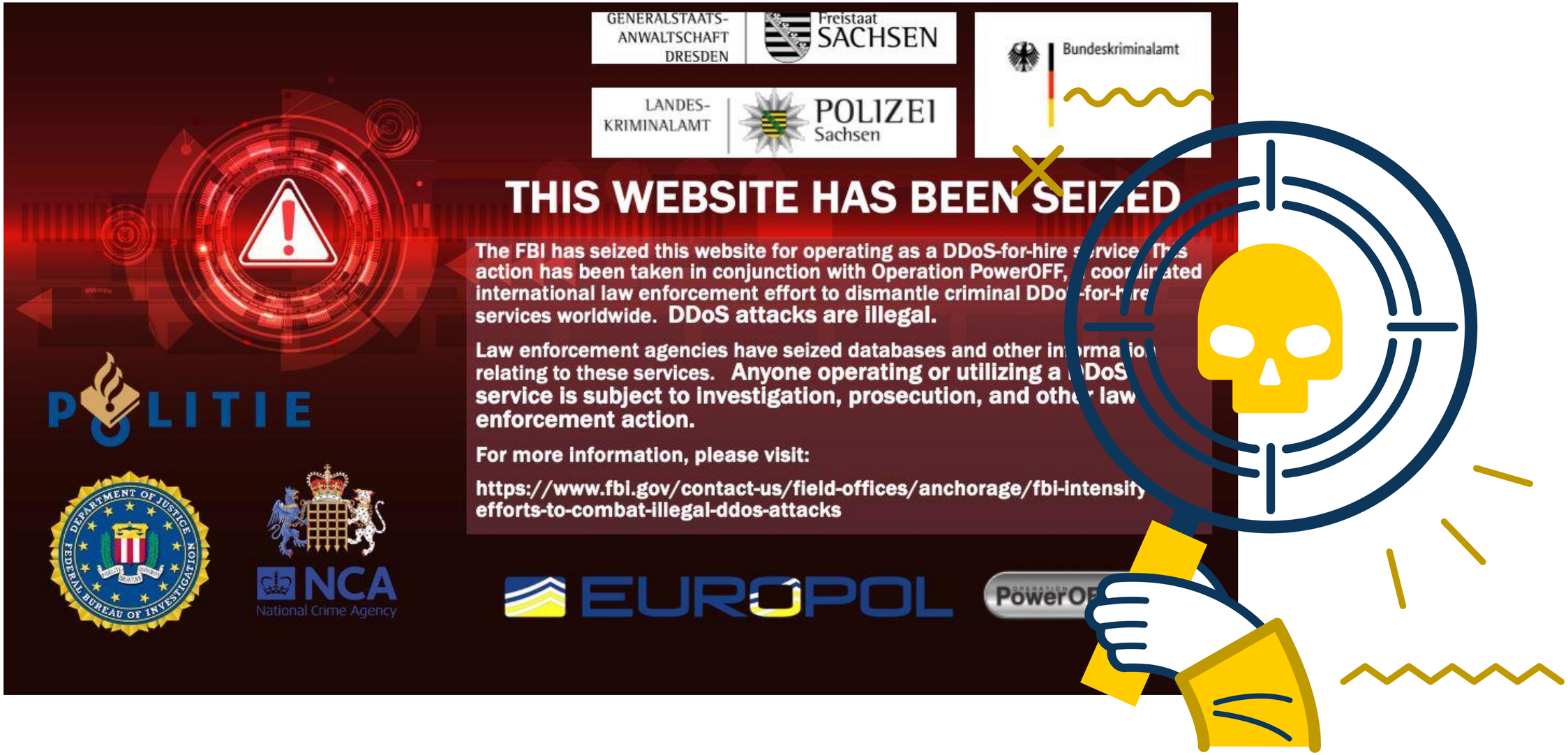
DPRK IT WORKERS

IRGC-AFFILIATED CYBER ACTOR



Wir geben Cybertätern ein Gesicht!

Wir geben Cybertätern ein Gesicht!



PROFESSIONALITÄT
TOLERANZ
VERANTWORTUNG

POLIZEI
Sachsen

Für Rückfragen, Ideen und Anregungen:

zac.lka@polizei.sachsen.de