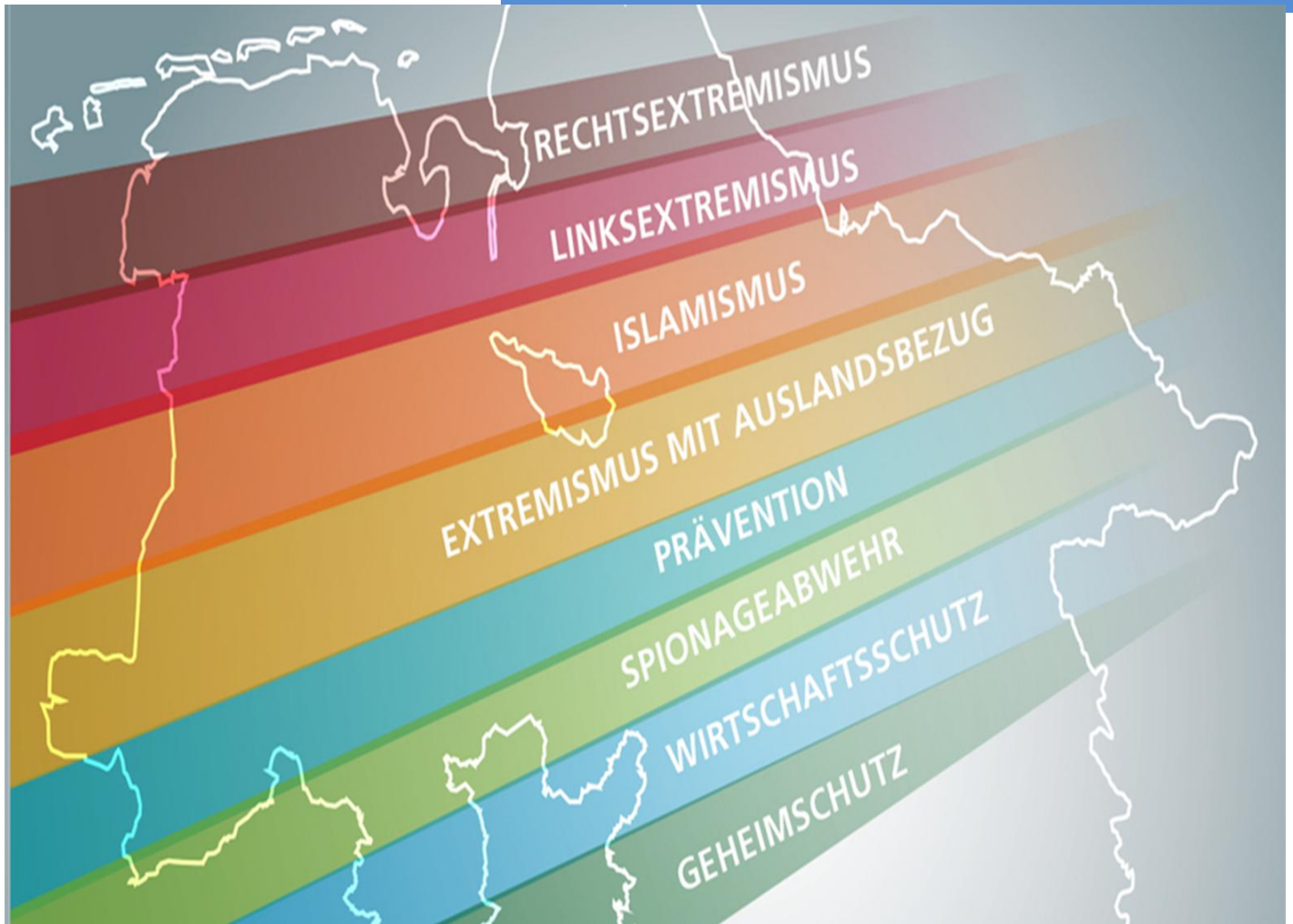
Niedersächsisches Ministerium
für Inneres, Sport und Digitalisierung
Verfassungsschutz

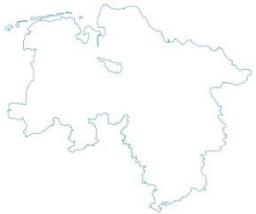
Hybride Bedrohungslagen aus Sicht des Verfassungsschutzes

Sonja Flemming | Verfassungsschutz Niedersachsen



Verfassungsschutz | Wirtschaftsschutz





Niedersächsisches Ministerium
für Inneres, Sport und Digitalisierung
Verfassungsschutz

Hybride Bedrohungen

VERUNSICHERUNG DER DEMOKRATISCHEN BEVÖLKERUNG

- Spionage
- Sabotage
- Cyberangriffe
- Einflussnahme auf freie Wahlen
- Desinformation



Spionage –
wen oder was es immer schon gab



Methoden der Spionage
Gestern und heute





39,00 €

Methoden der Spionage
Gestern und heute





Ab 3,42 €

Methoden der Spionage
Gestern und heute





Ab 0,20 €

Mitarbeitersensibilisierung

Man sagt,

„Cybersicherheit

muss Chefsache sein!“



Cyberangriffe aus nachrichtendienstlicher Sicht



Advanced persistent threat

Fortgeschrittene, andauernde Bedrohung

Ursprünglich:
Beschreibung für digitale Wirtschaftsspionage –
mittlerweile etwas „verwässert“.

Wer hat was wann wo getan?
APT-Angriffe aus nachrichtendienstlicher Sicht

- Cyberangreifergruppe
- Oft staatlich gesteuert
- ausgewählte Ziele - zielgerichtetes Vorgehen
- Angreifer handeln im Auftrag
- **Starke Einbeziehung sozialer Manipulation (SE)**
- Getarnte, ausgeklügelte Angriffsmethoden (KI)
- Großer Aufwand, komplexe Mehrstufigkeit
- Nutzung von bislang unbekannten Schwachstellen
- Angriff über längeren Zeitraum (oft Jahre)
- Ziel: über diesen Zeitraum Daten ausspähen oder anderweitig Schaden anrichten
- Zielobjekte: oft Politik, Regierung, Militär

WEIL ERFOGREICH!



[ˈsəʊʃl ˌɛndʒɪˈnɪərɪŋ]

Jede Handlung,
die eine Person dazu bringt,
eine Handlung zu ergreifen,
die in ihrem besten Interesse
sein kann - oder nicht.

Bestes Interesse – meins oder Deins?

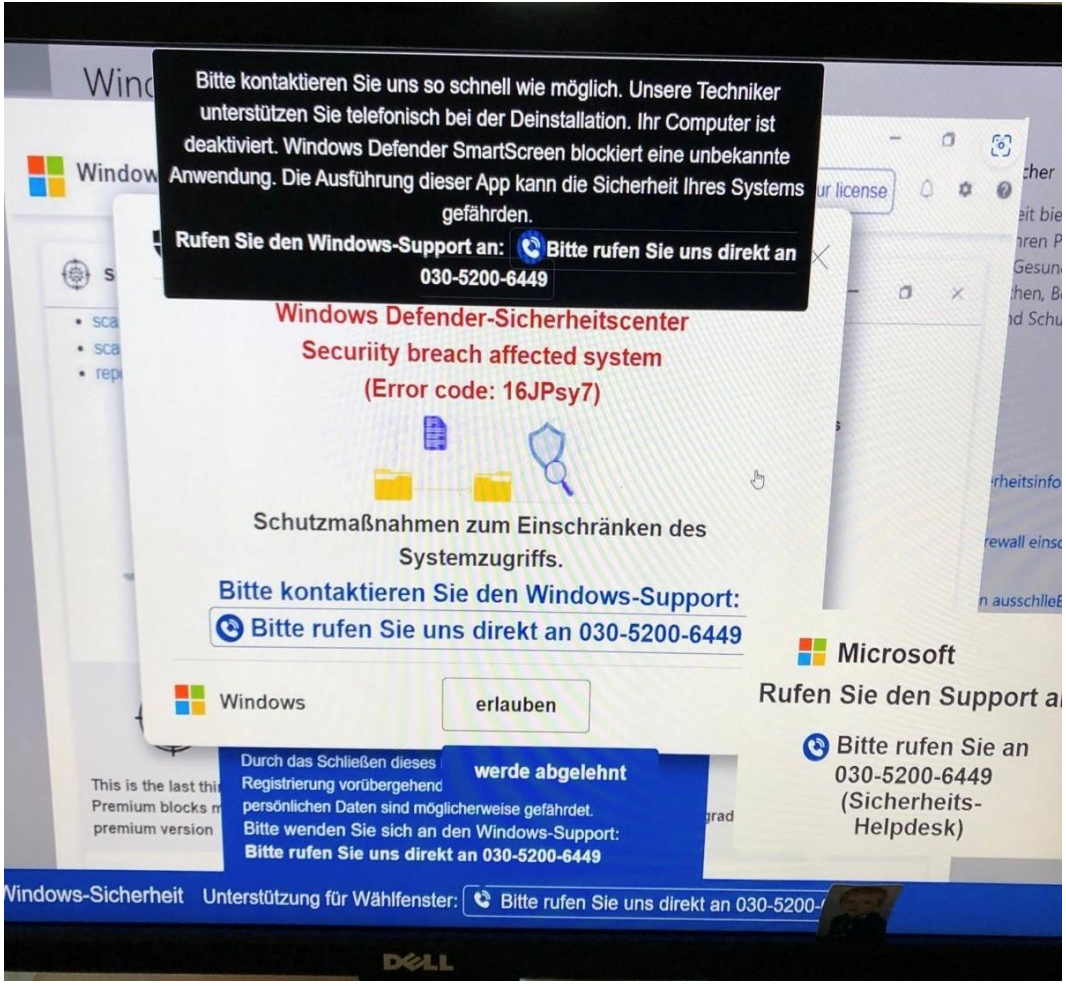








Windows-Fail



Individualisierte Mails

Betreff: Betreff: Bettwanzenbefall – Fristsetzung zur Schadensregulierung
Datum: 15. Juli 2026 um 11:11:33 MESZ
An: "hello@hiamo.com" <hello@hiamo.com>

Betreff: Wanzenalarm – Sofortige Maßnahmen gefordert

Liebes Team des Hotels,

Leider muss ich Ihnen eröffnen, dass ich Opfer eines Bettwanzenbefalls in Ihrem Hotel geworden bin.

Ich habe die Wanzen fotografiert und auch die Spuren ihres Befalls dokumentiert – die Beweise sind eindeutig.

Ich habe die Rezeption auf den Befall hingewiesen, aber man tat es als 'Einzelfall' ab. Eine gründliche Desinfektion wurde nicht veranlasst.

Ich verlange eine umfassende Kompensation, einschließlich der Kosten für meine medizinische Behandlung und die Reinigung meiner Kleidung.

Ich habe bereits einen Rechtsanwalt kontaktiert und werde die Angelegenheit notfalls gerichtlich klären.

Teilen Sie mir umgehend Ihre Entscheidung mit, damit ich über weitere Maßnahmen entscheiden kann.

Für weitere Korrespondenz stehe ich jederzeit zur Verfügung.

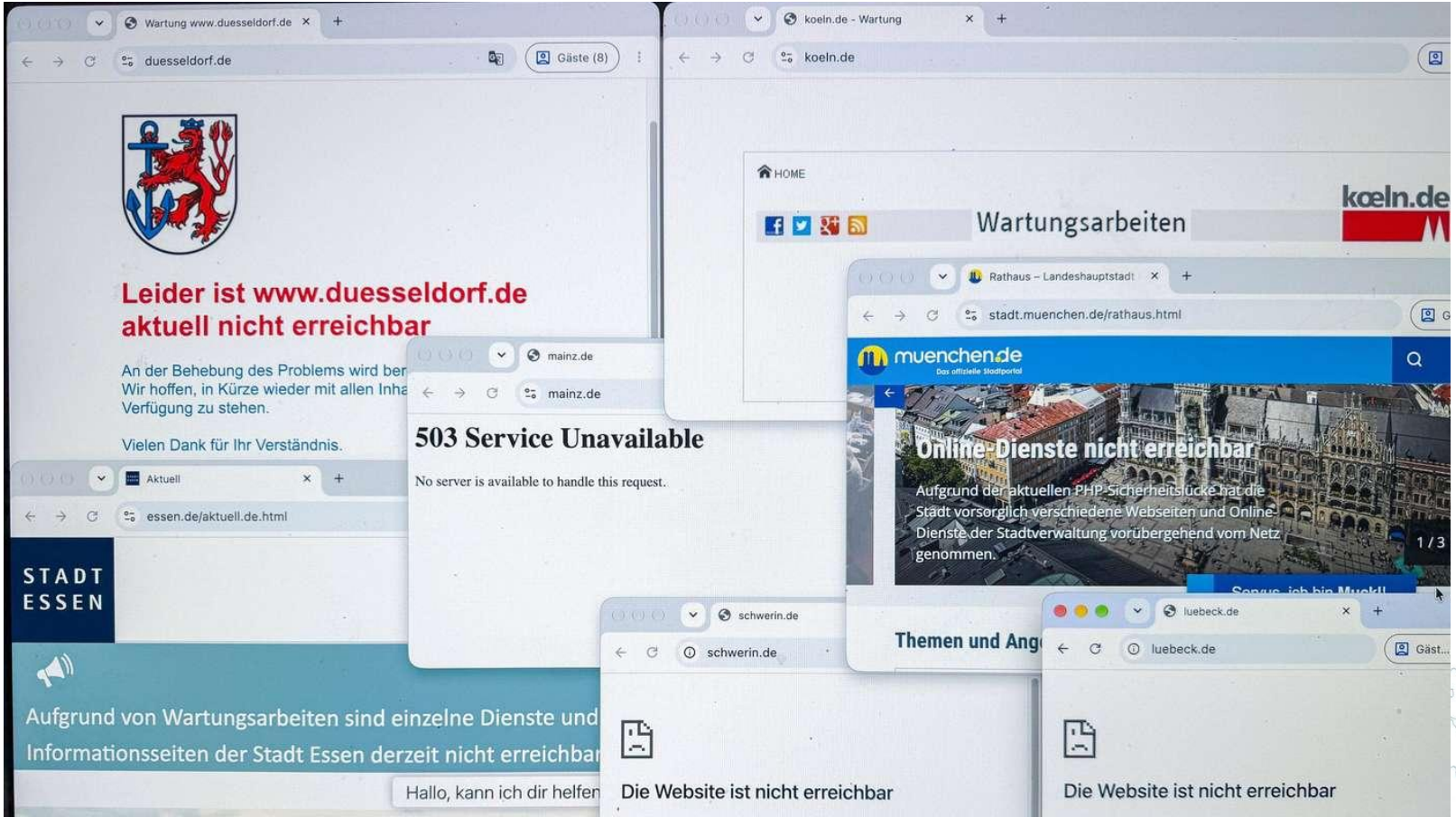


Mit freundlichen Grüßen,

Zimmer-Nr. 721 (Aufenthalt vom 1. bis 3. Juli 2026)
München, den 3. Juli 2026

„Auch wir haben solche Mails in den vergangenen Tagen bekommen, teilweise auch noch mit Kopfzeile von booking.com. Bei uns war noch ein Foto vom angeblichen Befall enthalten. Wir das angeklickt, ist es passiert. Also auch von unserer Seite kann nur äußerste Vorsicht und Sensibilisierung angeraten werden.“

KI findet PHP-Lücken
22.10.2026



Was ist passiert?

„Angreifer können diese (Sicherheitsupdates) mittels KI-gestützter Werkzeuge innerhalb kurzer Zeit analysieren und entsprechende Exploits generieren."

Thomas Caspers, BSI-Vizepräsident

„Wenn die Lösung präsentiert wird, wissen Kriminelle, wo die Schwachstellen des Systems stecken und wo sie – beschleunigt durch KI – zuschlagen müssen."

Behörden helfen verstärkt mit

Liste qualifizierter DDoS-Mitigation-Dienstleister

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.html

Liste zertifizierter IT-Sicherheitsdienstleisters

- https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/IS-Rev/Liste-IT-Sicherheitsdienstleister/liste-is-revi-is-pentester_node.html

Qualifizierte APT-Response Dienstleister

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf?__blob=publicationFile&v=42

Sichere Nutzung von Cloud-Diensten

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=1

Ansprechpartner in den Behörden

Ansprechpartner beim Verfassungsschutz:

- Hinweise zu evtl. Verdachtsfällen i. Z. m. Spionage/Sabotage
  - Spionageabwehr@mi.niedersachsen.de gesendet werden,
- bei Problemen i. Z. m. Cyberangriffen (ausl. Akteure)
  - Cyberabwehr@mi.niedersachsen.de

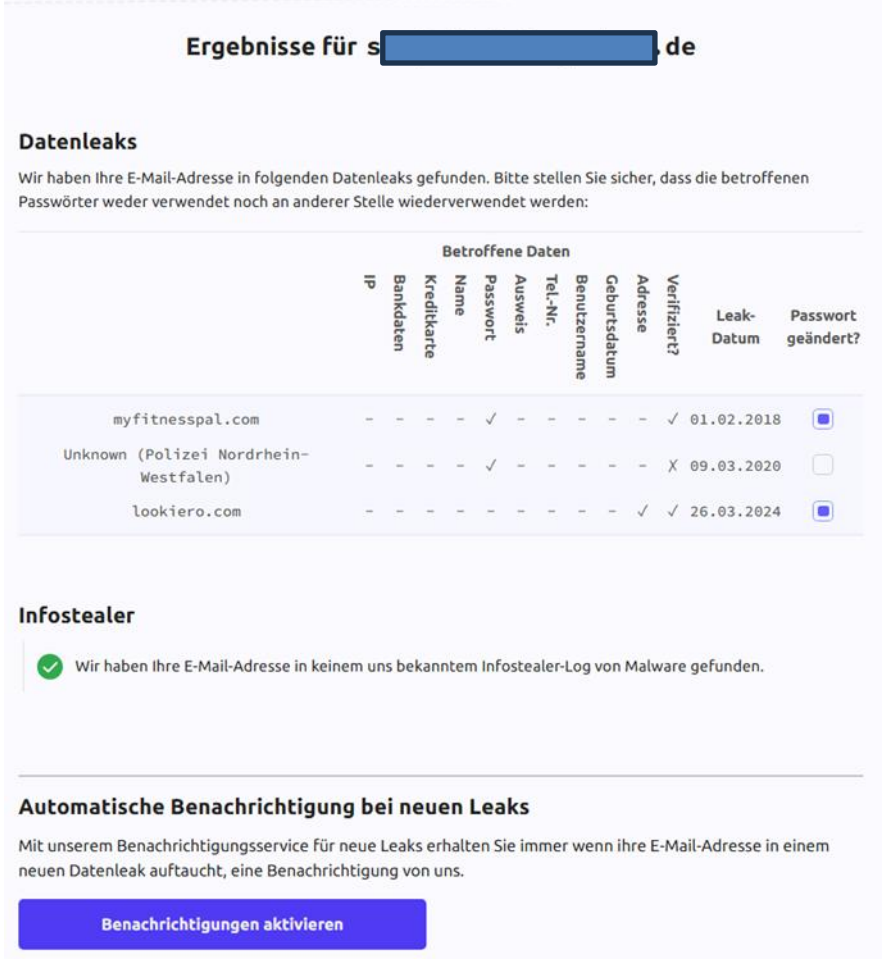
Ansprechpartner bei der Polizei:

- LKA Niedersachsen, Zentrale Ansprechstelle Cybercrime (ZAC) für die Wirtschaft in Niedersachsen:
  - in akuten Cyber-Angriffssituationen
    - Hotline: +49 511 9873-6230
    - zac@lka.polizei.niedersachsen.de
  - verdächtige Mails: trojaner@polizeilabor.de
  - https://www.zac-niedersachsen.de/index.php
- persönlicher Ansprechpartner vor Ort PLUS der örtliche Staatsschutz



https://www.verbraucherzentrale.nrw/wissen/digitale-welt/onlinedienste/so-finden-sie-heraus-ob-ihre-logindaten-gestohlen-wurden-92617

	HPI Identity Leak Checker	Identity Leak Checker	Have I been pwned?
Betreiber	Hasso-Plattner-Institut (HPI) der Universität Potsdam	EIDI der Universität Bonn	Troy Hunt, Internet-Sicherheitsexperte und Blogger
Sprache der Seite	deutsch	deutsch	englisch
So funktioniert es	E-Mail-Adresse ins Suchfeld eingeben. Danach erhalten Sie eine E-Mail, in der Sie lesen können, ob Login-Daten mit Ihrer Mail-Adresse im Internet veröffentlicht wurden.	E-Mail-Adresse ins Suchfeld eingeben. Danach erhalten Sie eine E-Mail, in der Sie lesen können, ob Login-Daten mit Ihrer Mail-Adresse im Internet veröffentlicht wurden.	E-Mail-Adresse oder Nutzernamen ins Suchfeld eingeben. Danach zeigt die Seite an, ob Login-Daten mit Ihren Angaben im Internet veröffentlicht wurden.
Info, von welchen Accounts die Daten stammen?	Teilweise	Ja	Ja
Datensätze (lt. Angabe der Betreiber)	etwa 14,5 Milliarden, Aktualisierungen bei Bedarf	keine Angabe	etwa 17,3 Milliarden, Aktualisierungen bei Bedarf
Adresse	sec.hpi.uni-potsdam.de/leak-checker/search	https://leakchecker.uni-bonn.de/	haveibeenpwned.com



Ergebnisse für s[redacted]de

Datenleaks

Wir haben Ihre E-Mail-Adresse in folgenden Datenleaks gefunden. Bitte stellen Sie sicher, dass die betroffenen Passwörter weder verwendet noch an anderer Stelle wiederverwendet werden:

	Betroffene Daten												
	IP	Bankdaten	Kreditkarte	Name	Passwort	Ausweis	Tel.-Nr.	Benutzername	Geburtsdatum	Adresse	Verifiziert?	Leak-Datum	Passwort geändert?
myfitnesspal.com	-	-	-	-	✓	-	-	-	-	-	✓	01.02.2018	■
Unknown (Polizei Nordrhein-Westfalen)	-	-	-	-	✓	-	-	-	-	-	X	09.03.2020	
lookiero.com	-	-	-	-	-	-	-	-	-	✓	✓	26.03.2024	■

Infostealer

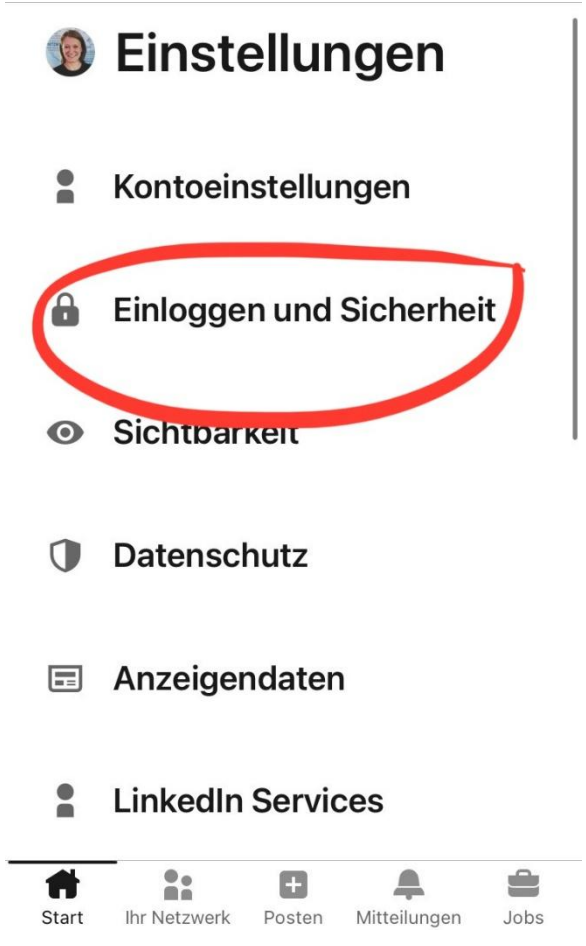
Wir haben Ihre E-Mail-Adresse in keinem uns bekanntem Infostealer-Log von Malware gefunden.

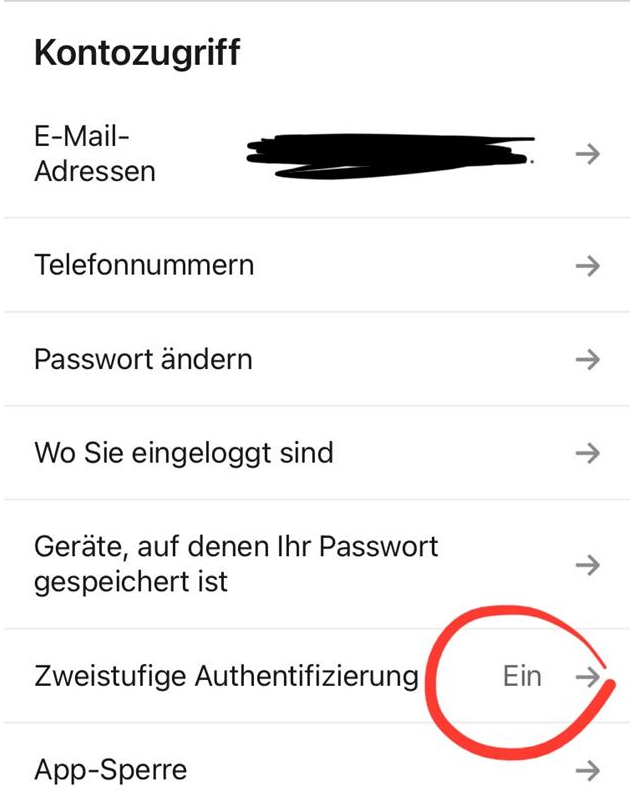
Automatische Benachrichtigung bei neuen Leaks

Mit unserem Benachrichtigungsservice für neue Leaks erhalten Sie immer wenn ihre E-Mail-Adresse in einem neuen Datenleak auftaucht, eine Benachrichtigung von uns.

Benachrichtigungen aktivieren

Es kann (manchmal) so einfach sein





Und dann auch noch die physische Dimension

„Über Jahre haben die Unternehmen vor allem in Cybersicherheit investiert.

Darüber, dass die Gefahr einfach durchs Werkstor laufen könnte, haben sie kaum nachgedacht."

Oliver Fein (CSO Helsing)

Und was bedeutet das konkret?



So viele Möglichkeiten!



Beispiel:
Einbruch und Diebstahl von 20€ aus der Kaffeekasse



Beispiel:
auffällige Personen vor / an relevanten









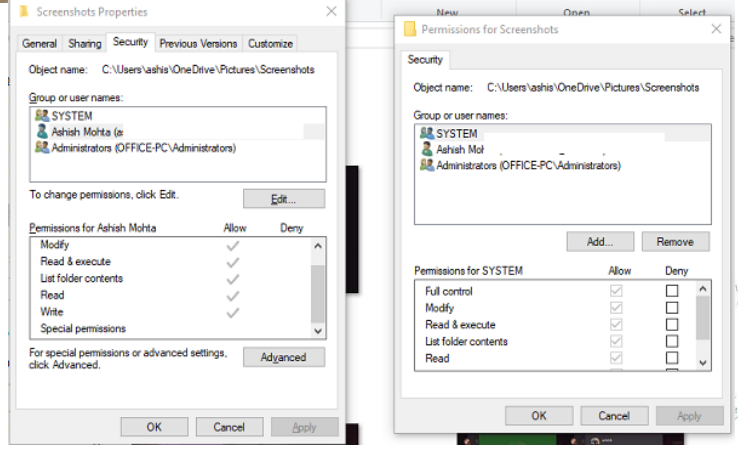
Beispiel:
Azubi packt seinen Koffer und nimmt mit….











Beispiel:
VK / VKontakte („ImKontakt“)



Jeden Monat besuchen 79,5 Millionen Russen VK - wenn wir auch das ausländische Publikum mitzählen, kommen wir auf 101,7 Millionen Nutzer pro Monat.

Beispiel:
Veröffentlichungen durch Unbekannte

Ioan Alin Tomus
Local Guide · 53 Rezensionen · 28 Fotos

★★★★★ vor 2 Monaten

Ich reise kreuz und quer durch Deutschland, aber die Parkmöglichkeiten dieser Firma sind wirklich außergewöhnlich. Es gibt acht sichere Stellplätze, eine Dusche, Toiletten und eine kleine, saubere Küche für die Lkw-Fahrer (und so müssen wir sie auch zurücklassen). Hut ab vor [redacted] dafür! 😊 🤗 ...

Übersetzt von Google · Original ansehen (Rumänisch)



Firmennennung

Rumänisch

Fotostrecke

Antwort vom Inhaber vor einem Monat
Vielen Dank für Ihre hervorragende Bewertung und Ihren großen Einsatz, diesen Leitfaden so hilfreich und benutzerfreundlich zu gestalten. Wir freuen uns sehr, dass Sie mit unserer Zusammenarbeit zufrieden sind.

Übersetzt von Google · Original ansehen (Englisch)

Englisch

Informationsweitergabe um jeden Preis





Human Risk Consulting GmbH

Vorbereitung auf den Notfall





VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

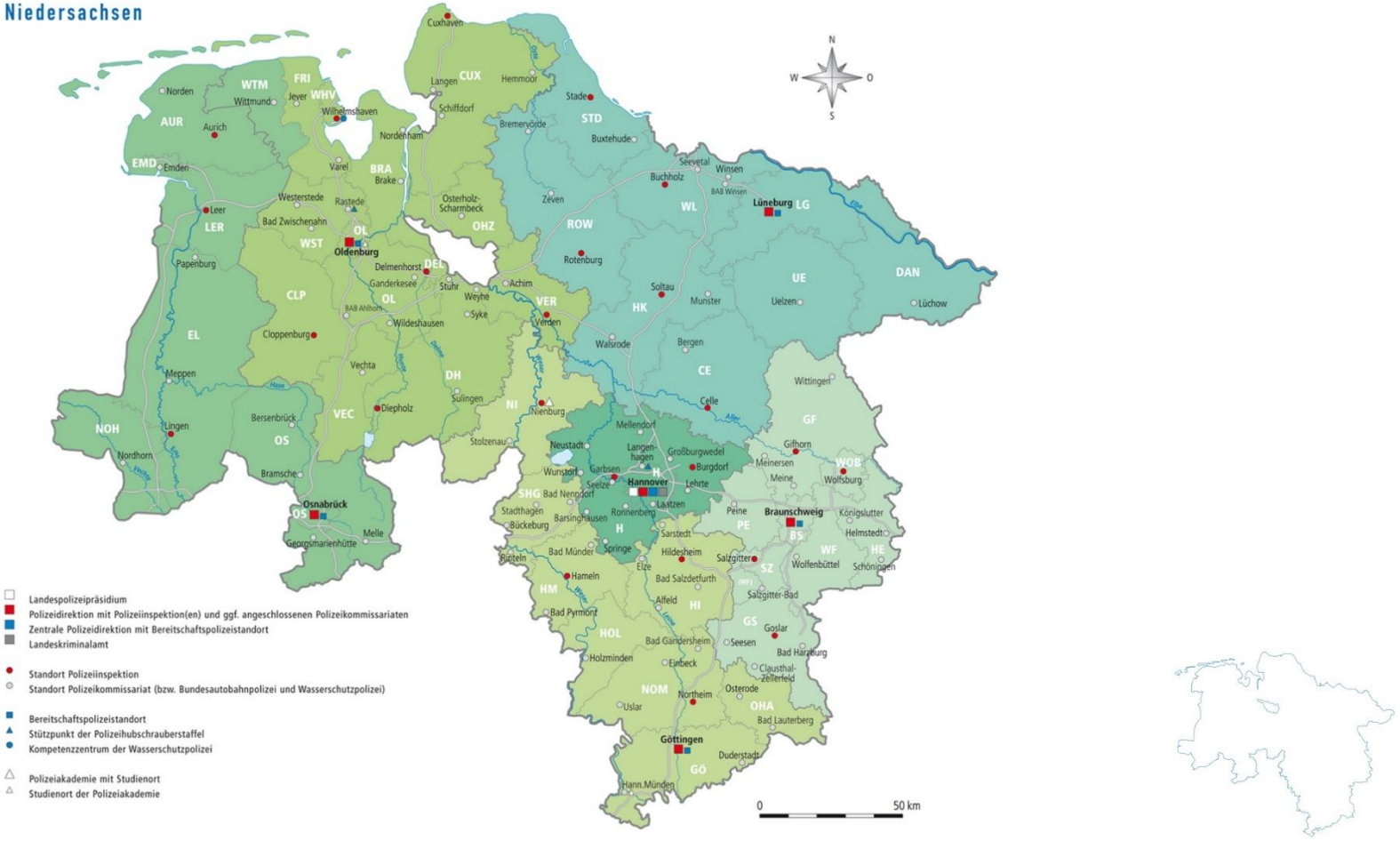
Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Vernetzung bitte über „110“ hinaus



Angebote

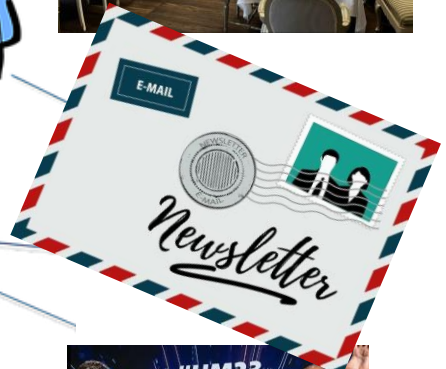




SPOC

LANDESKRIMINALAMT NIEDERSACHSEN
ZENTRALE ANSPRECHSTELLE CYBERCRIME

KRITIS









Niedersächsisches Ministerium
für Inneres, Sport und Digitalisierung
Verfassungsschutz

Wirtschaftsschutz | Verfassungsschutz





Sachgebiet Wirtschaftsschutz

Sonja Flemming
Niedersächsisches Ministerium
für Inneres und Sport
Abteilung 5
(Verfassungsschutz)

Postfach 4420
30044 Hannover
0511 / 6709-247

Wirtschaftsschutz@mi.niedersachsen.de
www.verfassungsschutz.niedersachsen.de