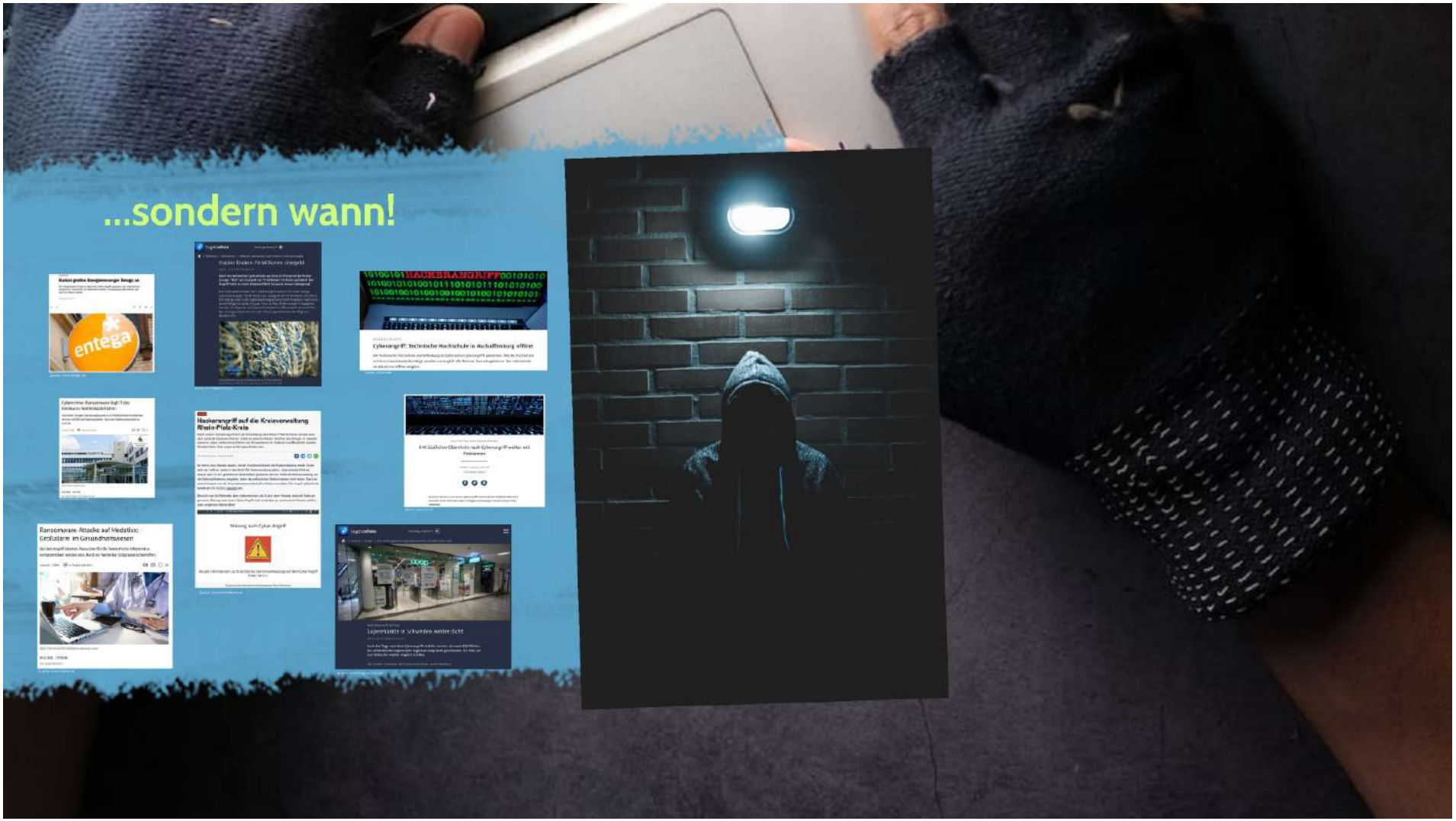
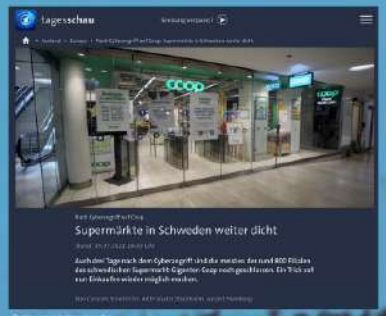

Cyberangriffe auf Unternehmen
Stillstand auf Knopfdruck
Es ist nicht die Frage ob...


...sondern wann!
entega
HACKERANGRIFF
Cyberangriff: Technische Hochschule in Aschaffenburg offline
Hackerangriff auf die Kreisverwaltung Rhein-Pfalz-Kreis
Ransomware-Attacke auf Medatixx: Großalarm im Gesundheitswesen

...sondern wann!



Darmstadt

Hacker greifen Energieversorger Entega an

Der Energieanbieter Entega ist Opfer eines Online-Angriffs geworden. Dem Unternehmen zufolge sind E-Mail-Konten der Mitarbeiter betroffen, Versorgungsausfälle drohten aber nicht. Die Polizei ermittelt.

12.06.2022, 17.23 Uhr

Quelle: www.spiegel.de

NOCH NICHT ALLE DIENSTE WIEDER VERFÜGBAR

IHK Südlicher Oberrhein nach Cyberangriff weiter mit Problemen

STAND: 7.9.2022, 11:01 UHR

VON OWUSU KÜNZEL

Auch vier Wochen nach einem Cyberangriff sind bei der IHK Südlicher Oberrhein nicht alle Online-Dienste wieder verfügbar. Einladungen werden teils per Post versendet.

Quelle: www.swr.de

ngstrojaner zu: Im Wolfenbütteler Krankenhaus
earbeitet. Auch eine Stadtverwaltung hat es

Aktuelles

Hackerangriff auf die Kreisverwaltung Rhein-Pfalz-Kreis

Nach einem Hackerangriff auf die Verwaltung des Rhein-Pfalz-Kreises wendet sich jetzt Landrat Clemens Körner (CDU) in einem offenen Brief an die Bürger. In diesem warnt er, dass vertrauliche Daten von Einwohnern im Darknet veröffentlicht werden könnten bzw. dies sogar schon geschehen sei.

Tom Wannenmacher, 1. November 2022

Es könne noch Monate dauern, bis die Funktionsfähigkeit der Kreisverwaltung wieder hergestellt sei, heißt es weiter in dem Brief. Die Kreisverwaltung selbst, habe keinerlei Einfluss darauf, was mit den gestohlenen Datensätzen passieren könnte. Sollte die Kreisverwaltung auf die Zahlungsforderung eingehen, seien die vertraulichen Daten trotzdem nicht sicher. Das Landeskriminalamt und die Generalstaatsanwaltschaft in Koblenz ermitteln. Der Angriff selbst dürfte bereits am 24.10.2022 passiert sein.

Besucht man die Webseite, dann bekommt man, als Nutzer denn Hinweis, dass die Seite wegen einer Störung nach einem Cyber-Angriff nicht erreichbar sei, sowie einen Hinweis auf den oben erwähnten offenen Brief:

Screenshot der Webseite der Kreisverwaltung Rhein-Pfalz-Kreis

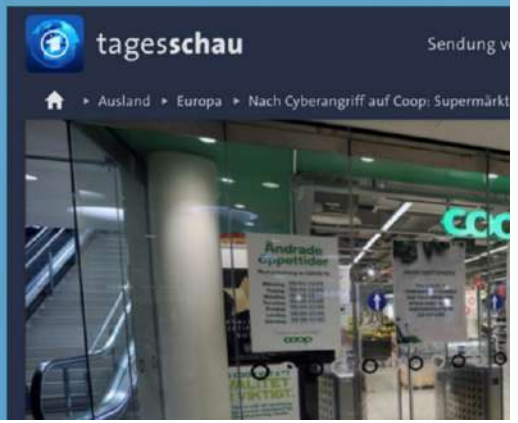
Quelle: www.mimikama.at

Quelle: www

ke auf Medatixx:
ndheitswesen

er für die Telematische Infrastruktur
l ein Viertel der Arztpraxen ist betroffen.

149



dem Cyber-Angriff

tagesschau

Sendung verpasst?

Ausland ▸ Europa ▸ Nach Cyberangriff auf Coop: Supermärkte in Schweden weiter dicht

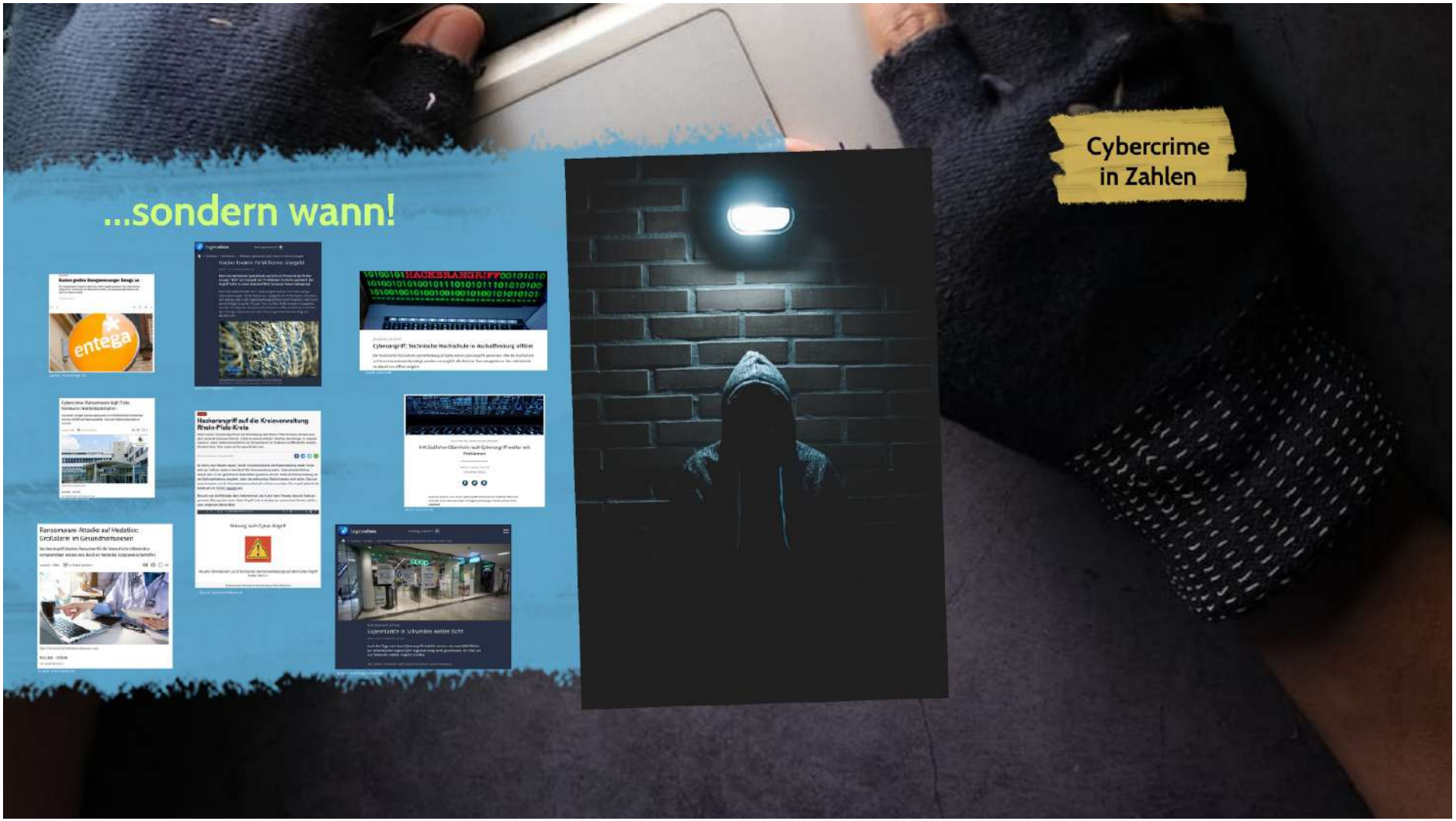
Nach Cyberangriff auf Coop

Supermärkte in Schweden weiter dicht

Stand: 05.07.2021 14:43 Uhr

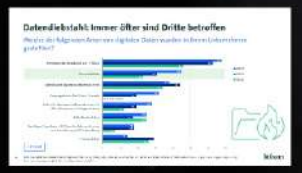
Auch drei Tage nach dem Cyberangriff sind die meisten der rund 800 Filialen des schwedischen Supermarkt-Giganten Coop noch geschlossen. Ein Trick soll nun Einkaufen wieder möglich machen.

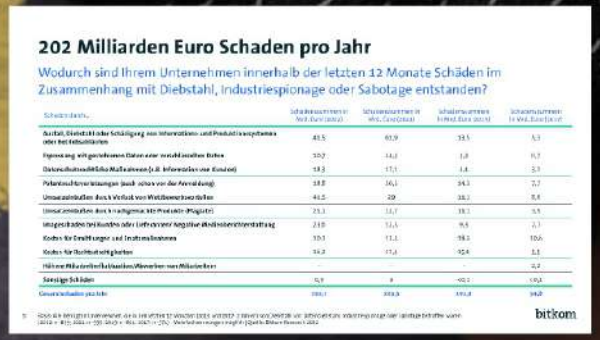
Von Carsten Schmiester, ARD-Studio Stockholm, zurzeit Hamburg


...sondern wann!
Cybercrime in Zahlen
entega
HACKERANGRIFF
Cyberangriff: Technische Hochschule in Aschaffenburg offline
Hackerangriff auf die Kreisverwaltung Rhein-Pfalz-Kreis
Ransomware-Attacke auf Medatixx: Großalarm im Gesundheitswesen

bitkom

Quelle: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

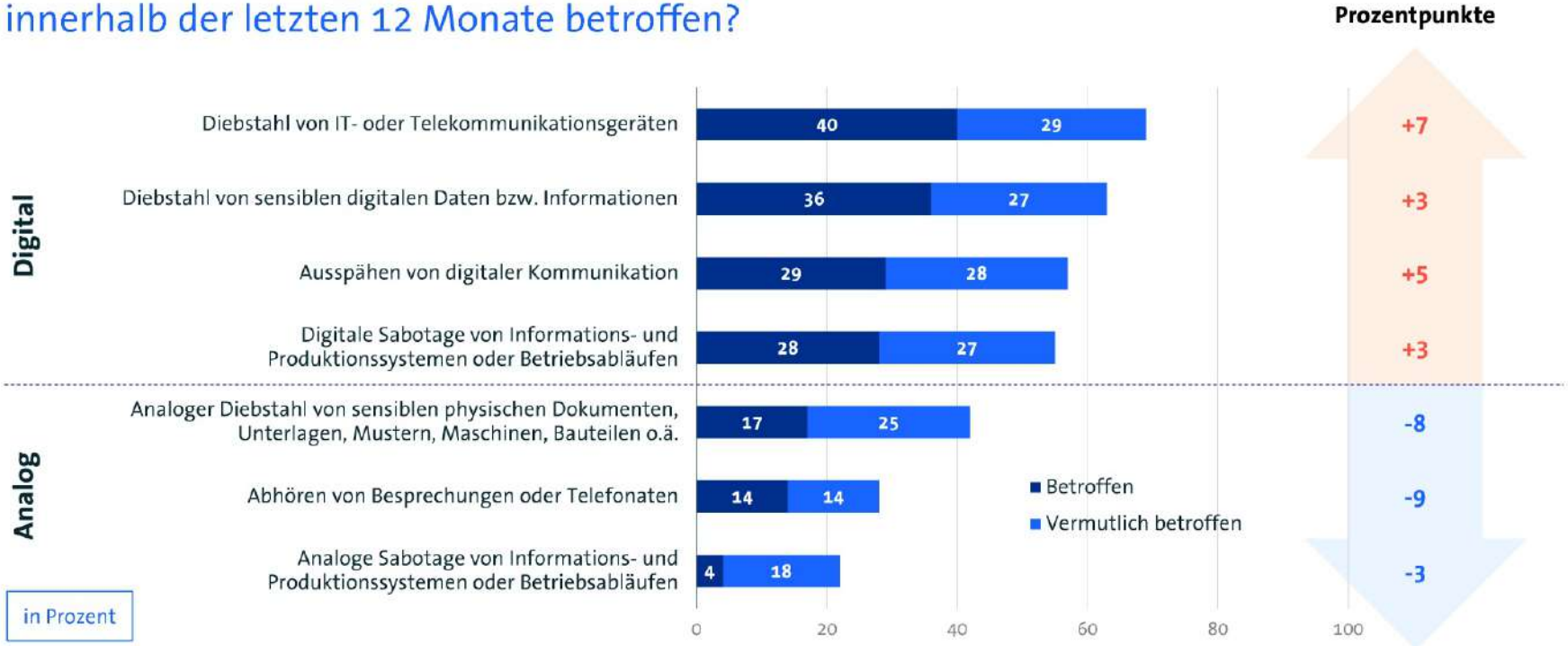




Kriminalstatistik

Angriffe verlagern sich in den digitalen Raum

Von welchen der folgenden Handlungen war Ihr Unternehmen innerhalb der letzten 12 Monate betroffen?

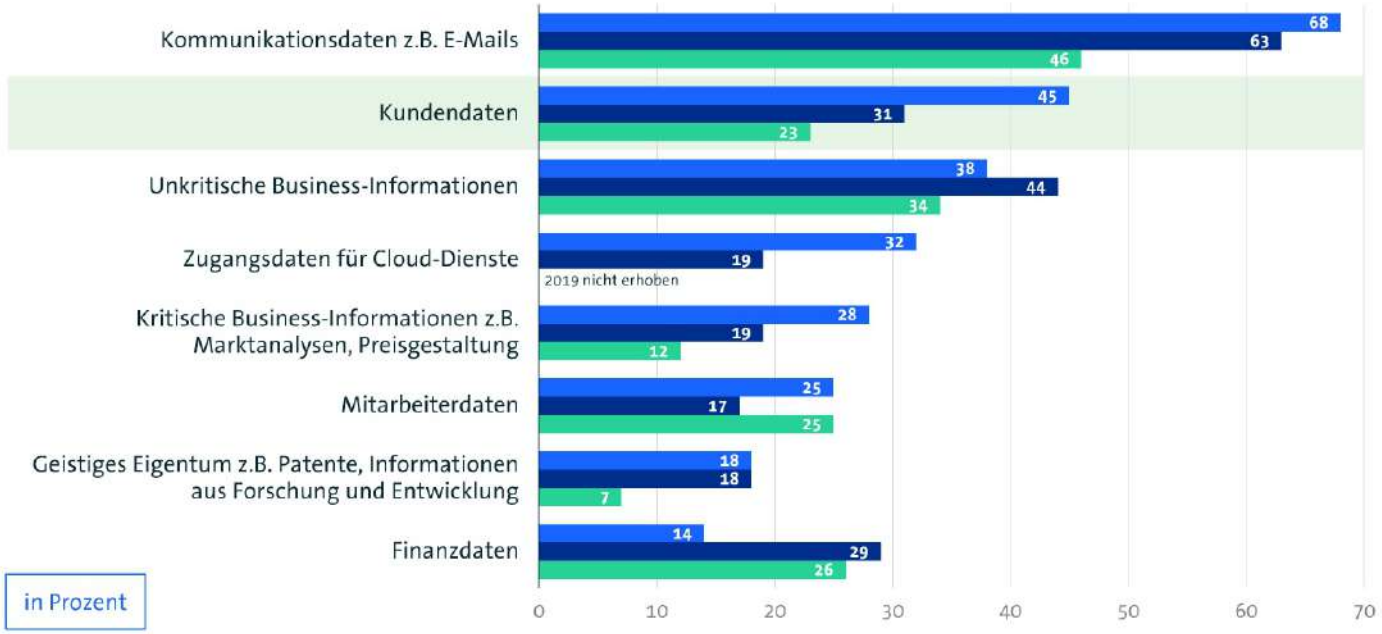


3 Basis: Alle befragten Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

bitkom

Datendiebstahl: Immer öfter sind Dritte betroffen

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?



4 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von sensiblen digitalen Daten betroffen waren (2022: n=383; 2021: n=330; 2019: n=229) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

202 Milliarden Euro Schaden pro Jahr

Wodurch sind Ihrem Unternehmen innerhalb der letzten 12 Monate Schäden im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadenssummen in Mrd. Euro (2017)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	41,5	61,9	13,5	5,3
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	10,7	24,3	5,3	0,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	18,3	17,1	4,4	3,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	18,8	30,5	14,3	7,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	41,5	29	11,1	8,6
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	21,1	22,7	11,1	3,5
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	23,6	12,3	9,3	7,7
Kosten für Ermittlungen und Ersatzmaßnahmen	10,1	13,3	18,3	10,6
Kosten für Rechtsstreitigkeiten	16,2	12,4	15,6	5,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	-	2,2
Sonstige Schäden	0,9	0	<0,1	<0,1
Gesamtschaden pro Jahr	**202,7**	**223,5**	**102,9**	**54,8**

9 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019 und 2017: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801; 2017: n=571) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

202 Milliarden Euro Schaden pro Jahr

Wodurch sind Ihrem Unternehmen innerhalb der letzten 12 Monate Schäden im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadenssummen in Mrd. Euro (2017)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	41,5	61,9	13,5	5,3
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	10,7	24,3	5,3	0,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	18,3	17,1	4,4	3,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	18,8	30,5	14,3	7,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	41,5	29	11,1	8,6
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	21,1	22,7	11,1	3,5
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	23,6	12,3	9,3	7,7
Kosten für Ermittlungen und Ersatzmaßnahmen	10,1	13,3	18,3	10,6
Kosten für Rechtsstreitigkeiten	16,2	12,4	15,6	5,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	-	2,2
Sonstige Schäden	0,9	0	<0,1	<0,1
Gesamtschaden pro Jahr	**202,7**	**223,5**	**102,9**	**54,8**

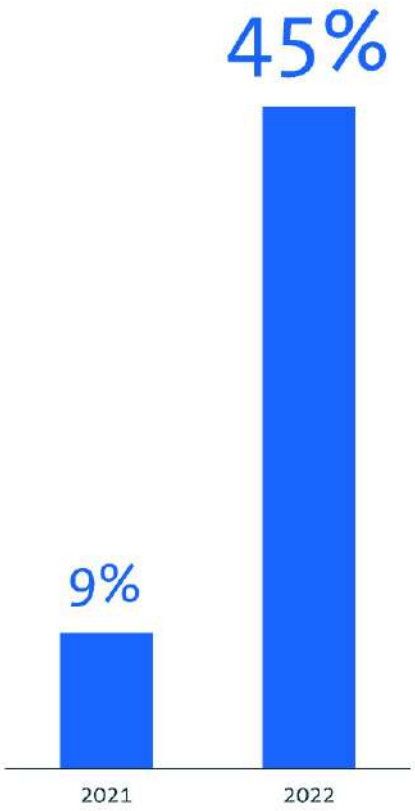
9 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019 und 2017: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801; 2017: n=571) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

Cyberattacken bedrohen Existenz vieler Unternehmen

Inwiefern stimmen Sie der Aussage zu bzw. nicht zu?

Cyberangriffe **bedrohen unsere** geschäftliche **Existenz**

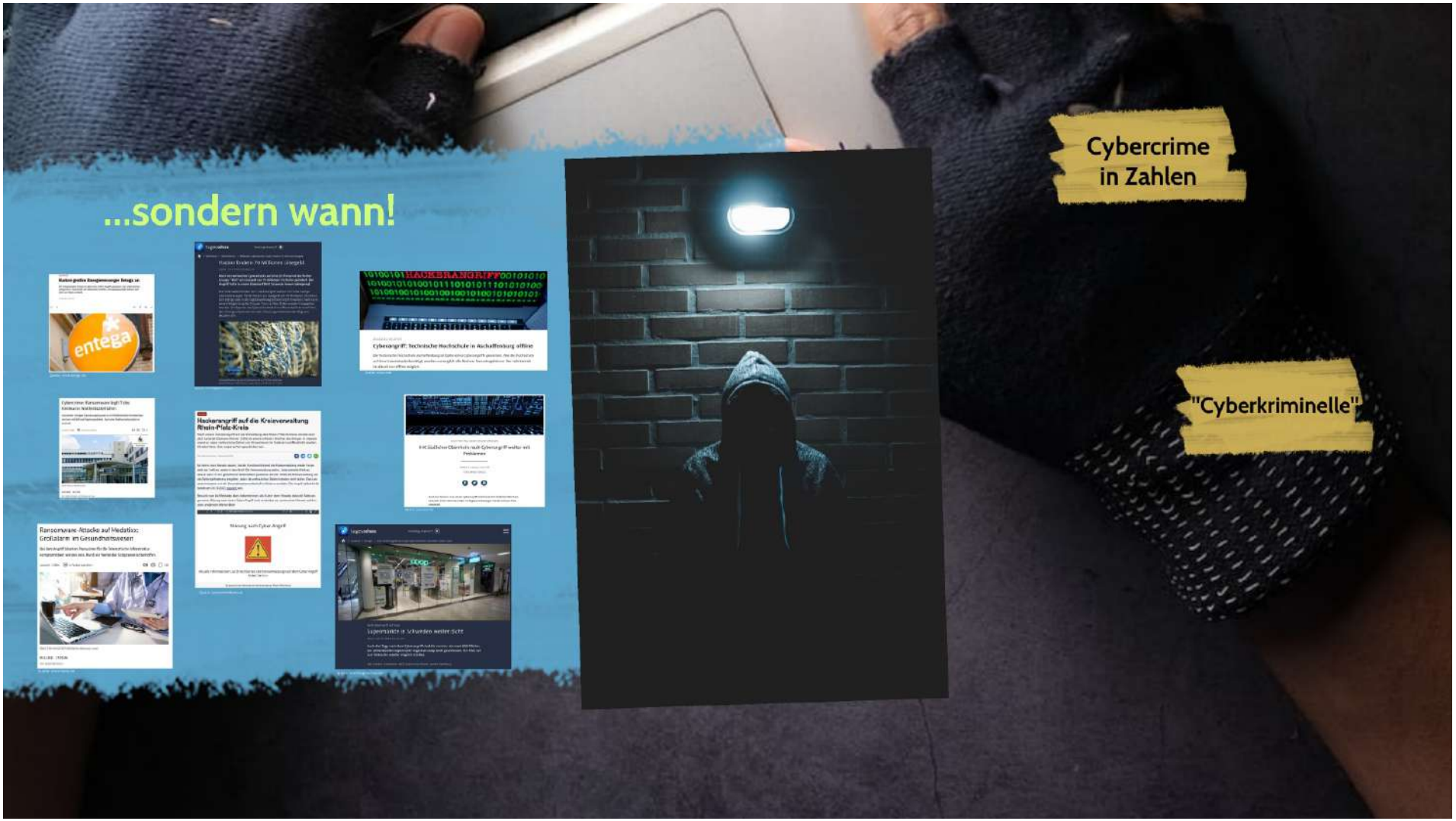


5 Basis: Alle befragten Unternehmen (n=1.066) | Quelle: Bitkom Research 2022

bitkom

Cybercrime i.e.S.

Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten


...sondern wann!
Cybercrime in Zahlen
"Cyberkriminelle"
entega
HACKERANGRIFF
Hackerangriff auf die Kreisverwaltung Rhein-Pfalz-Kreis
Ransomware-Attacke auf Medatixx: Großalarm im Gesundheitswesen


Es gibt nicht DEN Täter...
Quelle: Bundeslagebild Cybercrime 2021

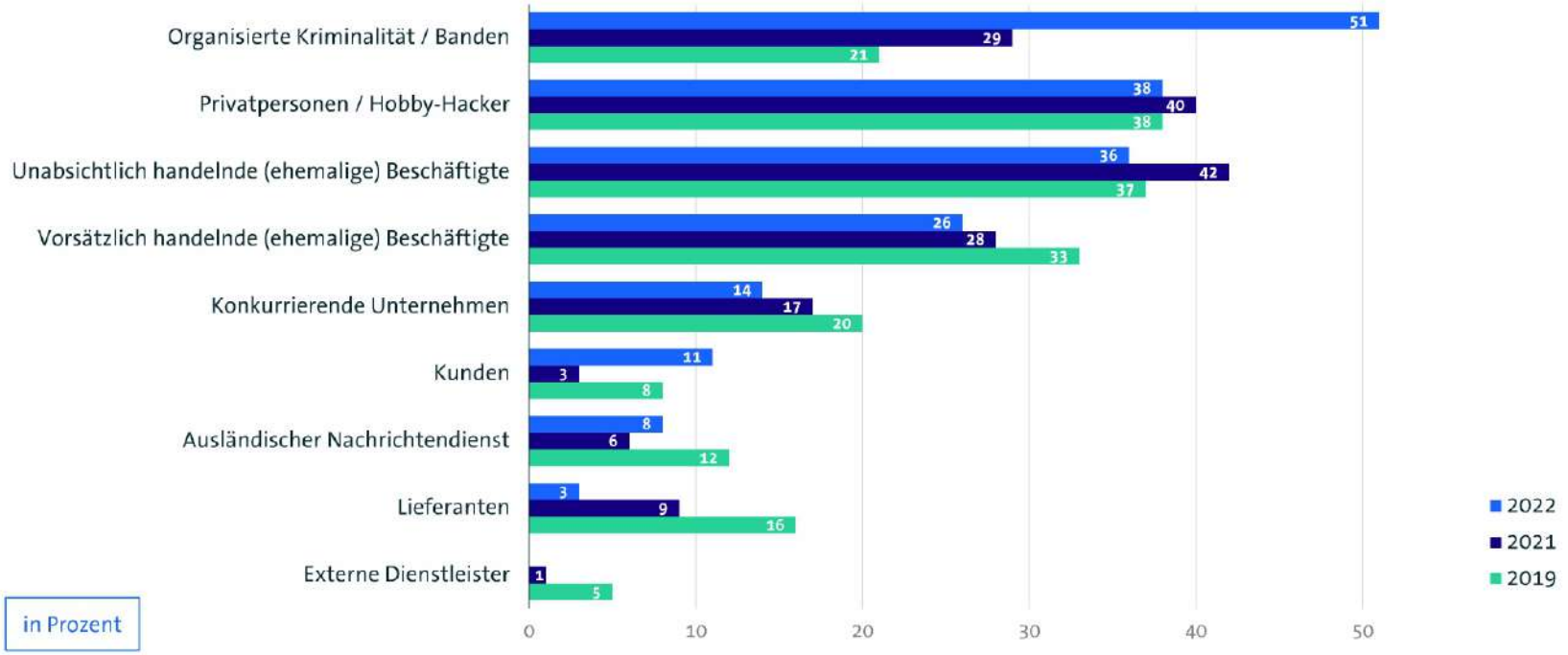
Service	Preis in US $ (gesamt oder pro Nutzungszeitraum / pro Einheit)	
BankingTrojaner		
▪ **Desktop-Version**	1.000 - 10.000 $	bei Kauf
▪ **Mobile-Version**	1.000 - 10.000 $	bei Kauf
RAT (Remote Administration Tool)	60 - 530 $ ca. 3.000 $	pro Monat bei Miete bei Kauf
Mining Bots	50 – 150 $	pro Monat bei Miete
Crypting	0 - 100 $ 30 - 500 $	bei Kauf von einem Crypt bei einem Wochen-Abo mit 50 Crypts pro Tag
DDoS-as-a-Service	80 - 1.500 $	pro Monat bei Miete
Bulletproof Hosting		
▪ **Shared**	5 - 50 $	pro Monat bei Miete
▪ **Dedicated**	50 - 700 $	pro Monat bei Miete
Counter-AV-Service	10 $	pro Monat und 300 Scans
Infection-on-Demand (Phishing-Services o.ä.)	Ab 100 $	pro Monat
Stealer Logs	5 -15 $ 400 – 900 $	pro Stück pro Monat für Abonnement

Abbildung 8: Übersicht krimineller Services der Underground Economy/ im Darknet

Quelle: Bundeslagebild Cybercrime 2021

Attacken auf die Wirtschaft werden professioneller

Von welchem Täterkreis gingen Handlungen in den letzten 12 Monaten aus?

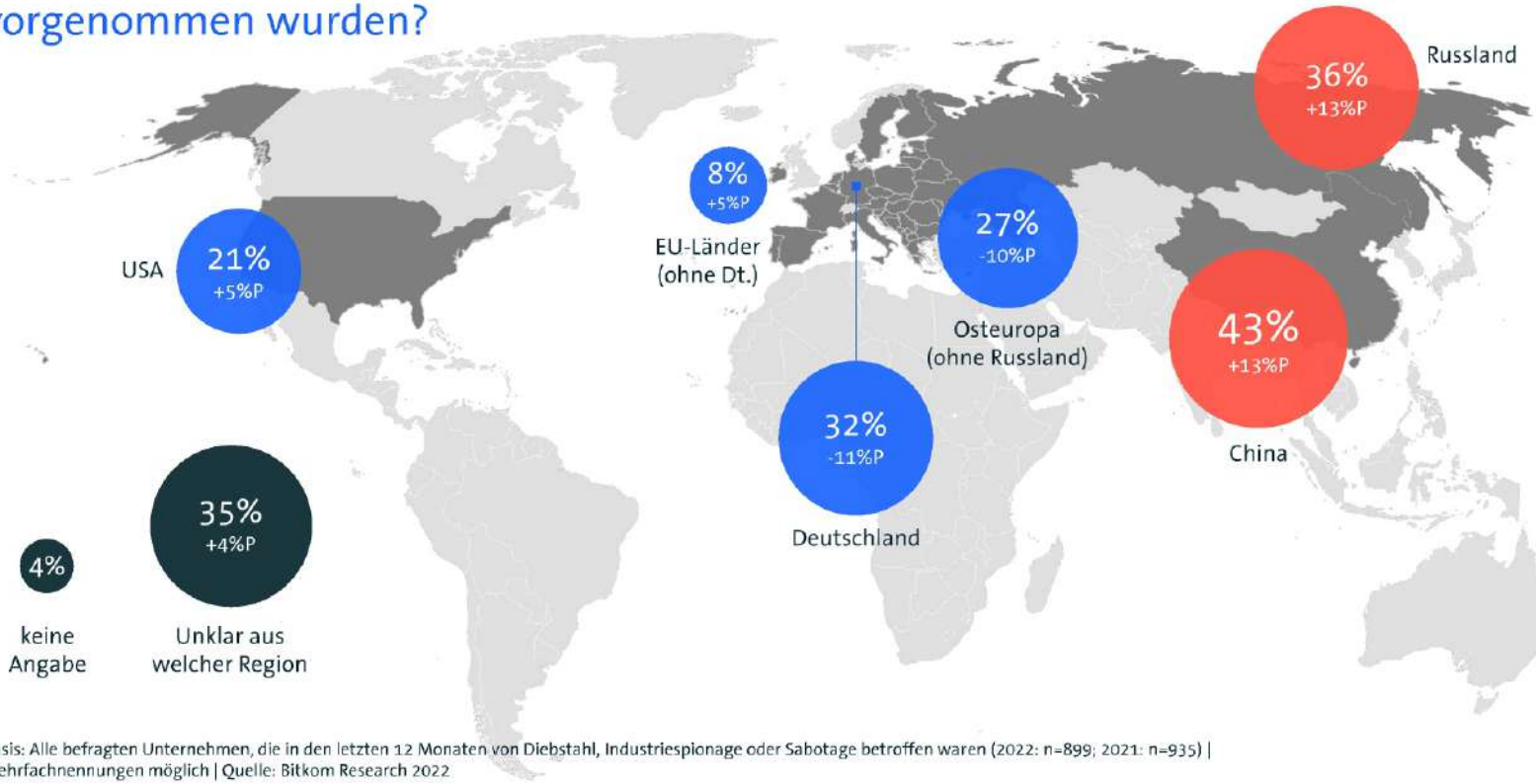


11 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935; 2019: n=801) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

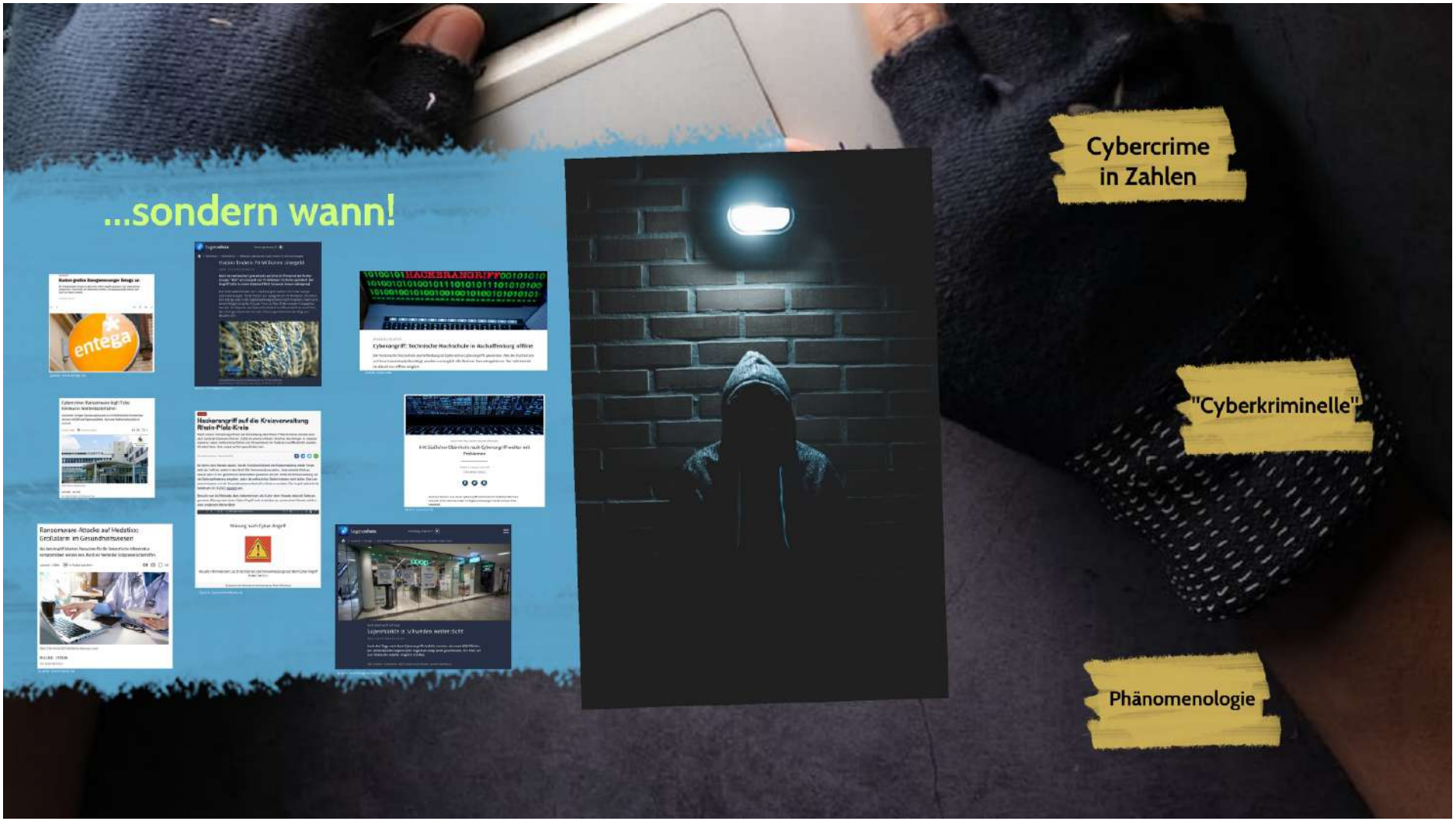
Angriffe auf Deutschland: Der Osten rückt in den Fokus

Konnten Sie feststellen, von wo aus bzw. aus welcher Region diese Handlungen vorgenommen wurden?



10 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten von Diebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

bitkom

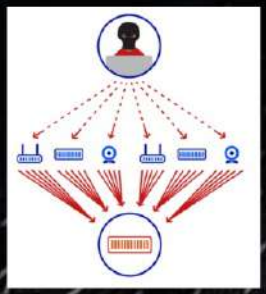

...sondern wann!
Cybercrime in Zahlen
"Cyberkriminelle"
Phänomenologie

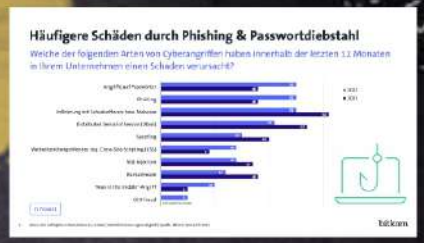

Was ist Cybercrime?
Cybercrime ist eines der sich am dynamischsten verändernden Kriminalitätsphänomene. Täter passen sich flexibel an technische und gesellschaftliche Entwicklungen an, agieren global und greifen dort an, wo es sich aus ihrer Sicht finanziell lohnt.
DDoS
Social Engineering
Phishing
CEO Fraud BEC
Ransomware

DDoS - Distributed Denial of Service

Gezielte Überlastung eines Servers (z.B. Webseite einer Firma) mit einer sehr hohen Anzahl von Anfragen

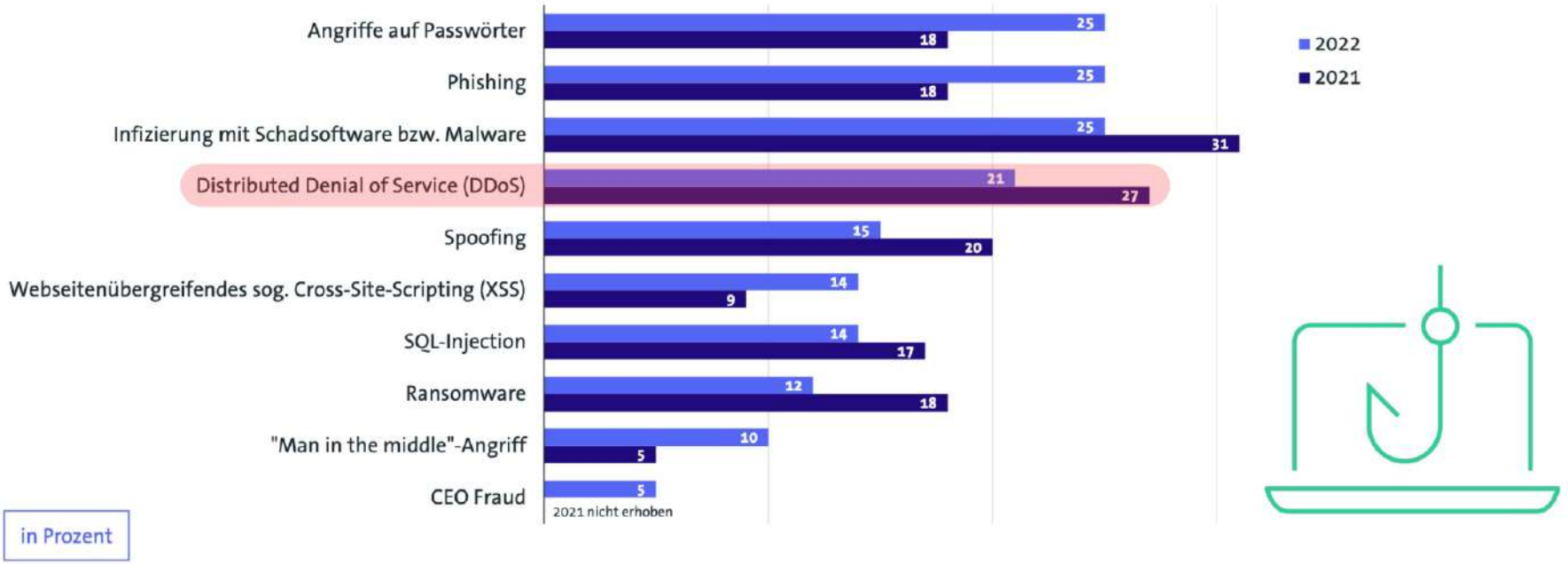
Angriff erfolgt über zuvor infizierte Fremdrechner, Steuerung über CC Server (Command & Control)





Häufigere Schäden durch Phishing & Passwortdiebstahl

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



7 Basis: Alle befragten Unternehmen (n=1.066) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

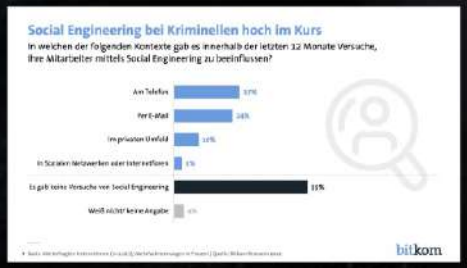
bitkom

Social Engineering

"Schwachstelle" Mensch

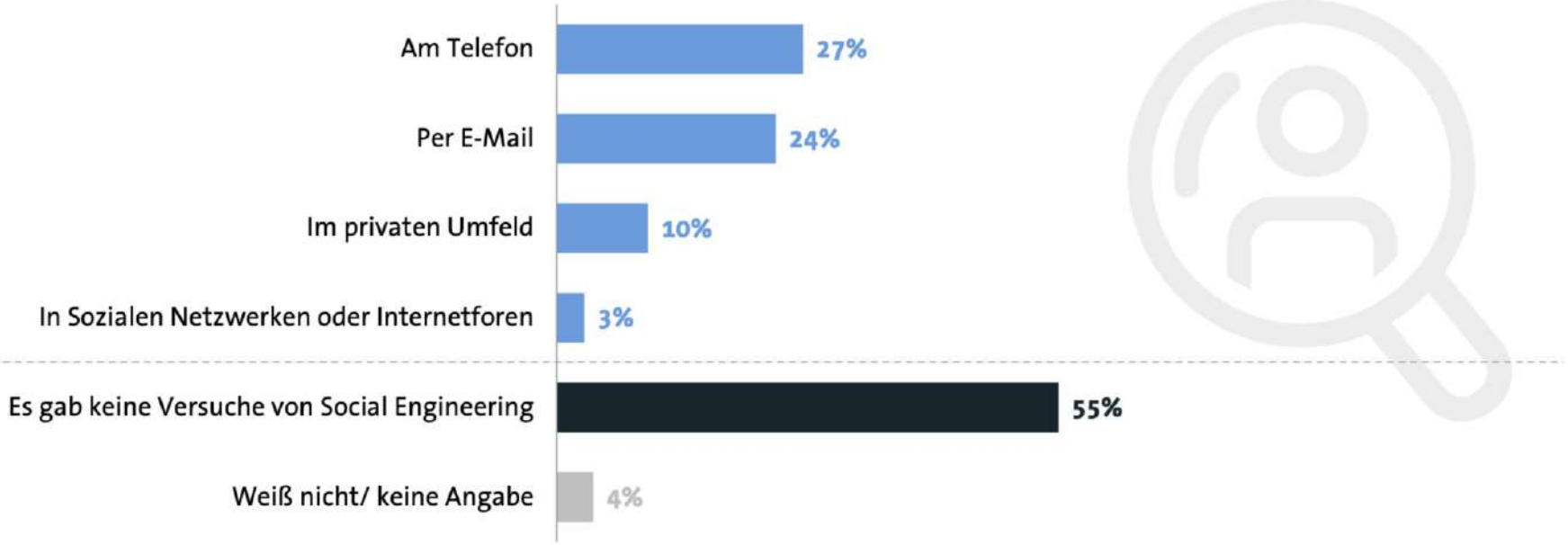
Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität werden ausgenutzt

Chef, Systemadministrator, soziale Netzwerke, Kollegen, Online-"Freunde"



Social Engineering bei Kriminellen hoch im Kurs

In welchen der folgenden Kontexte gab es innerhalb der letzten 12 Monate Versuche, Ihre Mitarbeiter mittels Social Engineering zu beeinflussen?



9 Basis: Alle befragten Unternehmen (n=1.067); Mehrfachnennungen in Prozent | Quelle: Bitkom Research 2021

bitkom

Phishing
(Password Fishing)

Steht am Anfang vieler Delikte

Spear Phishing

Smishing

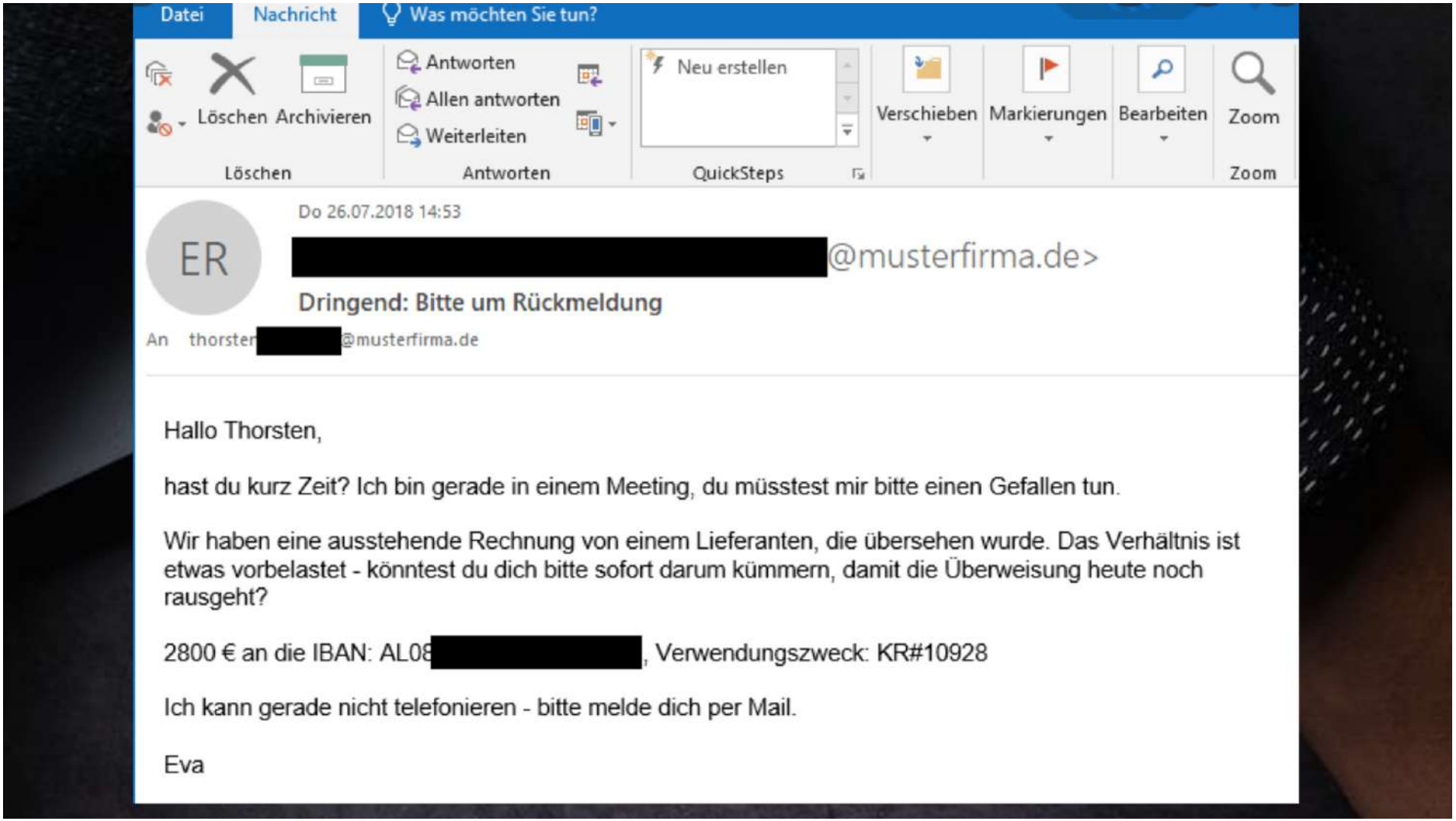
CEO Fraud / BEC

Täter verschafft sich zunächst umfassende Informationen über Unternehmen und Mitarbeiter (Social Engineering, frei zugängliche Quellen)

Aufbau einer dringenden Situation und "schmeicheln" des Opfers als Vertrauensperson (CEO-Fraud)

Manipulation von E-Mail-Verkehr (BEC)

Überweisung an unberechtigten Empfänger


Datei
Nachricht
Was möchten Sie tun?
Löschen
Archivieren
Antworten
Allen antworten
Weiterleiten
Neu erstellen
Verschieben
Markierungen
Bearbeiten
Zoom
Löschen
Antworten
QuickSteps
Zoom
ER
Do 26.07.2018 14:53
[redacted]@musterfirma.de>
Dringend: Bitte um Rückmeldung
An thorster[redacted]@musterfirma.de
Hallo Thorsten,
hast du kurz Zeit? Ich bin gerade in einem Meeting, du müsstest mir bitte einen Gefallen tun.
Wir haben eine ausstehende Rechnung von einem Lieferanten, die übersehen wurde. Das Verhältnis ist etwas vorbelastet - könntest du dich bitte sofort darum kümmern, damit die Überweisung heute noch rausgeht?
2800 € an die IBAN: AL08[redacted], Verwendungszweck: KR#10928
Ich kann gerade nicht telefonieren - bitte melde dich per Mail.
Eva

Ransomware

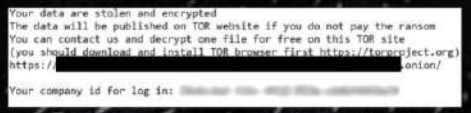
Digitale Erpressung

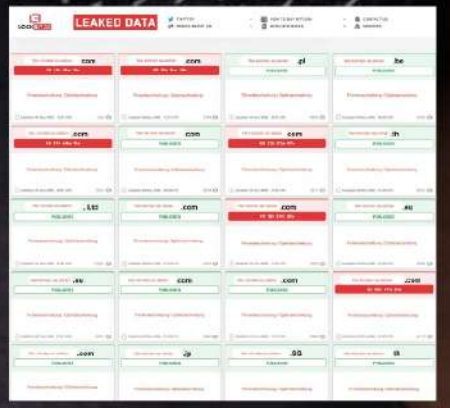
Verschlüsselung

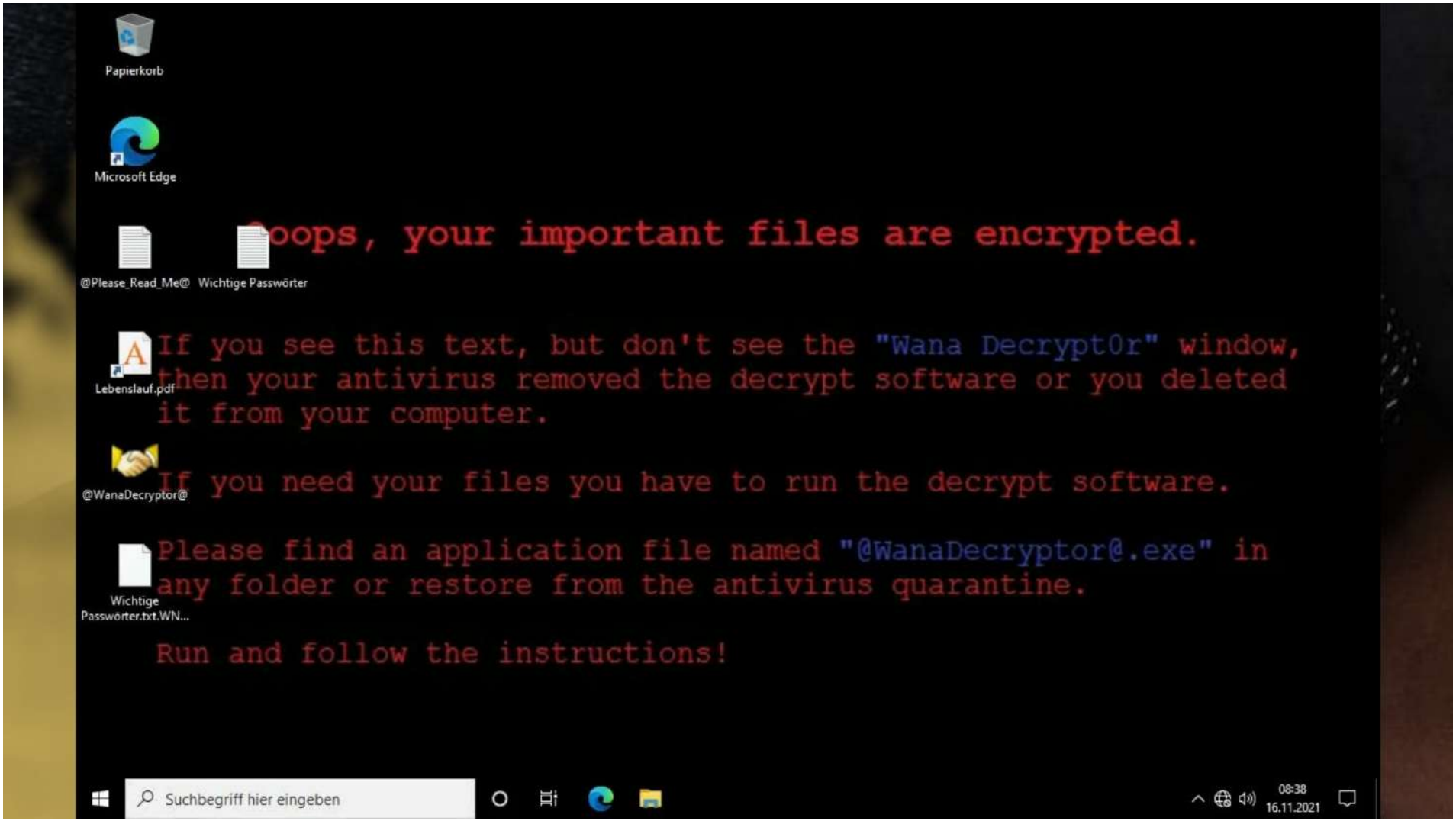
Kryptowährungen

Conti, Ryuk, BlackBasta u.v.m.

Double Extortion






Papierkorb
Microsoft Edge
@Please_Read_Me@
Wichtige Passwörter
Lebenslauf.pdf
@WanaDecryptor@
Wichtige Passwörter.txt.WN...
oops, your important files are encrypted.
If you see this text, but don't see the "Wana DecryptOr" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.
If you need your files you have to run the decrypt software.
Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.
Run and follow the instructions!
Suchbegriff hier eingeben
08:38
16.11.2021

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation.
More than a year ago, world experts recognized the impossibility of deciphering by any means except the original decoder.
No decryption software is available in the public.
Antiviruse companies, researchers, IT specialists, and no other persons cant help you encrypt the data.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT DELETE readme files.

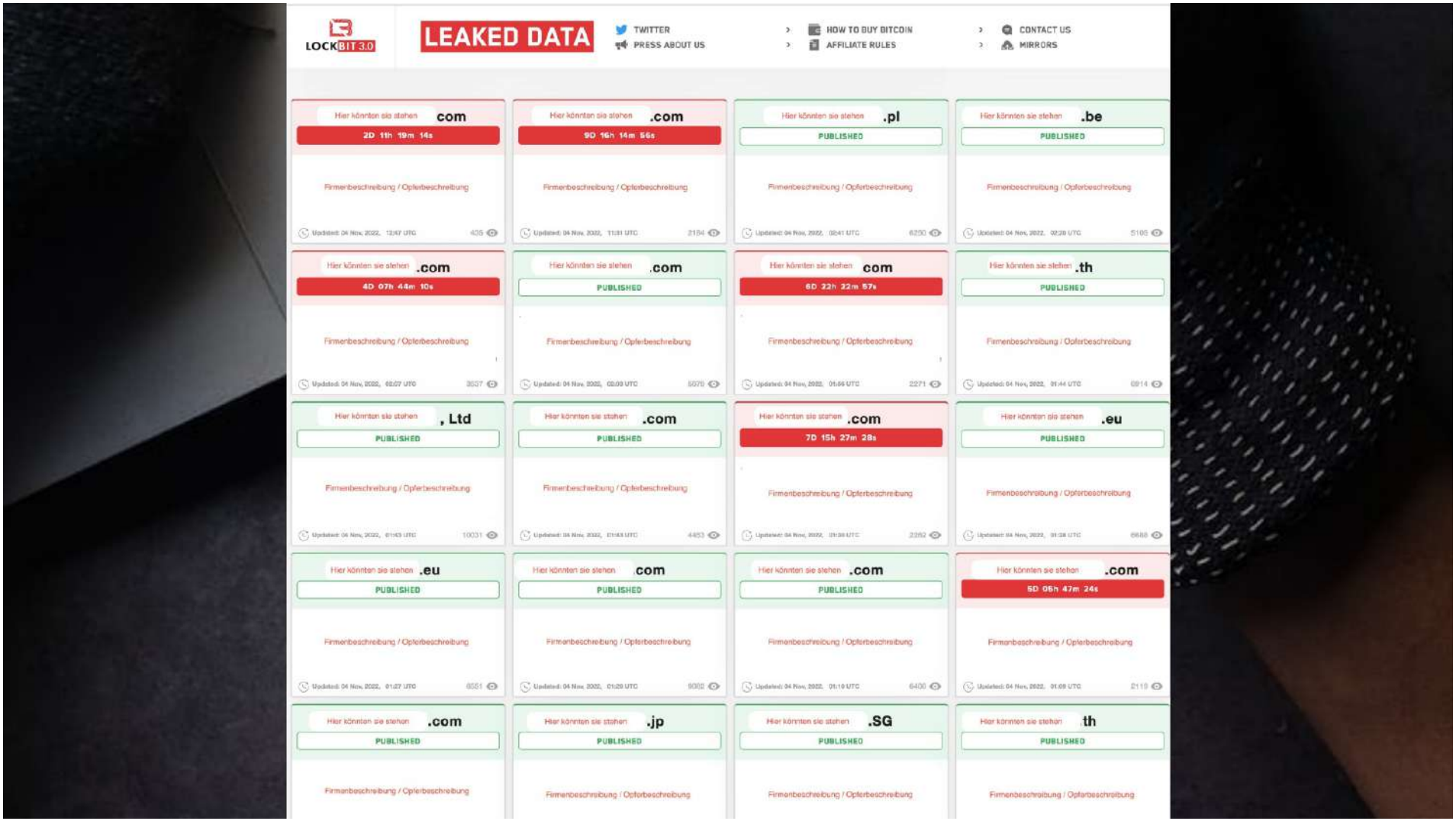
To confirm our honest intentions.Send 2 different random files and you will get it decrypted.
It can be from different computers on your network to be sure that one key decrypts everything.
2 files we unlock for free

To get info (decrypt your files) contact us at
[redacted]@protonmail.com
or
[redacted]@tutanota.com

You will receive btc address for payment in the reply letter

Ryuk

No system is safe


LOCKBIT 3.0
LEAKED DATA
TWITTER
PRESS ABOUT US
HOW TO BUY BITCOIN
AFFILIATE RULES
CONTACT US
MIRRORS
Hier könnten sie stehen .com
2D 11h 19m 14s
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .com
9D 16h 14m 56s
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .pl
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .be
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .com
4D 07h 44m 10s
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .com
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen com
6D 22h 22m 57s
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .th
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen , Ltd
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .com
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .com
7D 15h 27m 28s
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .eu
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .eu
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .com
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .com
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .com
5D 06h 47m 24s
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .com
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .jp
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen .SG
PUBLISHED
Firmenbeschreibung / Opferbeschreibung
Hier könnten sie stehen th
PUBLISHED
Firmenbeschreibung / Opferbeschreibung


Beware of the headless chicken
Bewahren Sie Ruhe und handeln Sie nicht übereilt.
Organisieren Sie sich. Richten Sie einen Krisenstab (oder eine Projektgruppe) ein. Verteilen Sie Rollen und Zuständigkeiten.
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Organisatorisches/ich-habe-einen-it-sicherheitsvorfall-checkliste-organisatorisches_node.html
Allianz für Cyber-Sicherheit
TOP 12
MASSNAHMEN BEI CYBER-ANGRIFFEN
Diese Fragen sollten Sie sich stellen!
Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.
Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.
Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt?
Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen? Wurden alle angegriffenen Systeme identifiziert?
Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen durch relevante Maßnahmen adressiert und behoben?
Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?
Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?
Das Dokument ist ein gemeinsames Produkt nachfolgender Organisationen: Bundeskriminalamt, Charter of Trust, Deutscher Industrie- und Handelskammertag e.V., eco – Verband der Internetwirtschaft e.V., Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit e.V., VOICE – Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik
Stand: September 2019


Beware of the headless chicken
Bewahren Sie Ruhe und handeln Sie nicht übereilt.
Organisieren Sie sich. Richten Sie einen Krisenstab (oder eine Projektgruppe) ein. Verteilen Sie Rollen und Zuständigkeiten.
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Organisatorisches/ich-habe-einen-it-sicherheitsvorfall-checkliste-organisatorisches_node.html
Ihr Partner


Mit anderen Menschen
zusammen erreichen wir
mehr als alleine.
Dalai Lama (*1935)
(Das Lächeln des Himmels)
BSI
Bundesamt
für Sicherheit in der
Informationstechnik


Hilfe zur Selbsthilfe...und mehr
www.bsi.bund.de
MASSNAHMEN-KATALOG ZUM NOTFALLMANAGEMENT
- Fokus IT-Notfälle -
Bundesamt für Sicherheit in der Informationstechnik
CERT Bund
Erste Hilfe bei einem schweren IT-Sicherheitsvorfall
Arbeitspapier - Version 1.1
28.01.20
certbund@bsi.bund.de
Qualifizierte Dienstleister
Bei Cyber-Angriffen kann sowohl bei der Prävention als auch nach einem akuten Sicherheitsvorfall die Einbindung eines qualifizierten Dienstleisters sinnvoll sein.
Zur Auswahl dieser qualifizierten Dienstleister hat das BSI gem. § 3, Abs. 3 BSIG Auswahlkriterien zu verschiedenen Themengebieten veröffentlicht und mit dem unten beschriebenen wettbewerbsneutralen Verfahren qualifizierte Dienstleister identifiziert, die diese Anforderungen erfüllen.
Einstieg ins IT-Notfallmanagement für kleinere und mittelständische Unternehmen (KMU)
1. Vorbereitung
2. Bereitschaft
3. Bewältigung
4. Nachbereitung

Mit anderen Menschen zusammen erreichen wir mehr als alleine.

Dalai Lama (*1935)
(Das Lächeln des Himmels)

Bundesamt
für Sicherheit in der
Informationstechnik

BSI

Polizei

Zentrale Ansprechstelle Cybercrime

Die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamts Rheinland-Pfalz ist ein direkter Ansprechpartner für Wirtschaftsunternehmen, öffentliche und nichtöffentliche Institutionen bei Cybercrimevorfällen.

Aufgaben:
- Single-Point-of-Contact für Unternehmen und Behörden
- Professionelle Unterstützung und Beratung in Sicherheitsfragen
- Aufnahme von strafrechtlichen Sachverhalten
- Koordinierung von polizeilichen Ermittlungen

Erreichbarkeit:
Hotline: (06131) 65 - 64760
Mail: lka.cybercrime@polizei.rlp.de

Was will die Polizei?


Wie können wir
zusammenarbeiten?

en?

Ihre Firma

Was bringt es mir, die Polizei zu kontaktieren?
Die finden den oder die Täter doch sowieso nicht.

Täterermittlungen sind lediglich ein Strang.
Wir werden nicht jeden Hacker finden können. Aber wir können deren IT-Infrastruktur stören oder herunternehmen oder an ihr Geld kommen.

Strafverfolgung

Wenn ich die Polizei verständige, nimmt sie große Teile meiner Hardware mit und bringt sie nicht oder nicht zeitnah zurück.

Wir müssen nicht in jedem Fall bei Ihnen im Unternehmen aktiv werden. In vielen Fällen können Sie uns relevante Daten einfach aushändigen. Nur in Einzelfällen ist eine Datensicherung vor Ort durch die Polizei erforderlich, die wir natürlich mit Ihnen abstimmen.

Polizei und Staatsanwaltschaft ermitteln dann eher gegen mich, wenn sie etwas Belastendes gefunden haben. Dabei bin ich/sind wir das Opfer der Attacke und haben andere Sorgen.

Wir sind auf den Sachverhalt fokussiert, bei dem Sie geschädigt sind. Im Übrigen geben Sie uns die Daten, wir suchen nicht danach in Ihren Systemen.

Wenn ich heute mit der Polizei oder Staatsanwaltschaft spreche, steht morgen alles in der Presse!

Das Gegenteil ist der Fall, gerade in der frühen Phase der Ermittlungen werden generell keine proaktiven Presseauskünfte erteilt. Auch im weiteren Verlauf stimmen wir die Pressearbeit mit Ihnen ab.

Wenn ich Polizei und Staatsanwaltschaft einbinde, darf ich doch am Ende gar nichts mehr entscheiden, also etwa ob ich Erpressungsgeld zahle oder mit den Tätern kommuniziere.

Sie entscheiden - wir beraten. Sie können von unserer Erfahrung in solchen Angriffssituationen profitieren.

Was braucht die Strafverfolgung eigentlich?

Die Daten zu einem Angriff liegen bei Ihnen. In den Daten liegen die Spuren zu den Tätern und ihrer Infrastruktur.

Wir möchten **schnellstmöglich** mit diesen Daten arbeiten.

Wir benötigen von Ihnen:
Malwaresamples, (IP-Adressen aus) **Logfiles**, **E-Mailadressen**, von denen mit Ihnen kommuniziert wurde, jede Information zur **Täterkommunikation**, Hinweise auf **Leak-Pages**...

Wir wissen, dass es bei Ihnen **brennt**. Darauf werden wir Rücksicht nehmen. Die Rettung Ihres Unternehmens steht im Fokus Ihres Tuns.

Daten sind für uns auch von extrem großem Wert, wenn Sie im Eifer des Gefechts **nicht forensisch** gesichert wurden.

Unsere Empfehlung: Binden Sie die Polizei frühzeitig ein!

Lassen Sie Ihre Techniker oder beauftragte IT Security Unternehmen mit unseren Technikern sprechen und sich von uns beraten.

Wir finden einen Weg, Sie möglichst wenig zu belasten und so schnell wie möglich an notwendige Spuren zu kommen.


Cyberangriffe auf Unternehmen
Stillstand auf Knopfdruck
Es ist nicht die Frage ob...
Incident
Prevention

Machen Sie IT-Security zur Chefsache

Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheit

Bundesamt
für Sicherheit in der
Informationstechnik

Auftrag

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland.

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/unternehmen-und-organisationen_node.html

Informationen und Empfehlungen

Cyber-Sicherheitsempfehlungen nach Gefährdungen

Cyber-Sicherheitsempfehlungen nach Angriffszielen

Kleine und mittlere Unternehmen

Qualifizierte Dienstleister

Freie Software

Quantentechnologien und (Post-)Quanten-Kryptografie

Kryptografie

Künstliche Intelligenz

Cyber-Sicherheit für Weltraumanwendungen

Industrielle Steuerungs- und Automatisierungssysteme (ICS)

5G

SiSyPHuS Win10

ISI-Reihe

RZ -Sicherheit und Hochverfügbarkeit

IT-Sicherheitskennzeichen

Smart City

Automotive

Initiativen und Netzwerke

Allianz für Cyber-Sicherheit

Cyber-Sicherheitsnetzwerk

Nationales Koordinierungszentrum für Cybersicherheit

Cyber-Sicherheitslage

Technische Sicherheitshinweise und Warnungen

Analysen und Prognosen

Reaktion

Lageberichte

IT-Sicherheitsvorfall

Standards und Zertifizierung


Machen Sie IT-Security zur Chefsache
Bundesamt für Sicherheit in der Informationstechnik
Sicherheit auf allen Ebenen


Allianz für Cyber-Sicherheit
Warum Teilnehmer der Allianz für Cyber-Sicherheit werden?
Als Teilnehmer der Allianz für Cyber-Sicherheit profitieren Sie von
• der Expertise des BSI und der Partner der Allianz für Cyber-Sicherheit,
• dem vertrauensvollen Erfahrungsaustausch mit anderen Unternehmen und Institutionen zu Themen wie Angriffsvektoren, geeigneten Schutzmaßnahmen, Tipps zum Sicherheitsmanagement, Vorfallsbehandlung etc. sowie
• den exklusiven und für alle Teilnehmer kostenfreien Partner-Angeboten zum Ausbau Ihrer Cyber-Sicherheitskompetenz.
https://www.allianz-fuer-cybersicherheit.de/
DsiN Deutschland sicher im Netz
DsiN für Unternehmen
Kleine und mittlere Betriebe sind das Rückgrat der deutschen Wirtschaft – und entgegen vieler Annahmen ein beliebtes Ziel für Cyberangriffe. Jeder Betrieb sollte deshalb einen IT-Basisschutz umsetzen sowie ein IT-Sicherheitskonzept und Notfallpläne entwickeln. DsiN leistet Aufklärung und unterstützt Entscheider sowie Mitarbeiter in Betrieben mit konkreten Hilfestellungen und Tipps.
https://www.sicher-im-netz.de/dsin-für-unternehmen
Cyberschutz Rheinland-Pfalz
Der Verfassungsschutz Rheinland-Pfalz unterstützt die Cyber- und IT-Sicherheit rheinland-pfälzischer Unternehmen ab sofort mit einem neuen Angebot. Das Sicherheitsportal Cyberschutz Rheinland-Pfalz bündelt Informationen zu Cyberangriffen und zu konkreten technischen Absicherungsmöglichkeiten zum Schutz vor Cyberspionage und Cybersabotage. Das Angebot richtet sich insbesondere an kommunale Unternehmen der kritischen Infrastruktur. Weitere Informationen dazu in der Pressemeldung.
Schutz vor Cyberangriffen im Video erklärt
Cyberschutz Rheinland-Pfalz
Haben Sie Fragen zum Cyberschutz Rheinland-Pfalz?
Sie erreichen den Cyberschutz per E-Mail an cyberschutz[at]mdi.rlp.de.
Für einen Zugang benötigen wir eine Funktionsadresse ohne personenbezogenen Daten wie zum Beispiel it@ihrefirma.de.
Cyberrisiken mit realen Folgen
Ohne E-Mail und Internet, eigenem Firmennetz, Smartphones und PCs geht nichts. Die Digitalisierung der Wirtschaft ist im vollen Gange. Für Unternehmen wächst damit auch die Gefahr, Opfer eines Cyberangriffs zu werden. Die Angriffe können reale Folgen haben.
Häufig gestellte Fragen
Cyberschutz Rheinland-Pfalz
Wie funktioniert der Cyberschutz Rheinland-Pfalz? Wie bekommt man Zugang? Und welche Informationen erhält der Verfassungsschutz selbst?
Die FAQ geben Antworten auf die wichtigsten Fragen. Mehr Informationen dazu hier.
https://mdi.rlp.de/de/unsere-themen/verfassungsschutz/aufgabenfelder-und-extremismus-bereiche/cyberschutz/