Cybercrime

aus polizeilicher Sicht

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Marcel Christoph, KHK

SN4C

CyberCrime
Competence
Center
Sachsen

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Haben wir eigentlich ein Problem?

SN4C CyberCrime Competence Center Sachsen

Im Notbetrieb: Cyberangriff auf Stadtwerke Pirna

von MDR SACHSEN Stand: 06. Dezember 2021, 20:15 Uhr

Kriminelle haben vergangene Woche die Computer der Stadtwerke Pirna angegriffen. Ein Zugriff auf einen Teil der Systeme ist nicht möglich, so das Unternehmen, die Versorgungssicherheit sei jedoch gewährleistet.

Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf

Eine Patientin stirbt, nachdem ihr Rettungswagen wegen einer Cyberattacke umgeleitet werden musste. Der Fall illustriert die wachsenden IT-Risiken.

Christof Kerkmann Lars-Marten Nagel

18.09.2020 - 13:05 Uhr • Kommentieren • 12 x geteilt

Spreadshirt: Kundendaten von Hackern erbeutet

Hacker haben sich Zugriff auf Kundendaten verschafft – ändern Sie besser sofort Ihr Passwort.

13.07.2021, 12:27 Uhr von Daniela Leistikow

Die Firma Spreadshirt aus Leipzig bedruckt T-Shirts nach Wunsch. Doch wer dort schon mal bestellt hat, dessen Kontodaten und Passwörter sind nun in Gefahr.

Cyberangriff auf ViaSat mittels schädlichem Firmware-Update führt zu Kollateralschäden bei Windkraftanalagen

Durch den Ausfall der Endgeräte kam es in Folge auch zum flächendeckenden Ausfall des Satellitennetzwerkes KA-SAT, primär in der Ukraine aber auch in Europa. Während der Angriff vermeintlich auf die Ukraine abzielte, hatte der Ausfall KA-SATs auch Auswirkungen auf zahlreiche europäische Windkraftanlagen.

PKS – 2021 (2020)

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

- Bundesweit: **124.137** Fälle von Cybercrime im engeren Sinne (108.474)

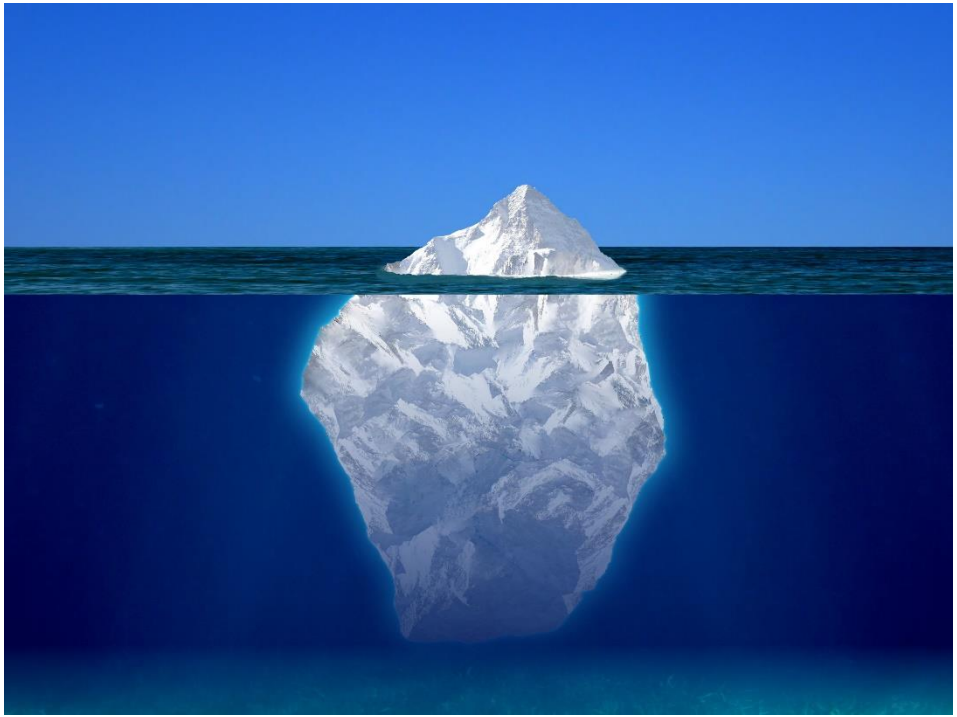
  383.469 Fälle mit dem Tatmittel Internet (320.323)

- Freistaat Sachsen: **3.325** Fälle von Cybercrime im engeren Sinne (3.115)

  13.156 Fälle mit dem Tatmittel Internet (10.770)

Was wir wissen

LANDES-
KRIMINALAMT
POLIZEI
Sachsen



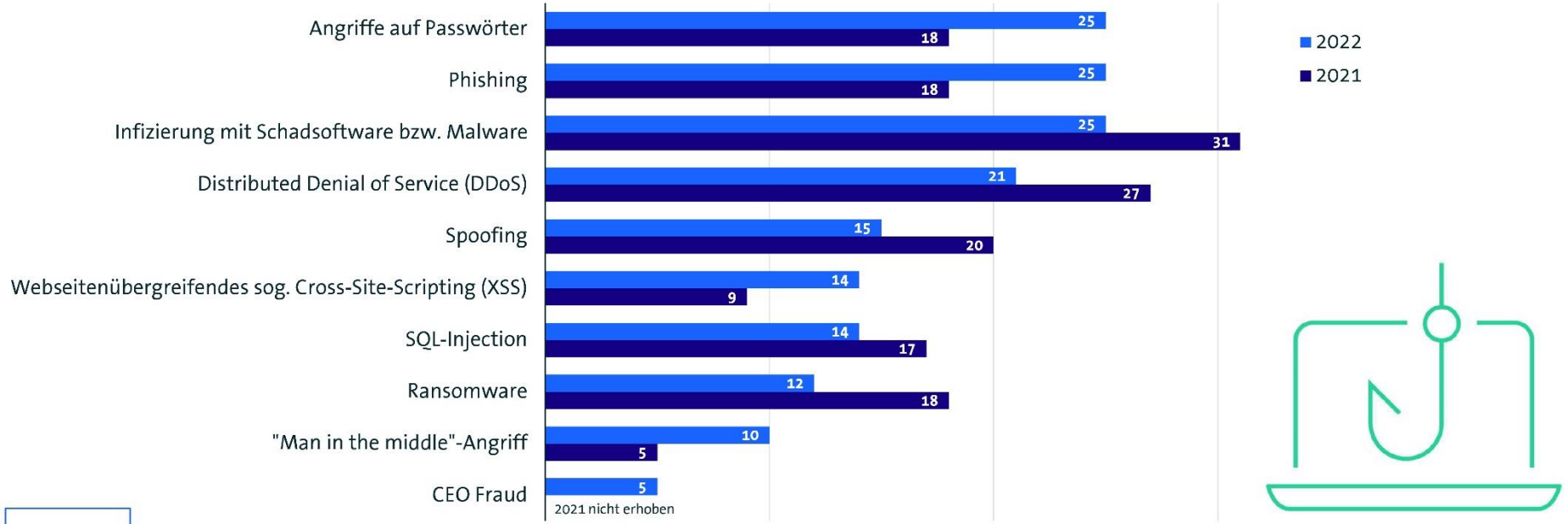
Hellfeld

Dunkelfeld

SN4C CyberCrime Competence Center Sachsen

Häufigere Schäden durch Phishing & Passwortdiebstahl

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



in Prozent

Basis: Alle befragten Unternehmen (n=1.066) | 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?

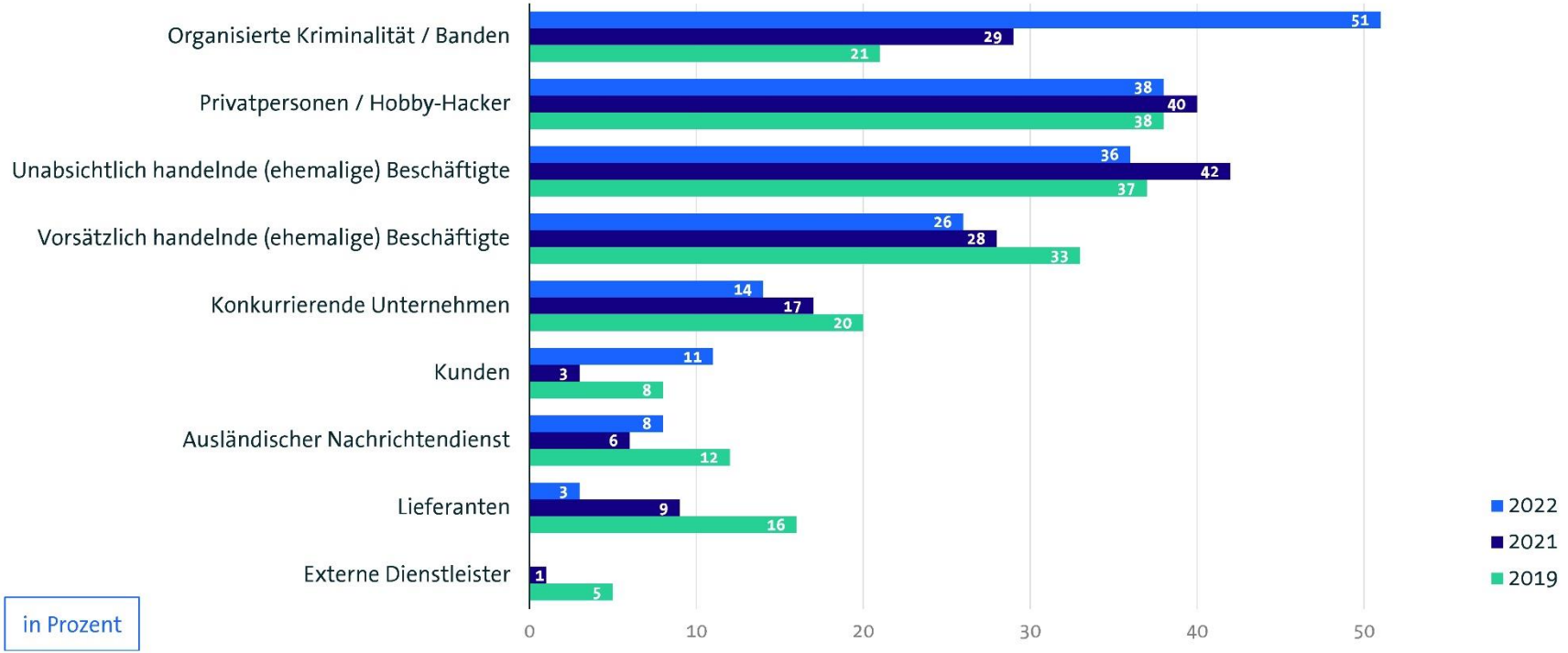
Schaden durch...	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadenssummen in Mrd. Euro (2017)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	41,5	61,9	13,5	5,3
Erpressung mit gestohlenen 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**

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

Attacken auf die Wirtschaft werden professioneller

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



in Prozent

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

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Ja haben wir!

Haben **wir** eigentlich ein **Problem**?

SN4C CyberCrime Competence Center Sachsen

Phänomene

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Erpressung - Ransomware
- Erpressung - DDoS-Angriffe
- Diebstahl digitaler Identitäten und Phishing
- Betrug - Business E-Mail Compromise
- Cybercrime as a Service

SN4C CyberCrime Competence Center Sachsen

Erpressung - Ransomware

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

SZ+ BSI warnt

Schadsoftware Emotet bringt weiter Daten in Gefahr

14. Januar 2020 um 20:24 Uhr | Lesedauer: Eine Minute

Der Trojaner Emotet verbreitet sich per E-Mail. Foto: Andrea Warnecke/dpa-tmn/Andrea Warnecke

SN4C CyberCrime Competence Center Sachsen

Erpressung - Ransomware

LANDES-KRIMINALAMT | POLIZEI Sachsen

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

SN4C CyberCrime Competence Center Sachsen

Erpressung - Ransomware

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

Corona-Schutz am Arbeitsplatz - Bundesministerium für Gesundheit

Von: Bundesministerium für Gesundheit <poststelle@bundesministerium-gesundheit.com>
An: [redacted]
Datum: 09.09.2020 9:19

Corona-Arbeitsschutzregeln

Bundesministerium
für Gesundheit

Sehr geehrte Damen und Herren,

Die Gesundheitsministerinnen und -minister der EU haben sich heute zu den EU-weiten Regeln für Corona-Schutz am Arbeitsplatz ausgetauscht. Das Bundesministerium für Gesundheit hat eine neue offizielle Corona-Arbeitsschutzregel vorgelegt. Ab sofort gelten weitere verbindliche Regeln für Corona-Schutz am Arbeitsplatz.

Wir bitten Sie, sich die neuen Regelungen gründlich durchzulesen und das

SN4C CyberCrime Competence Center Sachsen

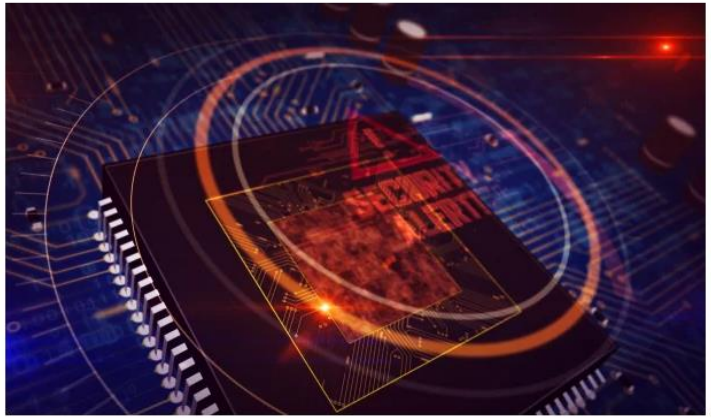
Neues Geschäftsfeld: Data-Leak

LANDES-KRIMINALAMT | POLIZEI Sachsen

Militärische Dokumente nach Ransomware-Angriff geleakt

Weil ein Unternehmen bei einer Ransomware-Erpressung nicht zahlte, sind geheime Papiere wie Spezifikationen für ein Mörserabwehrsystem im Netz aufgetaucht.

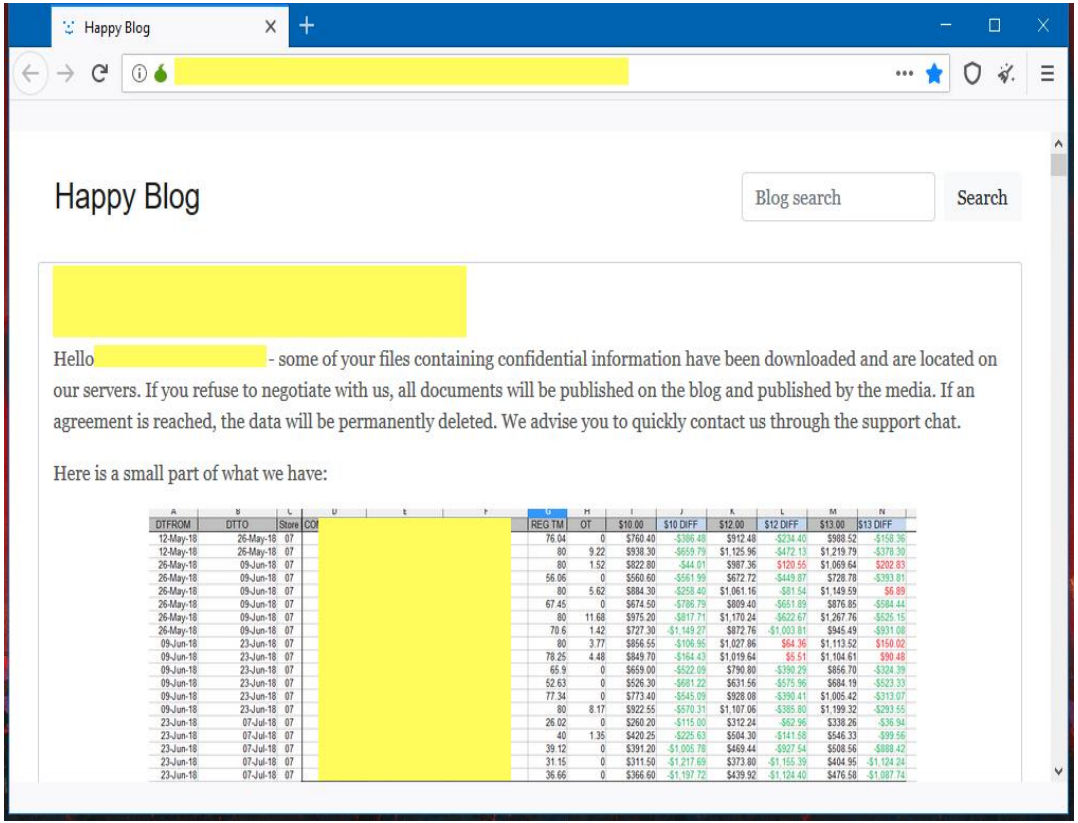
Lesezeit: 1 Min. In Pocket speichern 89



(Bild: Skorzewiak/Shutterstock.com)

12.04.2020 16:11 Uhr | Security

Von Markus Montz



DTFROM	DTTO	Store	COI	REG TM	OT	$10.00	$10 DIFF	$12.00	$12 DIFF	$13.00	$13 DIFF
12-May-18	26-May-18	07		76.04	0	$760.40	-$386.48	$912.48	-$234.40	$988.52	-$158.36
12-May-18	26-May-18	07		80	9.22	$936.30	-$659.79	$1,125.96	-$472.13	$1,219.79	-$378.30
26-May-18	09-Jun-18	07		80	1.52	$822.80	-$44.01	$987.36	$120.55	$1,069.64	$202.83
26-May-18	09-Jun-18	07		56.06	0	$560.60	-$561.99	$672.72	-$449.87	$728.78	-$393.81
26-May-18	09-Jun-18	07		80	5.62	$884.30	-$258.40	$1,061.16	-$81.54	$1,149.59	$6.89
26-May-18	09-Jun-18	07		67.45	0	$674.50	-$786.79	$809.40	-$651.89	$876.85	-$584.44
26-May-18	09-Jun-18	07		80	11.68	$975.20	-$817.71	$1,170.24	-$622.67	$1,267.76	-$525.15
26-May-18	09-Jun-18	07		70.6	1.42	$727.30	-$1,149.27	$872.76	-$1,003.81	$945.49	-$931.08
09-Jun-18	23-Jun-18	07		80	3.77	$856.55	-$106.95	$1,027.86	$64.36	$1,113.52	$150.02
09-Jun-18	23-Jun-18	07		78.25	4.48	$849.70	-$164.43	$1,019.64	$5.51	$1,104.61	$90.48
09-Jun-18	23-Jun-18	07		65.9	0	$659.00	-$522.09	$790.80	-$390.29	$856.70	-$324.39
09-Jun-18	23-Jun-18	07		52.63	0	$526.30	-$681.22	$631.56	-$575.96	$684.19	-$523.33
09-Jun-18	23-Jun-18	07		77.34	0	$773.40	-$545.09	$928.08	-$390.41	$1,005.42	-$313.07
09-Jun-18	23-Jun-18	07		80	8.17	$922.55	-$570.31	$1,107.06	-$385.80	$1,199.32	-$293.55
23-Jun-18	07-Jul-18	07		26.02	0	$260.20	-$115.00	$312.24	-$62.96	$338.26	-$36.94
23-Jun-18	07-Jul-18	07		40	1.35	$420.25	-$225.63	$504.30	-$141.58	$546.33	-$99.56
23-Jun-18	07-Jul-18	07		39.12	0	$391.20	-$1,005.78	$469.44	-$927.54	$508.56	-$888.42
23-Jun-18	07-Jul-18	07		31.15	0	$311.50	-$1,217.69	$373.80	-$1,155.39	$404.95	-$1,124.24
23-Jun-18	07-Jul-18	07		36.66	0	$366.60	-$1,197.72	$439.92	-$1,124.40	$476.58	-$1,087.74

Erpressung - DDoS-Angriffe

LANDES-KRIMINALAMT | POLIZEI Sachsen

Kaspersky-Studie

Dramatische Zunahme der DDoS-Angriffe

von Jens Stark - 18.02.2022

Foto: Fortinet

Noch nie hat der Security-Hersteller Kaspersky Lab anhand von Telemetriedaten so viele DDoS-Angriffe feststellen müssen wie im vierten Quartal 2021.

Erpressung - DDoS-Angriffe

LANDES-KRIMINALAMT | POLIZEI Sachsen

Von: Fancy Bear <abc123@startmail.com>
Gesendet: Mittwoch, 12. August 2020 14:30
An:
Betreff: DDoS attack on your network

We are the Fancy Bear and we have chosen XXX as target for our next DDoS attack.

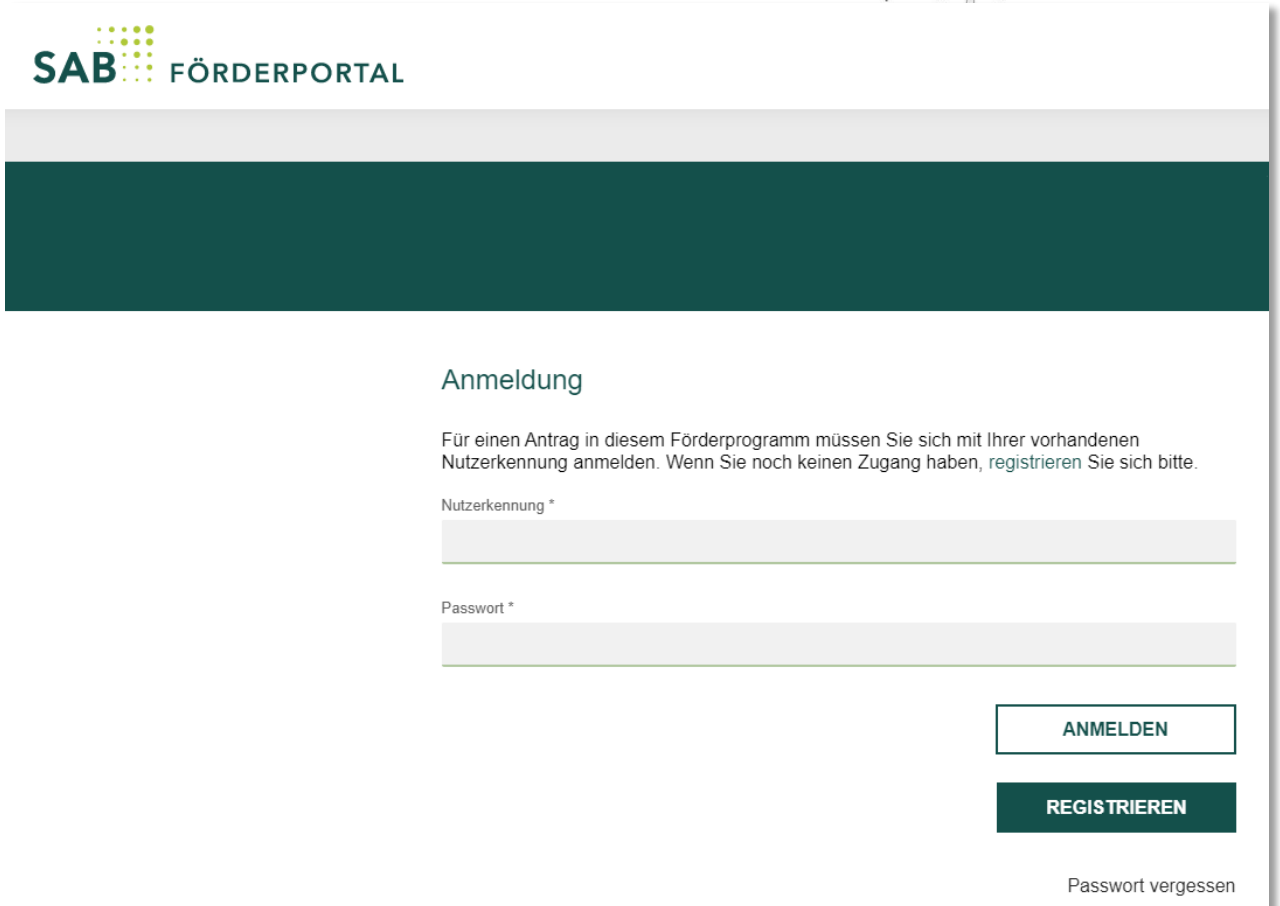
Please perform a google search for "Fancy Bear" to have a look at some of our previous work.

Your network will be subject to a DDoS attack starting at Wednesday (within 7 days). (This is not a hoax, and to prove it right now we will start a small attack on one of your IPs (212.149.50.15) that will last for 30 minutes. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.)

What does this mean? This means that your website and other connected services (like online banking) will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers.

How do I stop this? We will refrain from attacking your servers for a small fee. The current fee is 15 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth

Diebstahl digitaler Identitäten und Phishing



Diebstahl digitaler Identitäten und Phishing

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Fr 03.04.2020 02:32

Bauer <kurzarbeitergeld@arbeitsagentur.de>

Kurzarbeitergeld

An [redacted]

Sehr geehrter [redacted]

wie Sie schon vielleicht in den Medien gelesen haben, ist es zur Zeit möglich Ihre Mitarbeiter in Kurzzeitarbeit zu schicken.
Dies beudeutet, dass wir als Arbeitsagentur Ihnen Ihre Lohnausgaben an Ihre Mitarbeiter erstatten.
Ausserdem helfen wir Ihnen Zuschüsse für Ihr Unternehmen beim Bund und der Landesbank zu beantragen.
Sollten Sie diese Hilfen in Anspruch nehmen wollen, brauchen wir von Ihnen folgende Angaben:

- Name und Anschrift des Unternehmens
- Name und Andresse des Firmeninhabers
- Steuernummer des Unternehmens (falls vorhanden)
- Steuer ID Firmeninhabers
- Personalausweis oder Passnummer des Firmeninhabers
- Betriebsnummer (falls vorhanden)
- Anzahl der Mitarbieter
- Die Namen und Sozialversicherungsnummern der Mitarbeiter

Bitte senden Sie die Daten an: kurzarbeitergeld@arbeitsagentur-service.de

SN4C CyberCrime Competence Center Sachsen

Betrug - Business E-Mail Compromise

LANDES-KRIMINALAMT | POLIZEI Sachsen

Von: [redacted]@[redacted] <[redacted]@mail.com>
Gesendet: Montag, [redacted] März 2017 14:03
An: [redacted]
Betreff: Re: AW: AW: AW: Wichtig

7

Hallo Frau [redacted]

Ich bitte Sie eine Zahlung mit der Summe von 392 128,00- Euro. mit dem heutigen Wertstellungsdatum von der Commerzbank an die folgende IBAN auszuführen :

Achten Sie auf die richtige Schreibweise des Empfängers, insbesondere das Komma und der Punkt. FASTER DEVELOPMENT CO. , LIMITED

ZAHLUNGSEMPFÄNGER: FASTER DEVELOPMENT CO. , LIMITED
KONTONUMMER: OSA 7559 0520 3435 801
SWIFT: CMBCCNBS008
ADRESSE : 17/F MERCHANTS BANK TOWER NO.7088 SHENNAN BOULEVARD SHENZHEN 518040 P.R ,CHINE
BANK: CHINA MERCHANTS BANK

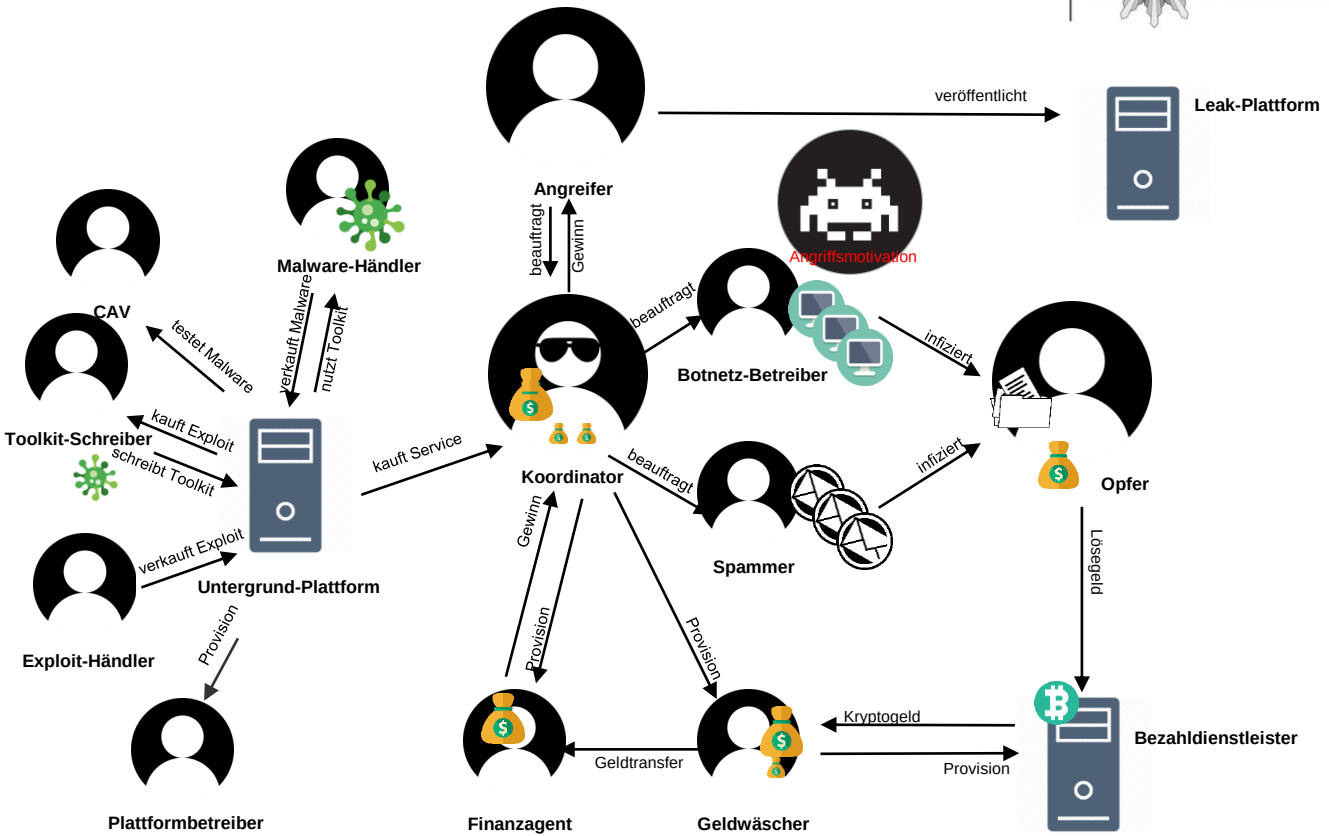
Betrag : 392 128,00 - Euro.
Datum : 06/03/2017
Zahlungszweck: PAYMENT FOR GOODS

Mit freundlichen Grüßen
[redacted]

SN4C CyberCrime Competence Center Sachsen

Cybercrime as a Service

gbhackers.com/cybercrime-as-a-service-ddos-attack/


veröffentlicht
Leak-Plattform
Angreifer
beauftragt
Gewinn
Angriffsmotivation
Malware-Händler
CAV
testet Malware
verkauft Malware
nutzt Toolkit
Toolkit-Schreiber
kauft Exploit
schreibt Toolkit
kauft Service
Koordinator
beauftragt
Botnetz-Betreiber
infiziert
Opfer
beauftragt
Spammer
infiziert
Lösegeld
verkauft Exploit
Untergrund-Plattform
Exploit-Händler
Provision
Gewinn
Provision
Provision
Plattformbetreiber
Finanzagent
Geldtransfer
Geldwäscher
Kryptogeld
Provision
Bezahldienstleister

Kurzes Fazit

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- agile Phänomenlage mit sich ständig anpassenden Vorgehensweisen
- sehr hohes Dunkelfeld (90%)
- Professionalität der Täter nimmt ständig zu
- Cybercrime schafft und basiert auf kriminellen Wertschöpfungsketten
- Ransomware als größte Bedrohung für Wirtschaftsunternehmen
- Täter sind global vernetzt, agieren international, arbeitsteilig und höchst orgainisiert

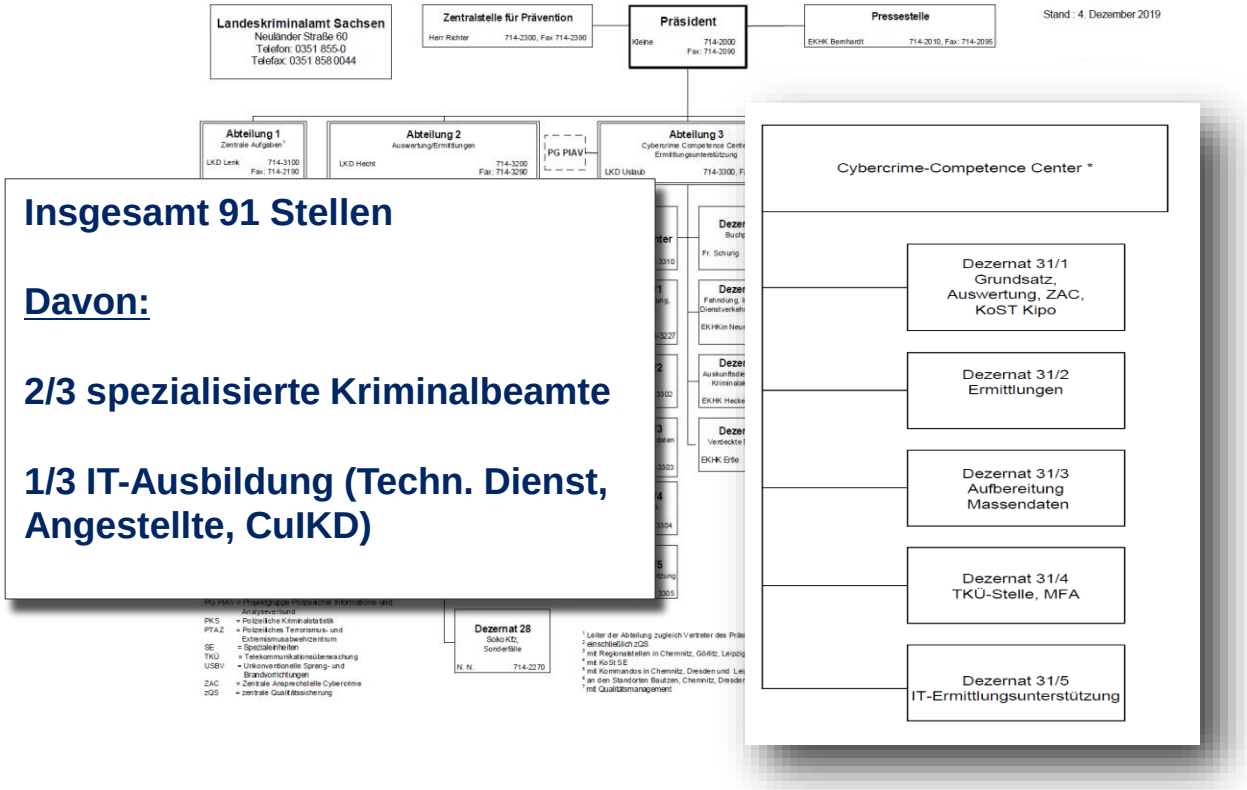
SN4C CyberCrime Competence Center Sachsen

Was **machen** wir?

Cybercrime-Competence Center

LANDES-
KRIMINALAMT

POLIZEI
Sachsen



Insgesamt 91 Stellen

<u>Davon:</u>

2/3 spezialisierte Kriminalbeamte

1/3 IT-Ausbildung (Techn. Dienst, Angestellte, CulKD)

SN4C CyberCrime Competence Center Sachsen

Zentrale Ansprechstelle Cybercrime

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- **Ansprechpartner** zum Thema Cybercrime für Unternehmen, Verbände und Behörden in Sachsen
- Nimmt **Sicherheitsvorfälle** mit Bezug zu Cybercrime auf (telefonisch oder per Mail) und leitet weitere **(Sofort-) Maßnahmen** ein
- **Berät** zum weiteren Vorgehen (Gefahrenabwehr und Strafverfolgung) nach Sicherheitsvorfällen mit Cybercrime Bezug
- **Förderung** der vertrauensvollen Zusammenarbeit zwischen Wirtschaftsunternehmen, Verbänden, Behörden und der Polizei

SN4C CyberCrime Competence Center Sachsen

Zentrale Ansprechstelle Cybercrime
Erreichbarkeit

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

E-Mail:	zac.lka@polizei.sachsen.de
Telefon:	+49 351 855 3226
Internet:	www.polizei.sachsen.de

SN4C CyberCrime Competence Center Sachsen

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Danke für Ihre Aufmerksamkeit!

Wie können Sie Ihr Unternehmen schützen?

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Präventive Maßnahmen - Awareness (Achtsamkeit)

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

- Bewusstsein gegenüber der Gefahren durch Cybercrime
- Auseinandersetzung mit Sicherheitsvorfällen – Incident Response
- Verantwortung für die bei Ihnen gespeicherten Daten, auch Kundendaten
- Backup nach der 3-2-1 Regel
- Kosten für Schutzmaßnahmen < Kosten eines Cyber-Angriffs

SN4C CyberCrime Competence Center Sachsen

Präventive Maßnahmen - Schutz für Unternehmen

LANDES-KRIMINALAMT | POLIZEI Sachsen

- Auseinandersetzung mit der Thematik:
  - Internetseite der Allianz für Cyber-Sicherheit (BSI)
  - Branchenverbände z.B. ASW, IHK, HWK, Bitkom etc.
  - Flyer „Cyberattacken gegen Unternehmen“

    bka.de/flyercyberattackeunternehmen