LANDESPRÄVENTIONSRAT

Freistaat SACHSEN

Fachtag 2021

Dokumentation

Landes Präventionsrat Sachsen
Einer mit Allen!
www.lpr.sachsen.de

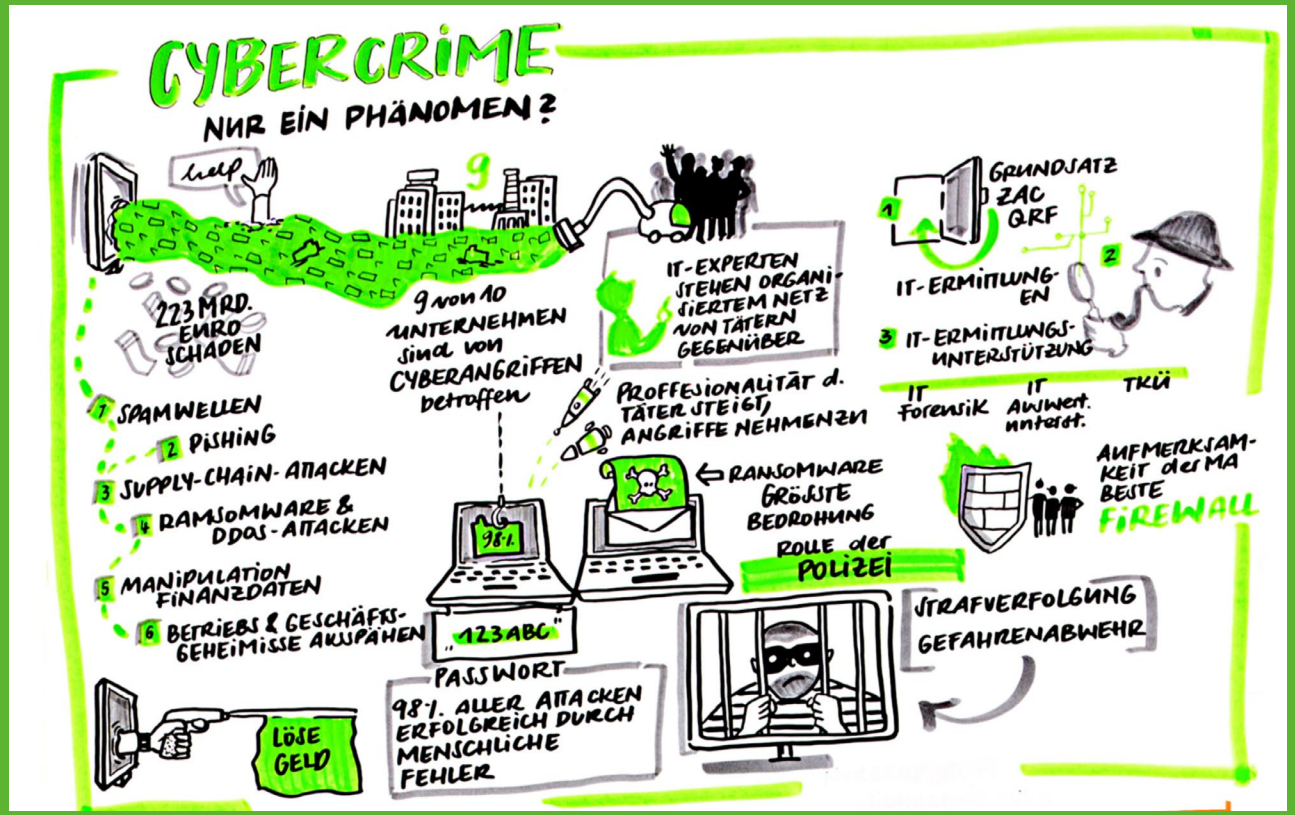
ASSKomm
Allianz Sichere Sächsische Kommunen

B3 INSTITUT FÜR BERATUNG, BEGLEITUNG UND BILDUNG e.V.

Fachtag 2021

Kommunale Prävention – Reagieren, bevor es zu spät ist

Cybercrime – nur ein Phänomen?



Referent Henrik Hohenlohe

Landeskriminalamt Sachsen

Cybercrime

Nur ein Phänomen?

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Henrik Hohenlohe, Kriminaldirektor

SN4C

CyberCrime
Competence
Center
Sachsen

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

EXKLUSIV Hacker verschlüsseln Daten

Mehr als 100 Behörden erpresst

Stand: 29.06.2021 05:00 Uhr

Laut einer Umfrage von *BR* und "Zeit Online" ist es Tätern in mehr als 100 Fällen gelungen, IT-Systeme von Behörden und öffentlichen Einrichtungen zu verschlüsseln. Die Bundesregierung hat über die Fälle keinen Überblick.

Von Maximilian Zierer und Hakan Tanriverdi, BR

Nach Hackerangriff

Vorlesen

Katastrophenfall ausgerufen: Landkreis Anhalt-Bitterfeld auch nächste Woche nicht arbeitsfähig

von MDR SACHSEN-ANHALT

TEILEN VIA

Stand: 09. Juli 2021, 14:02 Uhr

Der Landkreis Anhalt-Bitterfeld hat nach einem Hackerangriff den Katastrophenfall ausgerufen. Die Kreisverwaltung ist auch in der kommenden Woche nicht arbeitsfähig, wie sie mitgeteilt hat. Nach MDR-Informationen gibt es eine Lösegeldforderung gegen den Kreis. Derzeit können keine Dienstleistungen für die Bürger angeboten werden.

Kein Publikumsverkehr: Die Kreisverwaltung Anhalt-Bitterfeld ist nicht arbeitsfähig.

Bildrechte: MDR/Michael Rosebrock

PKS – 2020 (2019)

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

- Bundesweit: **108.474** Fälle von Cybercrime im engeren Sinne (100.514)

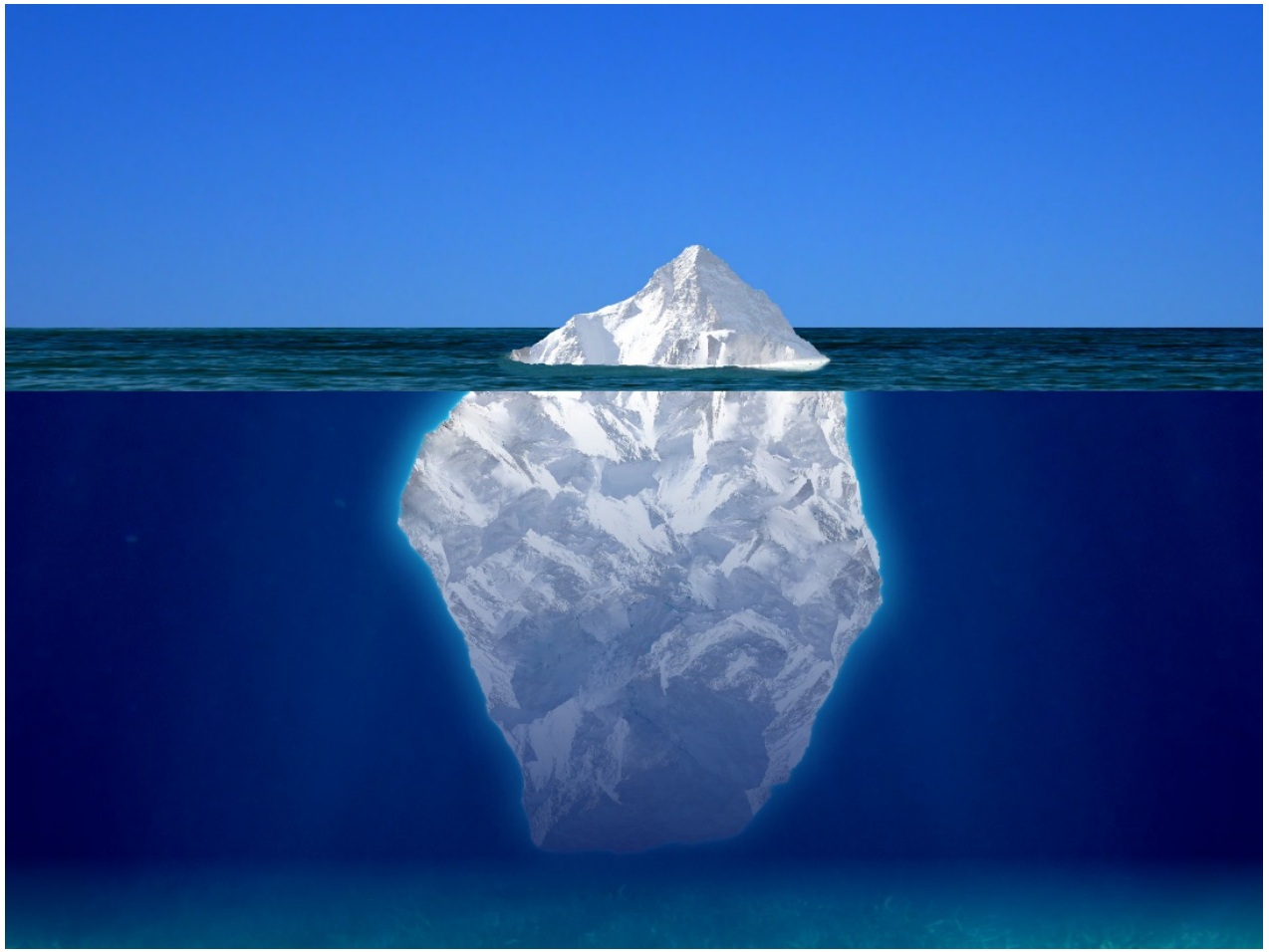
  320.323 Fälle mit dem Tatmittel Internet (294.665)

- Freistaat Sachsen: **3.120** Fälle von Cybercrime im engeren Sinne (2.655)

  10.600 Fälle mit dem Tatmittel Internet (8.212)

Was wir wissen

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

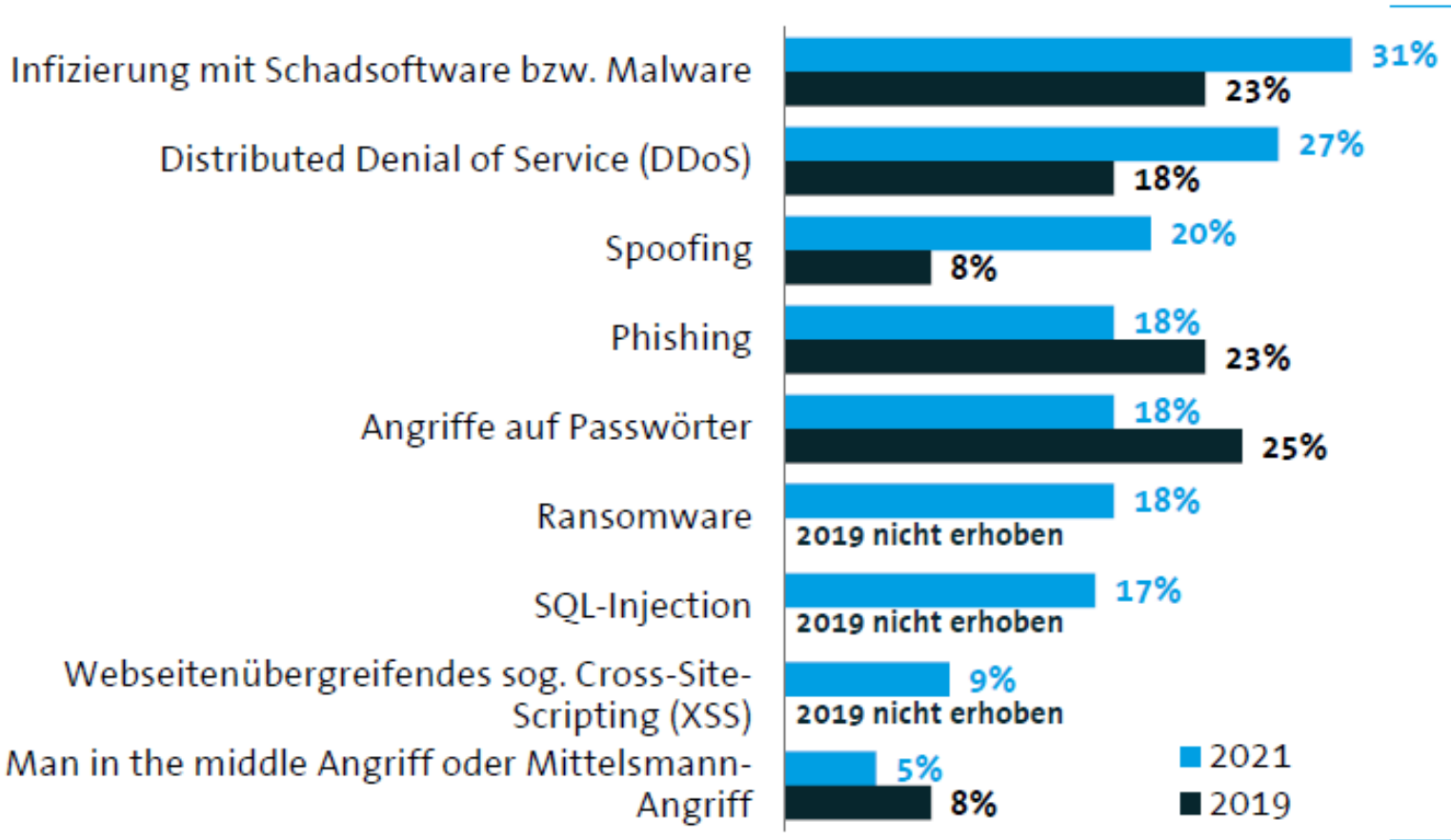


Hellfeld

Dunkelfeld

Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

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



Cyberangriffe haben bei

86%

der Unternehmen einen Schaden verursacht – **2019** waren es erst **70%**.

Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070); Mehrfachnennungen in Prozent, 2019: innerhalb der letzten zwei Jahre | Quelle: Bitkom Research 2021

bitkom

Schäden steigen auf 223 Mrd. Euro: Erpressung und Systemausfälle als treibende Faktoren (+358% ggü. 2019)

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

Schaden durch…	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadenssummen in Mrd. Euro (2017)	Schadenssummen in Mrd. Euro (2015)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	**61,9**	13,5	5,3	7,2
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	**24,3**	5,3	0,7	1,5
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	**17,1**	4,4	3,2	2,0
Patentrechtsverletzungen (auch schon vor der Anmeldung)	**30,5**	14,3	7,7	9,4
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	**29,0**	11,1	8,6	6,4
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	**22,7**	11,1	3,5	11,5
Imageschaden bei Kunden oder Lieferanten/Negative Medien-berichterstattung	12,3	9,3	7,7	5,9
Kosten für Ermittlungen und Ersatzmaßnahmen	13,3	18,3	10,6	-
Kosten für Rechtsstreitigkeiten	12,4	15,6	5,5	6,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	2,2	0,9
Sonstige Schäden	0	<0,1	<0,1	0,1
Gesamtschaden pro Jahr	**223,5**	**102,9**	**54,8**	**51,2**

Basis: Selbsteinschätzung aller befragten Unternehmen, die in den letzten 12 Monaten (vor 2021: in den letzten 2 Jahren) von Diebstahl, Industriespionage oder Sabotage betroffen waren (2021: n=935; 2019: n=801; 2017: n=571; 2015: n=550) | Quelle: Bitkom Research 2021

bitkom

Ja haben wir!

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

Aktuelle Phänomene

LANDES-
KRIMINALAMT

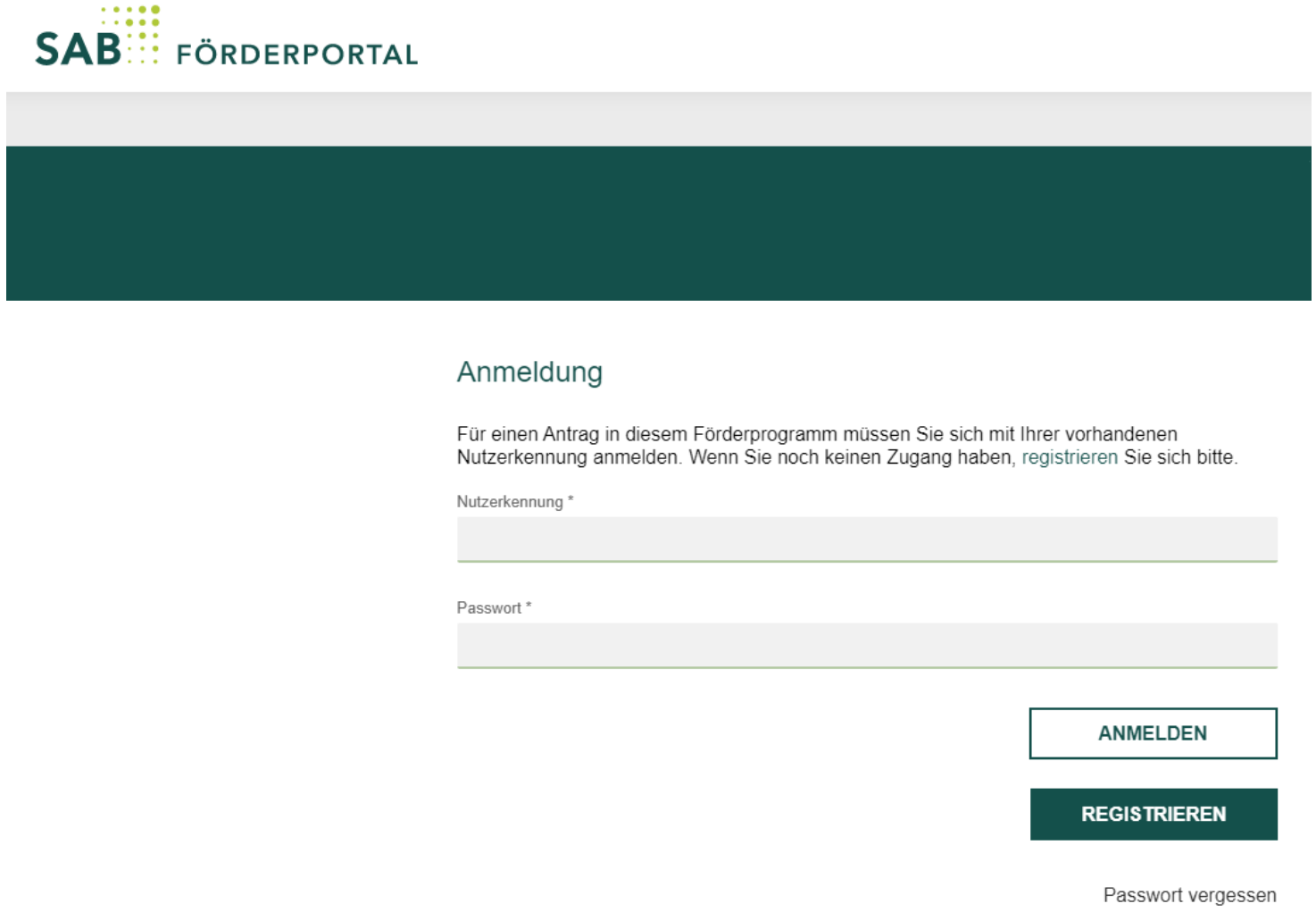
POLIZEI
Sachsen

- SPAM-Wellen
- Phishing und Identitätsdiebstahl
- Business Email Compromise / Supply-Chain-Attacken
- Erpressung mittels Ransomware oder DDoS-Attacken
- Manipulation von Konto- und Finanzdaten
- Erlangung von Betriebs- und Geschäftsgeheimnissen

Phishing

LANDES-
KRIMINALAMT

POLIZEI
Sachsen



DDoS-Erpressung

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 it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

The fee will increase by 10 Bitcoin for each day after deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: 1ACR27Hf2AW7zzYbiR28kAJwYZunD3dTMr

Once you have paid we will automatically get informed that it was your payment.

Please note that you have to make payment before the deadline or the attack WILL start!

What if I don't pay?

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do, there's no counter measure to this, uur attacks are extremely powerful - sometimes over 2 Tbps per second, so you will only end up wasting more money trying to find a solution (Cloudflare, Incapsula and similar services are useless). We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

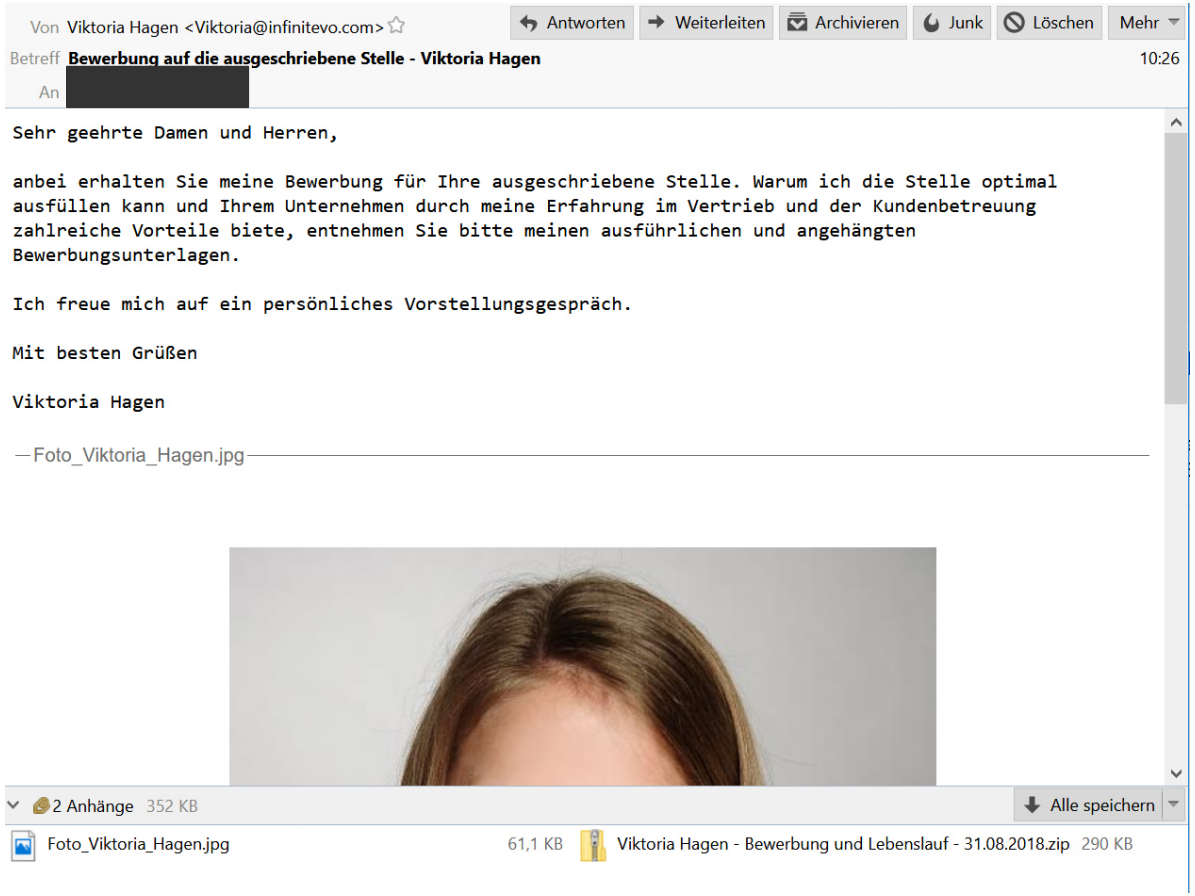
Once you have paid we won't start the attack and you will never hear from us again. Please note that no one will find out that you have complied.

SN4C CyberCrime Competence Center Sachsen

Digitale Erpressung mittels Verschlüsselungstrojanern

LANDES-
KRIMINALAMT

POLIZEI
Sachsen



SN4C CyberCrime Competence Center Sachsen

Digitale Erpressung mittels Verschlüsselungstrojanern

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 Dokument der neuen Corona-Arbeitsschutzregeln umgehend für alle Mitarbeiter in Ihrem Betrieb verfügbar zu machen.

Das Dokument der neuen Corona-Arbeitsschutzregeln finden Sie im Druckformat (A4) im Anhang dieser E-Mail.

Sollten Sie Fragen haben, können Sie uns Ihre Nachricht gerne an poststelle@bmg.bund(dot)de senden.

Wenn Sie die Sorge haben, sich mit dem Coronavirus infiziert zu haben: Wenden Sie sich telefonisch an Ihren Hausarzt oder wählen Sie die Nummer des ärztlichen Bereitschaftsdienstes: 116117.

Bundesministerium für Gesundheit
Dienstsitz Berlin
Friedrichstraße 108, 10117 Berlin

Anhänge:

- Bund-Arbeitsschutzregel-Corona-September.zip

SN4C CyberCrime Competence Center Sachsen

Digitale Erpressung mittels Verschlüsselungstrojanern

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

[redacted]@holidayland.de

Eingang - Posteo 09:47

Aw: Antikörpertest Coronavirus

An: [redacted]

Hallo,

Schau mal, wir müssen sicherstellen, dass dies keine Fehler enthält, bevor wir es weiterleiten. Nun sei ein Schatz und überprüfe dies für mich.

Danke schön

> Hall[redacted]Team, ich habe per Suche über Ihren Antikörpertest Coronavirus für 95EUR bzw. als Studie in Dresden gelesen. Ich selbst habe derzeit keine Symptome hatte aber im März engeren Kontakt zu Leuten mit Corona-typischen Symptomen, welche damals aber nicht mit einen PCR Test getestet wurden. Ich selbst hatte im März eine leichte Erkältung. Ich würde mich über eine Rückmeldung freuen, ob ein Antikörpertest von Ihrer Seite bei mir Sinn machen würde. Mit freundlichen Grüßen[redacted]

ZIP

DieKlage-01092
020-18...372.zip

SN4C CyberCrime Competence Center Sachsen

Digitale Erpressung mittels Verschlüsselungstrojanern

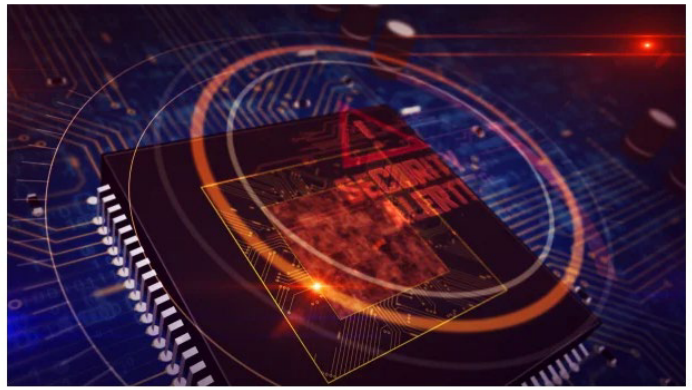
LANDES-KRIMINALAMT | POLIZEI Sachsen

Neues Geschäftsfeld: Data-Leak

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

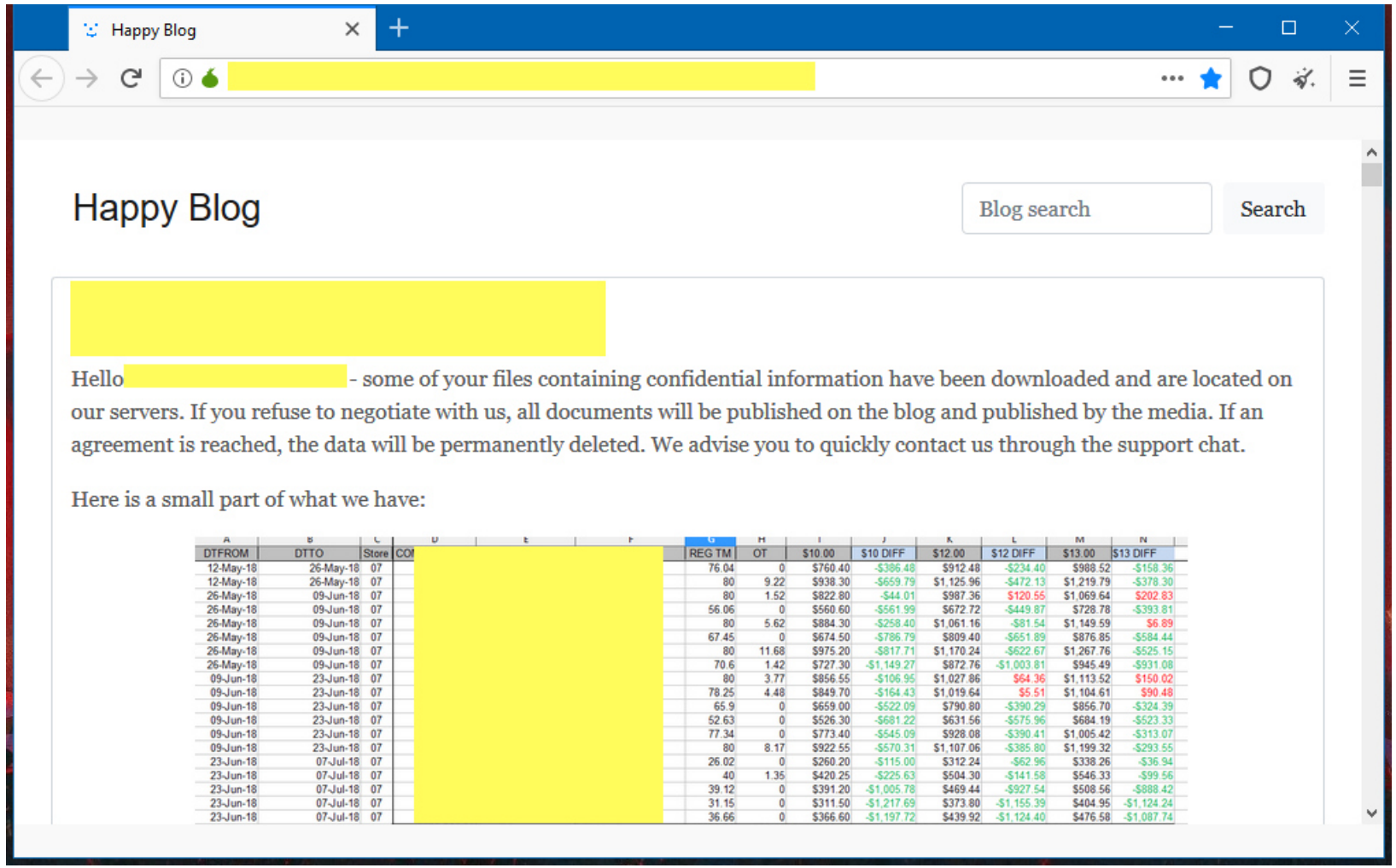


(Bild: Skorzewiak/Shutterstock.com)

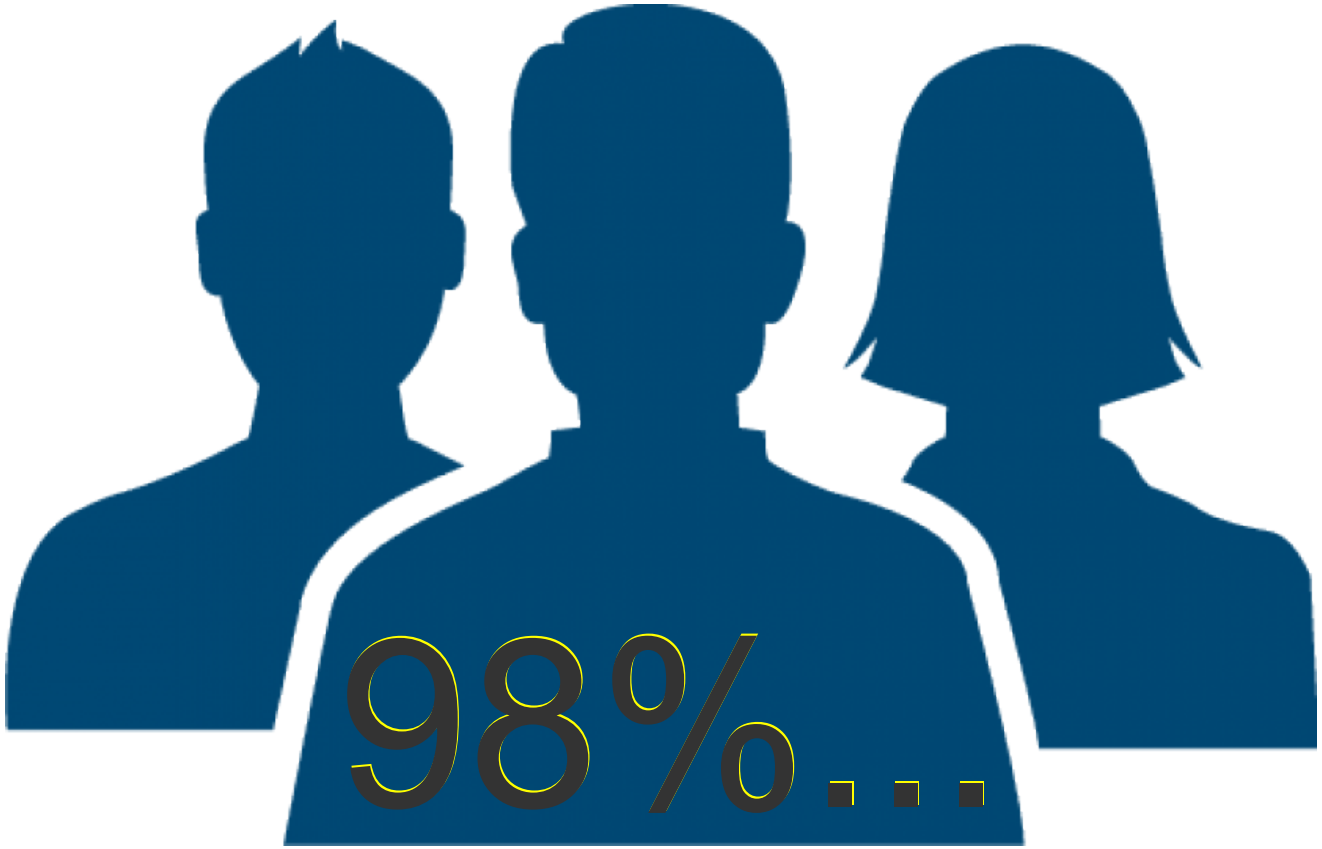
12.04.2020 16:11 Uhr | Security

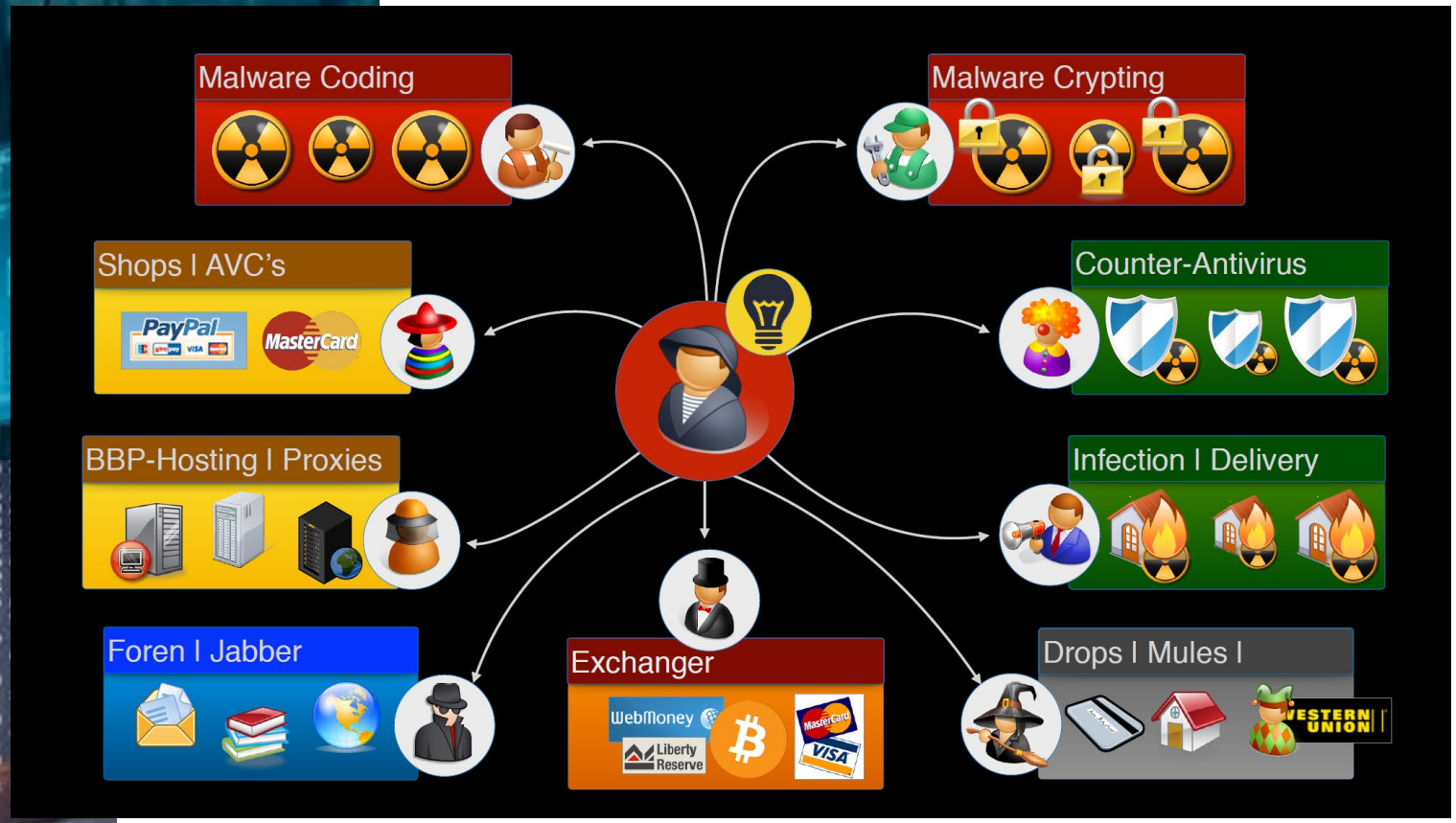
Von Markus Montz

SN4C CyberCrime Competence Center Sachsen



DTFROM	DTTO	Store	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	$938.30	-$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


98%...


Malware Coding
Malware Crypting
Shops I AVC's
PayPal
MasterCard
Counter-Antivirus
BBP-Hosting I Proxies
Infection I Delivery
Foren I Jabber
Exchanger
WebMoney
Liberty Reserve
MasterCard
VISA
Drops I Mules I
WESTERN UNION


Update
Internet Scam
Password
Crime
Trojans Horses
Virus Computer
Botnet
Malware
Firewall
Financial Fraud
Phishing
Hacker
WESTERN UNION

Geld

Politik

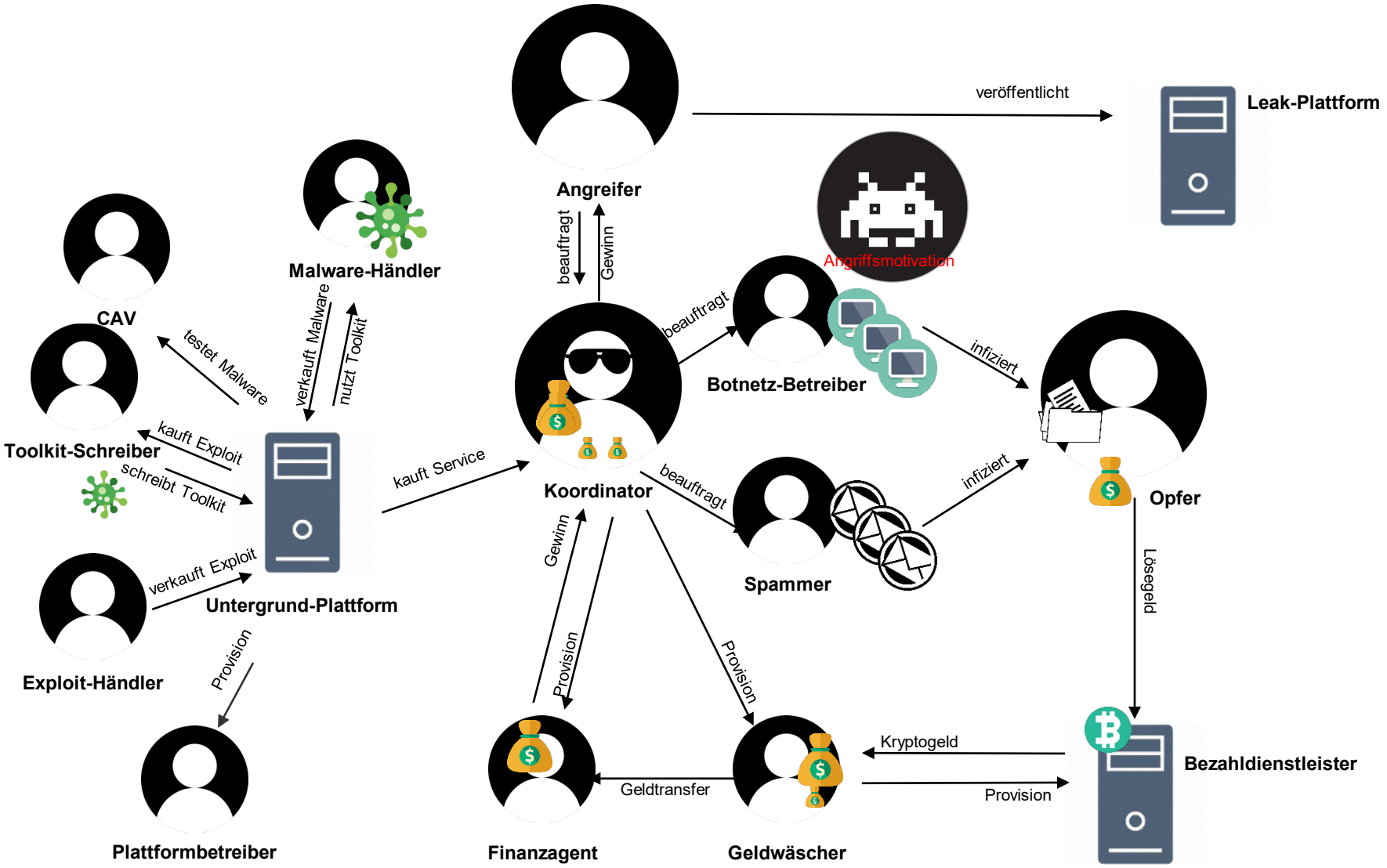
Religion

Persönliche Ziele

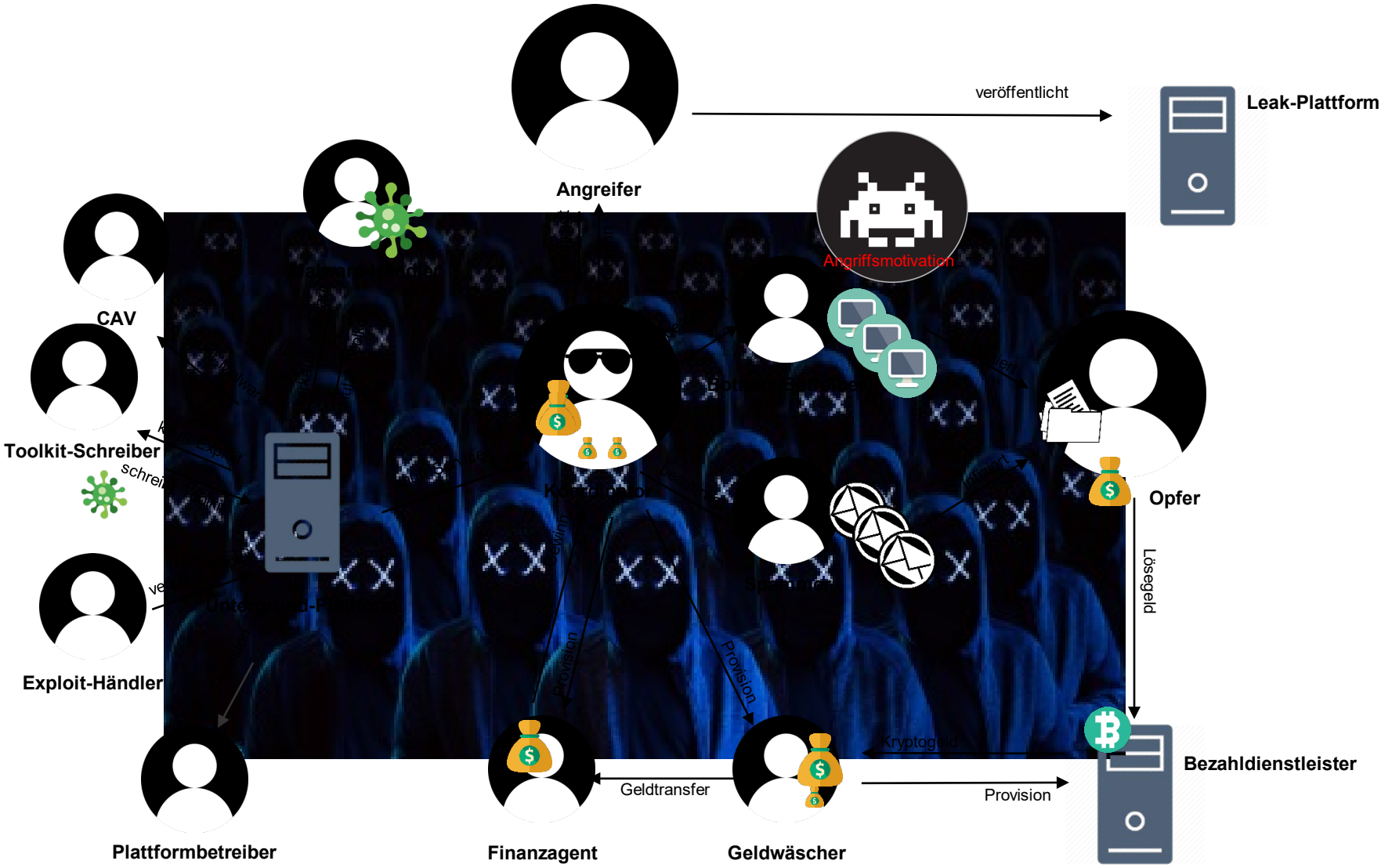
Politik

Geld

CaaS


Angreifer
veröffentlicht
Leak-Plattform
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
Kryptogeld
Provision
Bezahldienstleister
Plattformbetreiber
Finanzagent
Geldtransfer
Geldwäscher

CaaS


Angreifer
veröffentlicht
Leak-Plattform
Angriffsmotivation
CAV
Toolkit-Schreiber
Opfer
Lösegeld
Exploit-Händler
Provision
Provision
Kryptogeld
Bezahldienstleister
Geldtransfer
Provision
Plattformbetreiber
Finanzagent
Geldwäscher

Die Professionalität von Cyberkriminellen steigt weiter an.

Cybercrime erschafft und basiert auf kriminellen Wertschöpfungsketten.

Ransomware bleibt die größte Bedrohung für Wirtschaftsunternehmen.

Anzahl und auch Intensität von DDoS-Angriffen steigen rapide an.

Die Täter sind global vernetzt und agieren international, arbeitsteilig und höchst organisiert.

Die wichtigsten Schutzmechanismen gegen Cybercrime sind weiterhin sensible Internetnutzer.

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Was **machen** wir?

SN4C CyberCrime Competence Center Sachsen

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Polizei

IT-Sicherheit

SN4C CyberCrime Competence Center Sachsen

Rolle der Polizei

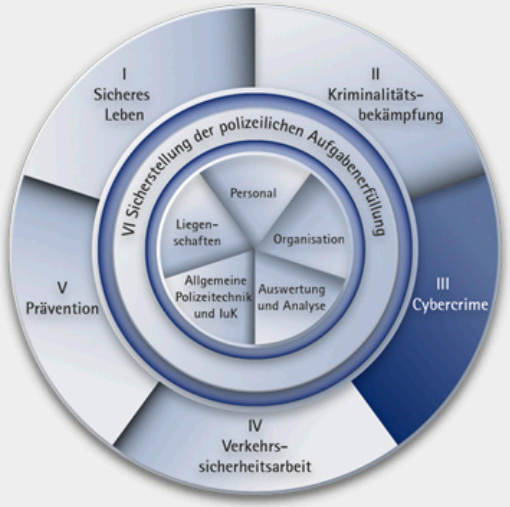
LANDES-
KRIMINALAMT

POLIZEI
Sachsen

- Strafverfolgung
  - Aufklärung einer Straftat und die Ermittlung von Tatverdächtigen
  - Erhebung des objektiven und subjektiven Tatbefundes
    - objektiv - Beweismittel (z.B. Daten, Screenshots, Daktyloskopische Spuren, DNA, Auskünfte von Providern und Geldinstituten)
    - subjektiv - Zeugenvernehmung, Beschuldigtenvernehmung
- Gefahrenabwehr
  - Abwehr und Bewältigung konkreter Gefahrenlagen

LANDES-KRIMINALAMT | POLIZEI Sachsen

Strategie der sächsischen Polizei



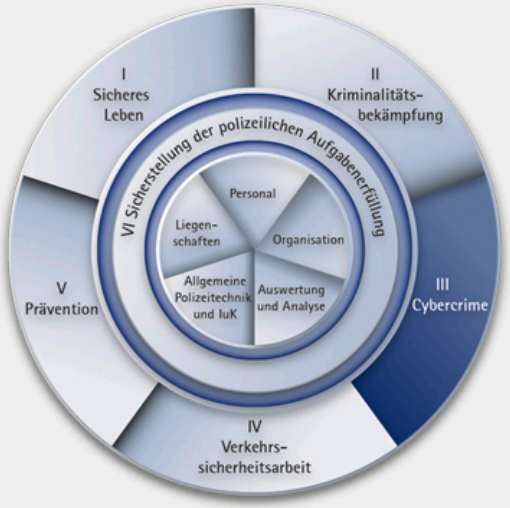
Strategiefeld III: Cybercrime

SN4C CyberCrime Competence Center Sachsen

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Strategie der sächsischen Polizei

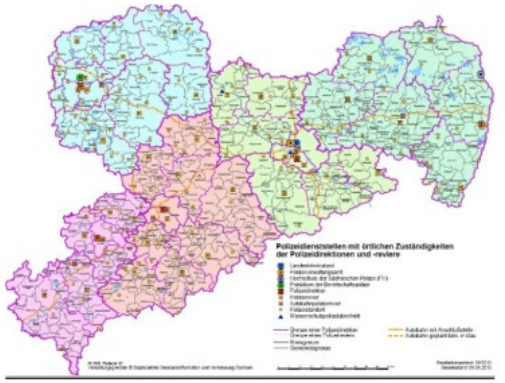


Strategiefeld III: Cybercrime

LKA:

SN4C CyberCrime Competence Center Sachsen

PDen :



Polizeidirektionen und LKA

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

**IT-Ermittlungs-
unterstützung**

IT-Ermittlungen

SN4C CyberCrime Competence Center Sachsen

Polizeidirektionen

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

IT-Ermittlungs-unterstützung

IT-Forensik

IT-Ermittlungen

SN4C CyberCrime Competence Center Sachsen

Landeskriminalamt

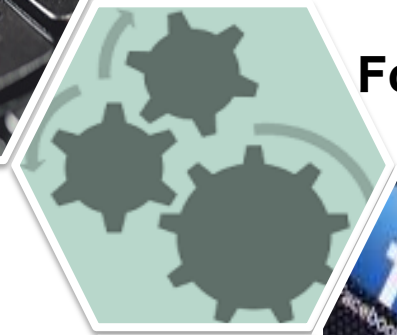
LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Grundsatz, ZAC,QRF

IT-Ermittlungen

IT-Ermittlungs-unterstützung



IT-Forensik

IT-Auswerte-unterstützung

TKÜ

SN4C CyberCrime Competence Center Sachsen

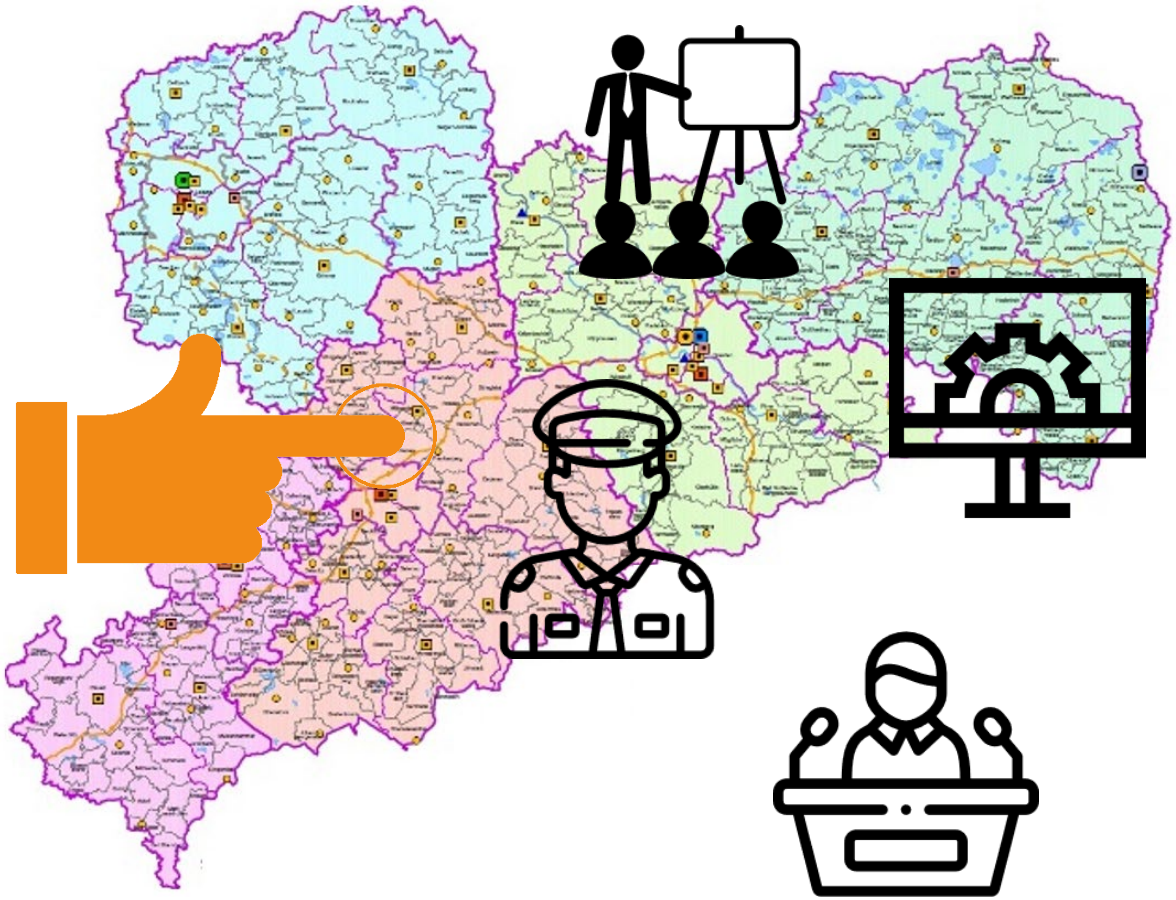
BKA

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

GENERALSTAATS-
ANWALTSCHAFT
DRESDEN

Freistaat
SACHSEN



[...]

SN4C CyberCrime Competence Center Sachsen

https://www.flaticon.com/de/kostenloses-icon/seo-training_48541

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

... und nun

gemeinsam!

SN4C CyberCrime Competence Center Sachsen

Schutz

- Erstellen und Umsetzen eines IT-Sicherheitskonzeptes, welche u.a. Maßnahmen für folgende Bereiche festlegen sollte:
  - Technische IT-Sicherheit (z.B. Firewalls, Verschlüsselung, Netztrennung etc.)
  - Organisatorische Sicherheit (z.B. Richtlinien, Notfallpläne)
  - Physische Sicherheit (z.B. Gebäudeschutz, Überwachung)
  - Personelle Sicherheit (z.B. Schulungen, Sicherheitsüberprüfungen)
- Holen Sie professionelle Hilfe und Beratung!

Awareness (Achtsamkeit)

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

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

Die Zentrale Ansprechstelle Cybercrime (ZAC)

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Kontakt:

LKA Sachsen

Neuländer Straße 60, 01129 Dresden

Telefon: 0351 855 3226

E-Mail: zac.lka@polizei.sachsen.de

SN4C CyberCrime Competence Center Sachsen

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Danke für Ihre Aufmerksamkeit!

LANDESPRÄVENTIONSRAT | Freistaat SACHSEN

Fachtag 2021

Kommunale Prävention – Reagieren, bevor es zu spät ist

Wir bedanken uns für Ihre Teilnahme an der ASSKomm-Fachtagung und hoffen, dass Sie den Tag mit der Dokumentation nochmals gut reflektieren können.

Gleichzeitig wollen wir Sie auf den 6. Landespräventionstag „Gewaltprävention.Unschlagbar!“ am 14./15. November 2022 hinweisen.

Alle weiteren Neuigkeiten zur Allianz Sichere Sächsische Kommunen finden Sie auf **www.asskomm.de**.

Landes Präventionsrat Sachsen
Einer mit Allen!
www.lpr.sachsen.de

ASSKomm
Allianz Sichere Sächsische Kommunen

B3 INSTITUT FÜR BERATUNG, BEGLEITUNG UND BILDUNG e.V.