Cybercrime

Nur ein Phänomen?

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Henrik Hohenlohe und Eric Fischer

SN4C

CyberCrime
Competence
Center
Sachsen

Agenda

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Was macht eigentlich die Polizei?
  - Henrik Hohenlohe, Kriminaloberrat – Leiter Cybercrime Competence Center Sachsen (SN4C) beim Landeskriminalamt
- Welche Phänomene gibt es und worauf muss man achten?
  - Eric Fischer, Kriminalkommissar – Zentrale Ansprechstelle Cybercrime (ZAC) beim SN4C

Trojaner legt Landtag lahm

Am Mittwoch haben Cyberkriminelle den Landtag von Sachsen-Anhalt lahmgelegt. Das Parlament muss offline bleiben. Telefone und Computer mussten am Vormittag vom Netz genommen werden.

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

Lage Hellfeld

Zahlen der PKS - 2019

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

- Bundesweit: **100.514** Fälle von Cybercrime im engeren Sinne

  294.665 Fälle mit dem Tatmittel Internet

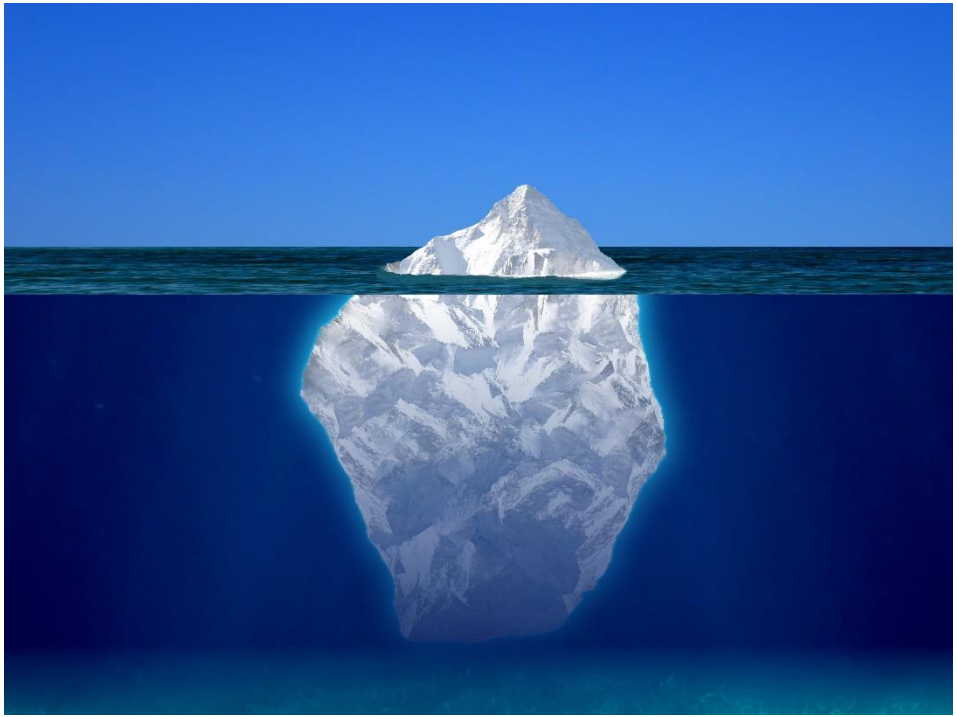
- Freistaat Sachsen: **1915** Fälle von Cybercrime im engeren Sinne

  8.212 Fälle mit dem Tatmittel Internet

SN4C CyberCrime Competence Center Sachsen

Was wir wissen

LANDES-
KRIMINALAMT
POLIZEI
Sachsen



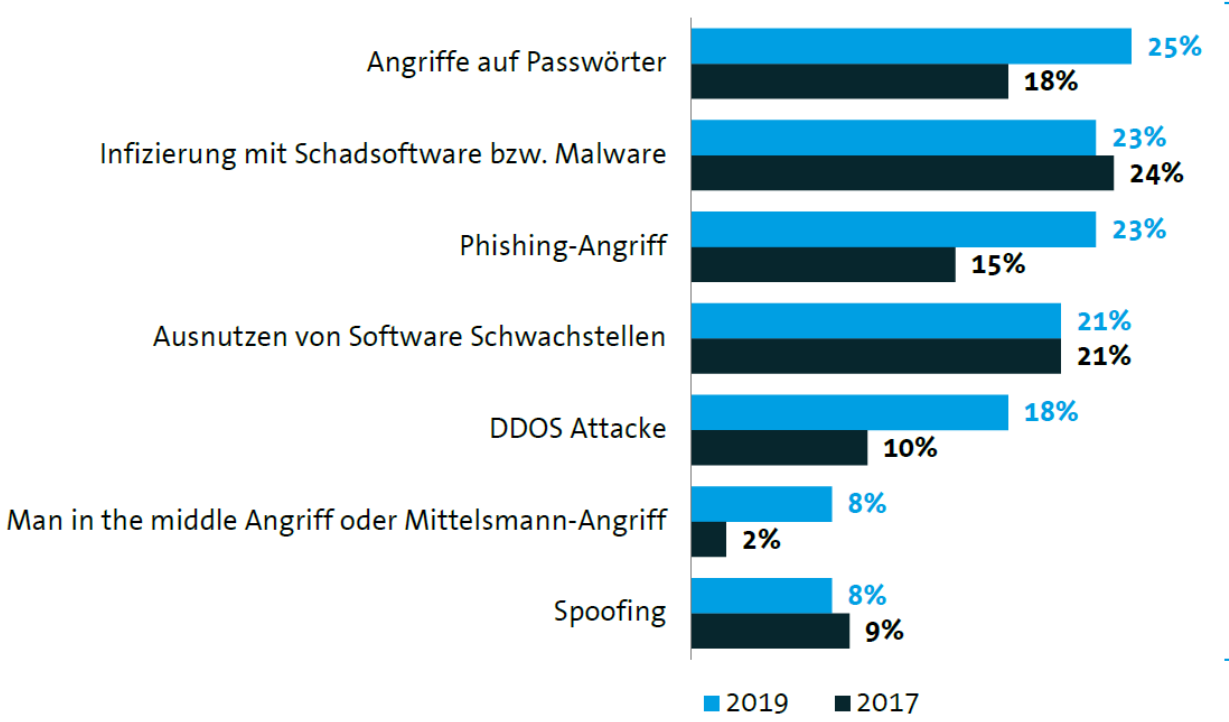
Hellfeld

Dunkelfeld

SN4C CyberCrime Competence Center Sachsen

Digitale Angriffe haben bei 7 von 10 Unternehmen Schäden erzeugt

Welche der folgenden Arten von digitalen Angriffen haben innerhalb der letzten zwei Jahre in Ihrem Unternehmen einen Schaden verursacht?



Digitale Angriffe haben bei

70%

der Unternehmen einen Schaden verursacht – 2017 waren es erst 43%.

 Basis: Alle befragten Unternehmen (2019: n=1.070; 2017: n=1.069); Mehrfachnennungen in Prozent

bitkom

Insgesamt 102,9 Mrd. Euro Schaden pro Jahr

Schäden in Deutschland nach Delikttyp in Mrd. Euro (Basis: Selbsteinschätzung)

Delikttyp	Schadenssummen in Mrd. Euro (2019)
Kosten für Ermittlungen und Ersatzmaßnahmen	36,5
Kosten für Rechtsstreitigkeiten	31,2
Patentrechtsverletzungen (auch schon vor der Anmeldung)	28,6
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	27,0
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	22,2
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	18,6
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	22,2
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	10,5
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	8,8
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-
Sonstige Schäden	<0,1
Gesamtschaden innerhalb der letzten 2 Jahre	**205,7**

Basis: Alle befragten Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2019: n=801; 2017: n=571; 2015: n=550)

bitkom

Was macht denn eigentlich die Polizei?
Strategie Cybercrime

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Polizei vs. IT-Sicherheit ?

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

Polizei

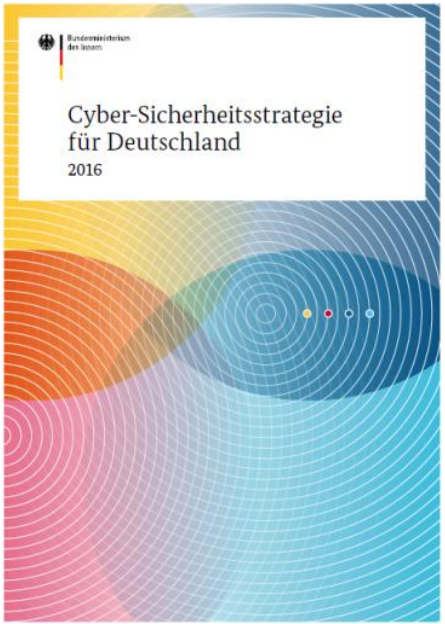
IT-Sicherheit

SN4C CyberCrime Competence Center Sachsen

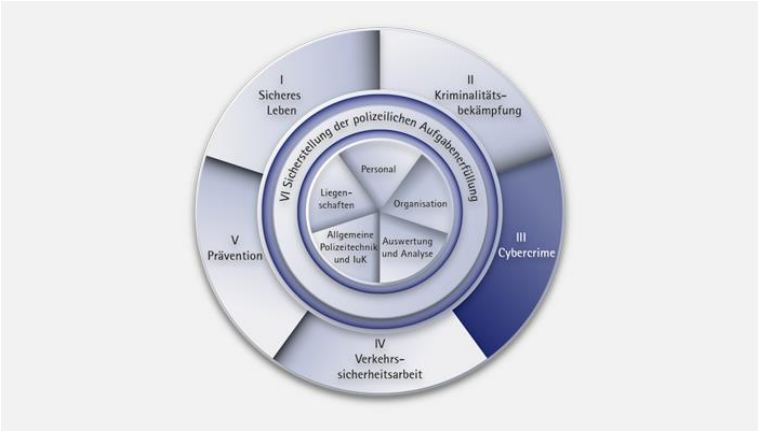
Rolle der Polizei

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



Strategie der sächsischen Polizei

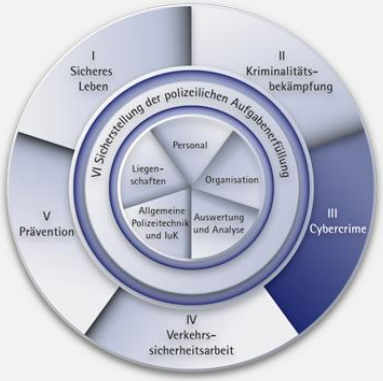


Strategiefeld III: Cybercrime

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Strategie der sächsischen Polizei

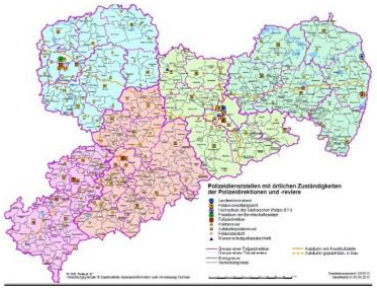


Strategiefeld III: Cybercrime

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

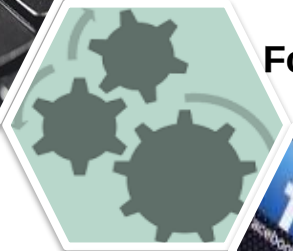
Landeskriminalamt

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

Grundsatz, ZAC,QRF

IT-Ermittlungen

IT-Ermittlungs-unterstützung



IT-Forensik

IT-Auswerte-unterstützung

TKÜ

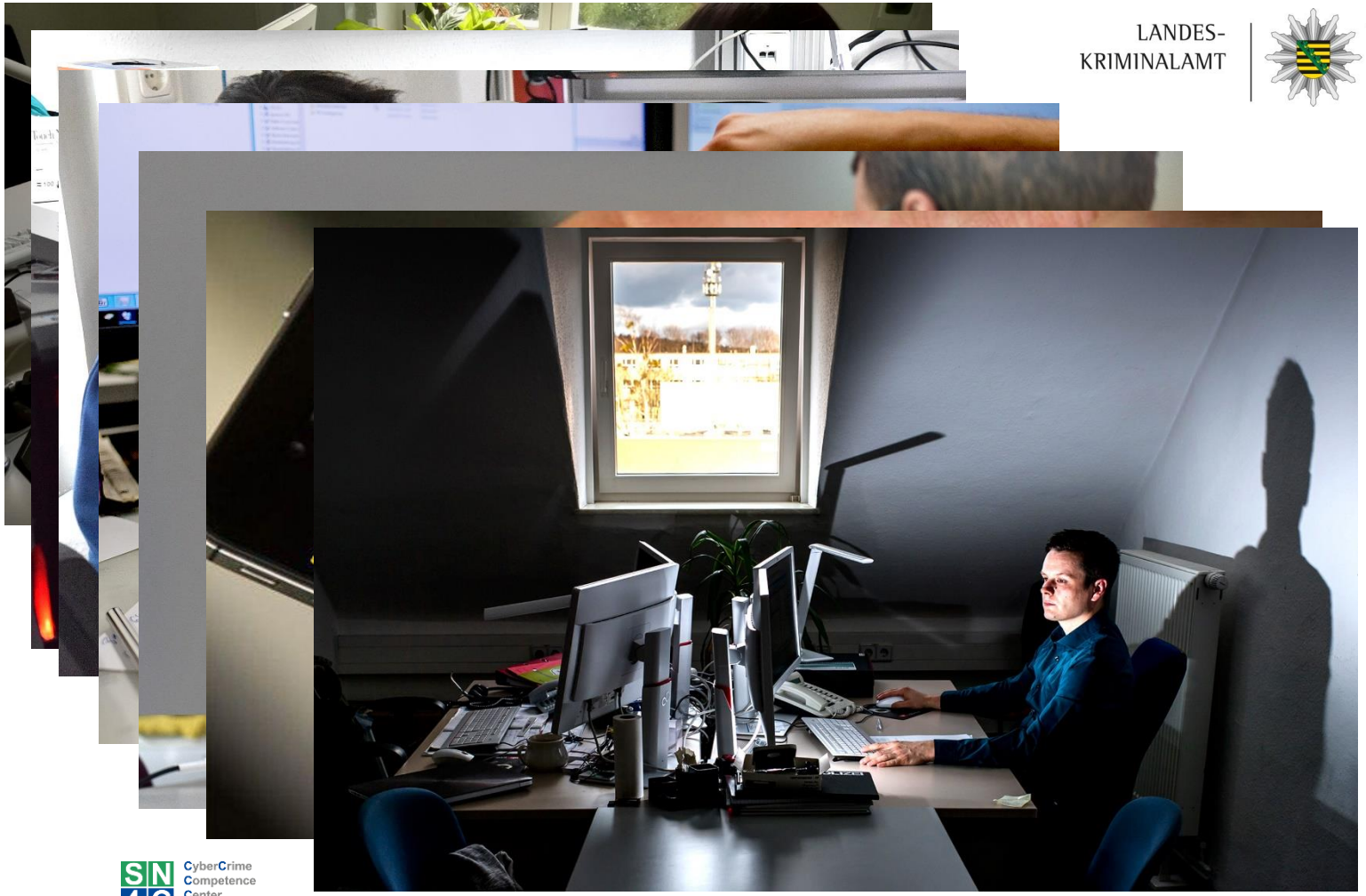
SN4C CyberCrime Competence Center Sachsen

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



LANDES-
KRIMINALAMT

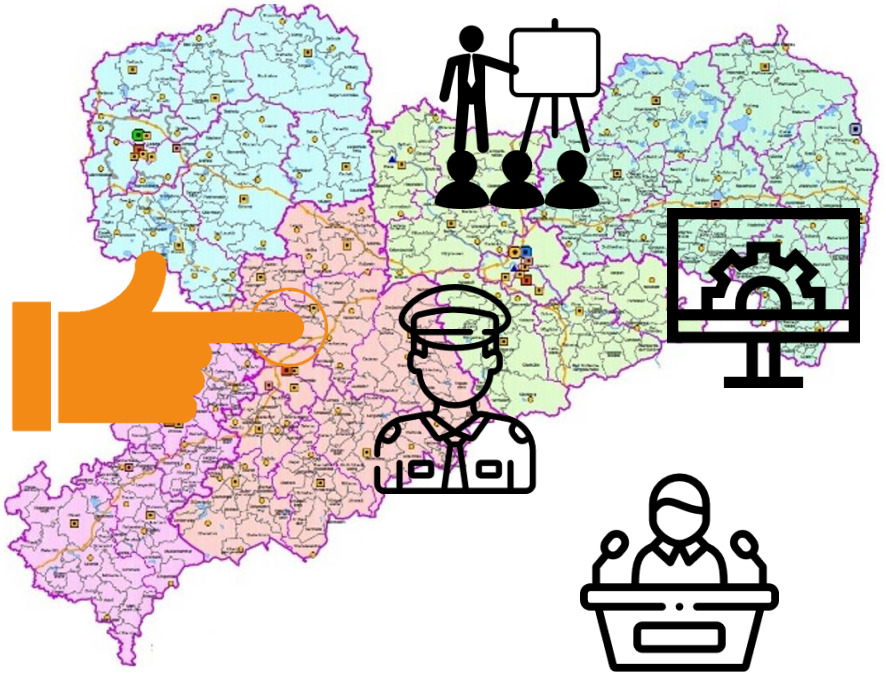
POLIZEI
Sachsen

SN4C CyberCrime Competence Center Sachsen

BKA

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

GENERALSTAATS-
ANWALTSCHAFT
DRESDEN
Freistaat
SACHSEN



[...]

SN 4C CyberCrime Competence Center Sachsen

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

Aktuelle Phänomene

LANDES-
KRIMINALAMT

POLIZEI
Sachsen

Warum sind Cyber-Angriffe möglich?

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

SN4C CyberCrime Competence Center Sachsen

Aktuelle Phänomene

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- SPAM-Wellen
- Phishing und Identitätsdiebstahl
- Fakeshops und Warenagenten
- Erpressung mittels Ransomware oder DDoS-Attacken
- Crime-as-a-Service
- Manipulation von Konto- und Finanzdaten
- Business Email Compromise
- Erlangung von Betriebs- und Geschäftsgeheimissen

SN4C CyberCrime Competence Center Sachsen

Aktuelle Phänomene

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

Die Professionalität von Cyberkriminellen steigt weiter an.

Cybercrime erschafft und basiert auf kriminellen Wertschöpfungsketten.

Ransomware bleibt die größte Bedrohung für Wirtschaftsunternehmen.

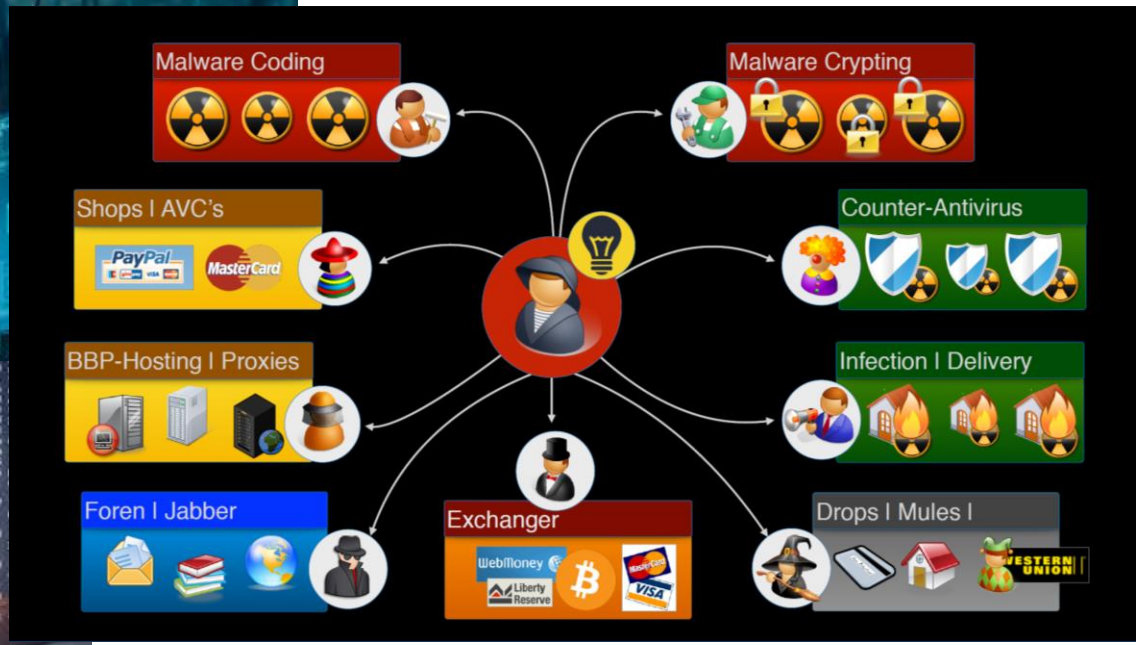
Anzahl und auch Intensität von DDoS-Angriffen steigen rapide an.

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

Die wichtigsten Schutzmechanismen gegen Cybercrime sind weiterhin sensible Internetnutzer.

SN4C CyberCrime Competence Center Sachsen

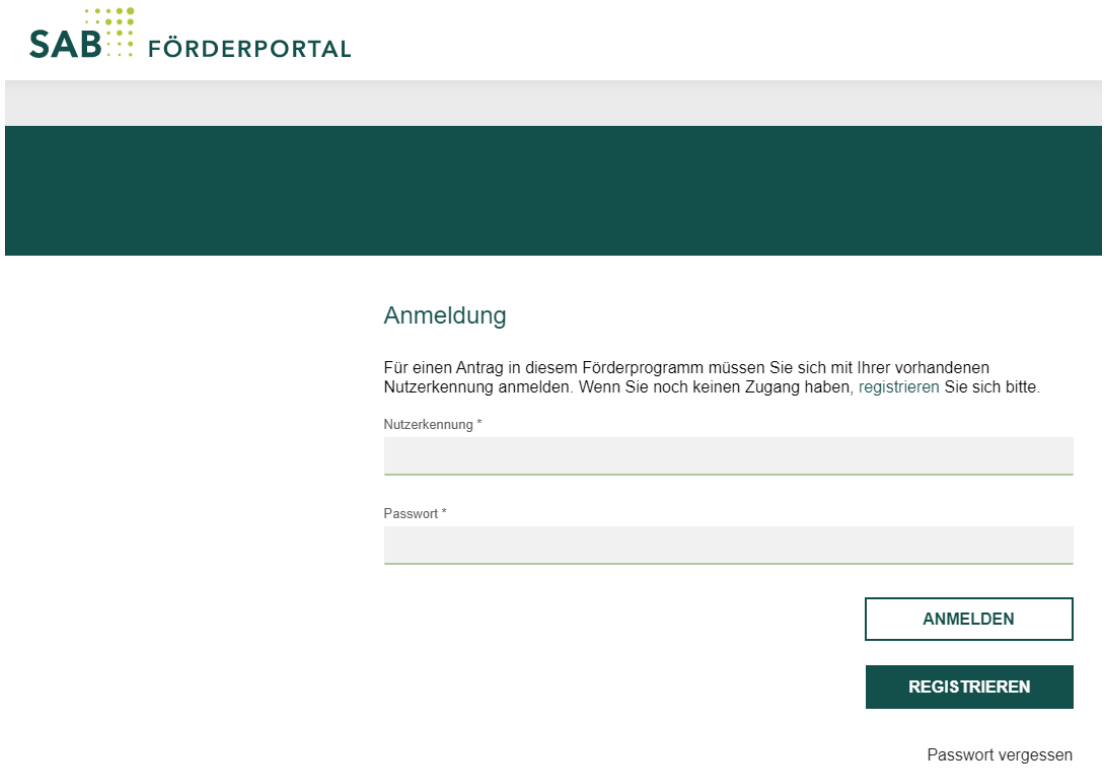
Täter?


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
VISA
Drops I Mules I
WESTERN UNION

Phishing

LANDES-
KRIMINALAMT

POLIZEI
Sachsen



SN4C CyberCrime Competence Center Sachsen

Phänomen-Scam

Fr 22.02.2019 17:29

info@[redacted]

Hohe Gefahr. Konto wurde angegriffen.

An info@[redacted]

Hallo!

Wie Sie vielleicht bemerkt haben, habe ich Ihnen eine E-Mail von Ihrem Konto aus gesendet.
Dies bedeutet, dass ich vollen Zugriff auf Ihr Konto habe.

Ich habe dich jetzt seit ein paar Monaten beobachtet.
Tatsache ist, dass Sie über eine von Ihnen besuchte Website für Erwachsene mit Malware infiziert wurden.

Wenn Sie damit nicht vertraut sind, erkläre ich es Ihnen.
Der Trojaner-Virus ermöglicht mir den vollständigen Zugriff und die Kontrolle über einen Computer oder ein anderes Gerät.
Das heißt, ich kann alles auf Ihrem Bildschirm sehen, Kamera und Mikrofon einschalten, aber Sie wissen nichts davon.

Ich habe auch Zugriff auf alle Ihre Kontakte und Ihre Korrespondenz.

Warum hat Ihr Antivirus keine Malware entdeckt?
Antwort: Meine Malware verwendet den Treiber.
Ich aktualisiere alle vier Stunden die Signaturen, damit Ihr Antivirus nicht verwendet wird.

Ich habe ein Video gemacht, das zeigt, wie du befriedigst dich... in der linken Hälfte des Bildschirms zufriedenstellen,
und in der rechten Hälfte sehen Sie das Video, das Sie angesehen haben.
Mit einem Mausklick kann ich dieses Video an alle Ihre E-Mails und Kontakte in sozialen Netzwerken senden.
Ich kann auch Zugriff auf alle Ihre E-Mail-Korrespondenz und Messenger, die Sie verwenden, posten.

Wenn Sie dies verhindern möchten, übertragen Sie den Betrag von 336€ an meine Bitcoin-Adresse
(wenn Sie nicht wissen, wie Sie dies tun sollen, schreiben Sie an Google: "Buy Bitcoin").

Meine Bitcoin-Adresse (BTC Wallet) lautet: 15mWFjVymAdqimVim2f1UgX6oSD4TYeGLE

Nach Zahlungseingang lösche ich das Video und Sie werden mich nie wieder hören.
Ich gebe dir 48 Stunden, um zu bezahlen.
Ich erhalte eine Benachrichtigung, dass Sie diesen Brief gelesen haben, und der Timer funktioniert, wenn Sie diesen Brief sehen.

Eine Beschwerde irgendwo einzureichen ist nicht sinnvoll, da diese E-Mail nicht wie meine Bitcoin-Adresse verfolgt werden kann.
Ich mache keine Fehler.

Wenn ich es herausfinde, dass Sie diese Nachricht mit einer anderen Person geteilt haben, wird das Video sofort verteilt.

Schöne Grüße!

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?

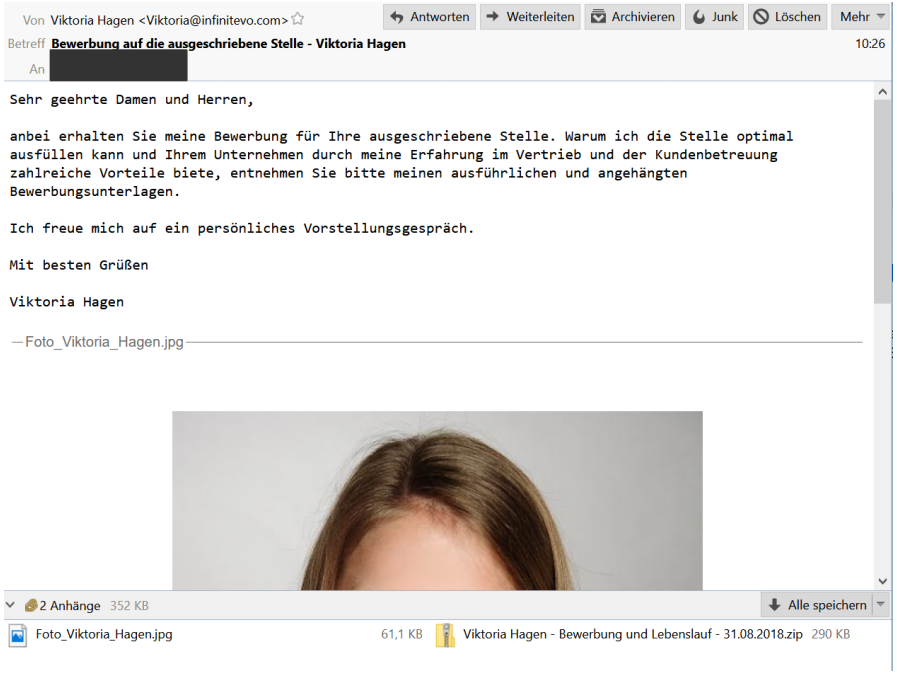
If you decide not to pay, we will start the attack on the indicated date and uphold it until you do, there's no counter measure to this, uur attacks are extremely powerful - sometimes over 2 Tbps per second, so you will only end up wasting more money trying to find a solution (Cloudflare, Incapsula and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

Digitale Erpressung mittels Verschlüsselungstrojanern

LANDES-
KRIMINALAMT
POLIZEI
Sachsen



SN 4C 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:

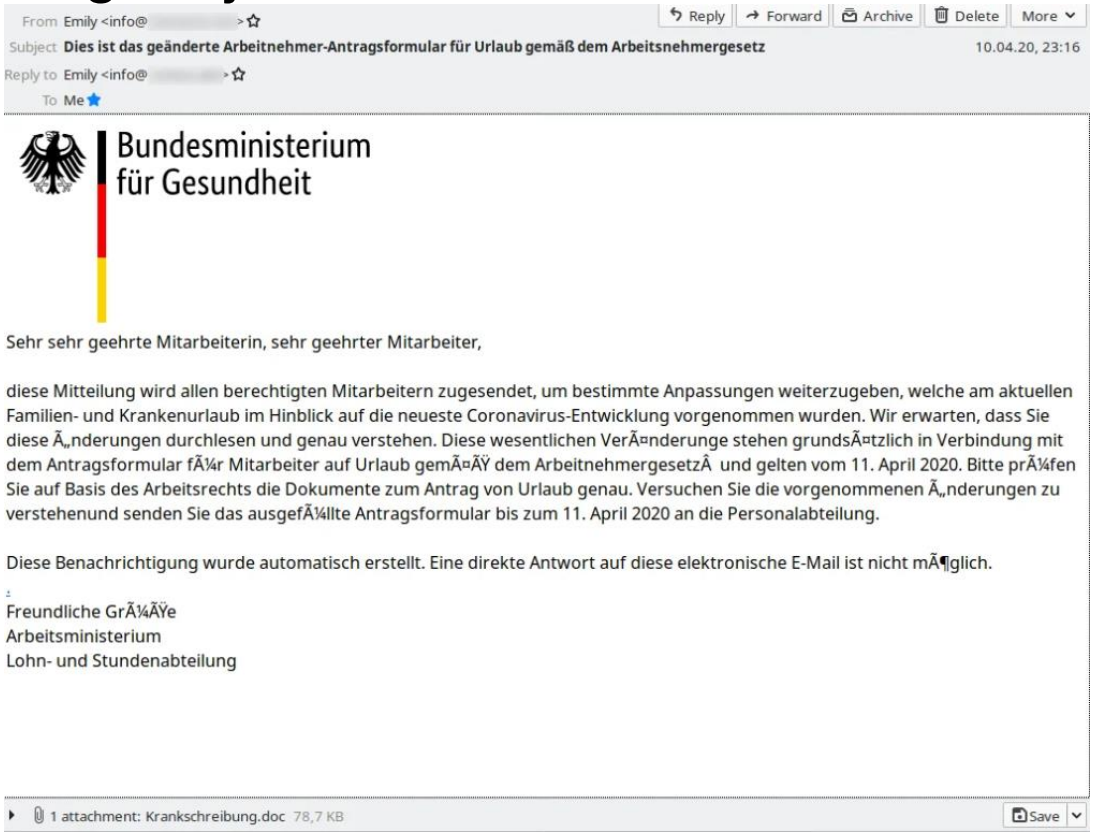
- Bund-Arbeitsschutzregel-Corona-September.zip

SN 4C 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

[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

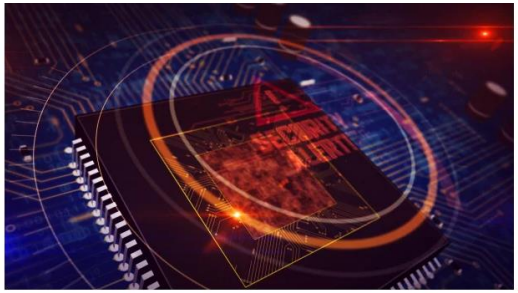
POLIZEI
Sachsen

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

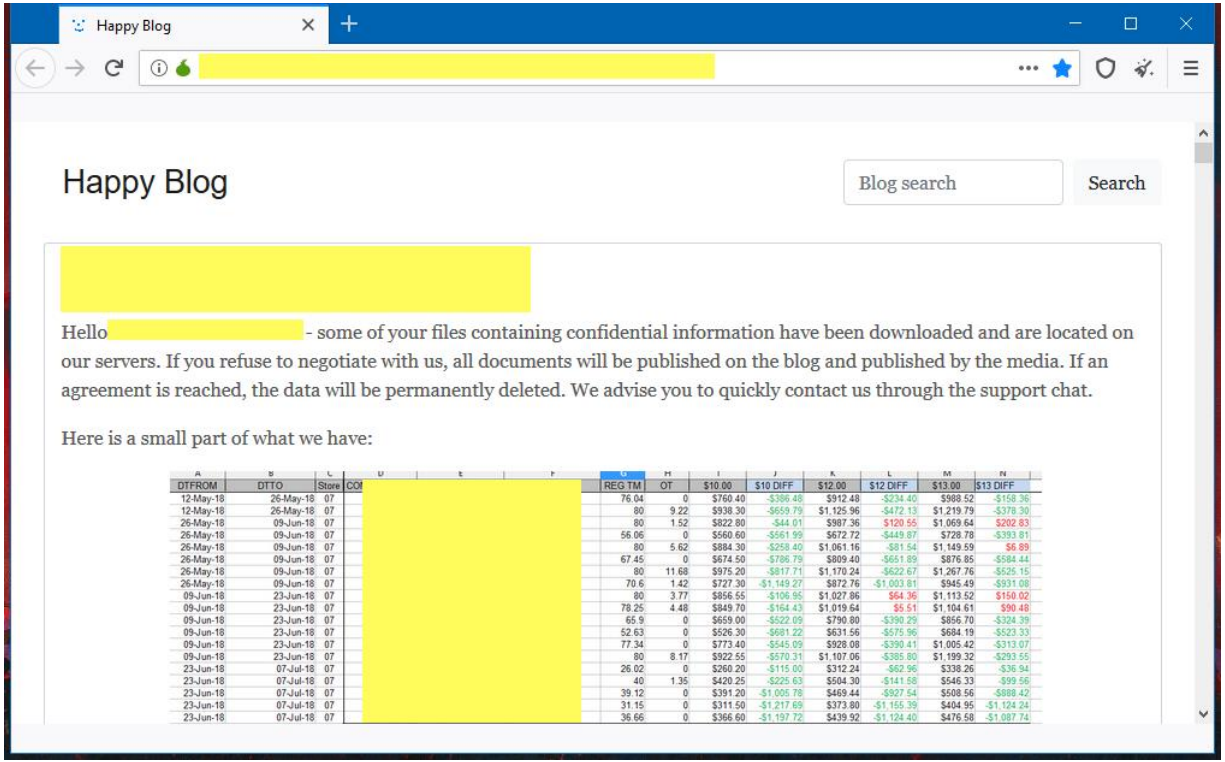


(Bild: Skorzewiak/Shutterstock.com)

12.04.2020 16:11 Uhr | Security

Von Markus Montz

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

Fazit

LANDES-
KRIMINALAMT
POLIZEI
Sachsen

- Phänomenbasierte Angriffe
- Immer in den wunden Punkt → Betroffenheit schaffen
- Situationsbedingte Verlagerung der Angriffsvektoren

→ Sensibilisierung wichtiger denn je!

→ Effektive Melde- und Alarmierungswege!

→ Schnelle Reaktion mindert den Impact!

→ Informieren! (zB: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html)

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!