POLIZEI
BERLIN

BERLIN

KHK Borries und KHK Huwald
LKA 724 Cybercrime
ZAC Berlin – Zentrale Ansprechstelle Cybercrime

POLIZEI
BERLIN

BERLIN

Basler Schulnetz gehackt
Darknet

Update / Vier Rettungsstellen in Berlin betroffen
Cyber-Angriff auf Krankenhäu

heise online > Security > Cyb
Cybergang Alp
Rüstungs

Heime und Kliniken in Berlin
Johannesstift ringt weiter mit den Folgen des Cyber-Angriffs
Do 24.10.24 | 18:11 Uhr | Von Yasser Speck

Cyberangriff Deutsche Flugs
von Hackern angegriff
Bürokommunikation lahmgelegt: Hacker ha
Flugsicherung angegriffen. Die Auswirkungen s
01.09.2024, 18:23 Uhr

Cyberangriff auf die dena

Cyberangriff auf die dena-Serverinfrastruktur - dena telefonisch und per Mail nicht erreichbar. IT-Sicherheitsmaßnahmen wurden ergriffen. Die dena-Pressestelle ist über die bekannten Mobilfunknummern erreichbar.

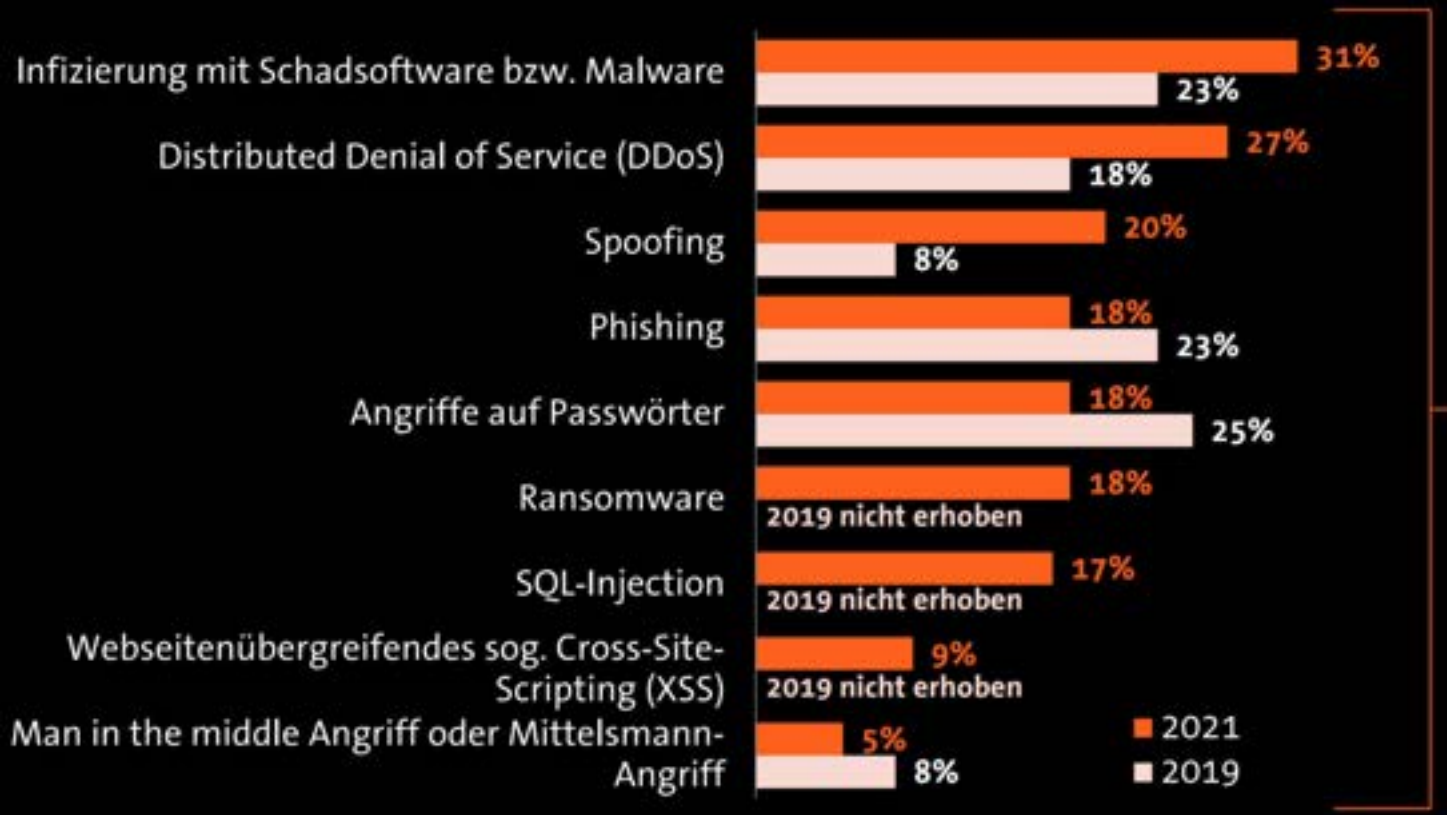
Berlin, den 14. November 2023. Die dena wurde am Wochenende durch einen Cyberangriff attackiert. Dabei wurde die

Rettungsd

Diakonie, Mariendorfer Weg
owicz | Bild: imago images/Sch
stift-Diakonie getroff
Systeme noch nicht
t bislang unklar.
asser Speck
der Johannesstift-Diak
Systeme dauert immer
Bedrohungslage und
schland und andere Lär

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%

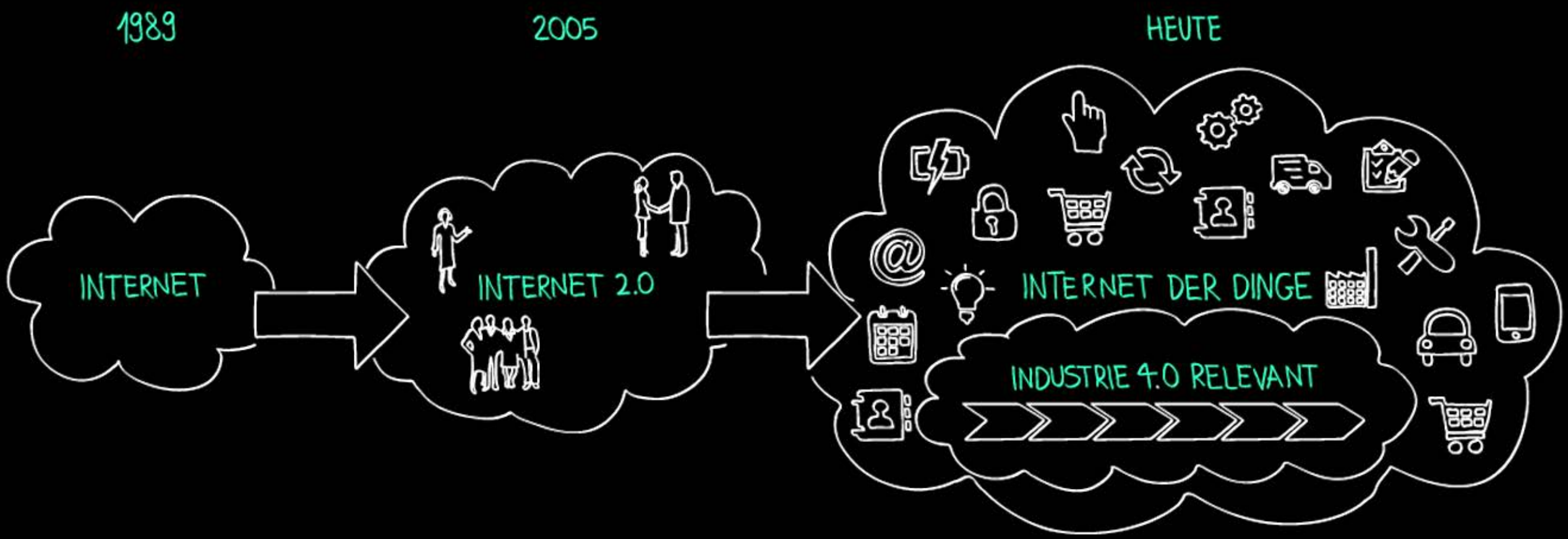
der Unternehmen einen Schaden verursacht – **2019** waren es erst **70%**.

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

Wirtschaftsschutz 2021, Bitkom e.V.

die Opferseite



+ proprietärer Kram
+ legacy Zeugs
+ mobile Gedöns

die Opferseite

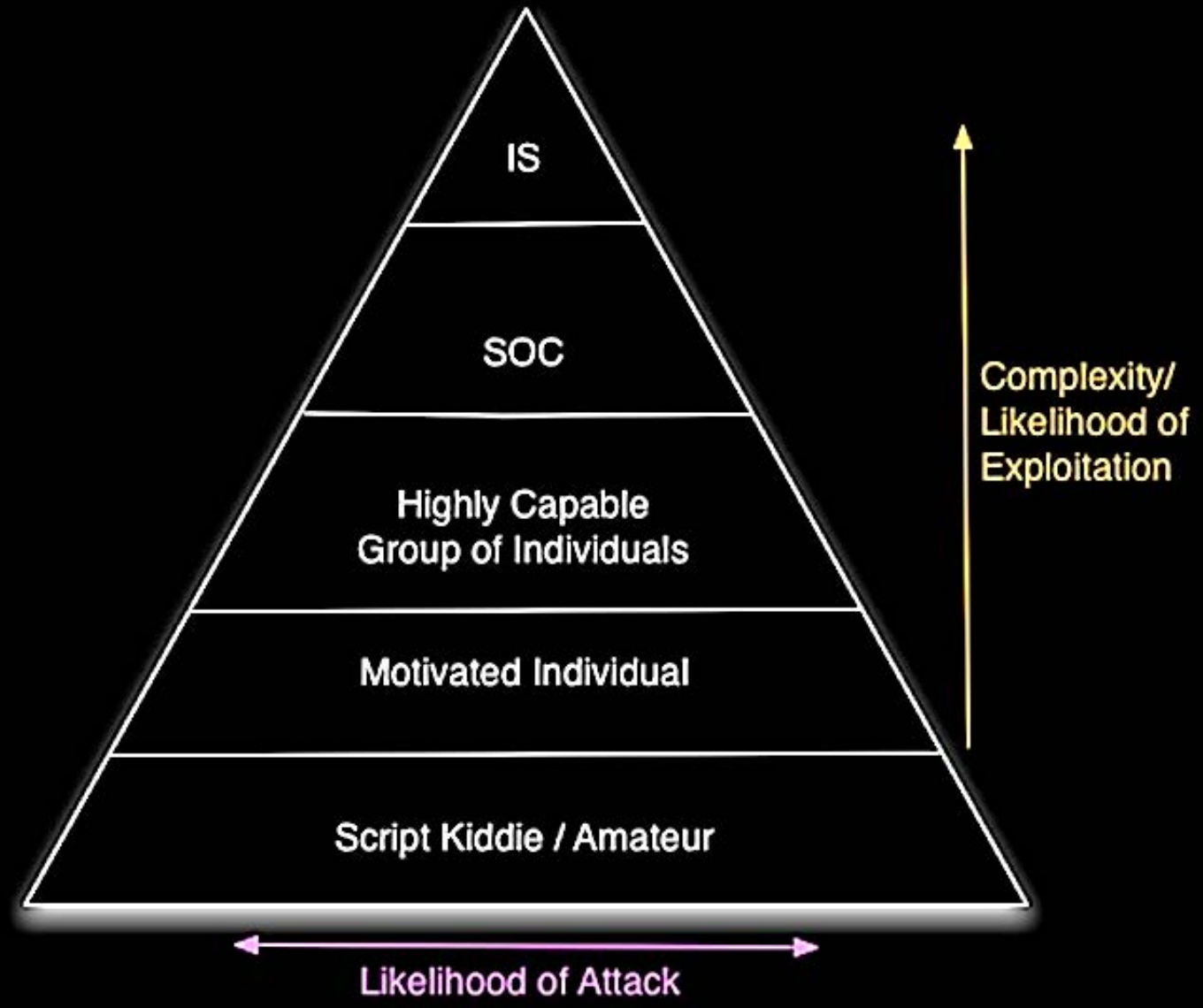
Unterscheidung von Angriffszielen in ...

1. Unternehmen, die bereits angegriffen wurden

2. Unternehmen, die bereits angegriffen wurden*

* jedoch noch nichts ahnen

die Gegenseite



IS = Intelligence services

SOC = Serious organized Crime

http://openstack.booktype.pro/security-guide/threat-classification-actors-and-attack-vectors/

die Gegenseite

Welcome to RansomLook !

March 25Th, 2025

Currently tracking **413** groups across **1596** relays & mirrors - **479** *currently online*

Got **541** DLS, **819** FS, **214** Chats and **22** Admin/Affiliates pages.

Currently tracking **117** forums & markets across **204** relays & mirrors - **96** *currently online*

Currently tracking **284** telegram channels.

There have been **53** posts within the last 24 hours

There have been **636** posts within the month of march

There have been **2412** posts within the last 90 days

There have been **2336** posts within the year of 2025

There have been **20743** posts since the dawn of ransomlook

There are **157** custom parsers indexing posts

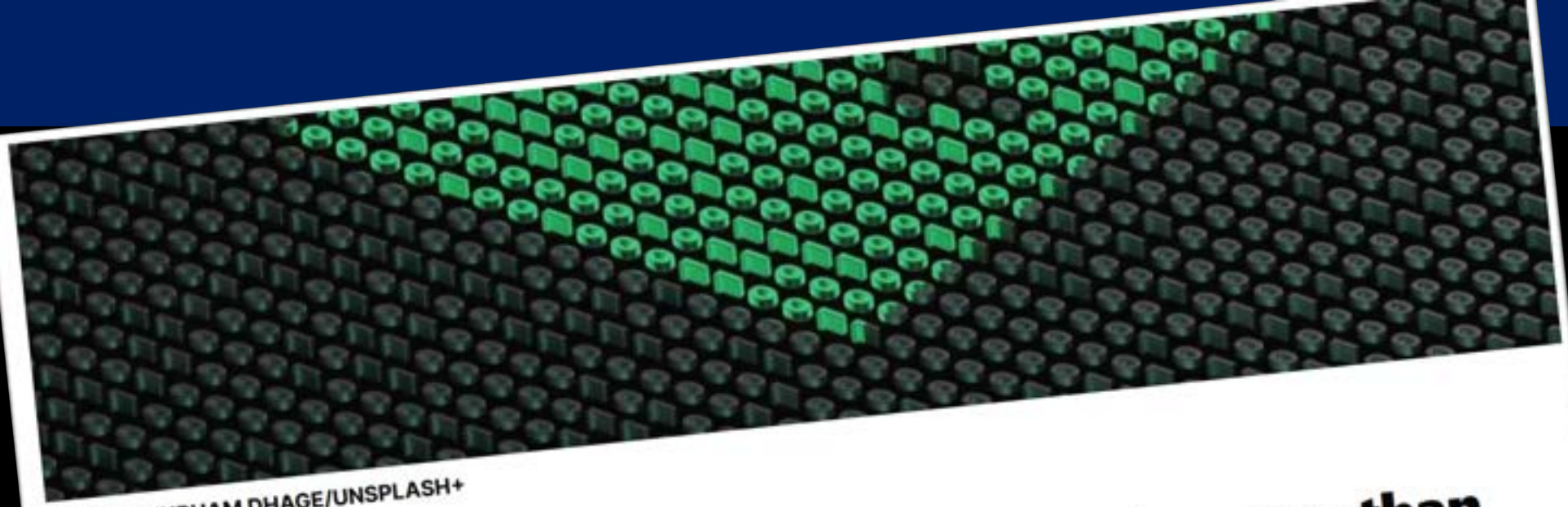


IMAGE: SHUBHAM DHAGE/UNSPLASH+

Jonathan Greig

August 15th, 2024

Ransomware gangs rake in more than $450 million in first half of 2024

More than $459 million was extorted from victims of ransomware attacks in the first half of 2024, highlighting a growing crisis that has affected all organizations from major corporations to local governments and hospitals, according to a new report.

Blockchain research company Chainalysis tracked cryptocurrency payments made to wallets controlled by ransomware actors, finding a $10 million increase in the amount of money earned from those criminals compared to last year's figure of $449.1 million.

POLIZEI
BERLIN

ansomware

BERLIN

POLIZEI BERLIN

Cybercrime: DDoS Angriffe

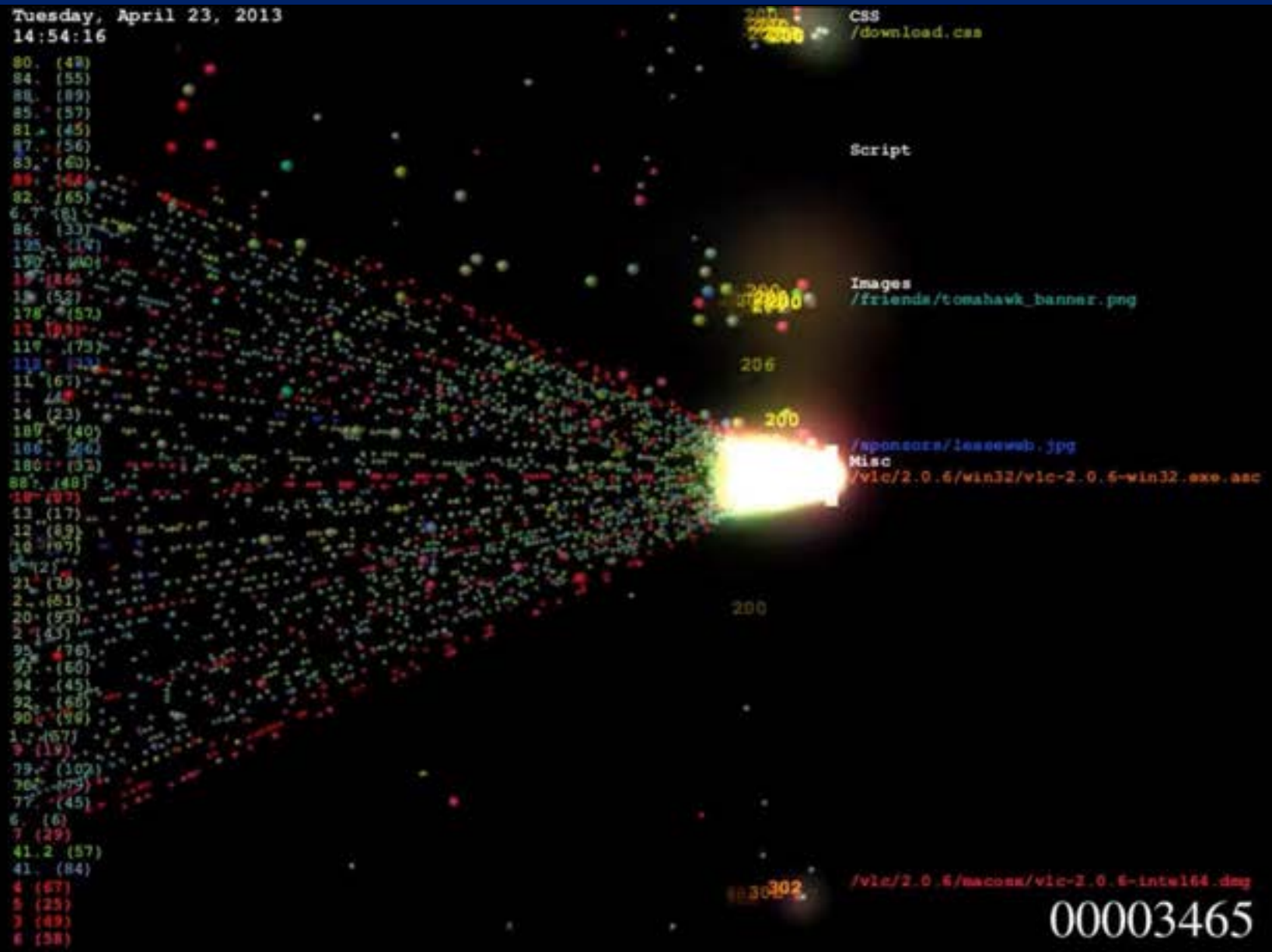
BERLIN

https://www.youtube.com/watch?v=hNjdBSoIa8k

POLIZEI BERLIN

Cybercrime: DDoS Angriffe

BERLIN



https://www.youtube.com/watch?v=hNjdBSola8k

Medienbericht: Cyberkriminelle spähten angeblich Regierungs-IT aus

Das Informationstechnikzentrum des Bundes warnt Mitarbeiter vor abgegriffener E-Mail-Kommunikation. Die Verantwortlichen wollten jedoch nur sensibilisieren.

(Bild: JARIRIYAWAT/Shutterstock.com)

11.05.2023, 00:01 Uhr Lesezeit: 3 Min. | Security

Von Marie-Claire Koch

"Unbekannte Hacker" haben Berichten zufolge drei für Ministerien und Behörden arbeitende IT-Unternehmen ausgespäht. Das gehe aus einem Warnschreiben des Informationstechnikzentrums des Bundes (ITZ Bund) von Ende April hervor, das dem Bayerischen Rundfunk (BR) vorliegt. Demnach sollen die Angreifer "sehr wahrscheinlich" die E-Mail-Kommunikation bei den betroffenen Firm

BR-RECHERCHE: HACKERANGRIFFE AUF DREI IT-DIENSTLEISTER DES BUNDES

Mai 11, 2023 | Hackerangriff aktuell | 0

Wie der Bayerische Rundfunk berichtet, haben unbekannte Cyberkriminelle offenbar drei deutsche IT-Unternehmen angegriffen, die für Bundesministerien und Behörden arbeiten. Das gehe aus einem Warnschreiben des Informationstechnikzentrums Bund (ITZ Bund) von Ende April hervor, das dem BR vorliege. Laut dem Warnschreiben wurden Daten ausgespäht und sehr wahrscheinlich große Mengen der E-Mail-Kommunikation abgefangen. Die erbeuteten E-Mails enthielten unter anderem personenbezogene Daten, Telefonnummern, aktuelle Projekte, Mailverläufe und angehängte Dokumente. Von dem Hackerangriff betroffen waren die Dortmunder IT-Unternehmen Adesso und Mat

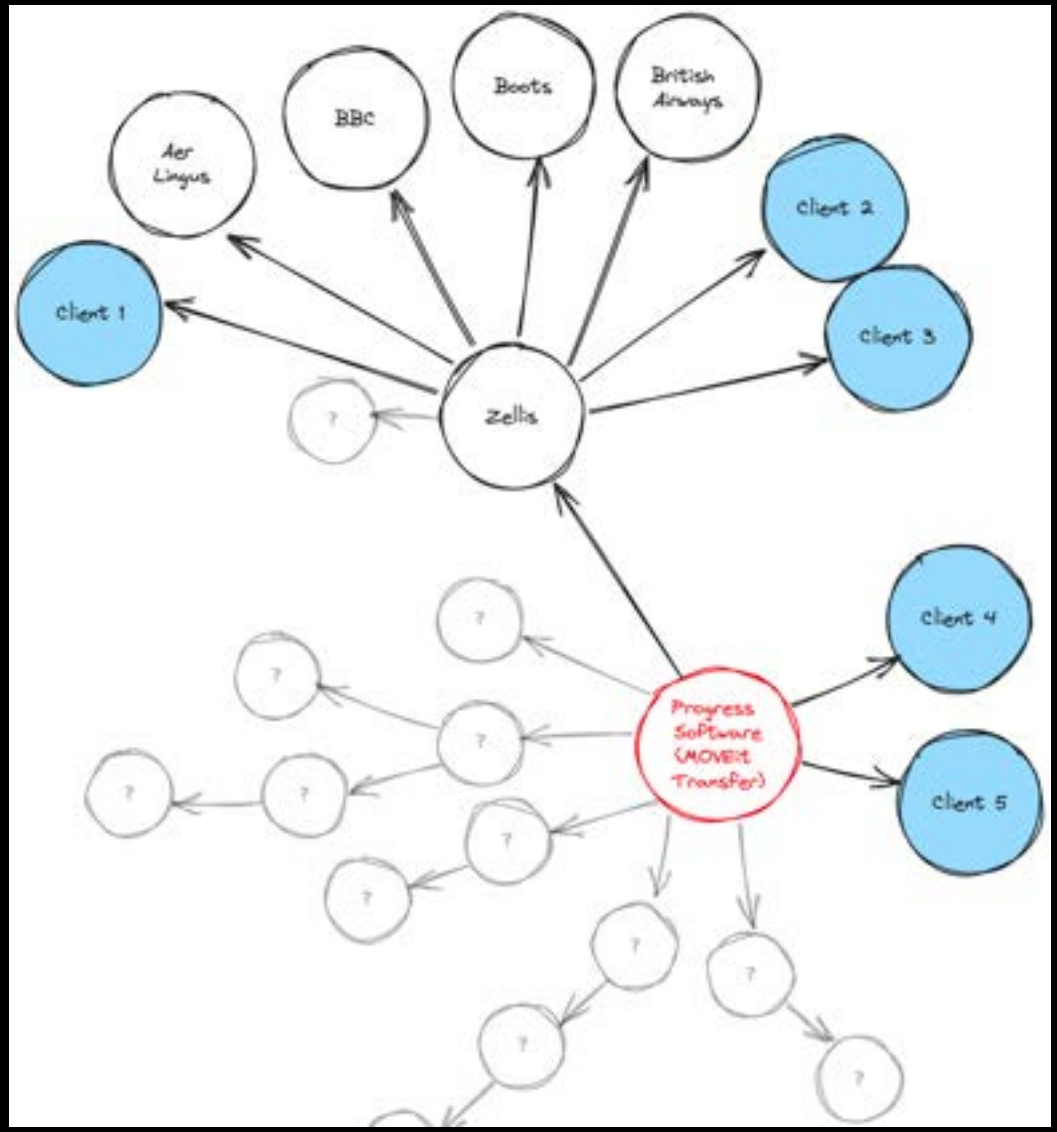
Supply Chain Angriffe

MOVEit Transfer Vulnerability: Lack of Supply Chain Visibility Exacerbates Breach

Risk Ledger
4,549 followers

June 14, 2023

Once a critical vulnerability has been identified, how long does it take for all affected organisations to realise they might be affected as well and to then investigate, identify if and how they have been impacted, and respond accordingly to mitigate the risk?



https://www.linkedin.com/pulse/moveit-transfer-vulnerability-lack-supply-chain-visibility/

POLIZEI BERLIN

Cyberc

BERLIN

Cyberattac

Wie hoch ist der
der auf Cyberatt

28%

57,7 Mrd. Euro
Andere
Schäden

Basis: Alle Unternehmen, die in

Datendiebstah

Welche der folgende
Unternehmen gesto

Kommunikationsdate

M

Zugangsdaten

Geistiges Eigentum z. B. Patent
aus Forschung

in Prozent

Basis: Alle Unternehmen, die in den letzten

Die psychischen Folgen eines Ransomware-Angriffs sind gravierend

25. Oktober, 2022 05:11

Der Spezialist für Informationssicherheit Northwave hat eine wissenschaftliche Untersuchung zu den psychischen Auswirkungen großer Ransomware-Angriffe gegen Unternehmen durchgeführt. Die Ergebnisse zeigen, welch tiefe Spuren eine solche Krise bei allen Betroffenen hinterlässt.

Zugleich machen sie deutlich, dass es auch nach der Überwindung des Angriffs selbst noch lange dauern kann, bis bei den IT- und Sicherheitsteams wieder Normalität einkehrt.

rime.pdf

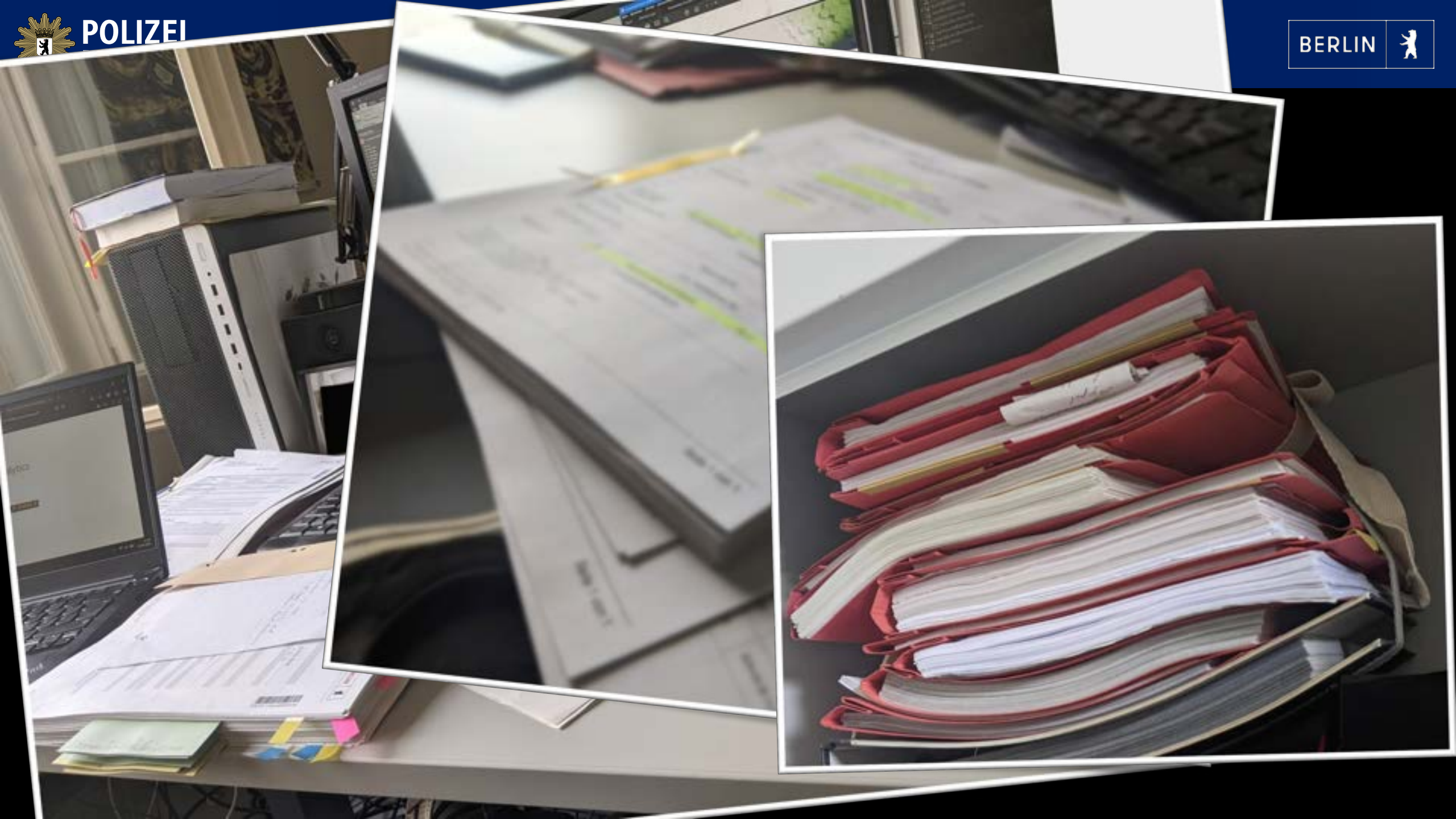
POLIZEI BERLIN

LKA 724 – Cybercrime und ZAC

BERLIN

POLIZEI

BERLIN



‘Operation Endgame’ Hits Malware Delivery Platforms

17 Comments

May 30, 2024

Law enforcement agencies in the United States and Europe today announced Operation Endgame, a coordinated action against some of the most popular cybercrime platforms for delivering ransomware and data-stealing malware. Dubbed “the largest ever operation against botnets,” the international effort is being billed as the opening salvo in an ongoing campaign targeting advanced malware “droppers” or “loaders” like IcedID, Smokeloader and Trickbot.

POLIZEI
BERLIN

BERLIN

BERLIN

LET'S TALK

GEFÄHRDUNGSLAGE CYBERSICHERHEIT:
WIE GUT SIND SIE AUFGESTELLT?

Lars Huwald

Astrid Frohloff

Rainer Stock

pwc VIBERA

Interview mit Olaf Borries

„Es wird Tätern viel zu häufig leicht gemacht“

Olaf Borries, Kriminalhauptkommissar bei der ZAC – Zentrale Ansprechstelle Cybercrime für die Wirtschaft im Landeskriminalamt Berlin – ist Experte beim Thema Cybercrime. Im Gespräch mit dem KV-Blatt erzählt er, welche Präventionsmaßnahmen Praxen treffen sollten.

Warum sind gerade Arztpraxen beliebte Angriffsziele von Cybercrime? Welche Motivation steckt hinter einem solchen Angriff?

In Arztpraxen werden sehr viele sensible Daten erzeugt und verwaltet, ohne die eine Praxis nicht arbeiten kann und die auch ein hohes Schadenspotential besitzen. Sollten Daten hier abgeflossen oder verschlüsselt sein, so ist der Handlungsdruck entsprechend hoch. Als Motiv sind sehr häufig, besonders im Bereich der Erpressung – Stichwort ‚Ransomware‘ –, finanzielle Interessen zu nennen.

praxis aufzubauen; zum Beispiel durch die Verschlüsselung der Daten. Eine Entschlüsselung erfolgt dann erst gegen die Zahlung eines Lösegeldes. Als Polizei raten wir grundsätzlich davon ab, zu zahlen. In der letzten Zeit kam es immer häufiger dazu, dass die Daten der geschädigten Institution vorher heruntergeladen wurden und es im Falle der Nichtbezahlung zur Drohung der Veröffentlichung der Daten führte. Ein weiterer Bereich – nach unserer Erfahrung nicht so im Fokus bei Arztpraxen – sind so genannte DDos-Angriffe. Darunter versteht man eine Überlastung von Internetseiten durch massive Anfragen, sodass ein Aufrufen der Seite nicht möglich ist. Dies wird dann oberfalls mit Erpressung verbunden.

POLIZEI BERLIN

Gegenmaßnahmen

BERLIN

POLIZEI BERLIN

Gegenmaßnahmen

BERLIN

POLIZEI
BERLIN

BERLIN

ZAC Zentrale Ansprechstellen Cybercrime
für die Wirtschaft der Länder und des Bundes

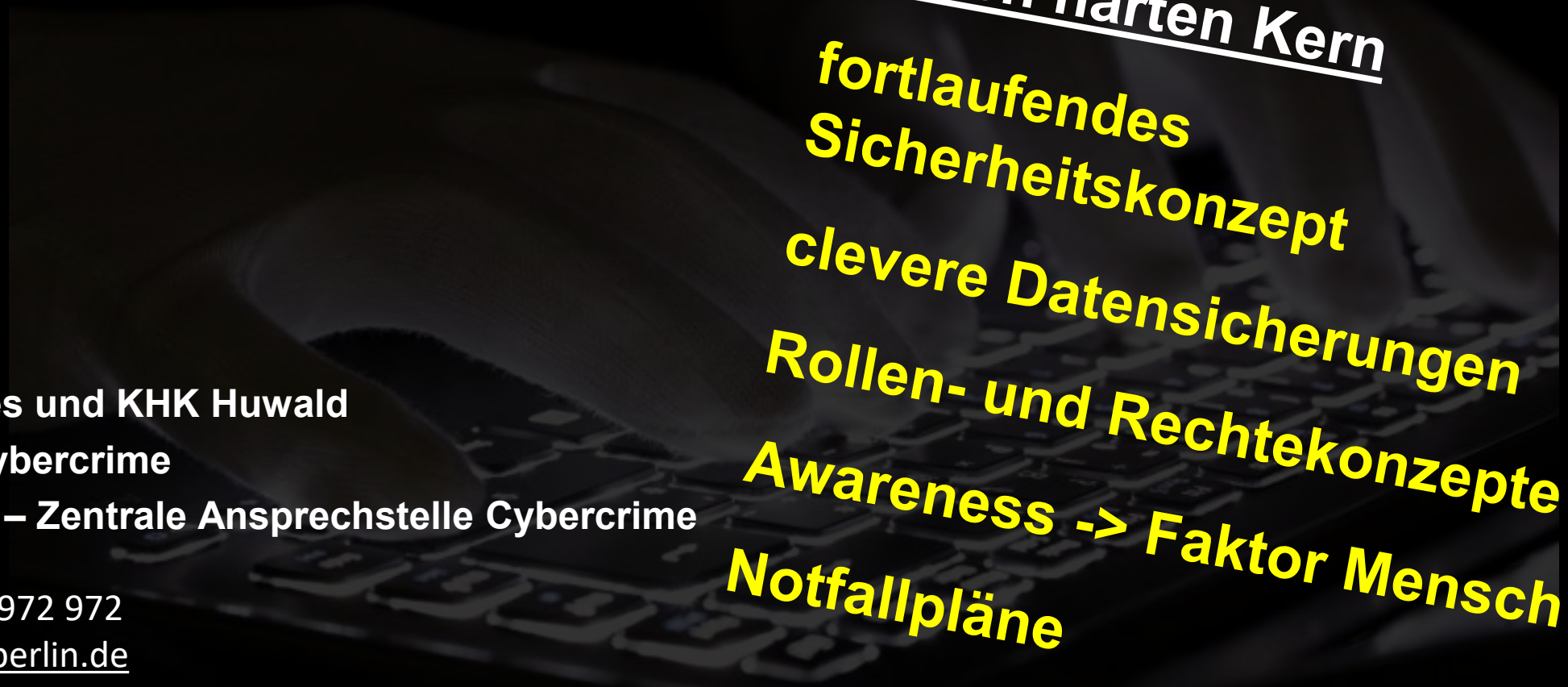
KHK Borries und KHK Huwald
LKA 724 Cybercrime
ZAC Berlin – Zentrale Ansprechstelle Cybercrime

+49 30 4664 972 972
zac@polizei.berlin.de

POLIZEI BERLIN

BERLIN

ZAC Zentrale Ansprechstellen Cybercrime
für die Wirtschaft der Länder und des Bundes



für den harten Kern

- fortlaufendes Sicherheitskonzept
- clevere Datensicherungen
- Rollen- und Rechtekonzepte
- Awareness -> Faktor Mensch
- Notfallpläne

KHK Borries und KHK Huwald
LKA 724 Cybercrime
ZAC Berlin – Zentrale Ansprechstelle Cybercrime

+49 30 4664 972 972
zac@polizei.berlin.de

POLIZEI
BERLIN

BERLIN

Polizei Berlin - Landeskriminalamt

ZAC – Zentrale Ansprechstelle Cybercrime
für die Wirtschaft, Behörden und Verbände

Friesenstr. 16
10965 Berlin

Tel.: 030 - 4664 / 972 972
E-Mail: zac@polizei.berlin.de

https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html