Wirtschaftstreffen 2022

Digitale Bedrohung
Cyberangriffe versus Cyberabwehr

Sponsoren:

UBS

JEHLE

RE/MAX Pratteln

De grüeni Leu isch los
Gärtnerei Leuenberger AG

ACKERMANN IMMOBILIEN AG

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cyber-Bedrohungen: Lage Schweiz und international

Max Klaus,

stv. Leiter operative Cybersicherheit OCS

1. NCSC
2. Lage und Akteure
3. Cyberangriffe: ausgewähltes Beispiel
4. Schlussfolgerungen / Empfehlungen

1. NCSC / MELANI

Wie alles begann

17.3508 MOTION

Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund

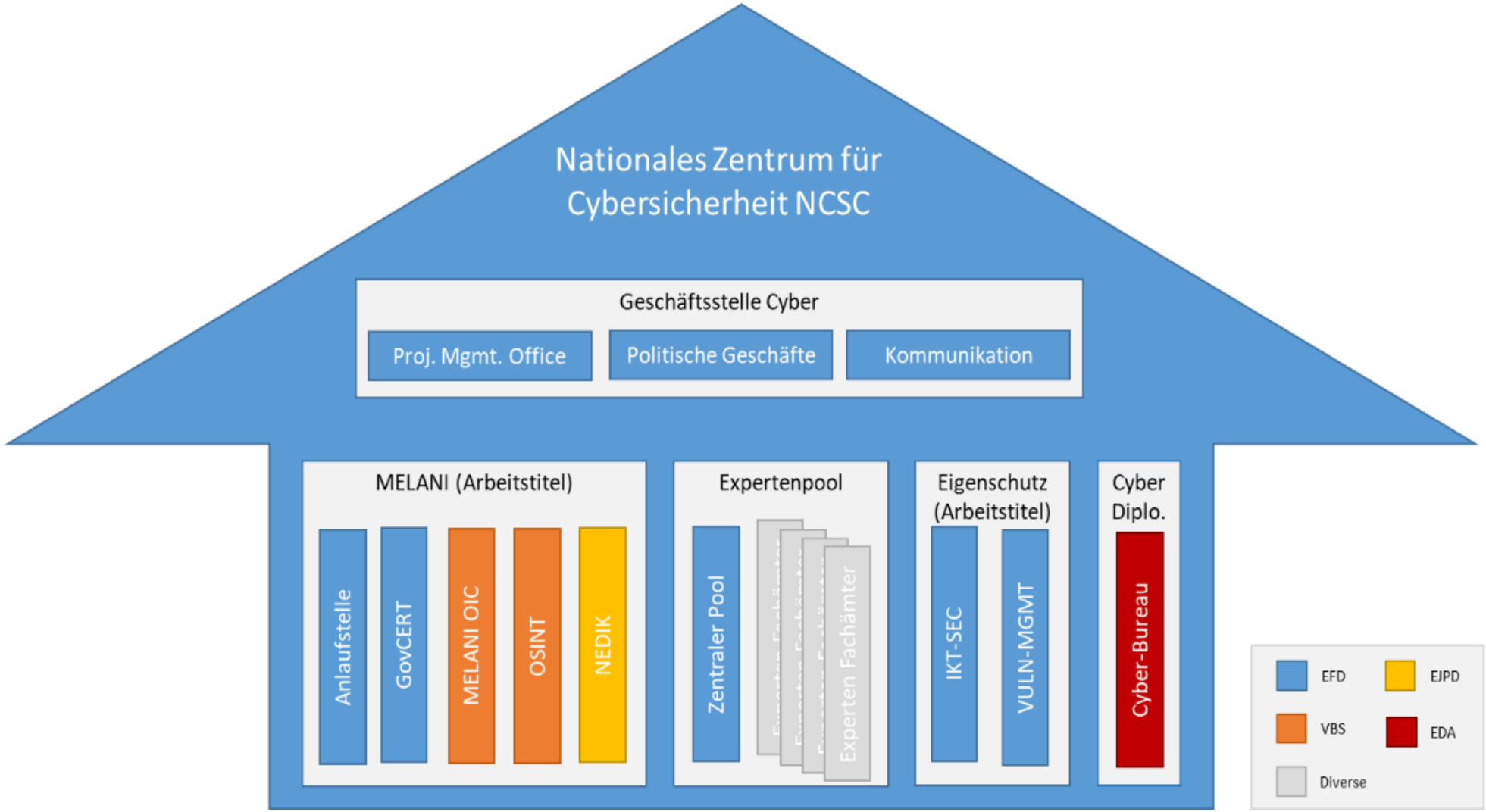
Eingereicht von:	EDER JOACHIM FDP-Liberale Fraktion FDP.Die Liberalen
Berichterstattung:	CLOTTU RAYMOND, GLÄTTLI BALTHASAR
Einreichungsdatum:	15.06.2017
Eingereicht im:	Ständerat
Stand der Beratungen:	Abgeschrieben

ALLES ZUKLAPPEN

EINGEREICHTER TEXT

Der Bundesrat wird beauftragt, im Zusammenhang mit der laufenden Überarbeitung der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) ein Cybersecurity-Kompetenzzentrum auf Stufe Bund zu schaffen und dafür die notwendigen Massnahmen einzuleiten. Diese Organisationseinheit hat die Aufgabe, die zur Sicherstellung der Cybersecurity notwendigen Kompetenzen zu verstärken und bundesweit zu koordinieren. Sie soll departementsübergreifend wirksam sein, das heisst insbesondere, dass sie im Bereich Cybersecurity über Weisungsbefugnis gegenüber den Ämtern verfügen soll. Das Kompetenzzentrum arbeitet mit Vertretern der Wissenschaft (Hochschulen, Fachhochschulen), mit der IT-Industrie und mit den grösseren Infrastrukturbetreibern (insbesondere Energie, Verkehr) zusammen.

Nationales Zentrum für Cybersicherheit NCSC



Nationales Zentrum für Cybersicherheit NCSC
Operative Cybersicherheit OCS

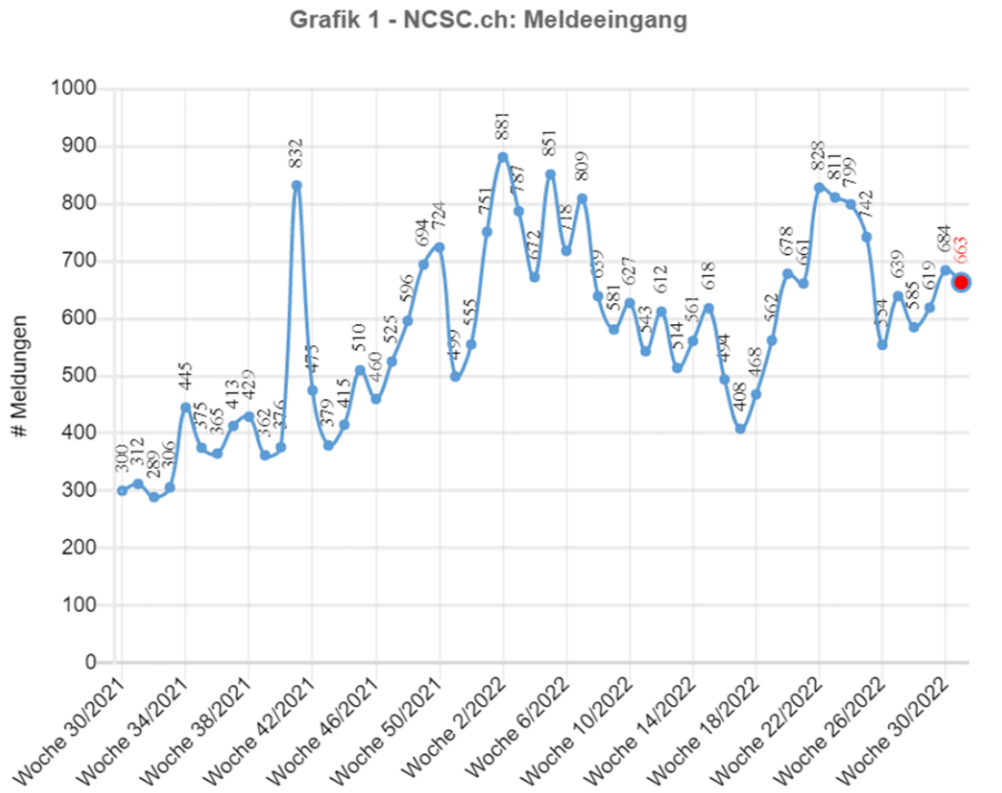
Rahmenbedingungen NCSC

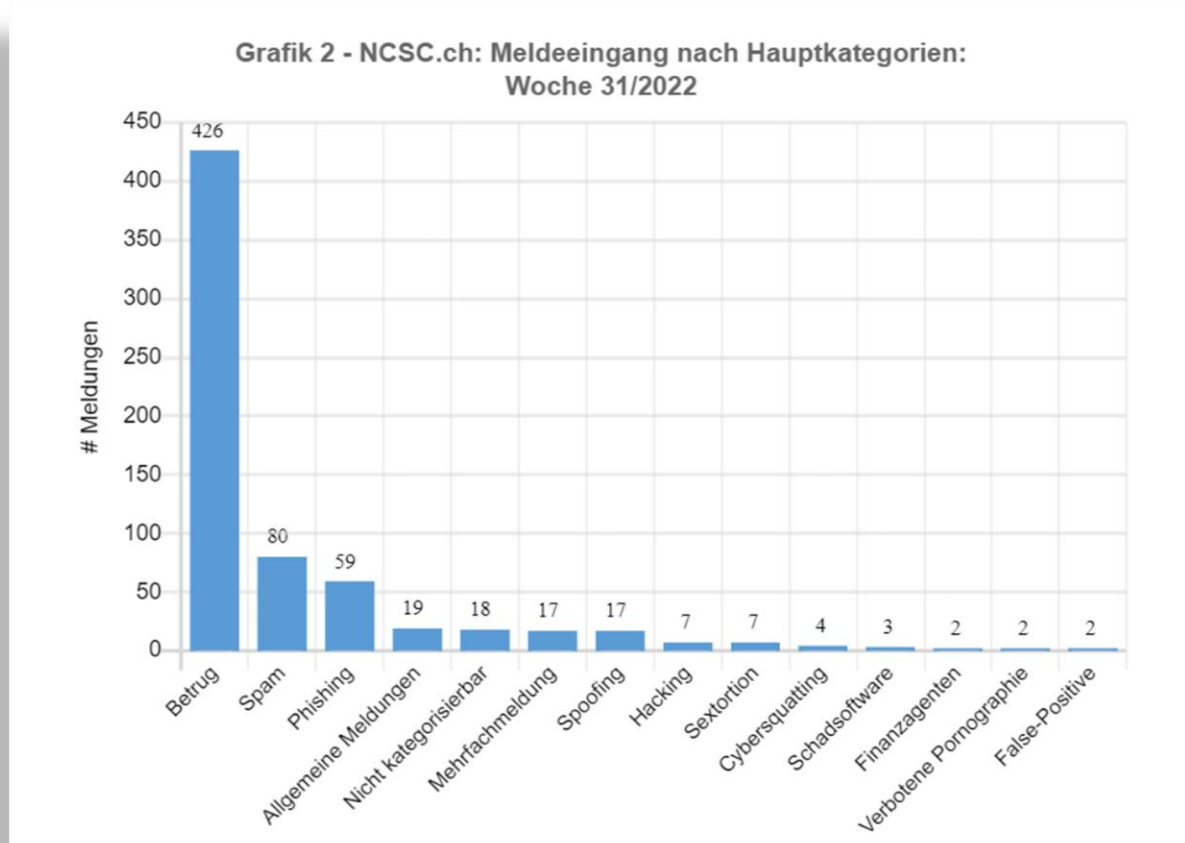
Keine Meldepflicht für Cybervorfälle

Subsidiarität

Keine Weisungsbefugnis ausserhalb der Bundesverwaltung

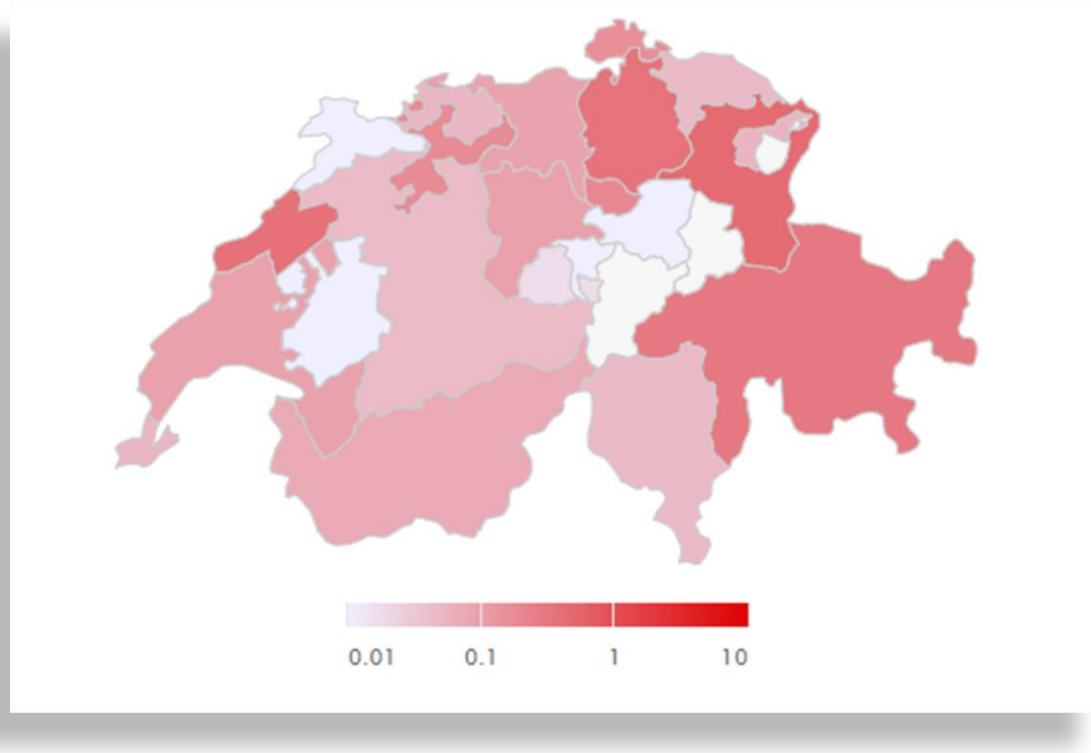
Kennzahlen NCSC (Woche 31/2022)





2. Lage und Akteure

Aktuelle Bedrohungslage



Wie gefährdet sind KMU?

SRF

AZ

Suche

Wirtschaft

Neue Zürcher Zeitung

Hacker attackieren mehrere Schweizer Firmen mit Verschlüsselungs-Trojanern

In den vergangenen Wochen sind namhafte Schweizer Unternehmen Opfer von Cyberattacken geworden. Jetzt warnt die Melde- und Analysestelle Informationssicherung des Bundes (Melani) vor einer neuen Vorgehensweise der Hacker.

© Keystone

Wochen vor allem KMU davor, die Gefahr zu unterschätzen.

KMU sind gefährdeter als Grossunternehmen!

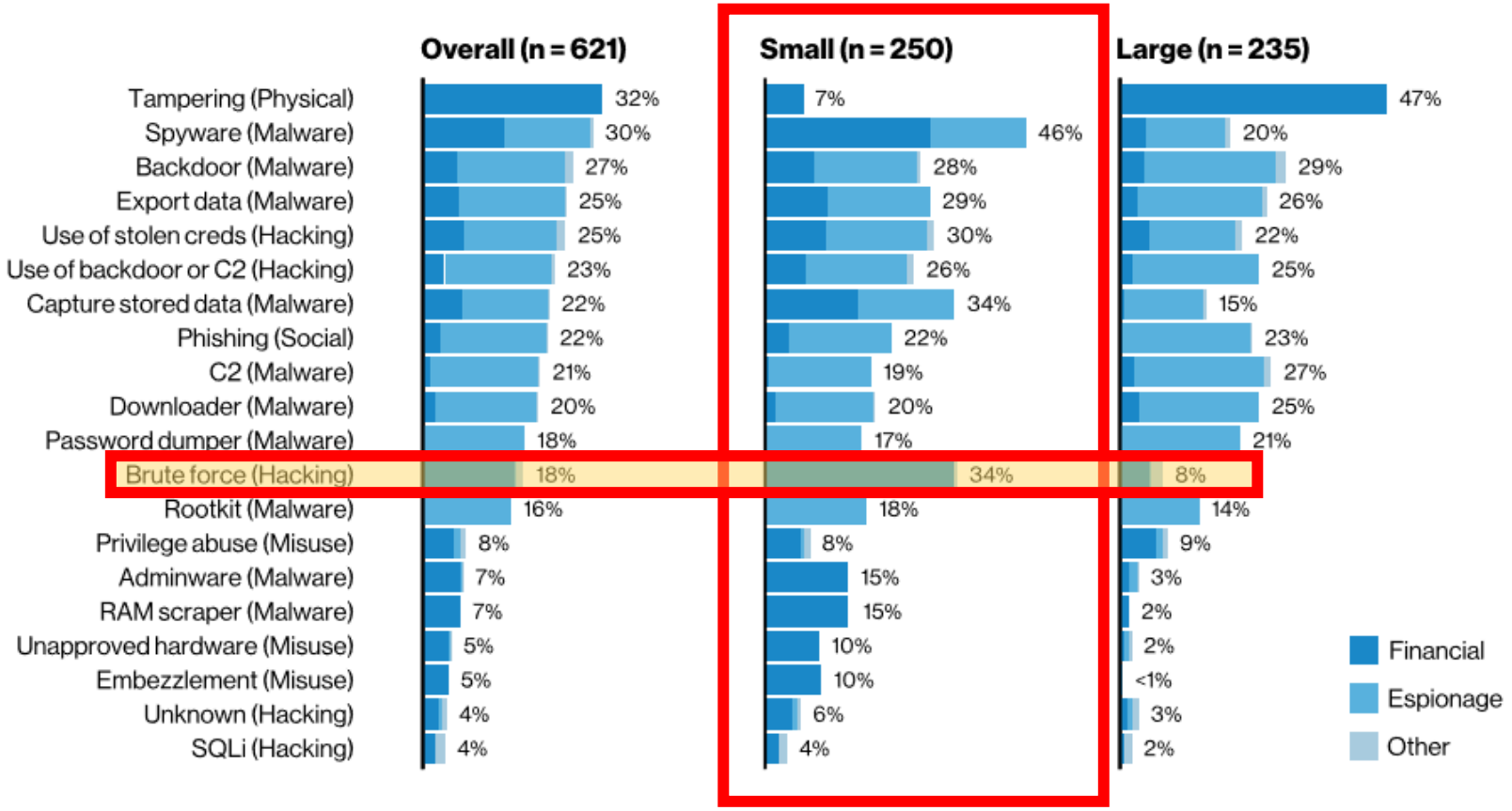
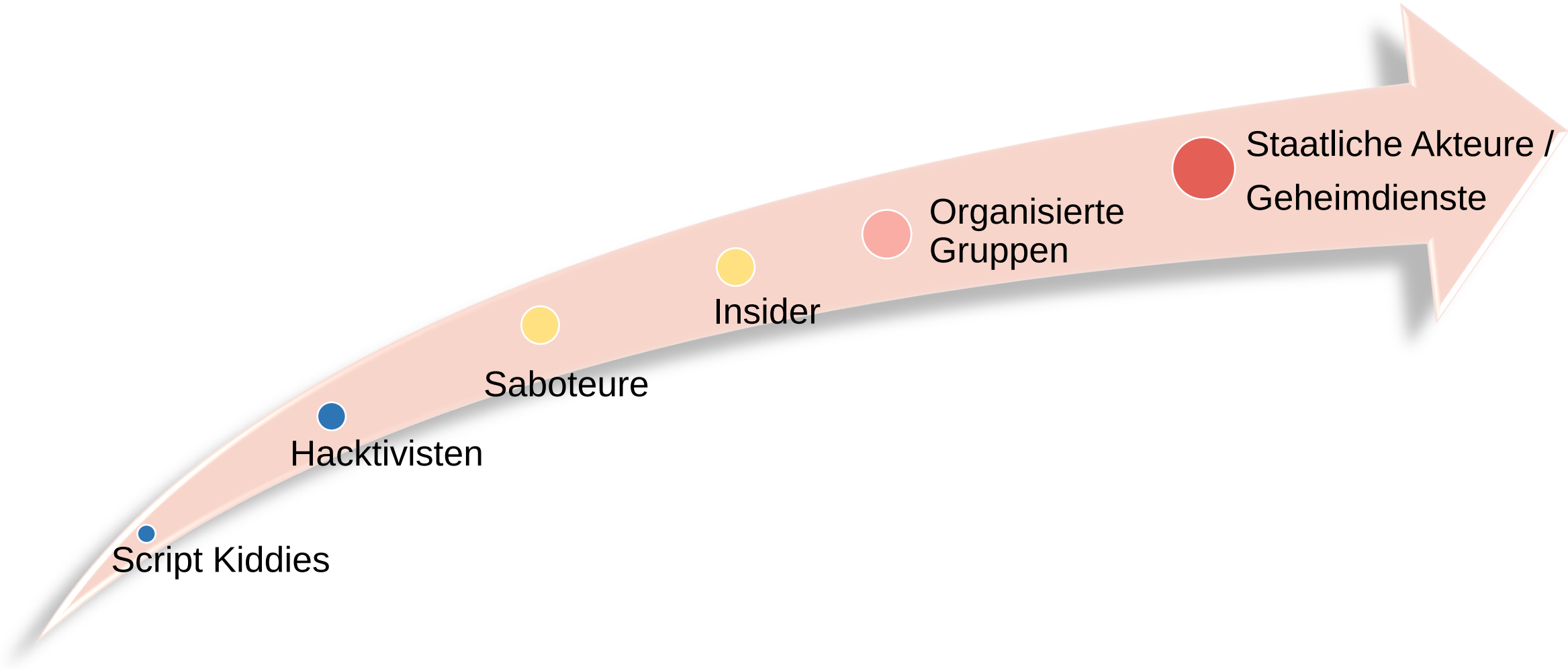
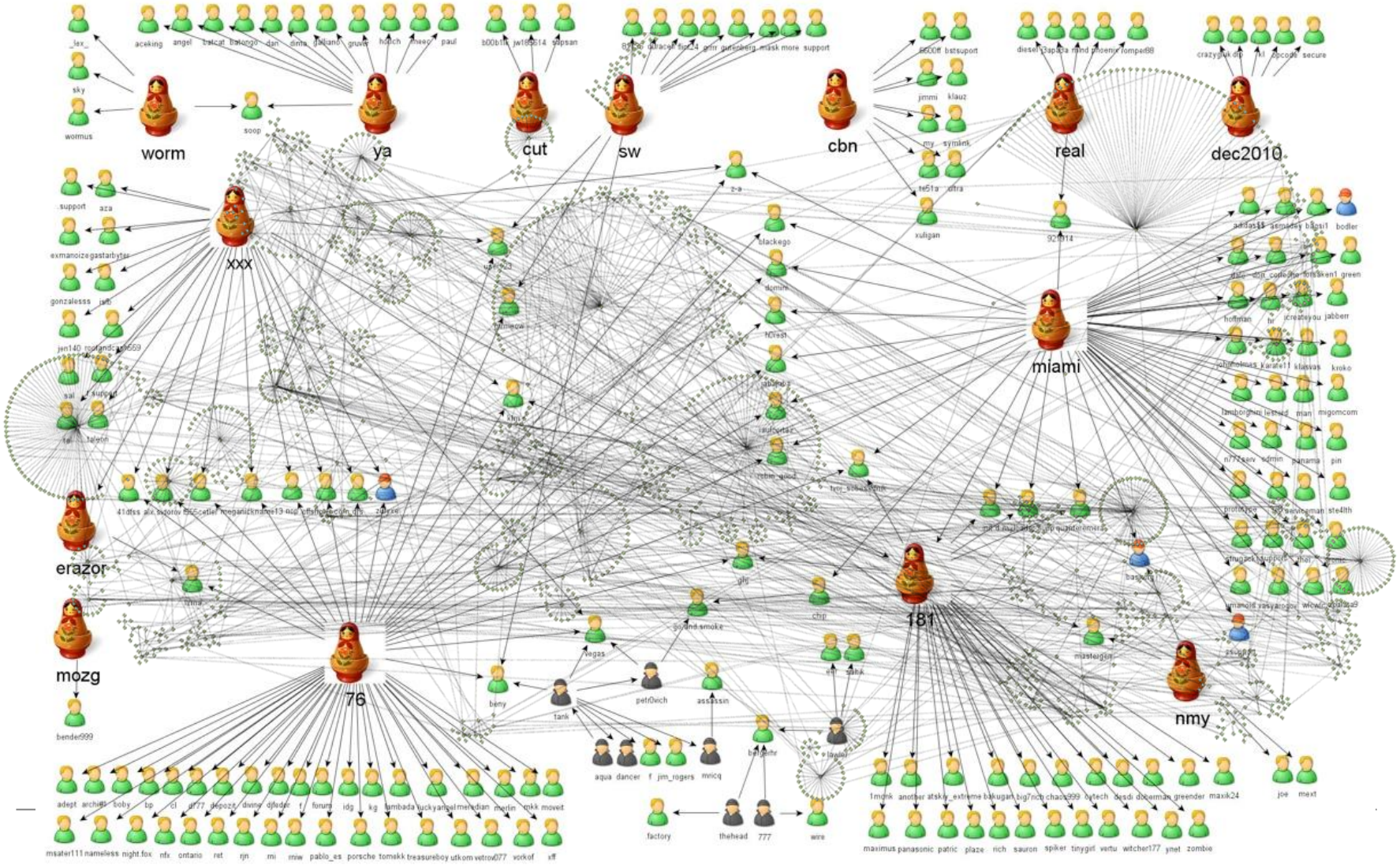


Figure 109. Top 20 threat actions (referencing the 2013 DBIR)

Akteure


Script Kiddies
Hacktivisten
Saboteure
Insider
Organisierte Gruppen
Staatliche Akteure / Geheimdienste

Die Arbeitsteilung bei Cyberattacken

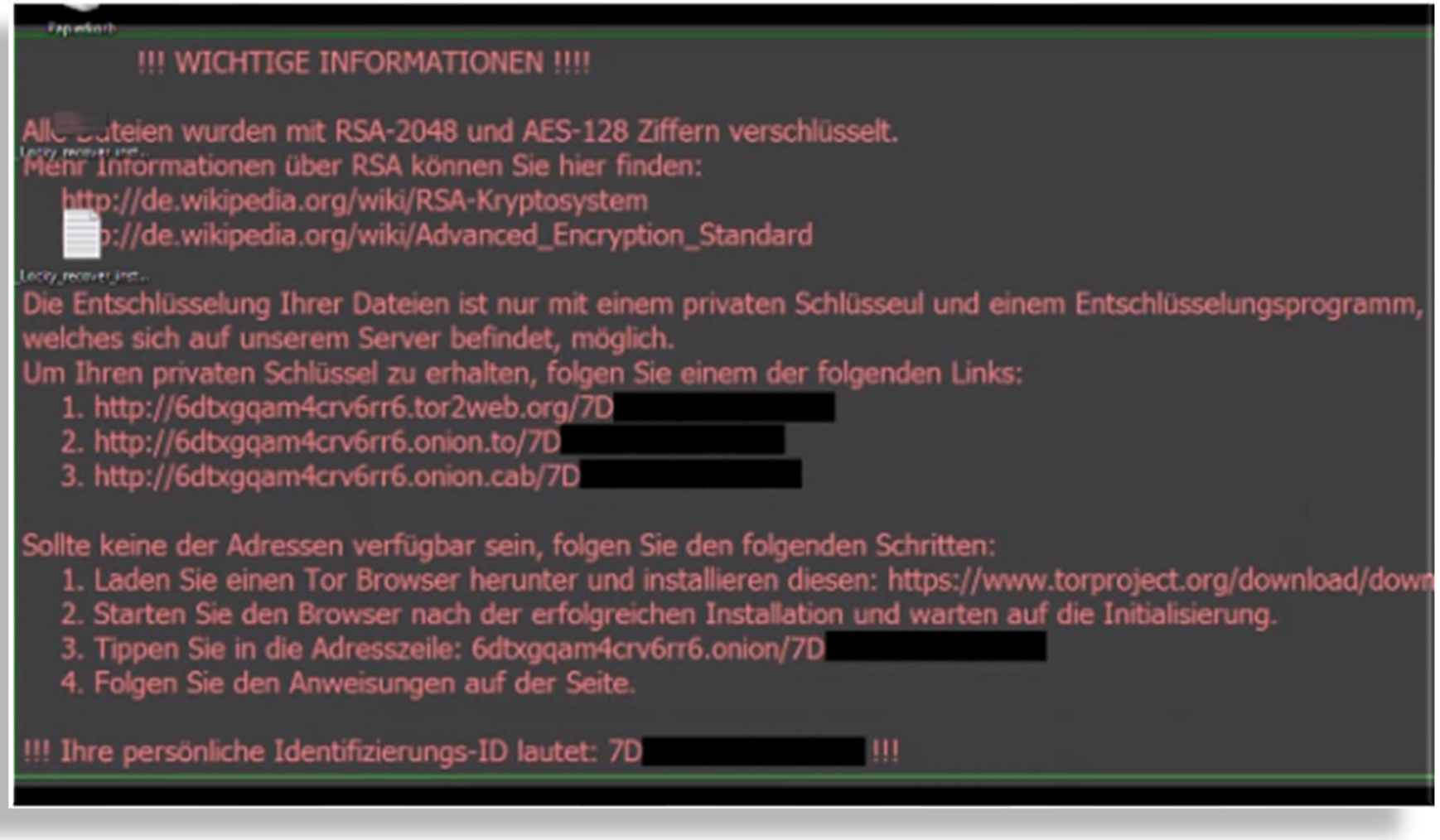


3. Cyberangriffe

Verschlüsselungstrojaner

http://www.trustedwatch.de

Hacker bieten hervorragenden Support!



Verschlüsselungstrojaner: Empfehlungen

- Regelmässige Datensicherung
- Datenträger nach Backup vom PC / Netz trennen
- Qualität der Backups sporadisch überprüfen
- Versuchen Sie, die Daten wiederherzustellen:
  www.nomoreransom.org
- Keinesfalls Lösegeld bezahlen!
- Meldung an ncsc.ch,
  allenfalls Anzeige gegen Unbekannt bei KaPo

4. Schlussfolgerungen

Schlussfolgerungen

- Die Bedrohungslage verändert sich laufend
- Meistens Angriffe nach dem Giesskannenprinzip, gezielte Angriffe selten
- Finanzieller Gewinn als Hauptmotivation
- Alle können Opfer eines Cyber-Angriffs werden
- Gesunder Menschenverstand als «Grundschutz» im privaten Bereich

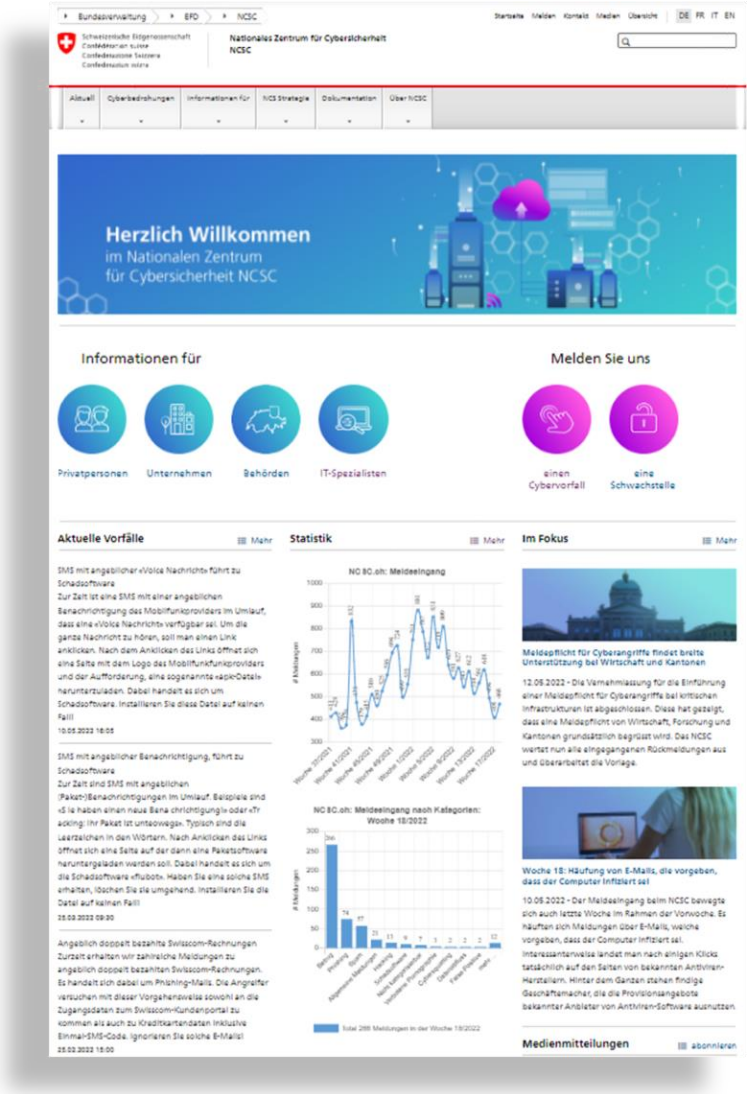
Empfehlungen: proaktiv (1/3)

Besuchen Sie unsere Website:
www.ncsc.admin.ch:

Informationen für:

- Privatpersonen
- Unternehmen
- Behörden
- IT-Spezialisten

Zahlreiche **kostenlose** Anleitungen, Checklisten, Whitepapers.

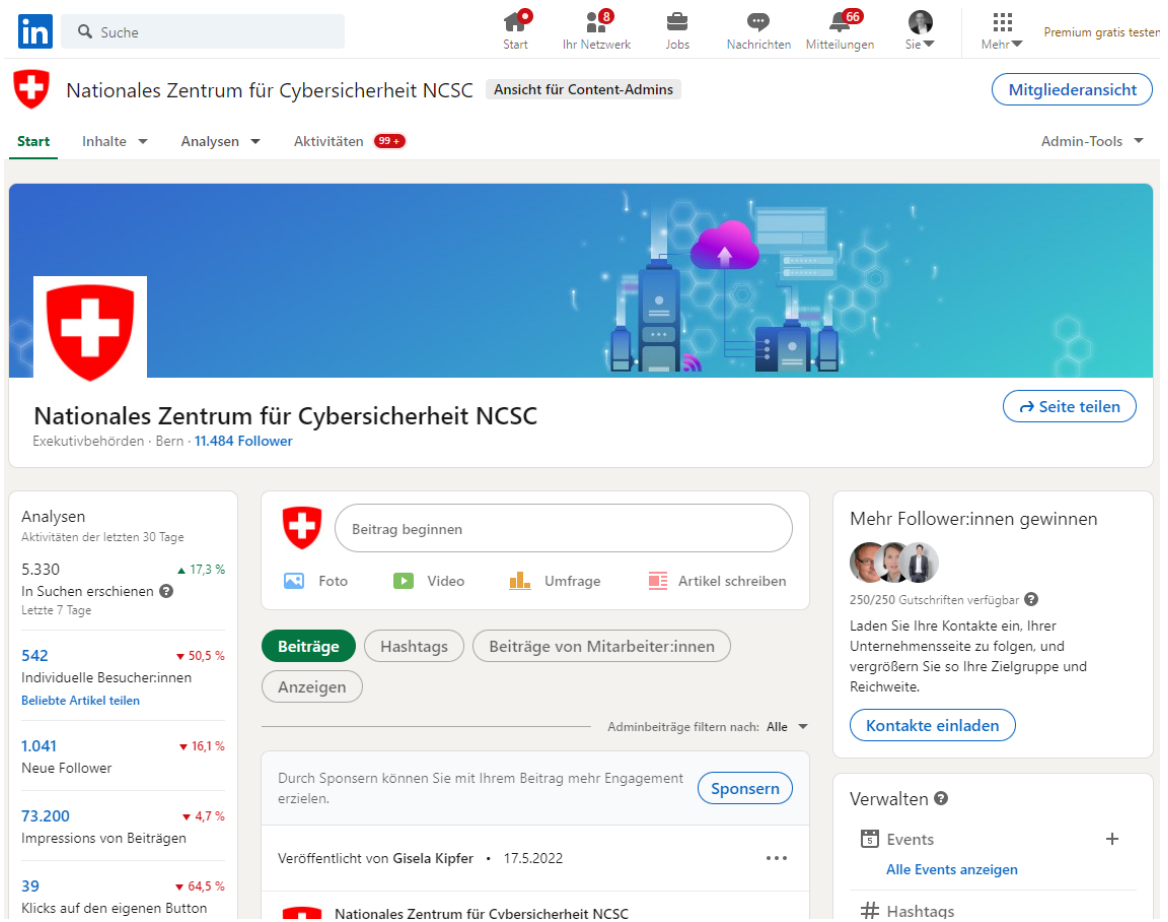


Empfehlungen: proaktiv (2/3)

Folgen Sie uns auf LinkedIn:

https://www.linkedin.com/company/70430924/admin/

- Aktuellste Informationen aus erster Hand
- Beschreibung neuer Vorgehensweisen der Angreifer
- usw.



Empfehlungen: proaktiv (3/3)

Das Übliche zuerst:

- Starke Passwörter / regelmässiger PW-Wechsel
- Virenschutz
- Firewall (blacklist usw.)
- Updates
- Backups

…

Aber:

- Technische Massnahmen allein genügen nicht!
- Organisatorische Massnahmen wie BCM, Krisenkommunikation usw. berücksichtigen!

Empfehlungen: reaktiv

Meldeformular NCSC:

https://www.report.ncsc.admin.ch/de/

Das NCSC garantiert:

- Anonyme Meldungen
- 100% Vertraulichkeit
- Keine Sanktionen (evtl. DSGVO der EU beachten!)
- In der Regel Erstantwort innerhalb von 24 Stunden.

Strafverfolgung:

- Privatpersonen: Kantonspolizei am Wohnsitz
- Unternehmen: Kantonspolizei am Geschäftssitz

Herzlichen Dank für Ihre Aufmerksamkeit

Max Klaus
Stv. Leiter Operative Cybersicherheit OCS
Stv. Leiter Melde- und Analysestelle Informationssicherung MELANI

Schwarztorstrasse 59
3003 Bern

KANTON AARGAU

DEPARTEMENT
VOLKSWIRTSCHAFT UND INNERES

Kantonspolizei Aargau

Digitale Kriminalität

31. August 2022 – Wirtschaftstreffen 2022

Adj Bernhard Droz
Dienstchef IT-Forensik & Cybercrime

"They told me it would not work, and if so, no one would have any interest in it."

"Sie haben mir gesagt, es würde nicht funktionieren, und falls doch, hätte ohnehin niemand Interesse daran."

Leonard Kleinrock, *1934, nachdem er seine Idee, Datenpakete über das Telefonkabel zu versenden, bei den Telefongesellschaften präsentierte.

KANTON AARGAU

Inhaltsverzeichnis

Aufgaben der Strafverfolgung

Evolution und Facetten der Cyberkriminalität

Prävention

Fazit

KANTON AARGAU

Digitalisierung verändert die Kriminalität

> Digitalisierung verändert die Gesellschaft

> Digitalisierung bietet mehr Komfort und viele ökologische und ökonomische Möglichkeiten, Chancen und Vorteile

> Analoge Formen der Tatbegehung werden immer mehr zu digitalen

Aufgaben der Polizei

Prävention

Straf-
verfolgung

Gefahren-
abwehr

→ Schutz und Reparatur von Infrastruktur obliegt den Eigentümern

KANTON AARGAU

Aufgaben der Polizei

→ auch bei Cybercrime

KANTON AARGAU

Wir sind auf Partner angewiesen

www.fedpol.admin.ch

www.europol.europa.eu

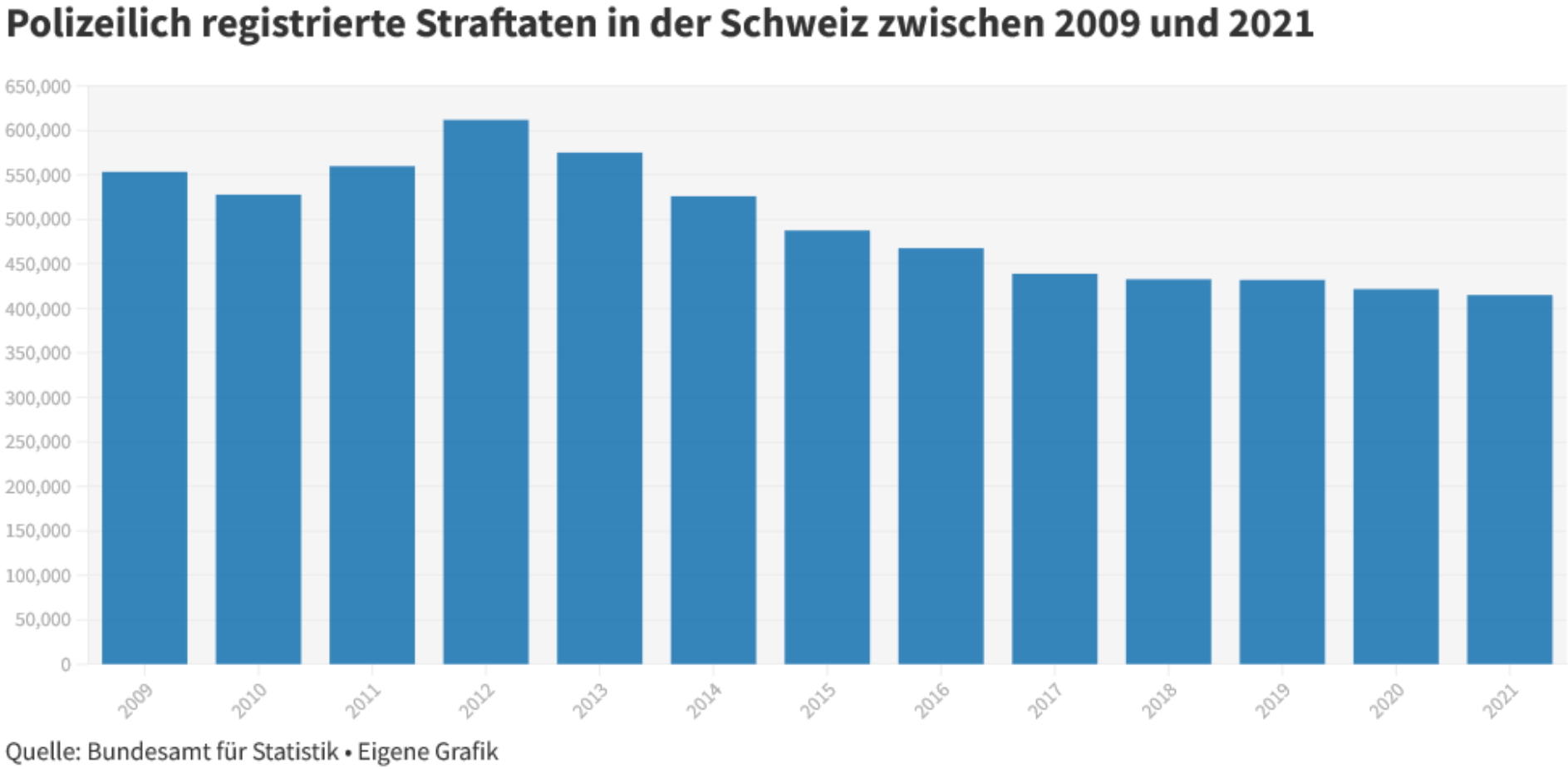
www.cybercrimepolice.ch

www.ncsc.ch

www.skppsc.ch www.ibarry.ch

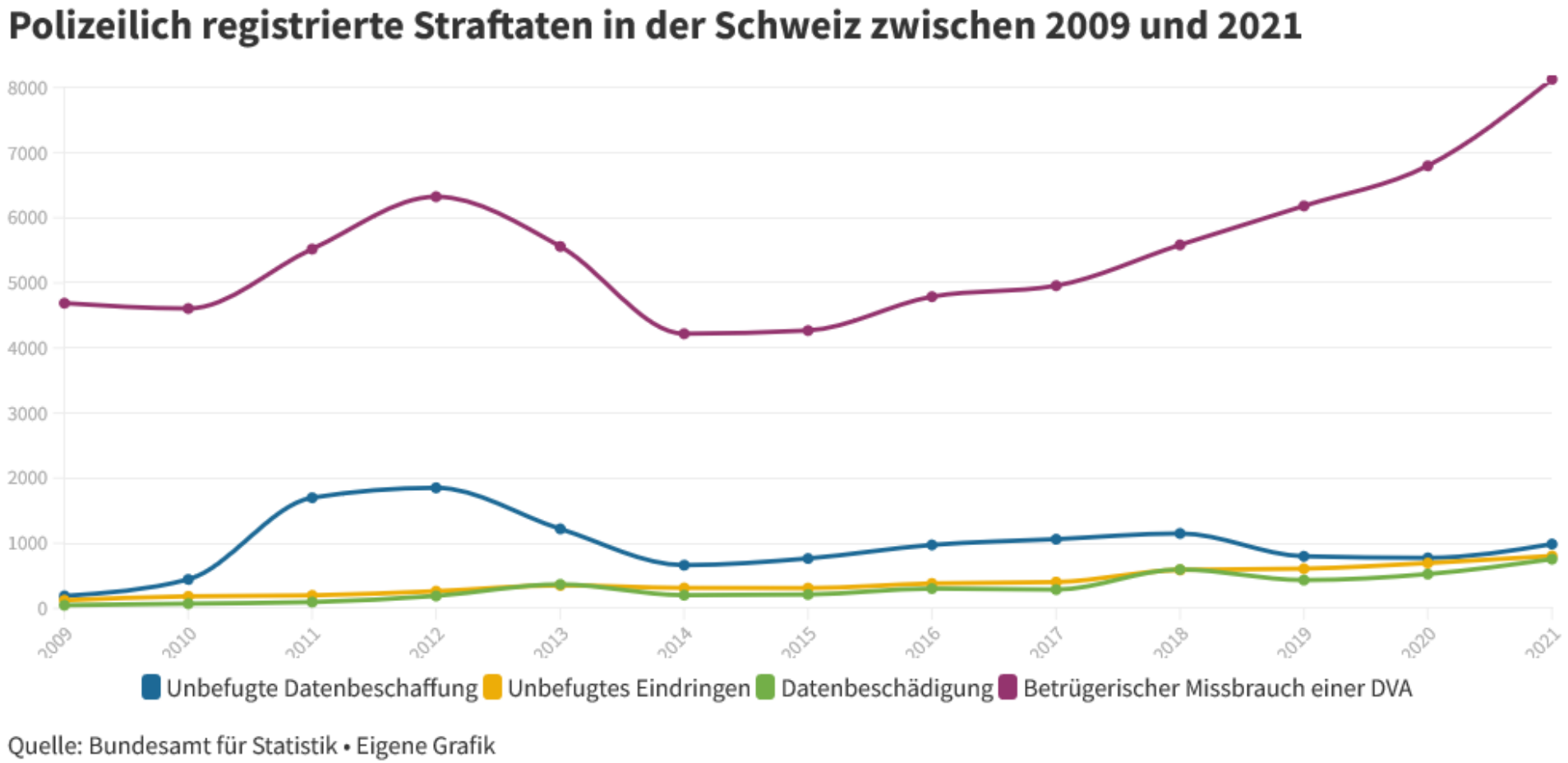
KANTON AARGAU

Evolution der Cyberkriminalität



KANTON AARGAU

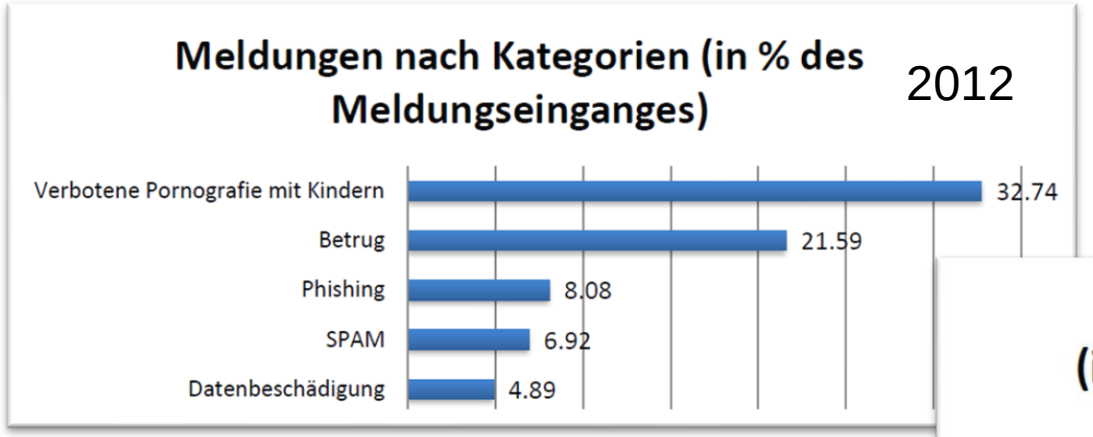
Evolution der Cyberkriminalität

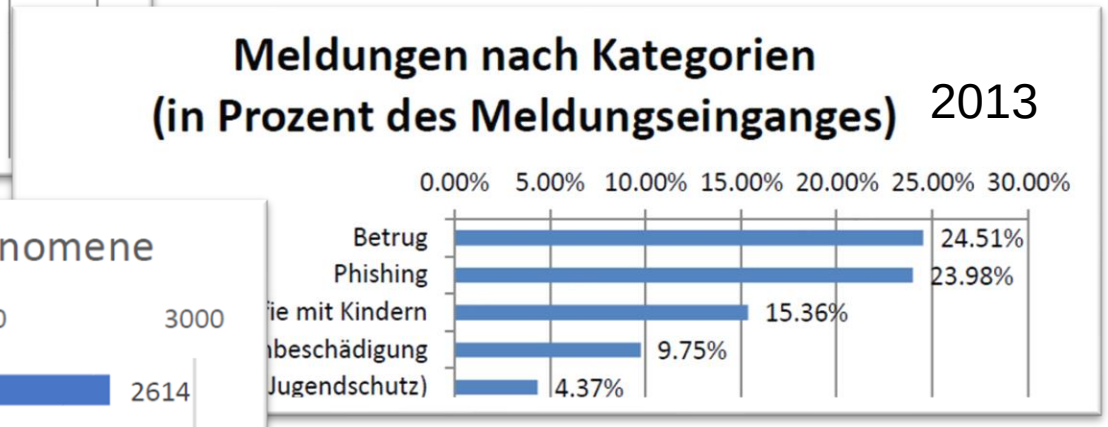


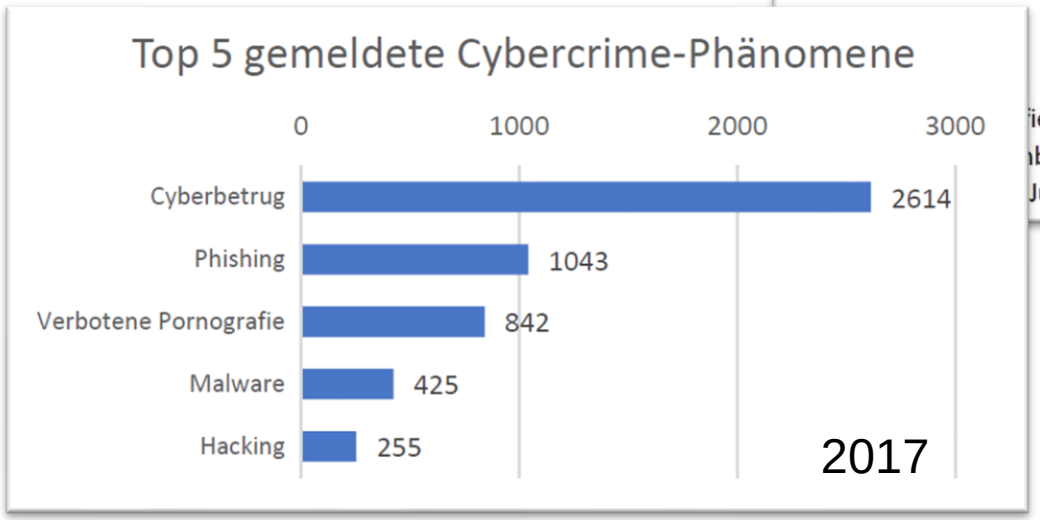
KANTON AARGAU

Evolution der Cyberkriminalität

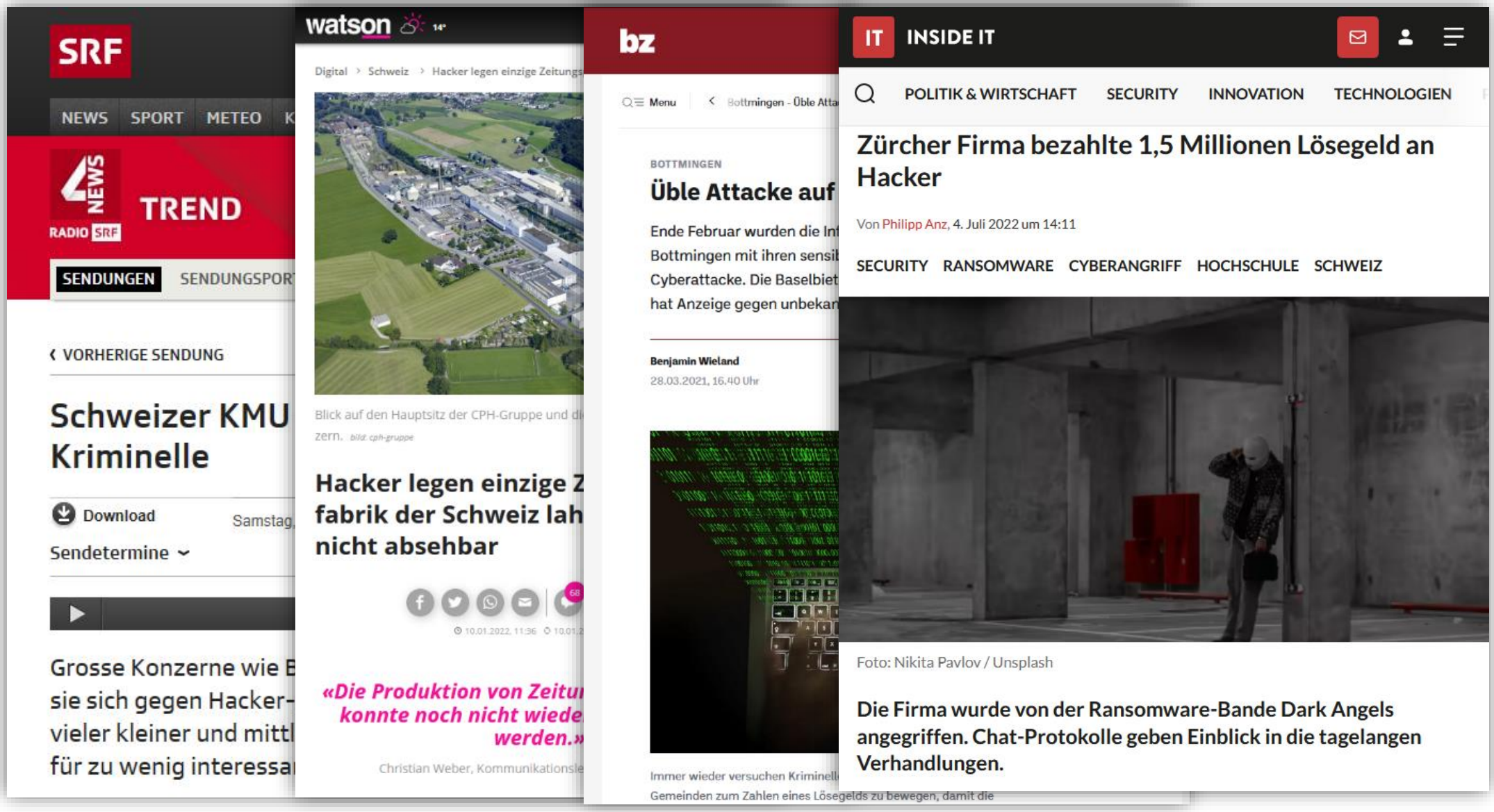
Jahresberichte fedpol/KOBIK





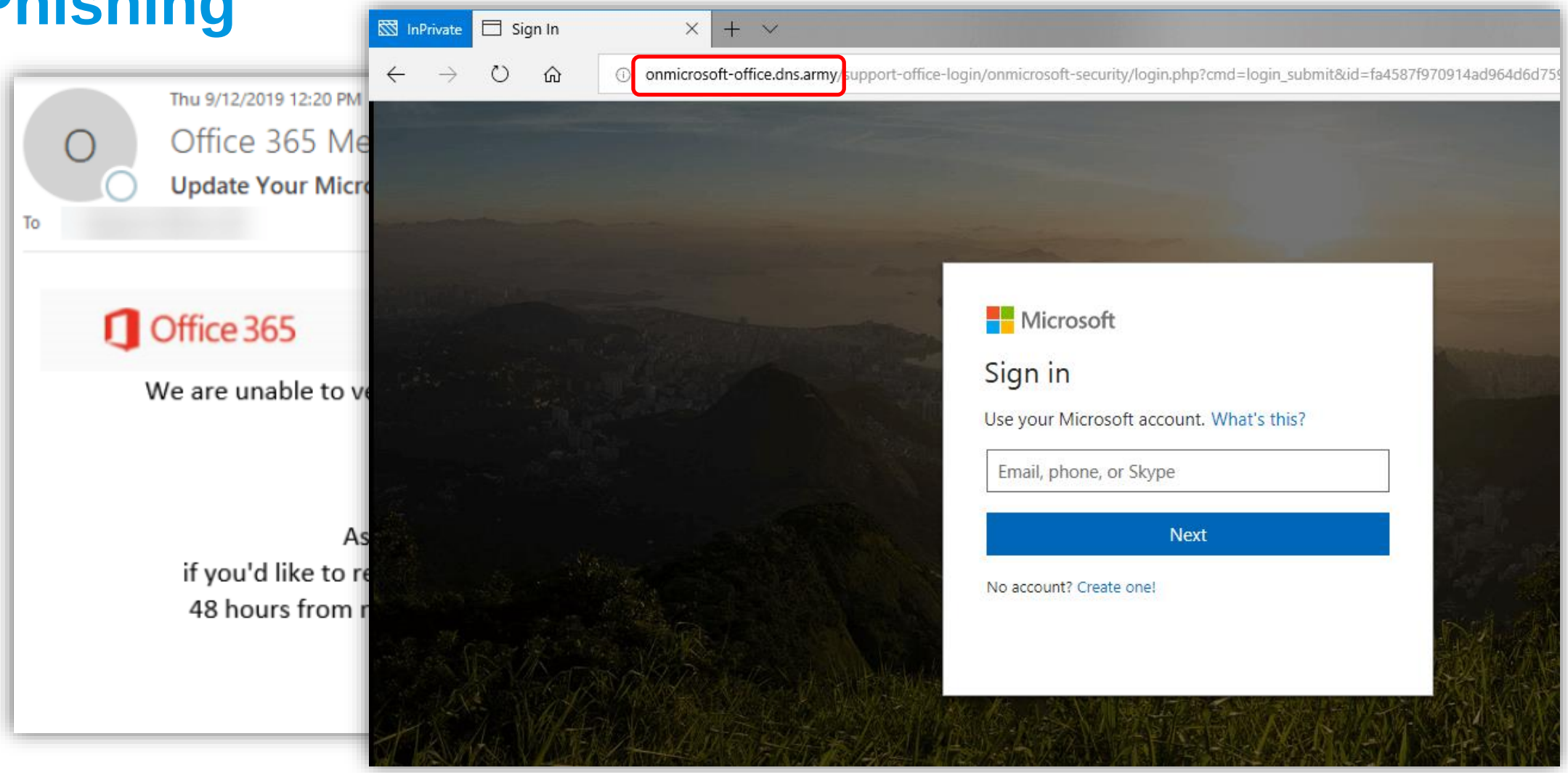


Screenshots fedpol


SRF
NEWS SPORT METEO
TREND
RADIO SRF
SENDUNGEN SENDUNGSPOR
VORHERIGE SENDUNG
Schweizer KMU
Kriminelle
Download
Samstag,
Sendetermine
Grosse Konzerne wie B
sie sich gegen Hacker-
vieler kleiner und mittl
für zu wenig interessa
watson
Digital › Schweiz › Hacker legen einzige Zeitungs
Blick auf den Hauptsitz der CPH-Gruppe und di
zern. bild: cph-gruppe
Hacker legen einzige Z
fabrik der Schweiz lah
nicht absehbar
«Die Produktion von Zeitu
konnte noch nicht wiede
werden.»
Christian Weber, Kommunikationsle
bz
Menu
Bottmingen - Üble Atta
BOTTMINGEN
Üble Attacke auf
Ende Februar wurden die Inf
Bottmingen mit ihren sensib
Cyberattacke. Die Baselbiet
hat Anzeige gegen unbekan
Benjamin Wieland
28.03.2021, 16.40 Uhr
Immer wieder versuchen Kriminell
Gemeinden zum Zahlen eines Lösegelds zu bewegen, damit die
IT INSIDE IT
POLITIK & WIRTSCHAFT SECURITY INNOVATION TECHNOLOGIEN
Zürcher Firma bezahlte 1,5 Millionen Lösegeld an Hacker
Von Philipp Anz, 4. Juli 2022 um 14:11
SECURITY RANSOMWARE CYBERANGRIFF HOCHSCHULE SCHWEIZ
Foto: Nikita Pavlov / Unsplash
Die Firma wurde von der Ransomware-Bande Dark Angels angegriffen. Chat-Protokolle geben Einblick in die tagelangen Verhandlungen.

KANTON AARGAU

Phishing



Screenshots: appriver.com

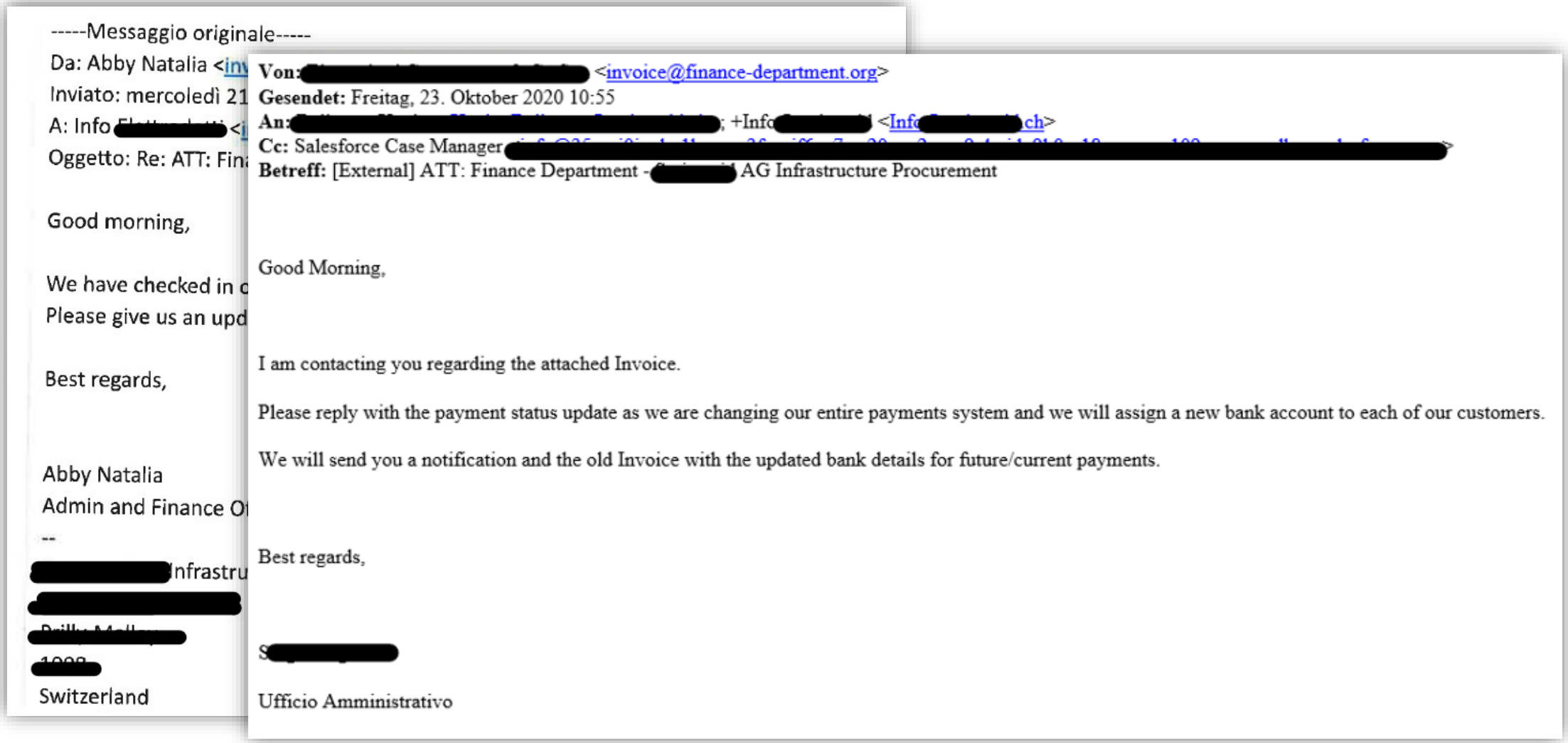
KANTON AARGAU

Phishing

- Vorsicht vor allen Mails, die eine dringende Aktion Ihrerseits und/oder Drohungen enthalten.
- Kontrollieren Sie die Zieladresse.
  microsoft.support.online - mircosoft.de - rnicrosoft.info
- Absolvieren Sie das Phishing-Quiz von Google unter https://phishingquiz.withgoogle.com/.
- Wenn man gephisht wurde: Passwort ändern, Kreditkarte sperren und/oder Bank informieren.
- Information an www.ncsc.ch / www.antiphishing.ch.
- Bei entstandenem Schaden: Strafanzeige gegen Unbekannt bei Polizei.

KANTON AARGAU

Business E-Mail Compromise



-----Messaggio originale-----
Da: Abby Natalia <[redacted]
Inviato: mercoledì 21
A: Info [redacted]
Oggetto: Re: ATT: Fina

Good morning,

We have checked in c
Please give us an upd

Best regards,

Abby Natalia
Admin and Finance Of
--
[redacted]nfrastru
[redacted]
[redacted]
[redacted]
Switzerland

Von: [redacted] <invoice@finance-department.org>
Gesendet: Freitag, 23. Oktober 2020 10:55
An: [redacted]; +Info [redacted] <Info [redacted]ch>
Cc: Salesforce Case Manager [redacted]
Betreff: [External] ATT: Finance Department - [redacted] AG Infrastructure Procurement

Good Morning,

I am contacting you regarding the attached Invoice.

Please reply with the payment status update as we are changing our entire payments system and we will assign a new bank account to each of our customers.

We will send you a notification and the old Invoice with the updated bank details for future/current payments.

Best regards,

S[redacted]

Ufficio Amministrativo

KANTON AARGAU

Business E-Mail Compromise

- Vorsicht vor allen Mails, die eine dringende Aktion Ihrerseits und/oder Drohungen enthalten.
- Halten Sie die geregelten Prozesse ein.
- Verifizieren Sie den Auftrag durch telefonische Rücksprache.
- Informieren Sie den Absender, dass sein E-Mail-Konto eventuell kompromittiert wurde.
- Wenn die Zahlung bereits getätigt wurde, informieren Sie umgehend die Bank.
- Werden in Ihrem Namen manipulierte Rechnungen versendet, ist davon auszugehen, dass Ihr E-Mail-Konto kompromittiert wurde.
- Information an www.ncsc.ch.
- Bei entstandenem Schaden: Strafanzeige gegen Unbekannt bei Polizei.

KANTON AARGAU

Facetten der Cyberkriminalität

- Anonymität des Internets auf Opfer- und Täterseite
- Hemmschwelle sinkt aufgrund der Distanz zwischen Tätern und Opfern.
- Bewusstsein und Selbstbefähigung verkleinern das Risiko.

"On the Internet, nobody knows you're a dog."

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

KANTON AARGAU

Prävention

- Sensibilisierung für Sicherheits- und Computerbedrohungen im Unternehmen.
- Incident Response Playbook: Bereiten Sie sich auf einen Cybervorfall vor!
- Schulung von Mitarbeitern durch einen spezialisierte Kurse.
- Klare Richtlinien für soziale Medien festlegen.
- Halten Sie die Schutzsysteme für Hard- und Software auf dem neuesten Stand.
- Durchsetzung von Passwortrichtlinien, Verwendung von Passwortmanager und 2-Faktor-Authentisierung.
- Sichern Sie Ihre Daten!

KANTON AARGAU

Prävention

www.polizei-ag.ch → Prävention → Cybercrime

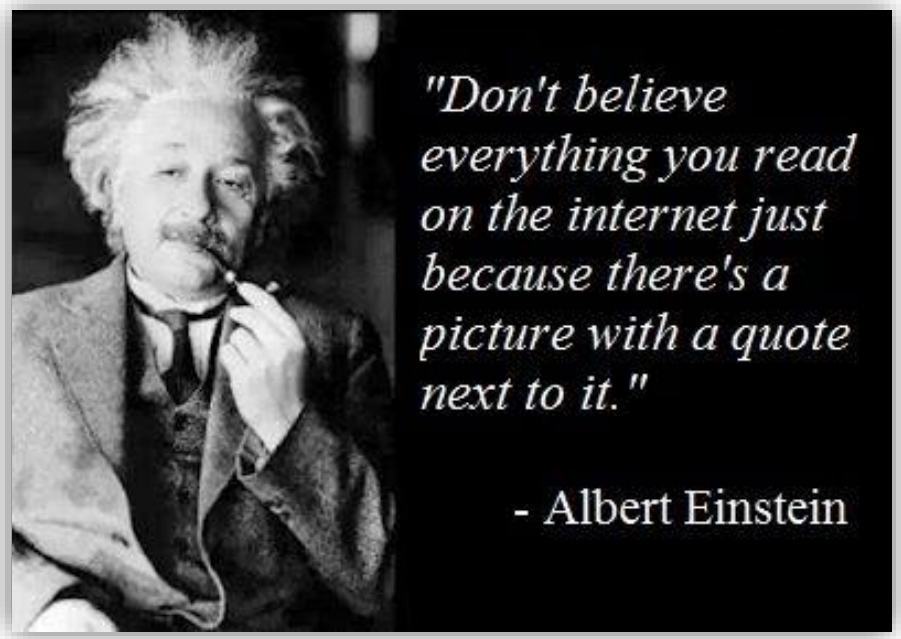
KANTON AARGAU

Fazit

> Halten Sie sich an Empfehlungen bezüglich Cybersecurity und Prävention.

> Machen Sie den #realitycheck

> Melden Sie sich bei der Polizei oder beim NCSC.



Es geht nicht nur um Sie, es geht auch darum, andere zu schützen!

digitalswitzerland
Schweizer Digitaltage

ZUSAMMEN GESTALTEN WIR DIE DIGITALE ZUKUNFT

13.09.2022 in Aarau und Liestal

https://digitaltage.swiss/

KANTON AARGAU

DEPARTEMENT
VOLKSWIRTSCHAFT UND INNERES

Kantonspolizei Aargau
Adj Bernhard Droz
Dienstchef IT-Forensik & Cybercrime
bernhard.droz@kapo.ag.ch

Wirtschaftstreffen 2022

Podiumsdiskussion

- **Max Klaus**, Stellvertretender Leiter zur Melde- und Analysestelle Informationssicherung und stellvertretender Leiter Operative Cybersicherheit im NCSC
- **Bernhard Droz**, Dienstchef IT-Forensik & Cybercrime (IFC) von der Kantonspolizei Aargau
- **Peter Bierhalter**, Geschäftsführer & Verwaltungsratsvorsitzender PRESSTRADE AG
- **Jürg Gasser**, Leiter Abteilung Finanzen & Ressourcen Stadt Rheinfelden

Wirtschaftstreffen 2022

Vielen Dank an die Referenten / Podiumsteilnehmer und an die Moderatorin

Wirtschaftstreffen 2022

Vielen Dank an die Sponsoren!