

# Cybercrime

## Aktuelle Bedrohungslage und Sicherheit im Internet

30. September 2024 – Fachtagung AZSV

**"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.

# 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



## Aufgaben der Polizei



→ auch bei Cybercrime

**Aargauer Zeitung**

Menu | Startseite > Aargau > Aarau >

**HACKERANGRIFF**

## Informatikserver der Stadt Aarau angegriffen – was heisst das für Aarau?

Die Stadt Baden wurde Opfer eines Cyberangriffs, aber ebenso der Stadt Aarau. Diese beiden Städte sind betroffen ist – derweil kommen aus beiden Städten Fragezeichen.

Florian Wicki  
05.12.2023, 15:30 Uhr  
Jetzt kommentieren

**Exklusiv für Abonnenten**



Die Stadt Baden wurde Opfer eines Cyberangriffs, aber ebenso der Stadt Aarau. Diese beiden Städte sind betroffen ist – derweil kommen aus beiden Städten Fragezeichen.

**watson** 10°

Digital > Schweiz > Hacker schlagen in der Schweiz zu: Die Comput...

**Beobachter Digital** Shop

**DRAMATISCHER ANSTIEG DER ANGRIFFE**

## Hacker stürzen sich auf Schweizer Firmen

Die Comput... schon wi... trifft es e...

Neue Zürcher Zeitung

### Cyberkriminelle haben den Textilmaschinenhersteller Saurer gleich zweimal angegriffen

Ein Ransomware-Angriff ist eine Cyberattacke, bei der der Opfer verschlüsseln, um ein Lösegeld (englisch: «ransom») zu erlangen.

*bildmontage: watson*

## Gefürchtete Cybercrime der Schweiz zu: Die unfassbare...

Im Schatten der Corona-Pandemie tobt die Cyberkriminalität meist unbemerkt werden Schweizer Unternehmen erbeutete Daten im Darknet gehandelt. Die Hacking-Opfer.

90

News folgen

26.01.2022, 05:28 | 07.02.2022, 08:51

**IT INSIDE IT**

POLITIK & WIRTSCHAFT SECURITY INNOVATIONEN

## In der Schweiz vergeht kein Tag ohne Ransomware-Angriff

Von Philipp Anz, 14. Juli 2023 um 09:00

SECURITY CYBERANGRIFF RANSOMWARE XPLAIN



Illustration: Midjourney

## Die Cyberkriminellen erzielen Rekordgewinn durch Lösegeldforderungen. Wie ist die Lage in der Schweiz?

**Blick** DE | FR 10° B+

NEWS

News | Daten des Fedpol im Darknet aufgetaucht

## Auch Zoll betroffen

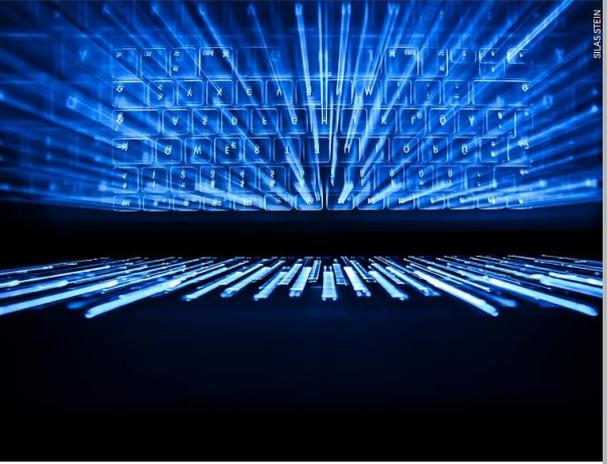
# Hacker veröffentlichen Fedpol-Daten im Darknet

Der nächste Cyberangriff erschüttert die Schweizer Behörden. Dieses Mal wurden das Bundesamt für Polizei und der Zoll Opfer von Hackern.

Publiziert: 03.06.2023 um 11:56 Uhr | Aktualisiert: 03.06.2023 um 14:27 Uhr

f X T E

9

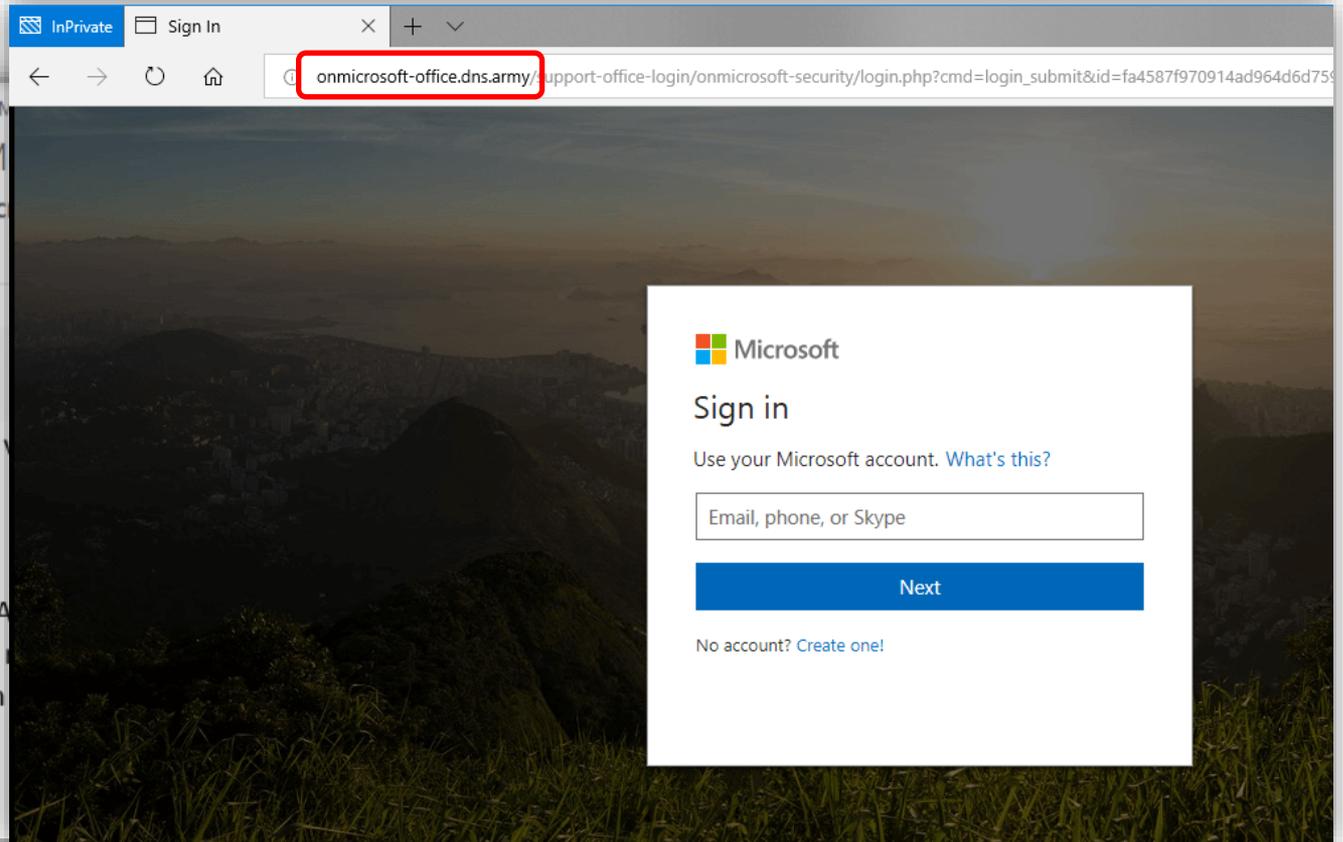
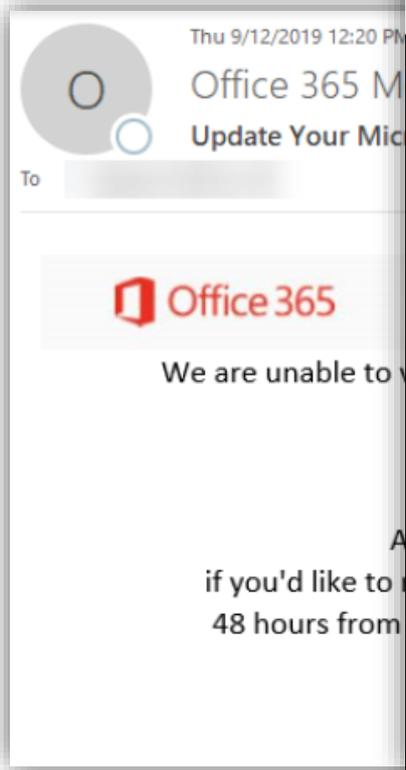


SILVIA STEIN

Hacker nutzten eine Schwachstelle auf den Servern einer Firma aus, die Daten des Bundes beherbergt (Archiv).

Screenshots: aargauerzeitung.ch, watson.ch, inside-it.ch, blick.ch

# Phishing



Screenshots: [appriver.com](https://www.appriver.com/) / [ncsc.ch](https://www.ncsc.ch/)

# Phishing – Delivery Services

The image displays three screenshots of phishing websites designed to look like legitimate delivery services. The first screenshot is for 'DIE POST', featuring a yellow header with the logo and a 'Betriebsdaten' section containing fields for 'Handel', 'Befehl', and 'Importiert'. Below this is a 'Mit Karte bezahlen' section with logos for VISA and Mastercard, and a 'Bezahlen Sie mit Kreditkarte' prompt. Input fields are provided for 'Kartennummer', 'Sicherheitscode', and 'Ablaufdatum'. A 'Zahlen' button is at the bottom. The second screenshot is for 'DHL Express', showing a failed delivery attempt notification. It includes a red envelope icon, the text 'A failed delivery attempt.', and instructions to confirm shipping and payment information. It also displays a date of '2022-07-15', a fee of '3,57 \$', and a tracking number field with the value 'JJ00020859' and a 'Keep going' button. The third screenshot is for 'dpdgroup', with a red cube logo and a 'Paketzustellung wartet auf Versandzahlung' header. It contains a message about payment confirmation, a 'Gesamt' of '2,99 euro', an 'Auftragsnummer' of 'UP20100253652CH', and a 'Sicheres Bezahlen mit Mastercard®' section with a 'Vollständiger Name' input field.

Screenshots: nscs.ch

# Phishing – Swisscom

Get a free website with **yola**

Start now



## Swisscom Login

Nom d'utilisateur ou numéro de mobile

Mot de passe



## Swisscom Login

Melden Sie sich bitte mit Ihrem Benutzernamen oder Ihrer Mobilnummer an.

Benutzername oder Mobilnummer

Passwort

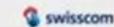
← Zurück

Weiter

Benutzername oder Passwort vergessen?

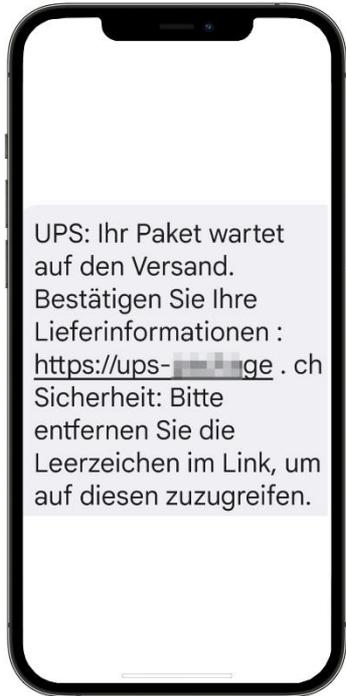
Registrieren

Hjælp ?



Screenshots: nsc.ch

# Smishing – Vishing – Quishing



Screenshots: cybercrimepolice.ch, iStock

# Phishing

- > Vorsicht vor allen Nachrichten, 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](http://www.ncsc.ch) / [www.antiphishing.ch](http://www.antiphishing.ch).
- > Bei entstandenem Schaden: Strafanzeige gegen Unbekannt bei Polizei.

# Ransomware

**LOCKBIT 2.0**

**ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!**

All your files stolen and encrypted  
for more information see  
**RESTORE-MY-FILES.TXT**  
that is located in every encrypted folder.

Would you like to earn millions of dollars?  
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.  
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.  
Open our letter at your email. Launch the provided virus on any computer in your company.  
Companies pay us the foreclosure for the decryption of files and prevention of data leak.  
You can communicate with us through the Tox messenger.

Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.  
If you want to contact us, use ToxID:  
[REDACTED]

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser  
[REDACTED]

Screenshot: trendmicro.com

# Ransomware

- > Regelmässige Datensicherung
- > Datenträger nach Backup vom PC / Netz trennen
- > Qualität der Backups sporadisch überprüfen
- > Versuchen Sie, die Daten wiederherzustellen: [www.nomoreransom.org](http://www.nomoreransom.org)
- > Keinesfalls Lösegeld bezahlen!
- > Information an [www.ncsc.ch](http://www.ncsc.ch)
- > Bei entstandenem Schaden: Strafanzeige gegen Unbekannt bei Polizei

# Business E-Mail Compromise

-----Messaggio originale-----

Da: Abby Natalia <[abby.natalia@infrastruttura.ch](mailto:abby.natalia@infrastruttura.ch)>

Inviato: mercoledì 21 ottobre 2020 10:55

A: Info <[info@infrastruttura.ch](mailto:info@infrastruttura.ch)>

Oggetto: Re: ATT: Fin

Von: [REDACTED] <[invoice@finance-department.org](mailto:invoice@finance-department.org)>

Gesendet: Freitag, 23. Oktober 2020 10:55

An: [REDACTED]; +Info <[Info@infrastruttura.ch](mailto:Info@infrastruttura.ch)>

Cc: Salesforce Case Manager <[Salesforce@infrastruttura.ch](mailto:Salesforce@infrastruttura.ch)>

Betreff: [External] ATT: Finance Department - [REDACTED] AG Infrastructure Procurement

Good morning,

We have checked in c

Please give us an upd

Best regards,

Abby Natalia

Admin and Finance O

--

[REDACTED]nfrastru

[REDACTED]

Drillo, M. H.

1000

Switzerland

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,

[REDACTED]

Ufficio Amministrativo

# Business E-Mail Compromise

- > Vorsicht vor allen Nachrichten, 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](http://www.ncsc.ch).
- > Bei entstandenem Schaden: Strafanzeige gegen Unbekannt bei Polizei.

# Das Ende des E-Mails



Verschlüsselung  
PGP S/MIME



Dateifreigabe-  
Dienste

# Was kann ich tun?

Cybersicherheit ist Chefsache!

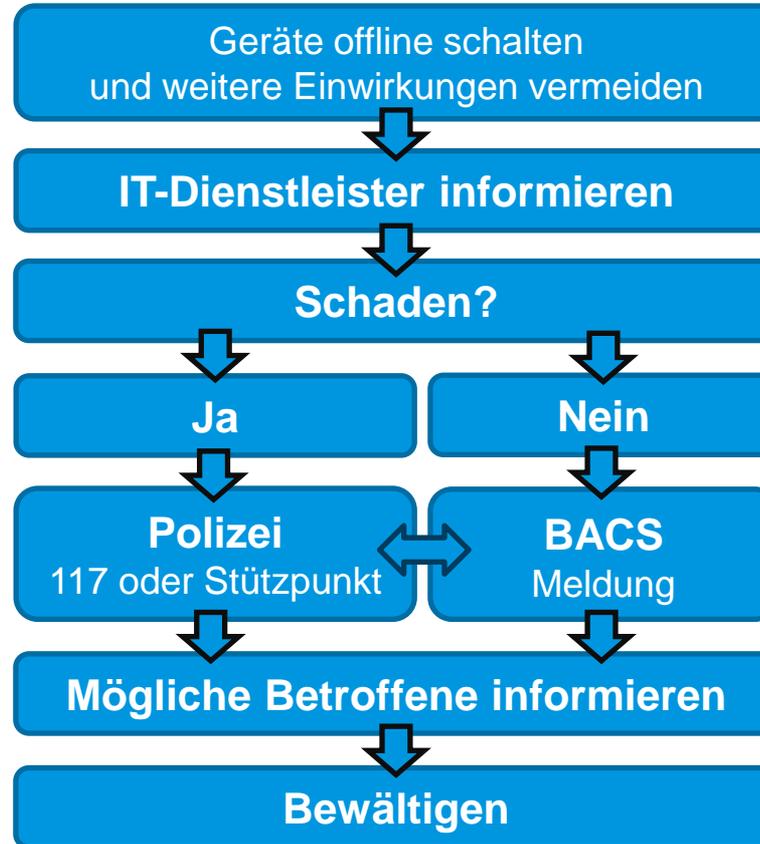
Bereiten sie sich vor!

Trainieren sie ihre Mitarbeiter!

Polizei ist Teil der Lösung!



# Cyberangriff - was nun?



# Awareness

Problembewusstsein und sicheres Verhalten im Internet.

- > Wer wurde bereits Opfer eines Datenlecks, eines Hacks oder von Cybercrime?
- > <https://haveibeenpwned.com/>

# Awareness

# eCyAd

## E-Learning zur Informationssicherheit für Behörden Zum Schutz der Schweiz vor Cyber-Risiken



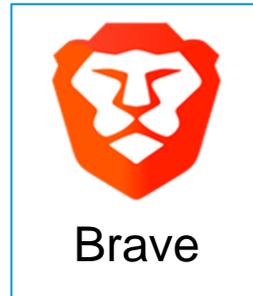
Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren  
Conférence des directrices et directeurs des départements cantonaux de justice et police  
Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia



Sicherheitsverbund Schweiz  
Réseau national de sécurité  
Rete integrata Svizzera per la sicurezza

<https://elearningcyber.ch/>

# Browser – Das Tor ins Internet



<https://www.mozilla.org/de/firefox/browsers/compare/>

# Browser-Erweiterungen (Addons)



uBlock origin



Consent-O-Matic



Facebook  
Container



Search by Image

# Passwörter



<https://bitwarden.com/>



<https://www.dashlane.com/>



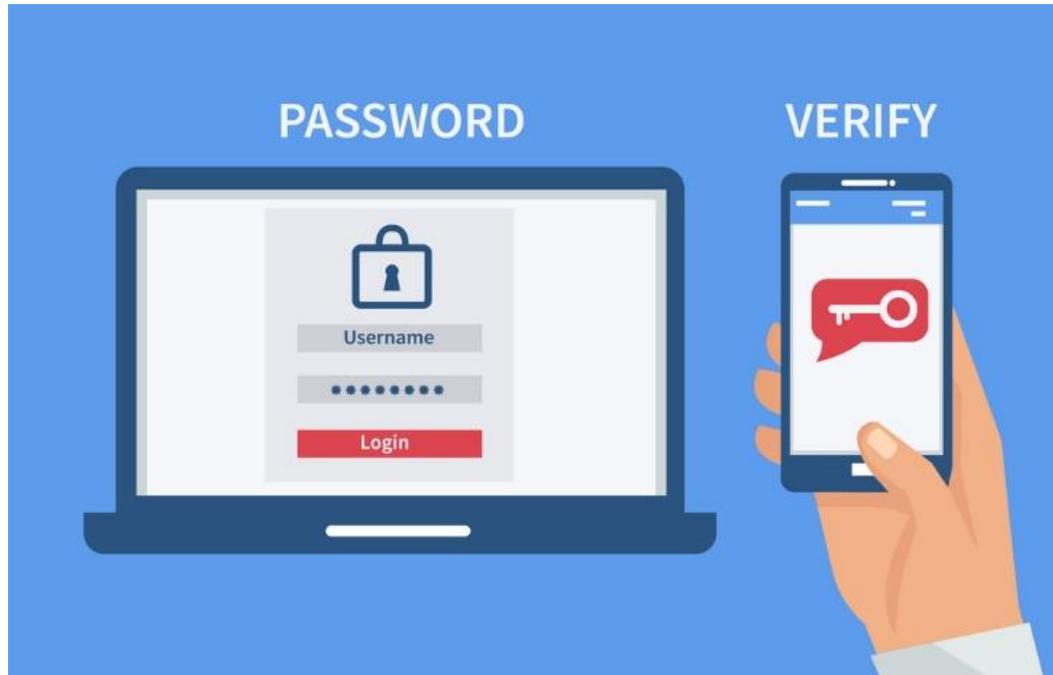
KeePass (XC)

<https://keepass.info/>  
<https://keepassxc.org/>



<https://1password.com/>

# 2FA



Bietet der von mir verwendete Dienst eine Zweifaktorauthentisierung an?

<https://2fa.directory>

# Awareness – unsere Partner



Schweizerische Kriminalprävention  
Prévention Suisse de la Criminalité  
Prevenzione Svizzera della Criminalità

<https://www.skppsc.ch>



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

**Bundesamt für Cybersicherheit BACS**

<https://www.ncsc.admin.ch>



<https://www.ibarry.ch/>

**CYBERCRIMEPOLICE.CH**  
Ein Engagement Ihrer Polizei

<https://www.cybercrimepolice.ch/>

# Bleiben Sie wachsam!

- > Halten Sie sich an Empfehlungen bezüglich Cybersicherheit und Prävention.
- > Machen Sie den #realitycheck
- > Melden Sie sich bei der Polizei oder beim BACS.



[www.ag.ch/cybercrime](http://www.ag.ch/cybercrime)