Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
**Nationales Zentrum für Cybersicherheit NCSC**
Nationale Anlaufstelle Cyber

# Zwei Jahre Anlaufstelle im NCSC – Erfahrungen und Entwicklungen

**43. Informationstagung der Schweizerischen Kriminalprävention in Basel**
**26. November 2021**

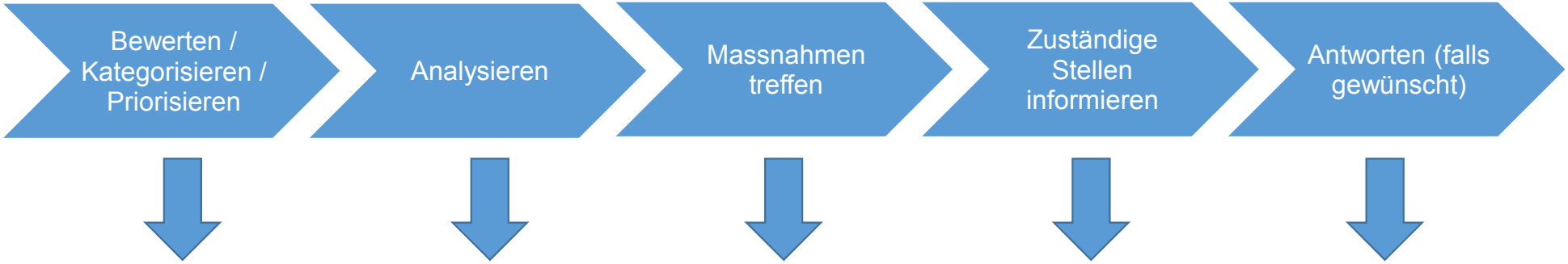
# Anlaufstelle NCSC

Die Anlaufstelle Cyber existiert seit dem **1. September 2019** und
bearbeitet seit dem **1. Januar 2020** Anfragen und Meldungen von Unternehmen und aus der Bevölkerung.

| Single Point of Contact | Meldungen | Vorfalls-meldungen | Statistik | Erste Hilfe (zur Selbsthilfe) * |
|---|---|---|---|---|
| Kontaktpflege mit Bundesstellen, Kantonen, Branchenverbänden, KMU, …<br><br>➔Enge Zusammen-arbeit mit anderen Stellen im Cyberbereich / Strafverfolgungs-behörden | Entgegennahme und Bearbeitung von Meldungen aus der Bevölkerung, sowie von KMUs und Partnern<br><br>Bewerten und konsequente Kategorisierung der Phänomene | Warnungen zu aktuellen Vorfällen | Erhebung von Fallzahlen als Unterstützung für eine effektive Beurteilung der nationalen Bedrohungslage | Tipps und Vorgehensweise bei Vorfällen |

* Folie von der SKP-Informationstagung 2019

# Meldeprozess - effizient und automatisiert




Verschiedene «Warteschlangen»
- Häufige Meldende
- Meldende ohne Antwort
- Meldende mit Antwort
- Meldungen von Partnern
- Meldungen von Schwachstellen

Möglichst automatisiert

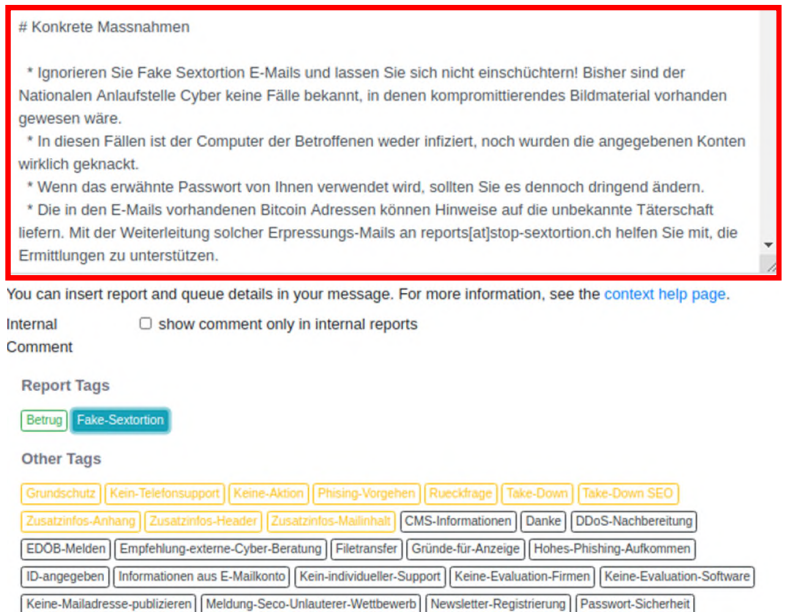
- Take-Down
- Information an involvierte Firmen
- Warnung veröffentlichen

Automatisiert
- Kapo
- fedpol
- SECO
- Swissmedic
- Usw.

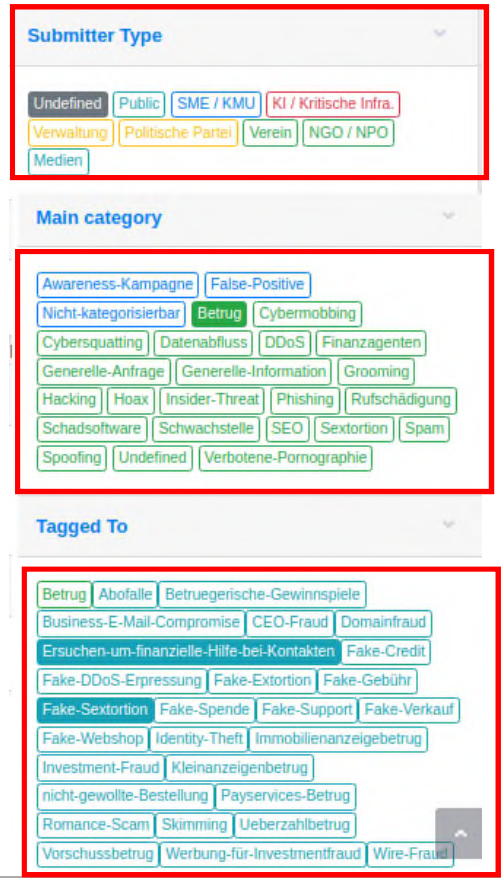
Standardisiert - aber doch persönlich

# Cyber Incident Workflow and Response Management
## (CIWORM)

Vorgefertigte Standardsätze und Antworten in 4 Sprachen für zahlreiche Situationen erlauben eine effiziente Bearbeitung




Jede Meldung wird noch zusätzlich manuell überprüft und falls nötig korrigiert.




Submitter Type

Kategorisierung der Phänomene gemäss Vorgaben

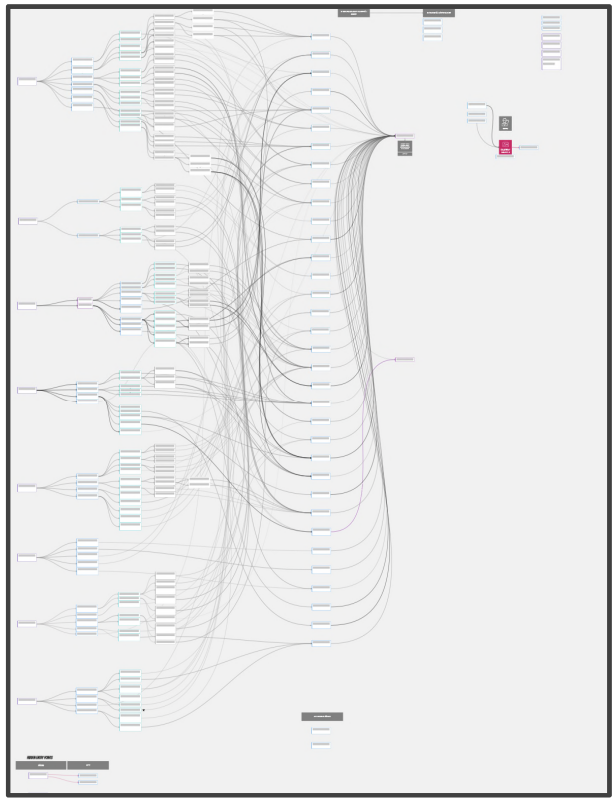
Individuelle Unter-Kategorien zur Verfeinerung des Lagebildes

# Herausforderung Kategorisierung

Für aussagekräftige Statistiken ist eine konsistente Kategorisierung zentral!

- Ausgangspunkt: Phänomenblätter von fedpol
- Mittlerweile 38 Hauptphänomene und diverse Unterphänomene
- Entwicklung neuer Phänomene ist sehr dynamisch
- Das Bedürfnis für detailliertere Statistiken steigt
- Unterscheidung «Neues Phänomen» oder «Variante eines Phänomens» ist anspruchsvoll
  - ➔ Definition Detaillierungsgrad
- Zunehmende Kombination zweier Phänomene
  - z. B. Kleinanzeigen Phishing
  - z. B. Fake Support Phishing

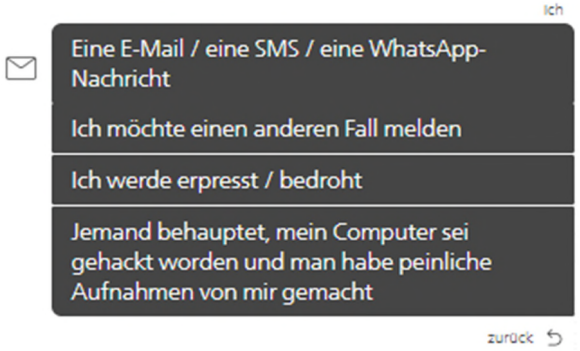
# Interaktives Meldeformular (1)



- Mit möglichst wenigen Schritten ans Ziel
- Mehr als 300 Fragen in 4 Sprachen
- 38 Zielphänomene mit konkreten und präventiven Tipps
- 8 Eingangspunkte mit verschiedenen Perspektiven (Technisch oder Schaden)
- Tipps werden eingeblendet, nachdem gemeldet wurde
- Die Angabe von allen persönlichen Angaben ist freiwillig

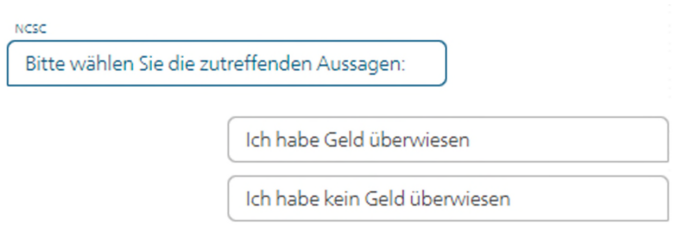
# Interaktives Meldeformular (2)

## Wenige kurze Fragen führen rasch zur Lösung

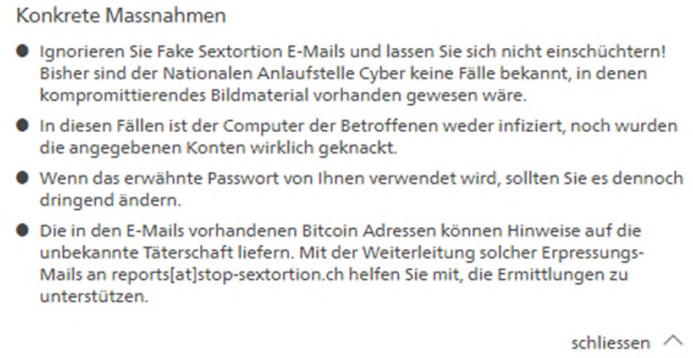



## Über 90% Trefferquote


## Schaden oder nur Meldung?




## Soforthilfe und präventive Massnahmen

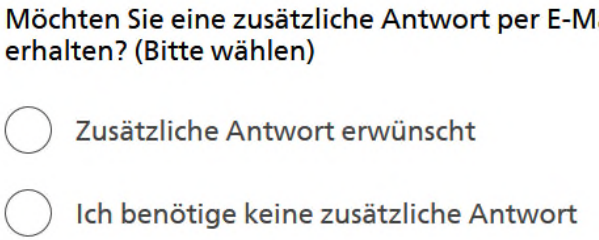


# Interaktives Meldeformular - Erkenntnisse

- Unterschiedliche Bedürfnisse von Expertinnen/Experten und Madame oder Monsieur Tout-le-Monde
- Einige wollen sich nicht durch einen Fragekatalog klicken, sondern einfach nur melden
- Es ist schwierig einzuschätzen, ob der Meldende noch weitere Informationen benötigt oder die gewünschten Informationen durch das Formular bekommen hat
- Unstrukturierte Übermittlung von Findings (URLs, Telefonnummern, BitCoin-Adressen) ergibt zusätzlichen Aufwand
- Das Übermitteln von Daten - insbesondere von E-Mails - über ein Formular ist für Meldende nicht einfach und führt zu erweitertem Aufwand auf unserer Seite

# Meldeformular Version 2.0 (seit August 21 online)


Möglichkeit direkt eine Meldung zu verfassen.
Meldende können das Phänomen direkt wählen.




Meldende können wählen, ob Sie eine Antwort möchten oder ob sie «nur» melden möchten.


Abhängig von bestimmten Phänomenen, wird gezielt nach Indikatoren gefragt. Beispielsweise wird im Fall von Fake Sextortion nach der Bitcoin-Adressen gefragt.

# Informationen


Generelle Informationen / Trends

Vorfall? Was nun?

Warnungen zu laufenden Angriffen

Aktuelle Statistik

Regelmässige Information zu aktuellen Vorfällen

# End of Week

Intern

Regelmässige Information

mit den aktuellen Zahlen und den wichtigsten Fällen

End-of-Week - Zusammenfassung

Zusammenfassung der Meldungen von 2. Januar 2021 bis 8. Januar 2021

Anzahl Meldungen pro Hauptkategorie

| *Hauptkategorie* | *Meldungen* | *davon Schadensfälle* |
|---|---|---|
| Betrug | 203 | 1 |
| Phishing | 85 | 2 |
| Schadsoftware | 14 | 2 |
| Nicht-kategorisierbar | 7 | 0 |
| Sextortion | 4 | 3 |
| False-Positive | 4 | 0 |
| Spam | 4 | 0 |
| Verbotene-Pornographie | 3 | 0 |
| Hacking | 2 | 0 |
| Cybersquatting | 2 | 0 |
| Finanzagenten | 1 | 0 |
| Datenabfluss | 1 | 0 |
| Undefinierte und allgemeine Meldungen resp. Informationen | 20 | 0 |
| **Total** | **350** | **8** |


Aktuelle Zahlen mit Schadensmeldungen
Stichwortartige Zusammenfassung der wichtigsten Fälle (ca. 10 – 15 pro Woche)

SKPPSC

# Wochenrückblick

Öffentlich

Regelmässige Information

Ein oder zwei interessante Fälle der vergangenen Woche möglichst einfach erklärt!

Wochenrückblicke NCSC

Ergebnisse 1 - 15 von 30 | 1 | 2 | Eine Seite vor

Die Woche 39 im Rückblick

05.10.2021 - Anlässlich der einsetzenden Herbstferien verzeichnete das NCSC in der letzten Woche einen tieferen Meldeeingang. Das NCSC hat beobachtet, dass die Betrüger bei «Fake Support» Anrufen neuerdings versuchen, auf andere Weise an ihre Opfer zu gelangen. Ergaunertes Geld muss irgendwann reingewaschen werden. Wie für diese Tätigkeit Personen gesucht werden, wird im zweiten Fall beschrieben.

Die Woche 38 im Rückblick

28.09.2021 - In der letzten Woche verzeichnete das NCSC wieder einen erhöhten Meldeeingang. Im Fokus standen betrügerische Gewinnspiele, die angeblich zum 50. Geburtstag von Coop versendet werden. Und bei Kleinanzeigenbetrug vom Typ, dass man trotz eines Verkaufes bezahlen soll, wird ein erheblicher Aufwand betrieben, um das Opfer zur Angabe von Kreditkartendaten zu bewegen.

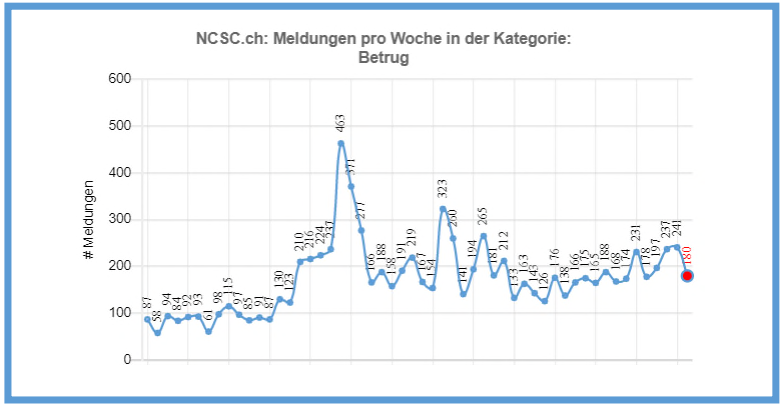
Die Woche 37 im Rückblick

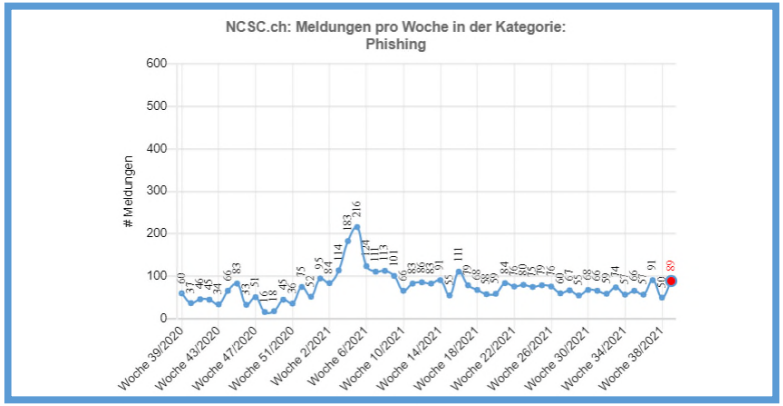
21.09.2021 - In der letzten Woche verzeichnete das NCSC einen erhöhten Meldeeingang. Aufgefallen sind diverse Varianten von angeblichen Drohungen unter anderem im Namen der Polizei. In der E-Mail wird gedroht, ein Strafverfahren gegen die Empfängerin oder den Empfänger einzuleiten, wenn nicht innerhalb von 72 Stunden geantwortet werde. Und wieder einmal verspricht eine Website Opfern von Investmentbetrug, die verlorenen Gelder zurückzuholen.

# Was wird gemeldet?
## Neue interaktive Statistik

Öffentlich

Regelmässige Information




**Erstes Halbjahr 2021**

10234 Meldungen

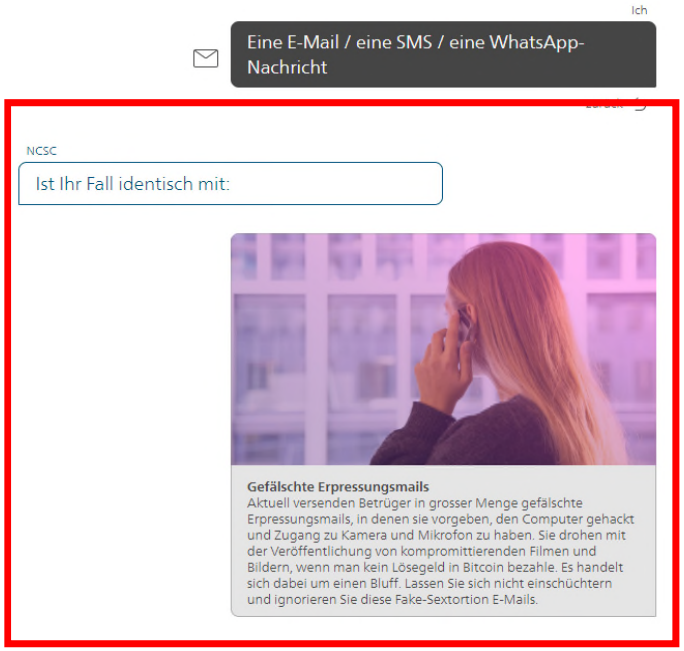
davon
2439 Phishing
1351 Fake Sextortion
1284 Vorschussbetrug
640 gefälschte Zollgebühren
307 Kleinanzeigenbetrug
252 Investment Betrug
239 CEO Betrug
91 Ransomware (vor allem Qlocker)

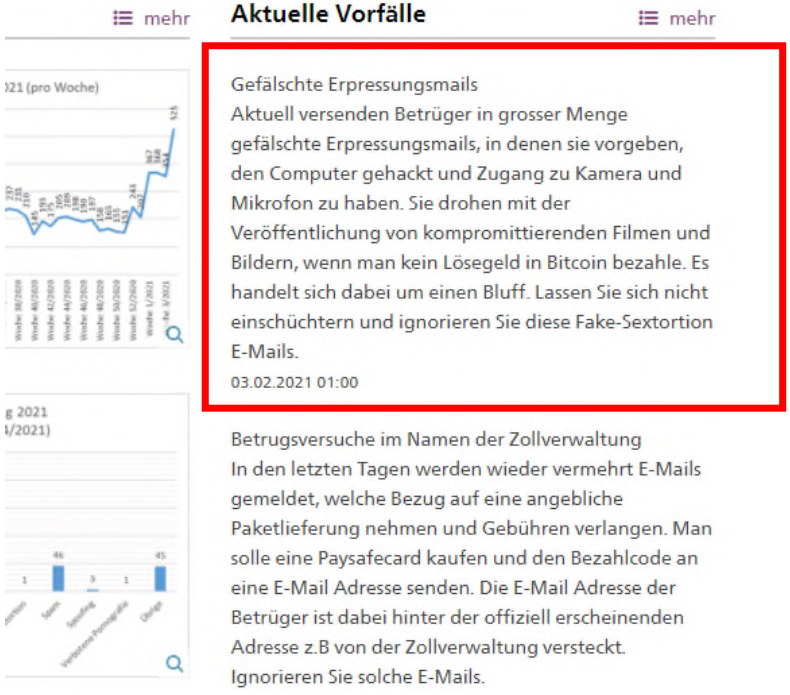
# Vorfallsmeldungen

Öffentlich

Warnung

Aktuelle Vorfallsmeldungen bei erhöhtem Meldeeingang direkt im Meldeformular oder auf der Startseite von www.ncsc.admin.ch

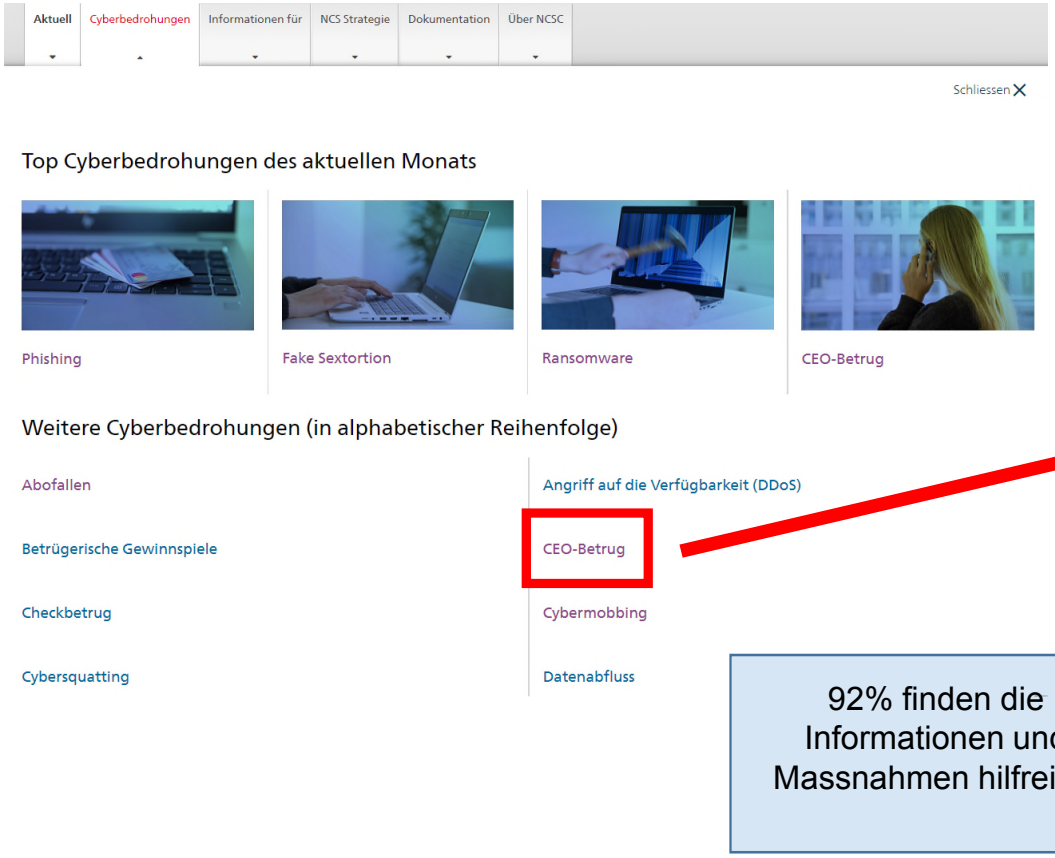


# Generell: Informationen und Trends

Öffentlich

Generelle Information




92% finden die Informationen und Massnahmen hilfreich!

# Vorfall - Was nun?

Öffentlich

Generelle Information

Die wichtigsten Massnahmen bei Vorfällen mit grossem Schadenspotential. Kurz erklärt, damit der Schaden nicht noch grösser wird.

Erfolgreiche Ransomware-Angriffe auf Schweizer Unternehmen

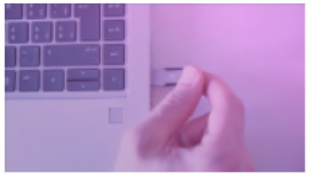
**18.08.2021 - Das NCSC hat in den letzten Monaten mehrere erfolgreiche Cyberangriffe gegen Schweizer Unternehmen beobachtet. Bei diesen haben Cyberkriminelle die Unternehmensnetzwerke mittels eines Verschlüsselungstrojaners (sogenannter «Ransomware») verschlüsselt und erfolgreich Lösegeld eingefordert.**

In den vergangenen Jahren hat das NCSC immer wieder eindringlich vor Cyberangriffen durch Ransomware gewarnt. Während es sich bei solchen Angriffen in der Regel um komplexe Attacken handelt, lassen sich die meisten davon relativ einfach verhindern. Häufigstes Einfallstor für erfolgreiche Angriffe mit Ransomware sind nicht gepatchte Systeme sowie Fernzugänge wie VPN (Virtual Private Network) und RDP (Remote Desktop Protocol), welche nicht mittels Zwei-Faktor-Authentisierung (2FA) abgesichert sind. Auch Warnmeldungen von installierter Sicherheitssoftware wie Virenschutz werden leider immer wieder auf kritischen Systemen wie Windows Domain-Controllern ignoriert.

Bereits im Februar 2020 hat das NCSC auf die Problematik aufmerksam gemacht:

Vorsicht: Weiterhin erhöhtes Sicherheitsrisiko durch Ransomware gegen KMUs

Ransomware - Was nun?



Datenabfluss - Was nun?

Webseite gehackt - Was nun?

Cyberattacke – was tun? Checkliste für CISOs

DDoS-Angriff - Was nun?

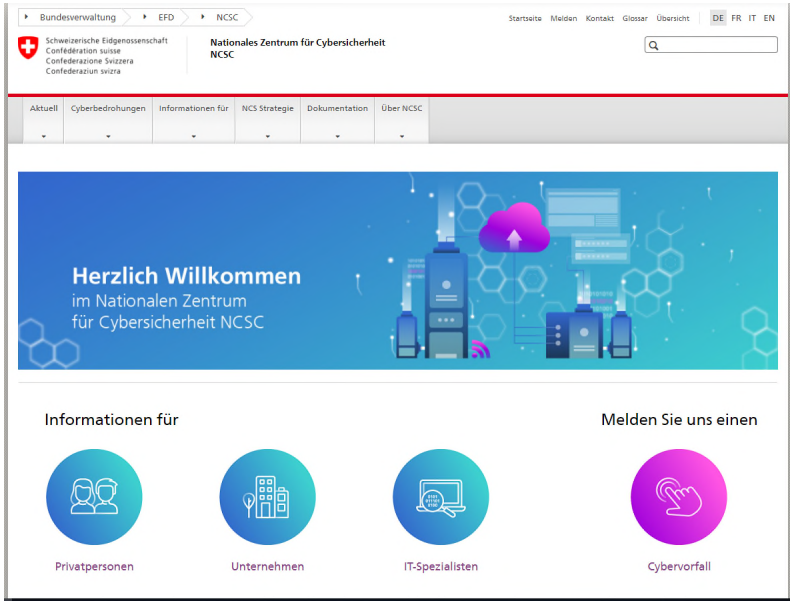
# Wer macht was?

| Polizei | Nationales Zentrum für Cybersicherheit NCSC | IKT-Support |
|---|---|---|
| • Gibt Ihnen Tipps zur Prävention<br>• Strafverfolgung. Nimmt Ihre Anzeige auf, sichert Spuren und ermittelt.<br>• Berät und Unterstützt Sie bezüglich weiteres Vorgehen und Täterkommunikation.<br>• Kontakt: Grundsätzlich jederzeit möglich. Auf jeden Fall bei einem akuten Angriff, z.B. Erpressung oder Schaden, z.B. Diebstahl. | • Gibt Ihnen Tipps zur Prävention<br>• Keine Strafverfolgung. Nimmt Ihre freiwillige Meldung auf und beantwortet Ihre Fragen.<br>• Unterstützt Sie und die Polizei bei der Identifizierung der Schadsoftware und Analyse.<br>• Kontakt: Freiwillige Meldung. Auch bei Ereignissen, die keinen Schaden verursacht haben oder im Versuchsstadium entdeckt wurden, z.B. Phishingmails | • Bespricht und setzt Präventionsmassnahmen mit Ihnen um.<br>• Evaluiert das Problem und liefert bei einem Angriff Informationen an die Polizei.<br>• Stellt Ihre Netzwerke wieder her und behebt Ihre Sicherheitsprobleme. |

# Ausblick

- Alarmierung (Newsletter, Twitter usw.)
- Automatisierte Schnittstelle NCSC -  Polizei
- Anbindung Meldeformular an die Möglichkeit einer elektronischen Anzeigeerstattung
- Systematische Erhebung von Daten nach einem Vorfall zwecks statistischer Auswertung
- Systematische Verwertung (auch für die Strafverfolgung) von Daten
  - Betrugsseiten
  - Telefonnummern
  - Bitcoin-Adressen
  - IBAN-Nummern
  - ……

# Vielen Dank für Ihre Aufmerksamkeit!




National Cyber Security Centre NCSC
Web: https://www.ncsc.admin.ch
E-Mail: outreach@ncsc.ch