



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

# Gefahren für Schweizer KMU

**Max Klaus**

stv. Leiter Operative Cybersicherheit OCS  
Nationales Zentrum für Cybersicherheit NCSC

- 1. Das NCSC**
- 2. Lage national und international**
- 3. Cyberangriffe**
- 4. Schlussfolgerungen / Empfehlungen**



# 1. Das NCSC





# 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:

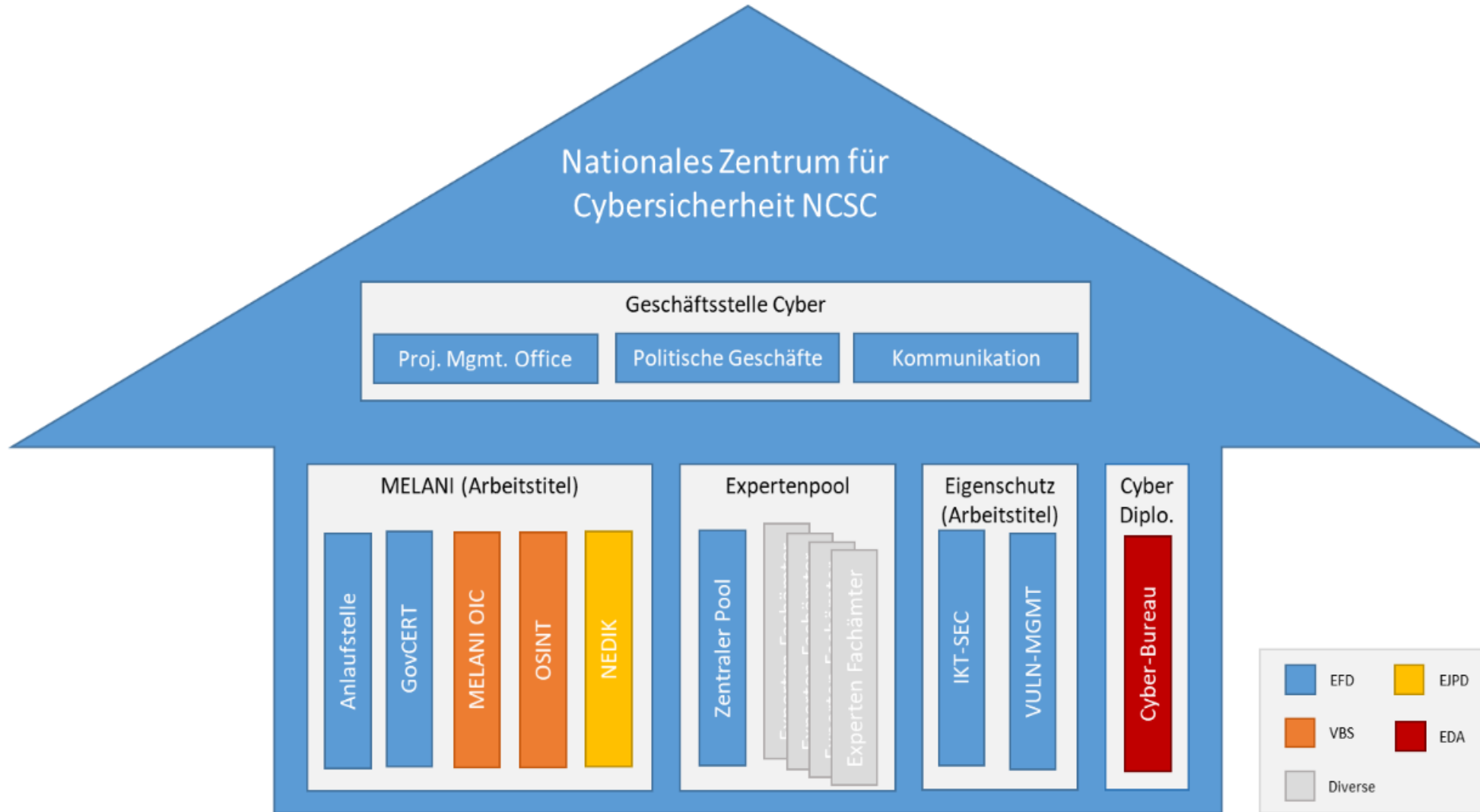
Abgeschrieben

 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

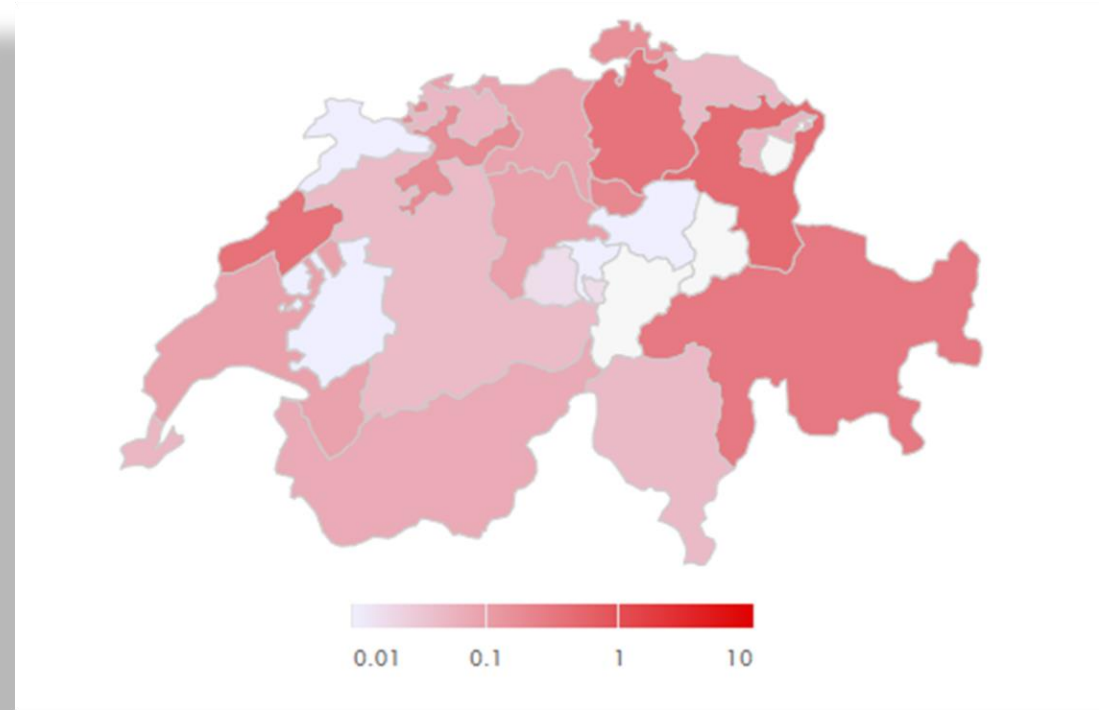


## 2. Lage national und international





# 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

Netzteil

Wochen vor allem KMU davor, die Gefahr zu unterschätzen.



# KMU sind gefährdeter als Grossunternehmen!

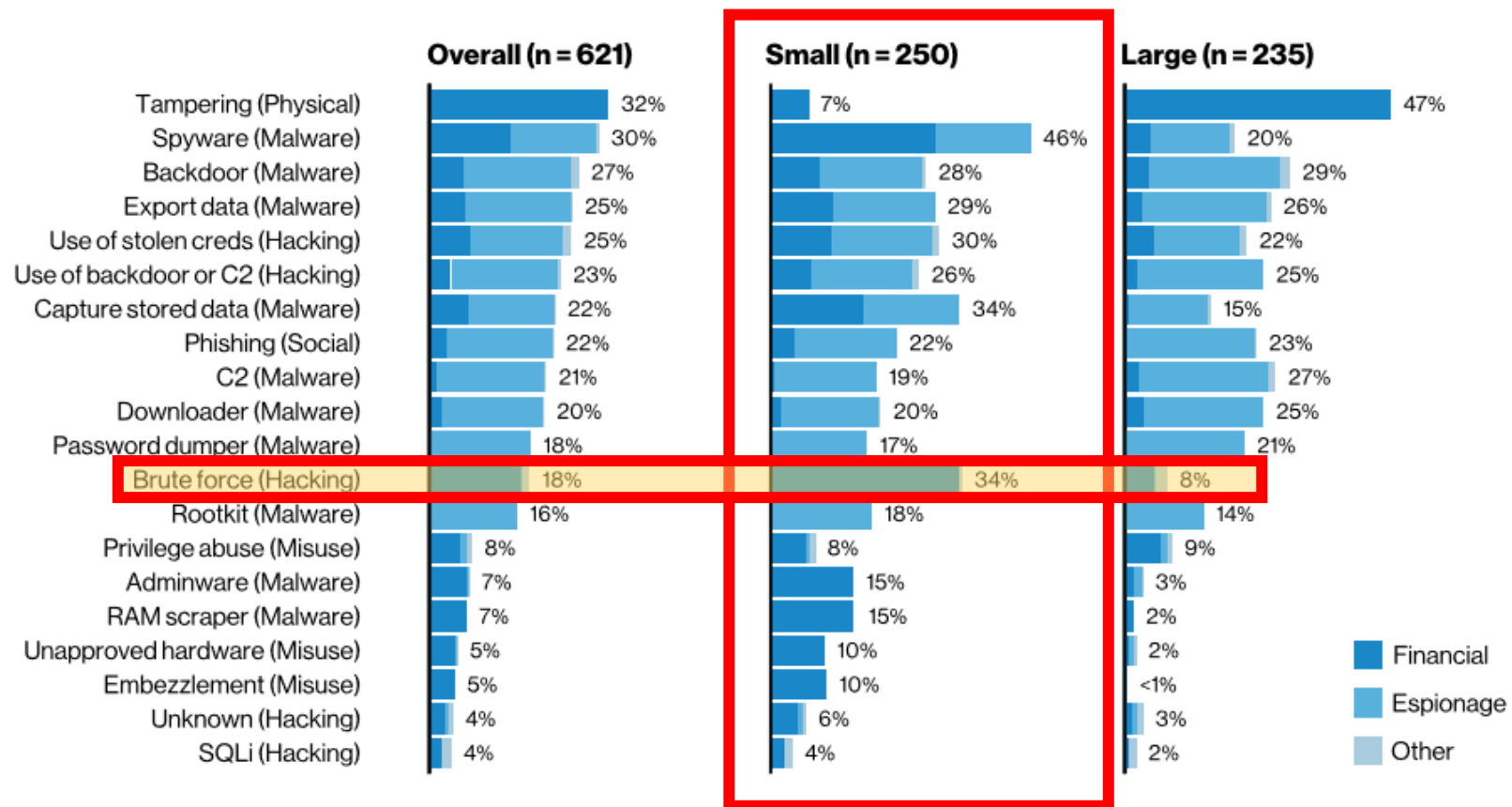


Figure 109. Top 20 threat actions (referencing the 2013 DBIR)

### **3. Verschlüsselungstrojaner**





# Hacker bieten hervorragenden Support!

```
!!! WICHTIGE INFORMATIONEN !!!!

Alle Dateien wurden mit RSA-2048 und AES-128 Ziffern verschlüsselt.
Mehr Informationen über RSA können Sie hier finden:
http://de.wikipedia.org/wiki/RSA-Kryptosystem
http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

Die Entschlüsselung Ihrer Dateien ist nur mit einem privaten Schlüssel und einem Entschlüsselungsprogramm,
welches sich auf unserem Server befindet, möglich.
Um Ihren privaten Schlüssel zu erhalten, folgen Sie einem der folgenden Links:
1. http://6dbxgqam4crv6rr6.tor2web.org/7D
2. http://6dbxgqam4crv6rr6.onion.to/7D
3. http://6dbxgqam4crv6rr6.onion.cab/7D

Sollte keine der Adressen verfügbar sein, folgen Sie den folgenden Schritten:
1. Laden Sie einen Tor Browser herunter und installieren diesen: https://www.torproject.org/download/download
2. Starten Sie den Browser nach der erfolgreichen Installation und warten auf die Initialisierung.
3. Tippen Sie in die Adresszeile: 6dbxgqam4crv6rr6.onion/7D
4. Folgen Sie den Anweisungen auf der Seite.

!!! Ihre persönliche Identifizierungs-ID lautet: 7D !!!
```



# Verschlüsselungstrojaner: Empfehlungen



- Regelmässige Datensicherung
- Datenträger nach Backup vom PC / Netz trennen
- Qualität der Backups sporadisch überprüfen
- Das Einspielen von Backups in einer ruhigen Minute üben
- Versuchen Sie, die Daten wiederherzustellen:  
[www.nomoreransom.org](http://www.nomoreransom.org)
- Keinesfalls Lösegeld bezahlen!
- Information an NCSC, allenfalls Strafanzeige gegen Unbekannt bei der Kantonspolizei

## 4. Schlussfolgerungen / Empfehlungen





# Schlussfolgerungen

- KMU sind stärker gefährdet als Grossunternehmen
- Der Mensch als schwächstes Glied in der Kette → Social Engineering
- Fast immer finanzielle Motivation für Cyberangriffe
- Gesunder Menschenverstand als «Grundschutz» im privaten Bereich



# Empfehlungen: proaktiv (1/2)

[www.ncsc.admin.ch](http://www.ncsc.admin.ch):

- Zahlreiche kostenlose Anleitungen, Checklisten, Whitepapers usw.
- Online-Meldeformular
- «Im Fokus»: Wöchentlich Informationen zu neuen Angriffsformen.

<https://www.linkedin.com/company/70430924/>:

- Aktuelle Informationen über Angriffe
- Informationen über die Tätigkeiten im NCSC

**Nationales Zentrum für Cybersicherheit NCSC**  
Operative Cybersicherheit OCS

The screenshot shows the NCSC website dashboard. At the top, it says "Herzlich Willkommen im Nationalen Zentrum für Cybersicherheit NCSC". Below this, there are two main sections: "Informationen für" and "Melden Sie uns". "Informationen für" includes icons for "Privatpersonen", "Unternehmen", "Behörden", and "IT-Spezialisten". "Melden Sie uns" includes icons for "einen Cybervorfall" and "eine Schwachstelle". Below these are three sections: "Aktuelle Vorfälle", "Statistik", and "Im Fokus". "Aktuelle Vorfälle" has a sub-section for "Angebliches SBB-Gewinnspiel" with a text description and a date "10.06.2022 11:20". "Statistik" features a line graph titled "NCSC.ch: Meldeeingang" showing the number of reports over time. "Im Fokus" has a sub-section for "Woche 23: Vermeintliches Gewinnspiel der SBB und die Wichtigkeit von schnellem Patchen" with a date "14.06.2022" and a text description.

The screenshot shows the LinkedIn page for the National Center for Cyber Security (NCSC). The page header includes the NCSC logo and the text "Nationales Zentrum für Cybersicherheit NCSC" and "Ansicht für Content-Admins". The main content area shows a post from "Nationales Zentrum für Cybersicherheit NCSC" dated "14.6.2022". The post text reads: "Vorsicht vor angeblichem Gewinnspiel im Namen der SBB. Dieses verbreitet sich mittels Schneeballsystem sehr rasch. Zudem zeigte sich einmal mehr, wie wichtig das Schliessen von Sicherheitslücken ist, sobald Patches zur Verf ... mehr anzeigen". The post includes a photo of a hand holding a smartphone displaying a website. The post has 82,569 impressions, 57 clicks, and 12,411 followers. The post is sponsored by "Daniel W. Sellaer und 57 weitere Personen".



# Empfehlungen: proaktiv (2/2)

## Das Übliche zuerst:

- Starke Passwörter / 2FA
- 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:

- Möglichkeit anonymer Meldungen
- 100% Vertraulichkeit
- Keine Sanktionen (evtl. DSGVO der EU beachten)
- In der Regel Erstantwort innert 24 Stunden.

## Strafverfolgung:

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



# Herzlichen Dank für Ihre Aufmerksamkeit



Max Klaus

Stv. Leiter operative Cybersicherheit OCS

Nationales Zentrum für Cybersicherheit NCSC  
Schwarztorstrasse 59  
3003 Bern

**Nationales Zentrum für Cybersicherheit NCSC**  
Operative Cybersicherheit OCS