Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

In der Schweiz gibt es keinen Gratiskäse mehr

Max Klaus
stv. Leiter operative Cybersicherheit OCS
stv. Leiter Melde- und Analysestelle Informationssicherung MELANI

Video zum Einstieg

Inhalte:

1. Das NCSC
2. Lage und Akteure
3. Cyberangriffe
4. Schlussfolgerungen / Empfehlungen

Wie alles begann

17.3508 MOTION

Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund

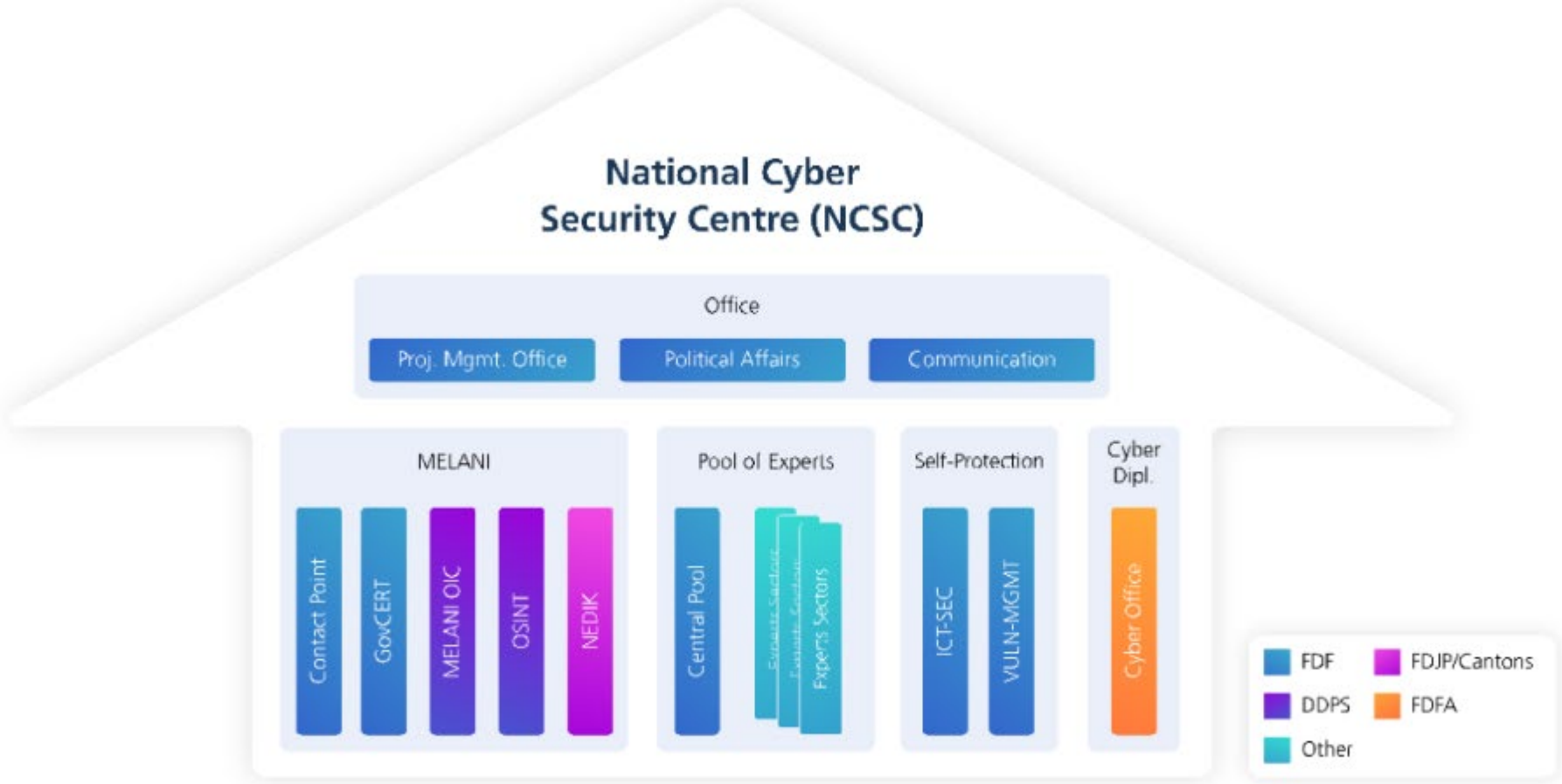
Eingereicht von:	 EDER JOACHIM FDP-Liberale Fraktion FDP.Die Liberalen
Berichterstattung:	CLOTTU RAYMOND, GLÄTTLI BALTHASAR
Einreichungsdatum:	15.06.2017
Eingereicht im:	Ständerat
Stand der Beratungen:	Abgeschrieben

ALLES ZUKLAPPEN

EINGEREICHTER TEXT

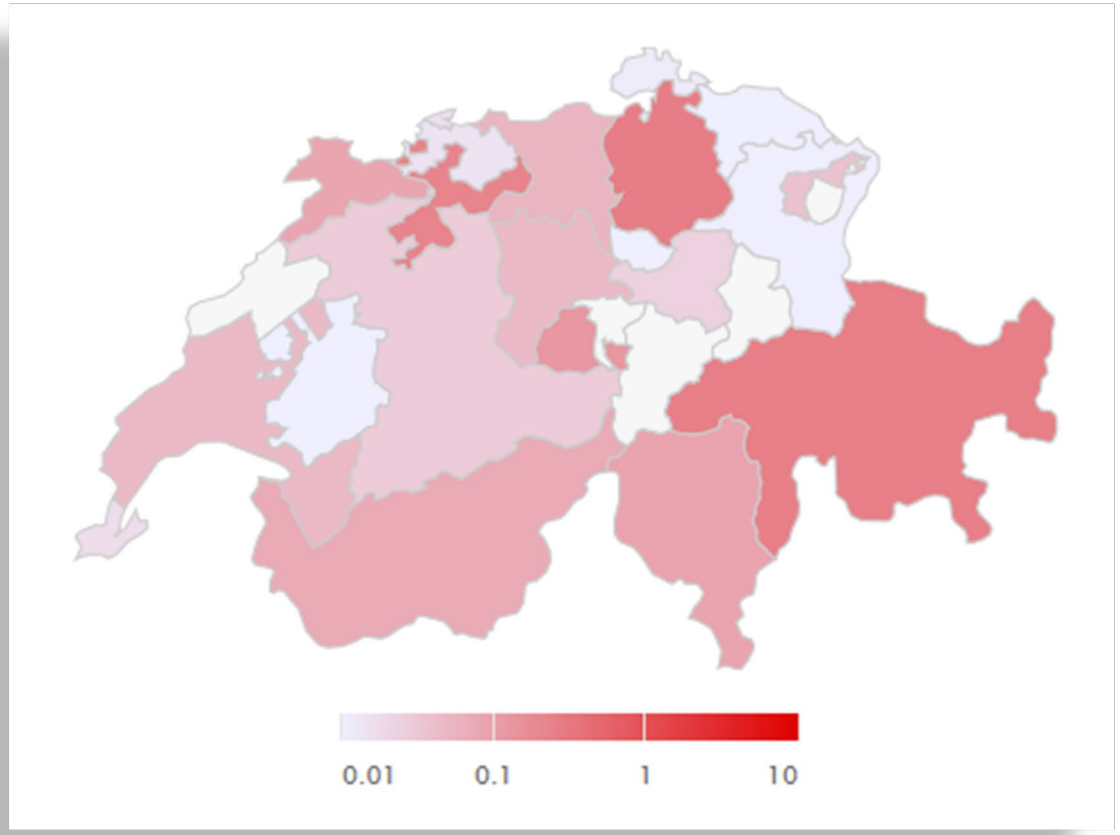
Der Bundesrat wird beauftragt, im Zusammenhang mit der laufenden Überarbeitung der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) ein Cybersecurity-Kompetenzzentrum auf Stufe Bund zu schaffen und dafür die notwendigen Massnahmen einzuleiten. Diese Organisationseinheit hat die Aufgabe, 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 und Akteure

Aktuelle Bedrohungslage



Wie gefährdet sind Gemeinden?

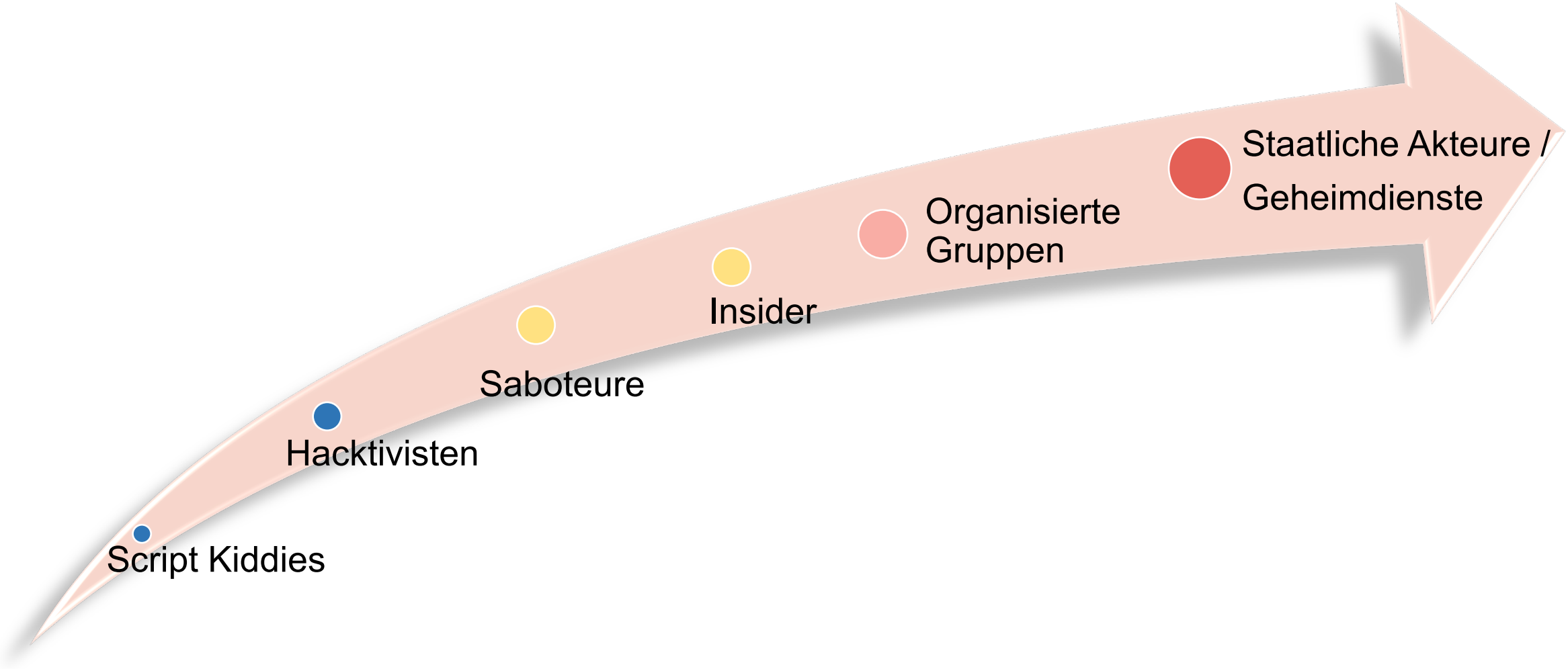
Diese Liste erhebt keinen Anspruch auf Vollständigkeit….

Datum	Gemeinde
November 2021	Rolle
Oktober 2021	Montreux
Oktober 2021	Mellingen
Oktober 2021	Stadt St. Gallen
März 2021	Bad Zurzach

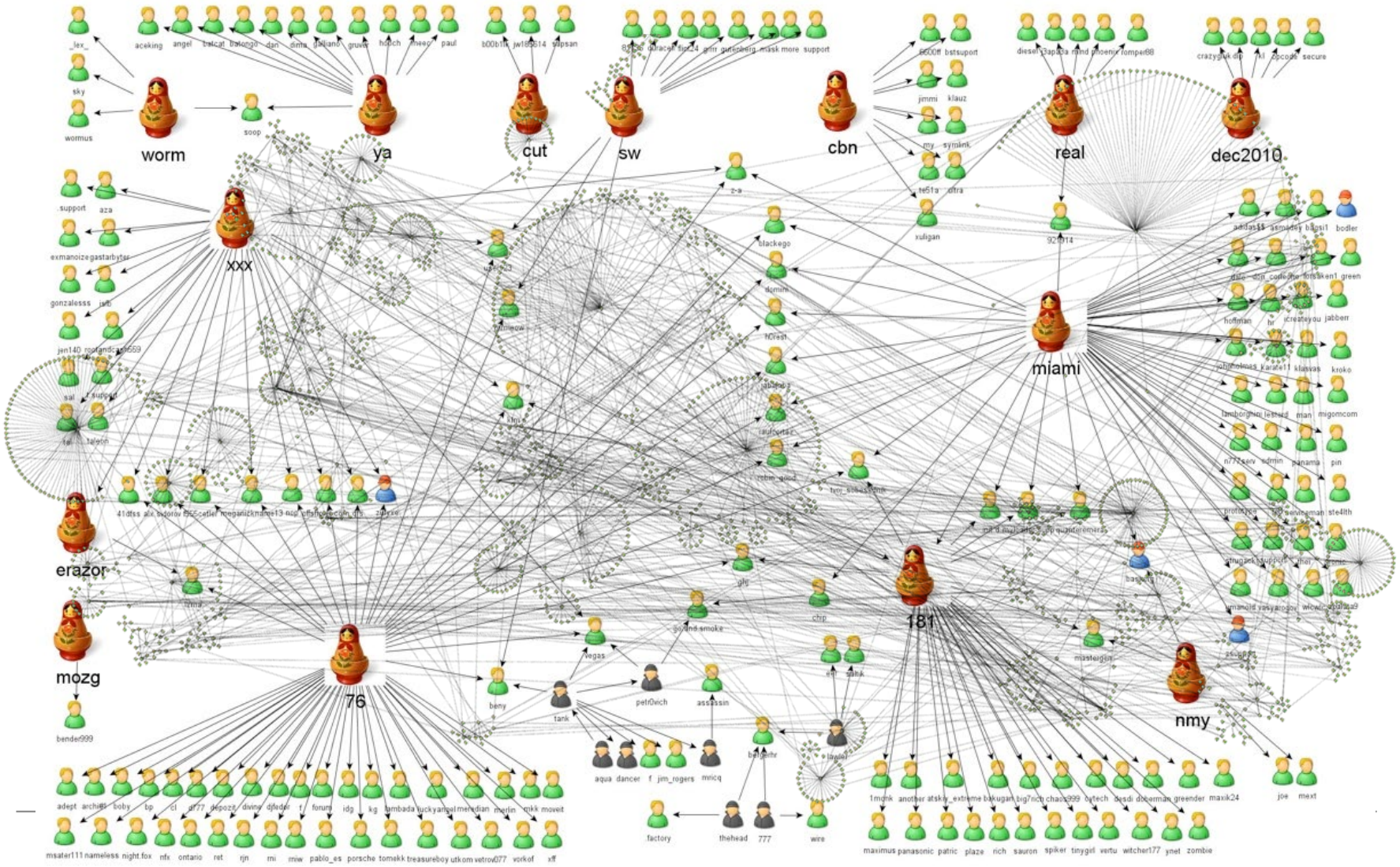
Warum ist das so?

- Sensible Daten (Steuerdaten, EL, Gesundheitsdaten usw.)
- Kleine Gemeindebudgets, IT-Security nicht als oberste Priorität
- Angriffe nach dem Giesskannenprinzip → „Zufallsopfer“
- Knappe Personalressourcen
- Zuwenig IT-Know-how
- Gemeinden reagieren nicht:

Akteure


Staatliche Akteure /
Geheimdienste
Organisierte
Gruppen
Insider
Saboteure
Hacktivisten
Script Kiddies

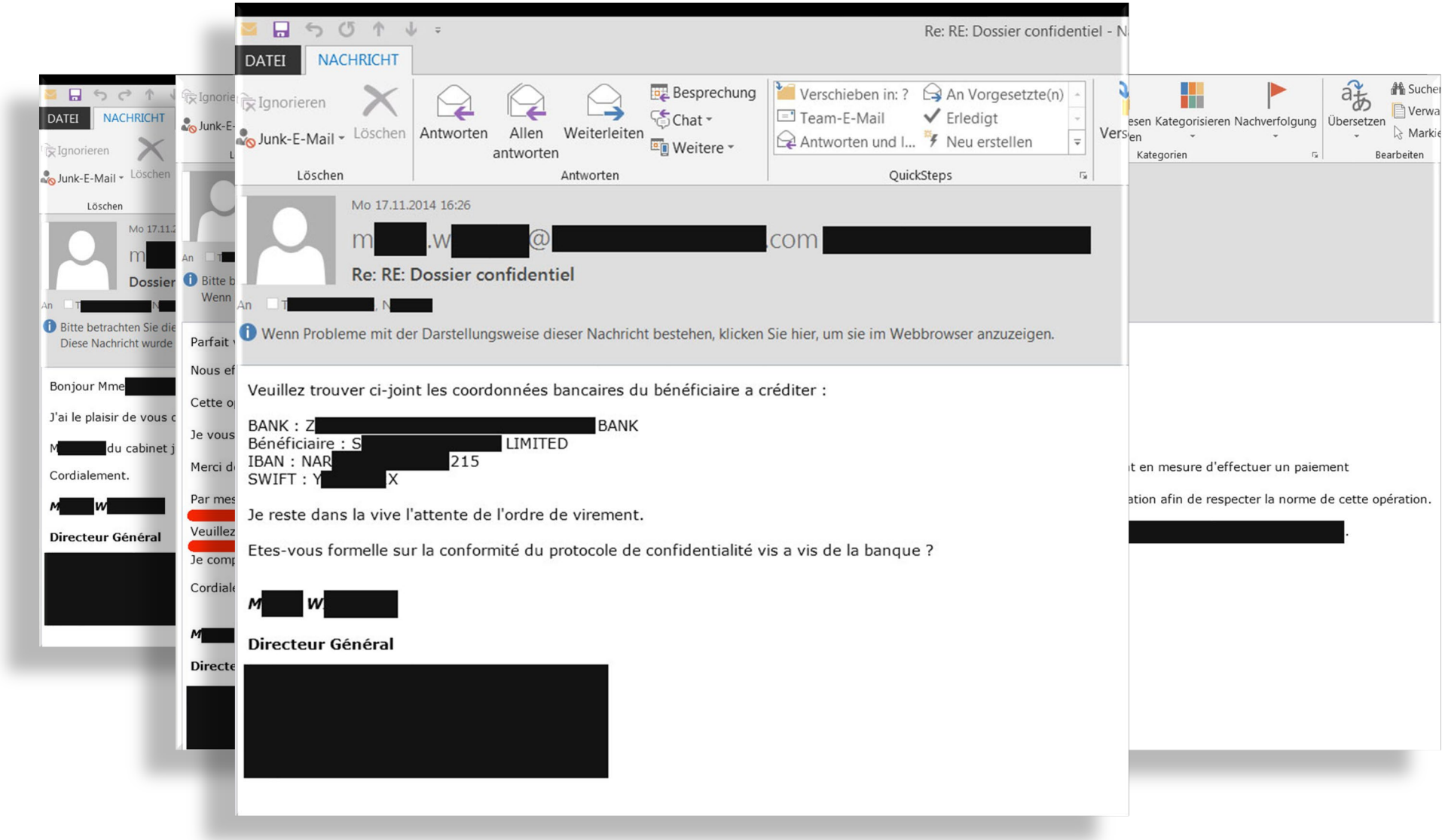
Die Arbeitsteilung bei Cyberattacken



3. Cyberangriffe

CEO Fraud

CEO Fraud


Re: RE: Dossier confidentiel - N
DATEI
NACHRICHT
Ignorieren
Junk-E-Mail
Löschen
Antworten
Allen antworten
Weiterleiten
Besprechung
Chat
Weitere
Verschieben in: ?
Team-E-Mail
Antworten und I...
An Vorgesetzte(n)
Erledigt
Neu erstellen
QuickSteps
Kategorisieren
Nachverfolgung
Kategorien
Übersetzen
Bearbeiten
Mo 17.11.2014 16:26
m[redacted].w[redacted]@[redacted].com[redacted]
Re: RE: Dossier confidentiel
Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.
Veuillez trouver ci-joint les coordonnées bancaires du bénéficiaire a créditer :
BANK : Z[redacted]BANK
Bénéficiaire : S[redacted] LIMITED
IBAN : NAR[redacted]215
SWIFT : Y[redacted]X
Je reste dans la vive l'attente de l'ordre de virement.
Etes-vous formelle sur la conformité du protocole de confidentialité vis a vis de la banque ?
M[redacted] W[redacted]
Directeur Général
[redacted]

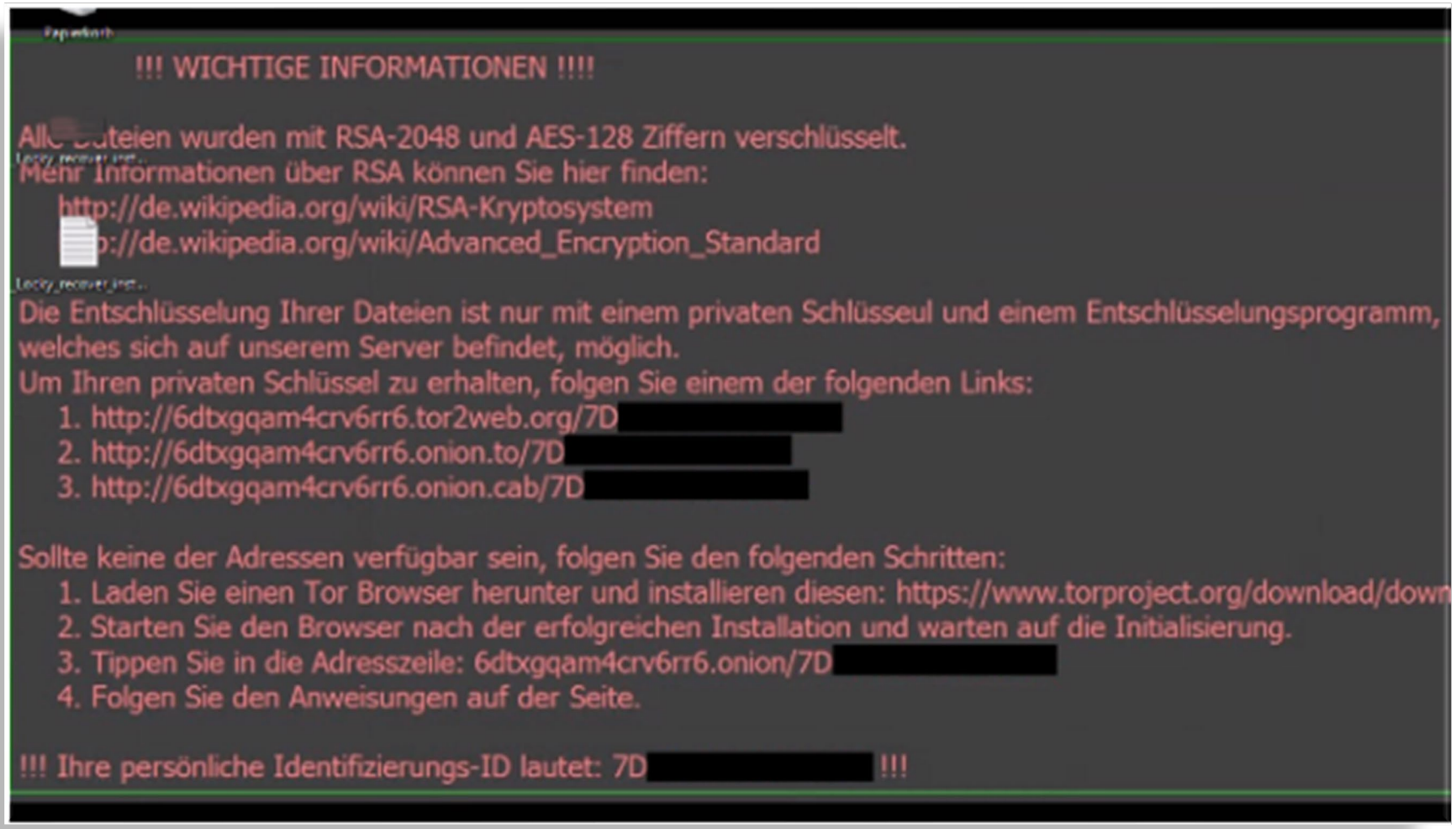
CEO Fraud: Empfehlungen

- Klare Weisungen bezüglich Zahlungen erteilen
- Keine internen Informationen weitergeben
- Im Zweifelsfall bei der GL nachfragen
- Vorsicht auch bei Mails von vermeintlich bekannten Personen
- Meldung an ncsc.ch,
  allenfalls Anzeige gegen Unbekannt bei KaPo

Erpressung

http://www.trustedwatch.de

Verschlüsselungstrojaner



!!! 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 Schlüsseul und einem Entschlüsselungsprogramm, welches sich auf unserem Server befindet, möglich.
Um Ihren privaten Schlüssel zu erhalten, folgen Sie einem der folgenden Links:

1. http://6dtxgqam4crv6rr6.tor2web.org/7D[redacted]
2. http://6dtxgqam4crv6rr6.onion.to/7D[redacted]
3. http://6dtxgqam4crv6rr6.onion.cab/7D[redacted]

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/down
2. Starten Sie den Browser nach der erfolgreichen Installation und warten auf die Initialisierung.
3. Tippen Sie in die Adresszeile: 6dtxgqam4crv6rr6.onion/7D[redacted]
4. Folgen Sie den Anweisungen auf der Seite.

!!! Ihre persönliche Identifizierungs-ID lautet: 7D[redacted] !!!

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 / Empfehlungen

Schlussfolgerungen

- KMU sind stärker gefährdet als Grossunternehmen
- Der Mensch als schwächstes Glied in der Kette → Social Engineering
- Gesunder Menschenverstand als «Grundschutz»
- Das NCSC unterstützt Sie im Bedarfsfall gerne

Empfehlungen: proaktiv

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

Unterstützung:

www.ncsc.ch

Anonyme Meldungen sind möglich

Strafverfolgung:

Privatpersonen: Kapo am Wohnsitz

Unternehmen: Kapo am Geschäftssitz

…und wie war das nochmal mit dem Käse?

Auszug aus einem russischen Hackerforum:

„Не в Швейцарии нет более бесплатный сыр“

(„In der Schweiz gibt es keinen Gratiskäse mehr“)

Herzlichen Dank für Ihre Aufmerksamkeit

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

Schwarztorstrasse 59
3003 Bern