



Cyber-Bedrohungen: Lage Schweiz und international

Max Klaus, stv. Leiter MELANI



Inhalte



Melde- und Analysestelle
Informationssicherung
MELANI



Bedrohungslage:
Veränderung; Lage
national/international;
Akteure



Cyber-Angriffe:
Ausgewählte Beispiele



Schlussfolgerungen und
Empfehlungen





Bundesrats-Auftrag / Public Private Partnership

	SCHWEIZERISCHER BUNDESRAT		Beschluss	20. August 2003
	CONSEIL FÉDÉRAL SUISSE		Décision	
	CONSIGLIO FEDERALE SVIZZERO		Decisione	

Aufbau und Betrieb einer Melde und Analysestelle Informationssicherung MELANI



Schutz kritischer Infrastrukturen in der Schweiz nur in enger Zusammenarbeit mit der Wirtschaft möglich → Public Private Partnership



Rahmenbedingungen für MELANI



Keine Meldepflicht für Cybervorfälle



Subsidiarität



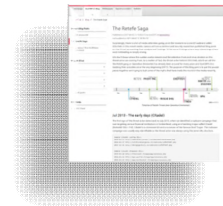
Keine Weisungsbefugnis ausserhalb der Bundesverwaltung



Öffentliche Produkte



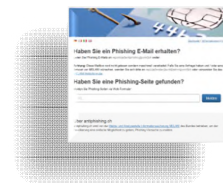
www.melani.admin.ch



Blog GovCERT.ch



[Halbjahresbericht](#)



www.antiphishing.ch



[Newsletter](#)



www.checktool.ch



Inhalte



Melde- und Analysestelle
Informationssicherung
MELANI



Bedrohungslage:
Veränderung; Lage
national/international;
Akteure



Cyber-Angriffe:
Ausgewählte Beispiele



Schlussfolgerungen und
Empfehlungen





Veränderung der Bedrohungslage

>100 Jahre



derstandard.at

Vor 10 Jahren



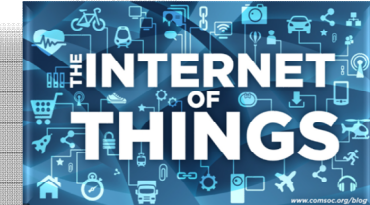
augsburgerallgemeine.de

heute



jdpower.com

morgen?



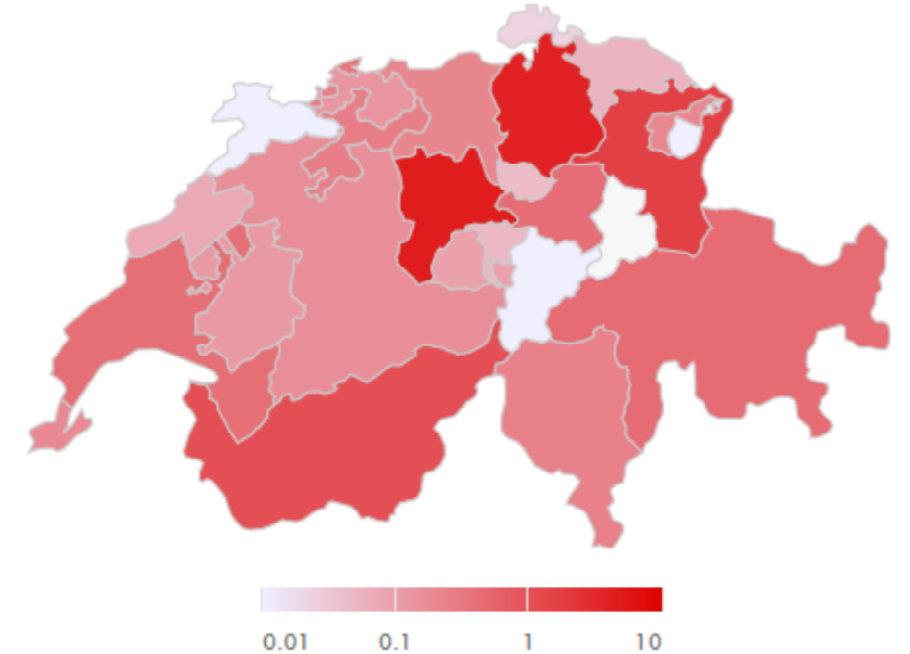
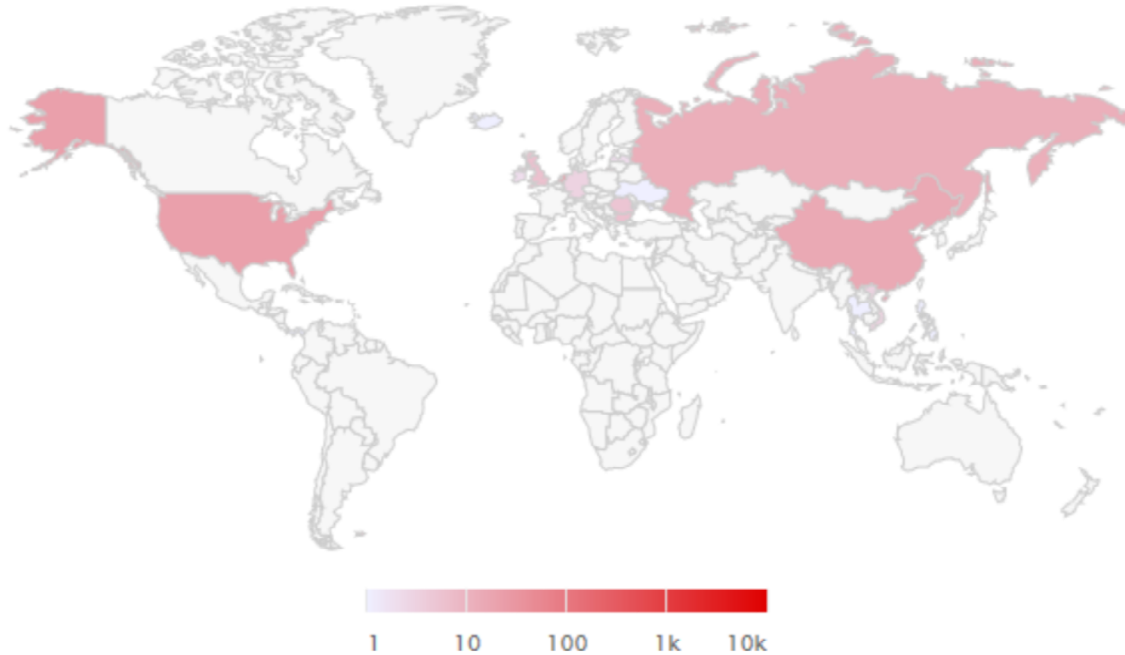
fossbytes.com

- Modernere Mittel
- Vernetzte Bevölkerung
- Zu geringes Sicherheitsbewusstsein



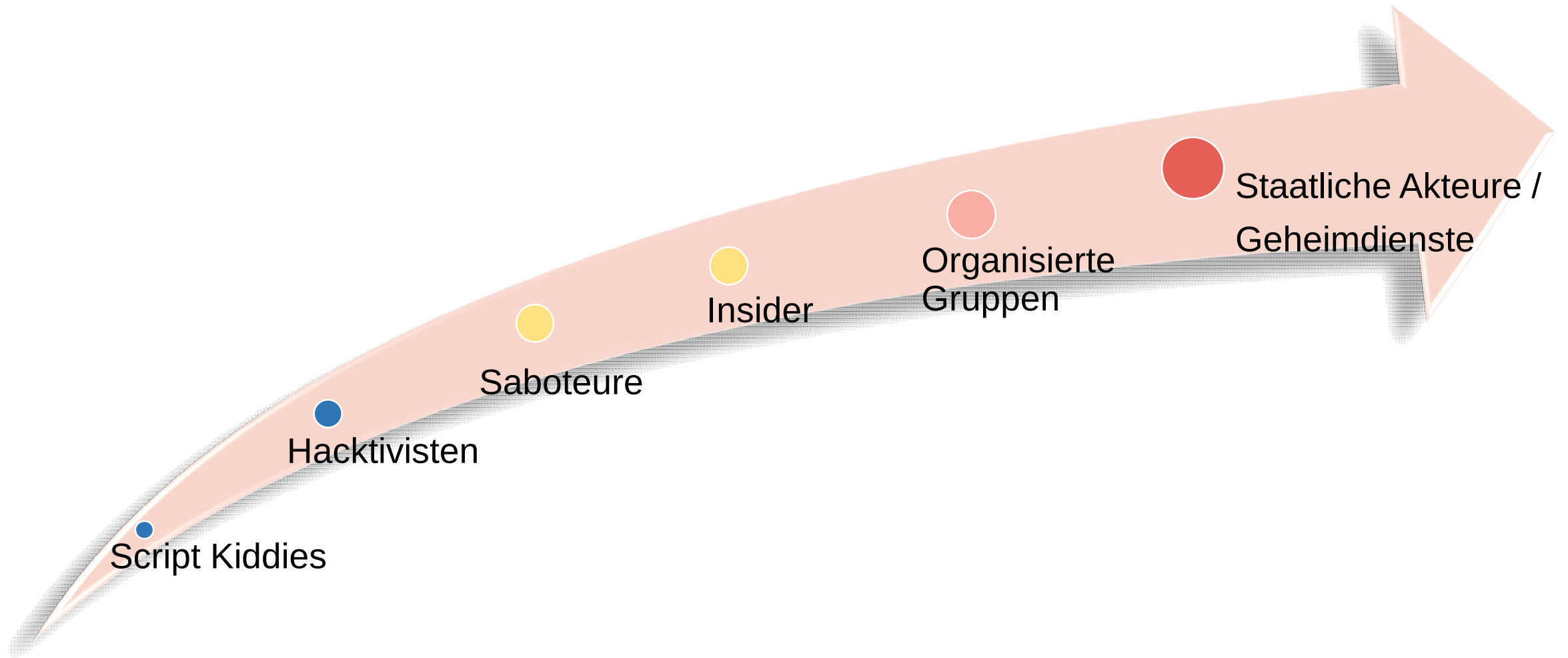
Aktuelle Bedrohungslage

Attacking systems density





Akteure





Inhalte



Melde- und Analysestelle
Informationssicherung
MELANI



Bedrohungslage:
Veränderung; Lage
national/international;
Akteure



Cyber-Angriffe:
Ausgewählte Beispiele



Schlussfolgerungen und
Empfehlungen





CEO Fraud





CEO Fraud

Re: RE: Dossier confidentiel - N

DATEI NACHRICHT

Ignorieren X

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

Mo 17.11.2014 16:26

m.w.@[redacted].com

Re: RE: Dossier confidentiel

An T. N.

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Parfait

Nous ef

Cette o

J'ai le plaisir de vous c

Je vous

M. du cabinet j

Merci d

Cordialement.

M. W.

Directeur Général

Je comp

Cordia

M.

Directe

Veuillez trouver ci-joint les coordonnées bancaires du bénéficiaire a créditer :

BANK : Z. BANK

Bénéficiaire : S. LIMITED

IBAN : NAR. 215

SWIFT : Y. 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. W.

Directeur Général

it en mesure d'effectuer un paiement

ation afin de respecter la norme de cette opération.

[redacted]



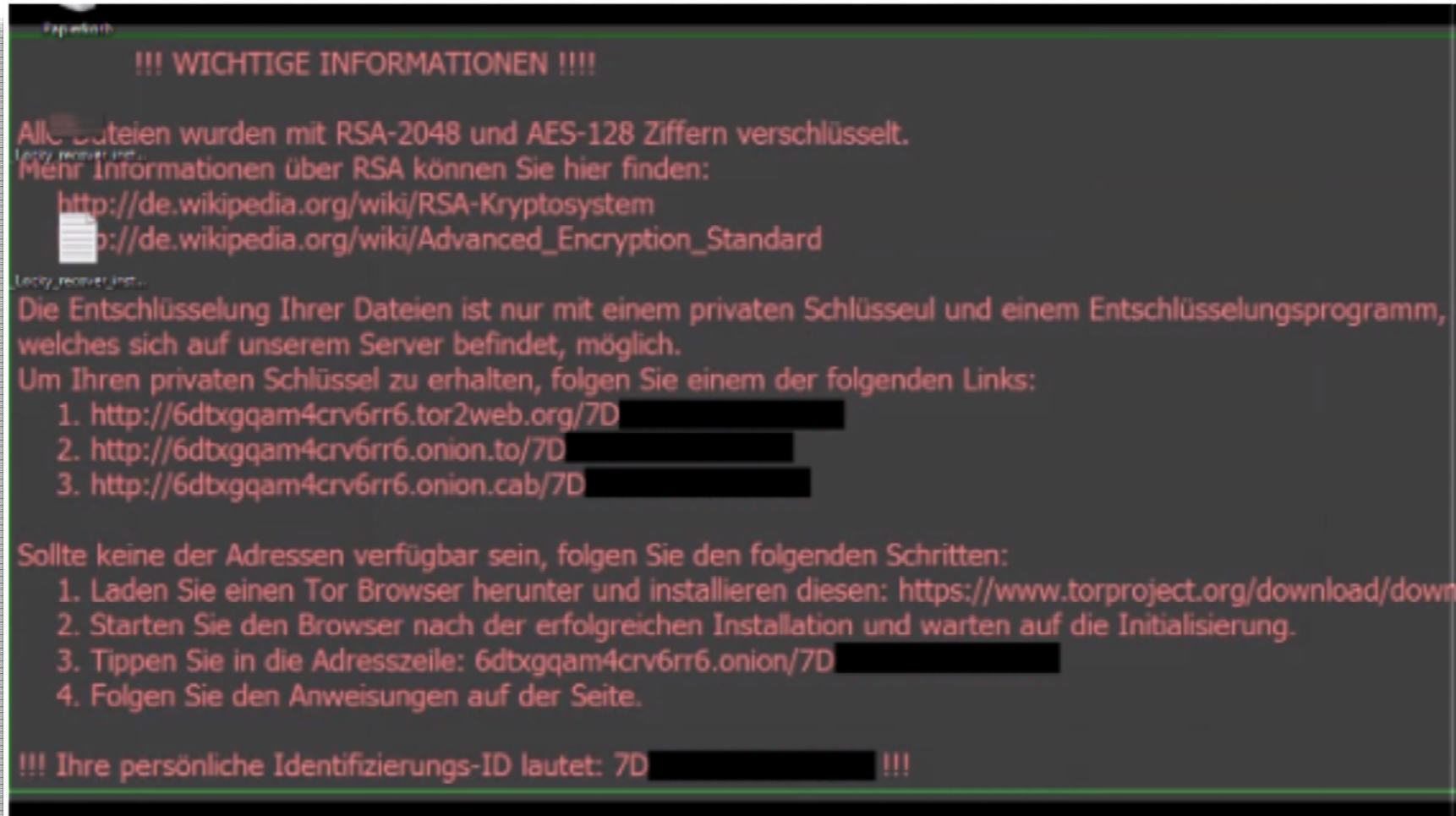
CEO Fraud: Empfehlungen



- Klare Weisungen bezüglich Zahlungen erteilen
- Keine internen Informationen weitergeben
- Im Zweifelsfall bei der GL nachfragen
- Vorsicht auch bei Mails von vermeintlich bekannten Personen
- Information an MELANI / fedpol, allenfalls Strafanzeige gegen Unbekannt bei KaPo



Verschlüsselungstrojaner





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

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

Grundsatzfrage:

Systeme abschotten: ja oder nein?

Unterstützung:

KI-Betreiber: reply@melani.admin.ch (best effort!)

KMU: fedpol (www.cybercrime.ch)

Anonyme Meldungen sowohl bei MELANI als auch bei fedpol möglich

Strafverfolgung:

Privatpersonen: Kapo am Wohnsitz

Unternehmen: Kapo am Geschäftssitz



Herzlichen Dank für Ihre Aufmerksamkeit



Max Klaus
Stv. Leiter Melde- und Analysestelle
Informationssicherung MELANI

Schwarztorstrasse 59
3003 Bern

