Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

Cyber-Gefahren: Aktuelle Bedrohungslage für KMU

Max Klaus, stv. Leiter MELANI

Inhalte

1. **Melde- und Analysestelle Informationssicherung MELANI**
2. Akteure
3. Cyber-Angriffe: Ausgewählte Beispiele
4. Schlussfolgerungen/Empfehlungen

Auftrag des Bundesrats / Public Private Partnership

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

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

Inhalte

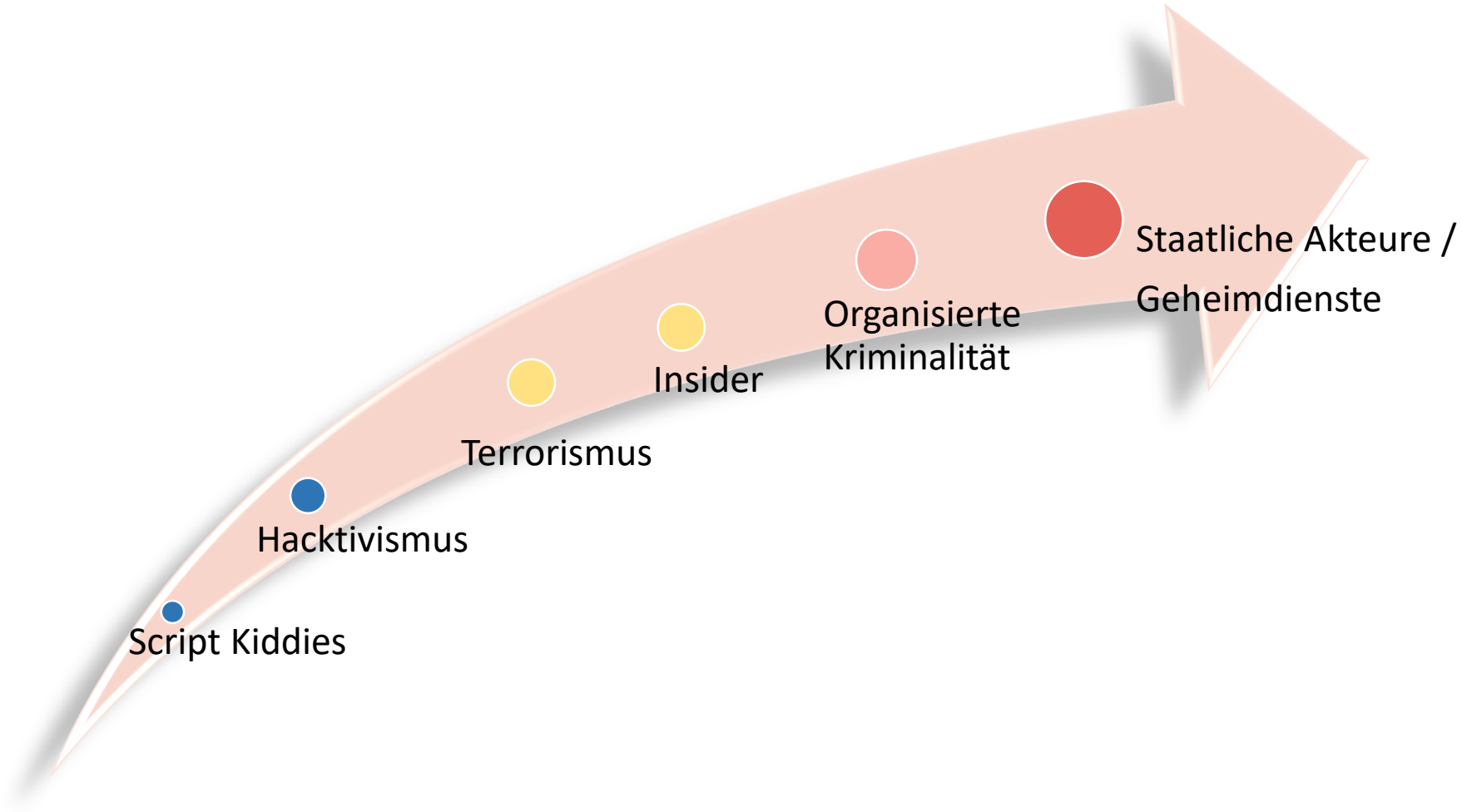
1. Melde- und Analysestelle Informationssicherung MELANI

2. **Akteure**

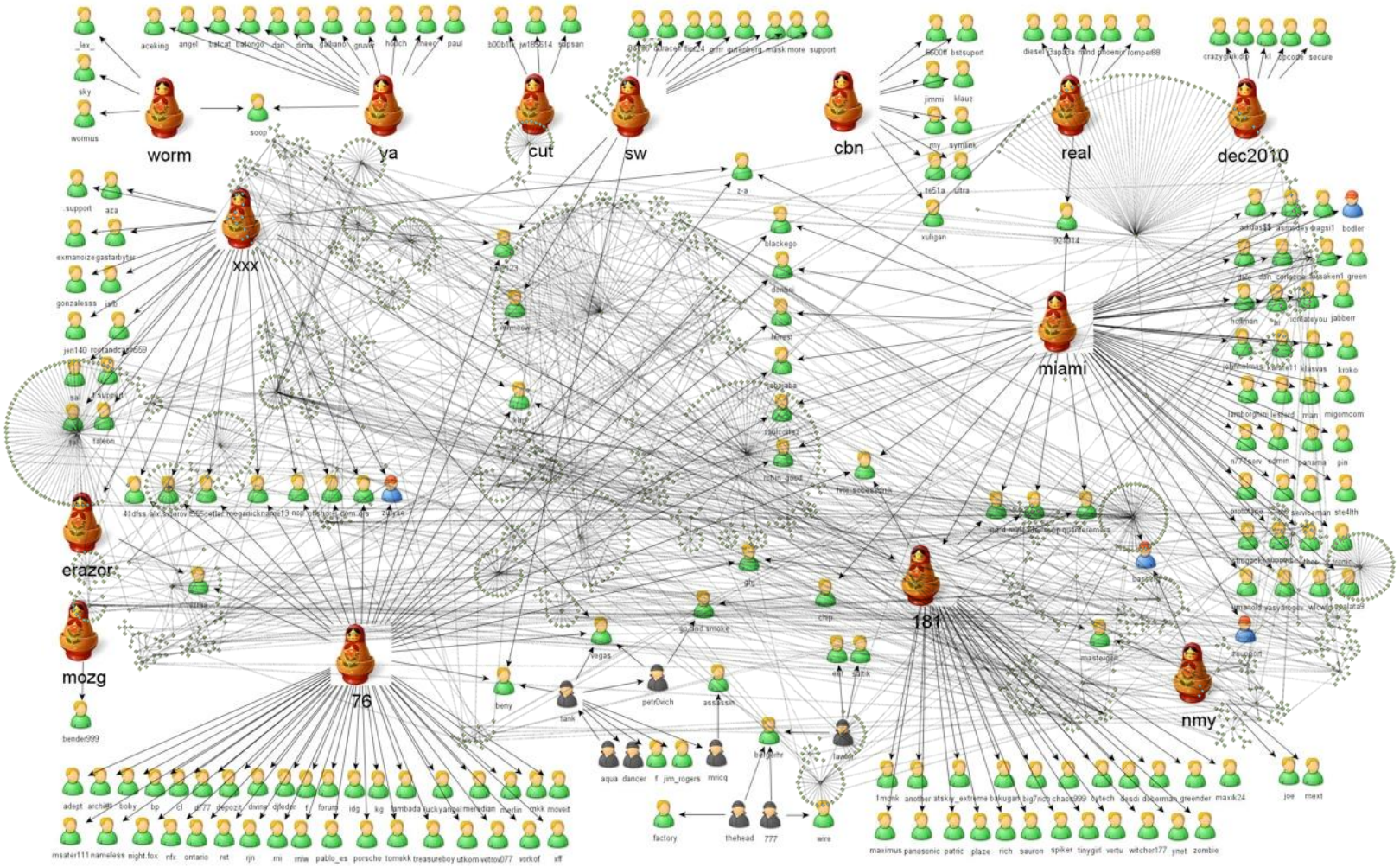
3. Cyber-Angriffe: Ausgewählte Beispiele

4. Schlussfolgerungen/Empfehlungen

Akteure


Staatliche Akteure /
Geheimdienste
Organisierte
Kriminalität
Insider
Terrorismus
Hacktivismus
Script Kiddies

Die Arbeitsteilung bei Cyberattacken



Am Anfang fast allen Übels: Social Engineering

https://www.youtube.com/watch?v=F7pYHN9iC9I

Inhalte

1. Melde- und Analysestelle Informationssicherung MELANI

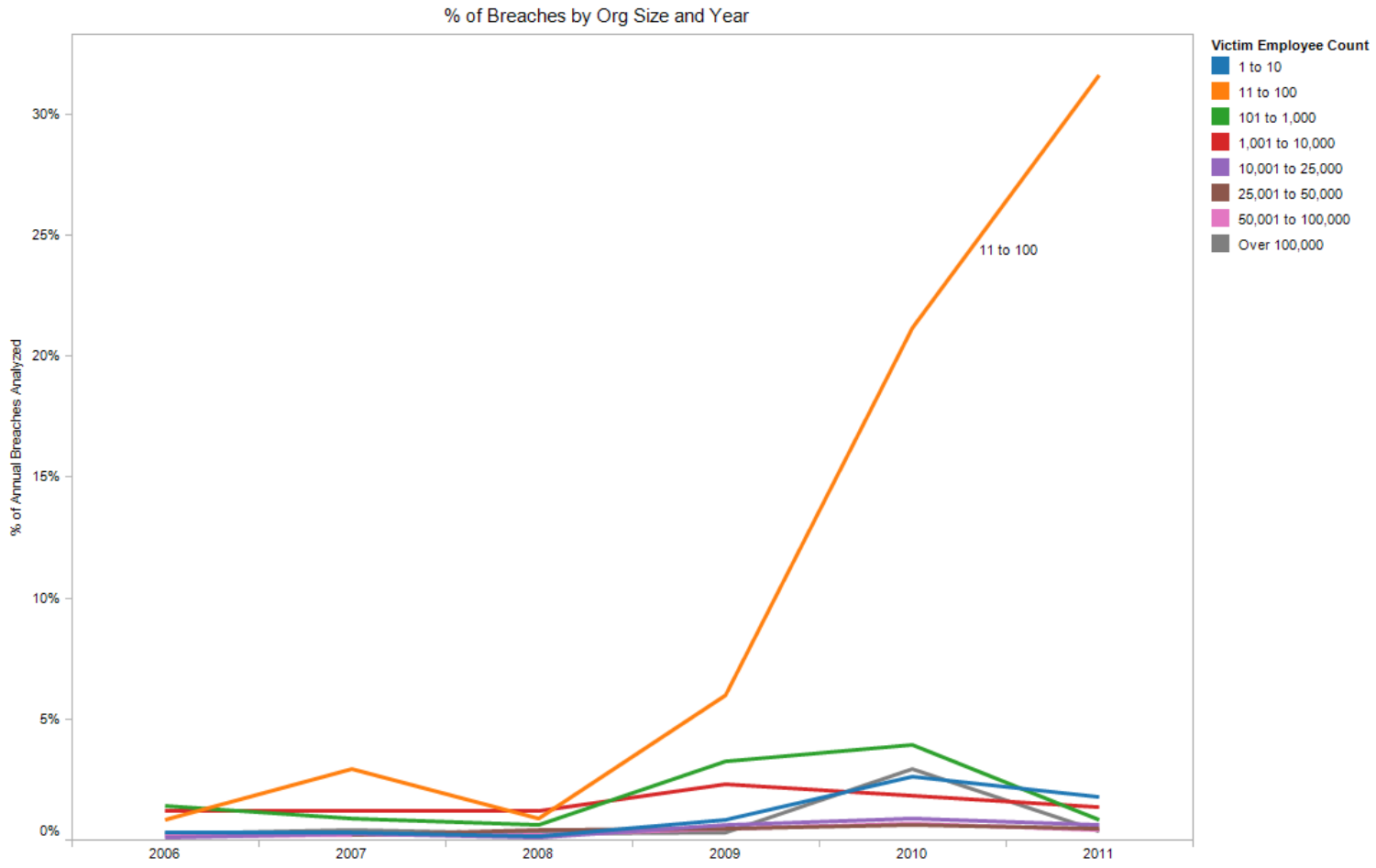
2. Akteure

3. Cyber-Angriffe: Ausgewählte Beispiele

4. Schlussfolgerungen/Empfehlungen

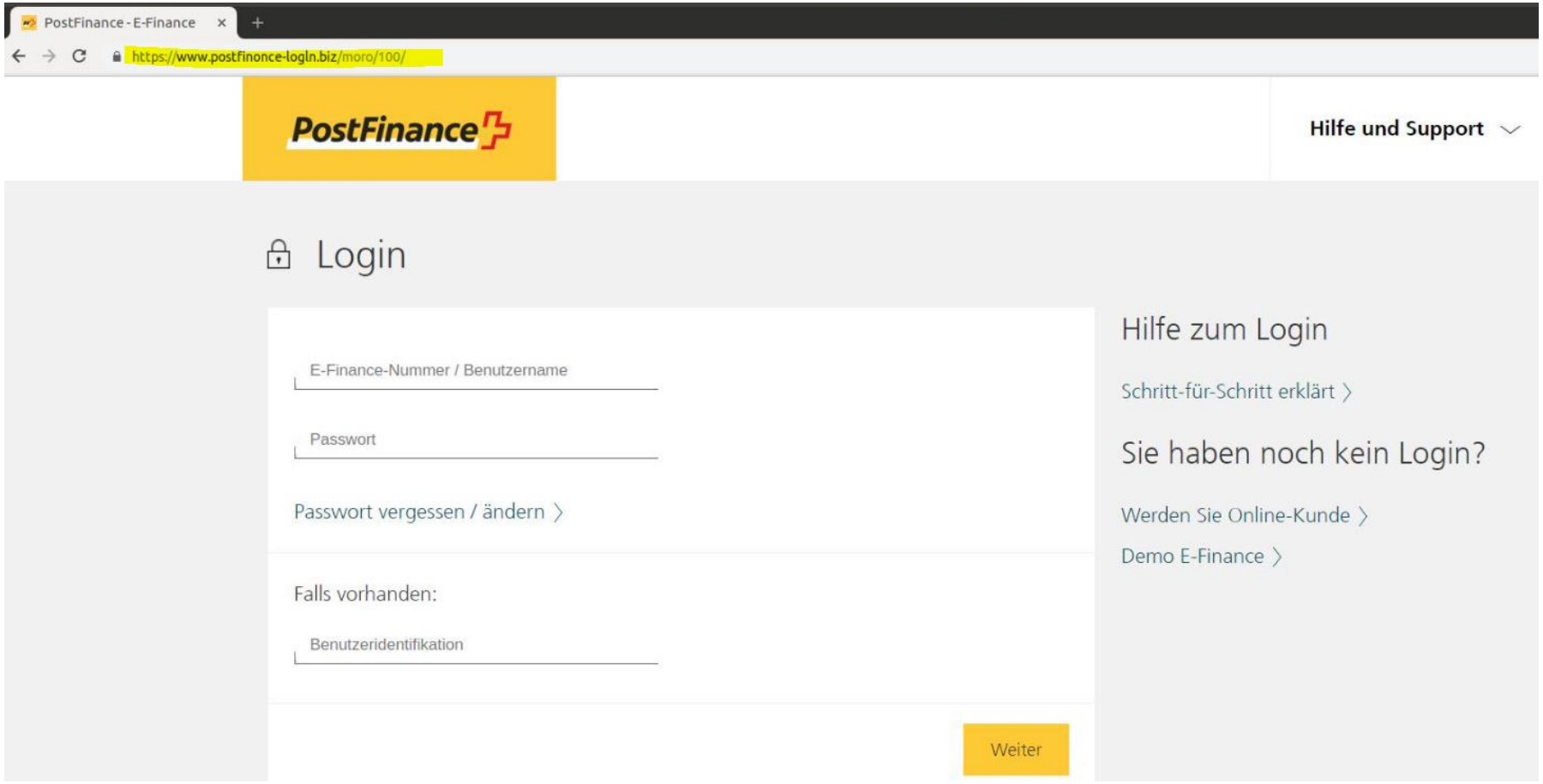
Wie gefährdet sind KMU?

KMU sind gefährdeter als Grossunternehmen!



Phishing (Password, Harvesting und Fishing)

Phishing: Beispiel aus der Schweiz



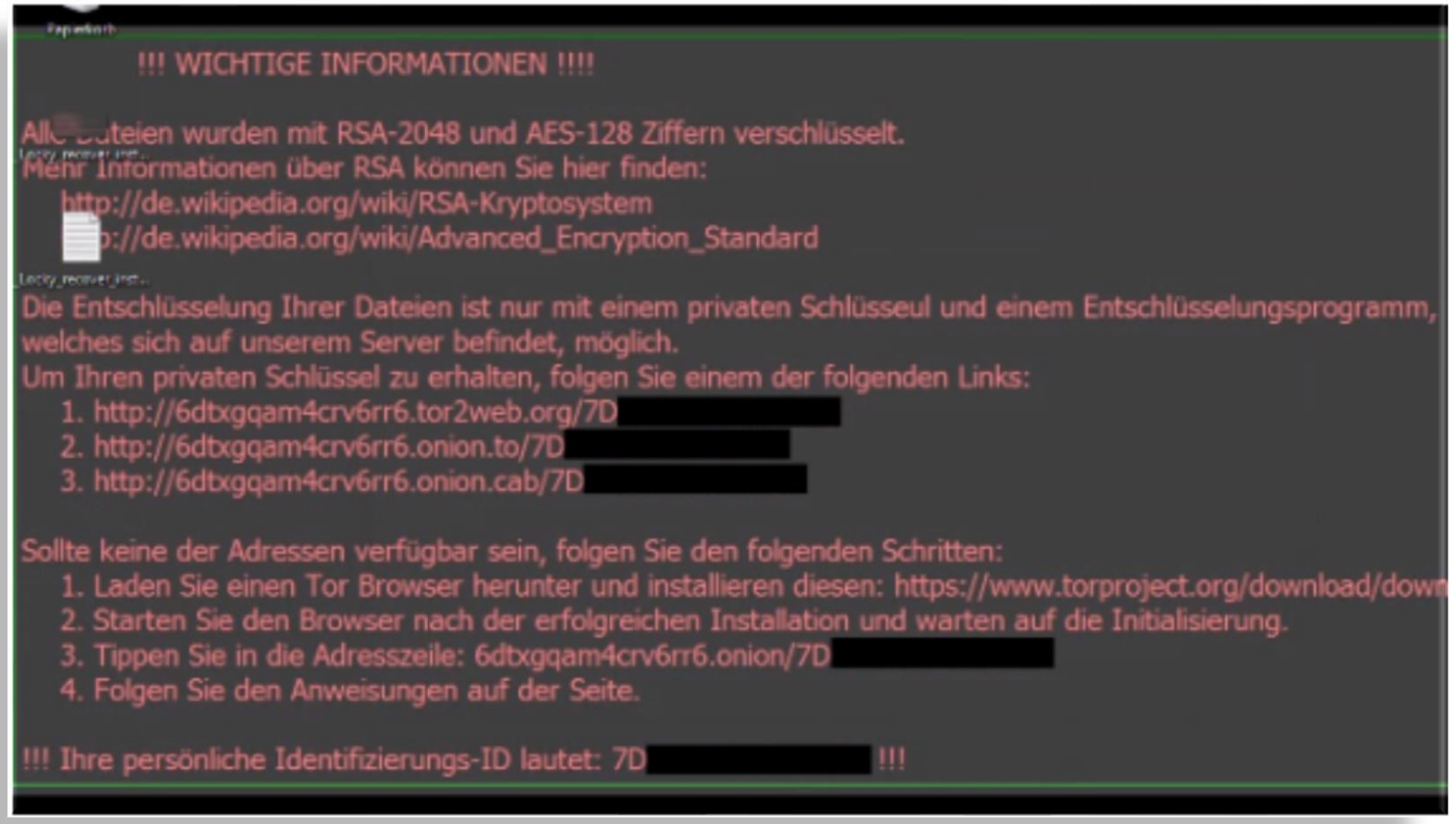
Phishing: Empfehlungen

- Keine Bank holt Benutzerinformationen telefonisch oder per Mail ein
- Vorsicht vor allen Mails, die eine Aktion Ihrerseits und/oder Drohungen enthalten
- Sofort Bank kontaktieren
- Information an MELANI / fedpol, allenfalls Strafanzeige gegen Unbekannt bei KaPo

Erpressung

http://www.trustedwatch.de

Verschlüsselungstrojaner



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!
- Information an MELANI / fedpol, allenfalls Strafanzeige gegen Unbekannt bei KaPo

Inhalte

1. Melde- und Analysestelle Informationssicherung MELANI

2. Akteure

3. Cyber-Angriffe: Ausgewählte Beispiele

4. **Schlussfolgerungen/Empfehlungen**

Schlussfolgerungen

- Informationstechnologie als zweischneidiges Schwert:

  Neue Möglichkeiten, aber auch neue Angriffsflächen

- Das organisierte Verbrechen verfügt über hervorragende Mittel und setzt diese gewinnbringend ein

- Angreifer wollen **Geld** verdienen und/oder einen Informationsvorsprung (Know-How-Gewinn zum Nulltarif) erzielen

- Der Mensch ist meistens das schwächste Glied in der Kette und wird deshalb meistens angregriffen.

Empfehlungen: proaktiv

Das Übliche zuerst:

- Starke Passwörter / regelmässiger PW-Wechsel
- Firewall (blacklist usw.)
- Updates
- Backups
- …

Aber:

- Technische Massnahmen allein genügen nicht!
- Organisatorische Massnahmen wie BCM, Krisenkommunikation usw. berücksichtigen!

Empfehlungen: reaktiv

Unterstützung für KMU:

- Bundesamt für Polizei (fedpol): www.cybercrime.ch
- Cyber-Security-Schnelltest für KMU: https://ictswitzerland.ch/themen/cyber-security/check/

Strafverfolgung:

- Privatpersonen: Kapo am Wohnsitz
- Unternehmen: Kapo am Geschäftssitz

Herzlichen Dank für Ihre Aufmerksamkeit

MELANI

Max Klaus
Stv. Leiter Melde- und Analysestelle
Informationssicherung MELANI

Schwarztorstrasse 59
3003 Bern