Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

Cyber-Bedrohungen

Max Klaus, stv. Leiter MELANI

Inhalte

1. **Melde- und Analysestelle Informationssicherung MELANI**

2. Bedrohungslage:
   Veränderung, Lage national/international, Akteure

3. Cyber-Angriffe: Ausgewählte Beispiele

4. Schlussfolgerungen/Empfehlungen

BR-Auftrag / PPP

	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

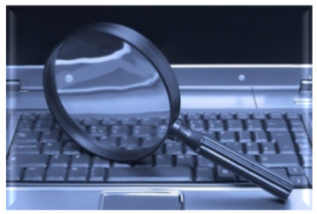
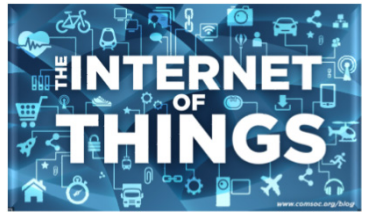
1. Melde- und Analysestelle Informationssicherung MELANI

2. **Bedrohungslage:**
   Veränderung, Lage national/international, Akteure

3. Cyber-Angriffe: Ausgewählte Beispiele

4. Schlussfolgerungen/Empfehlungen

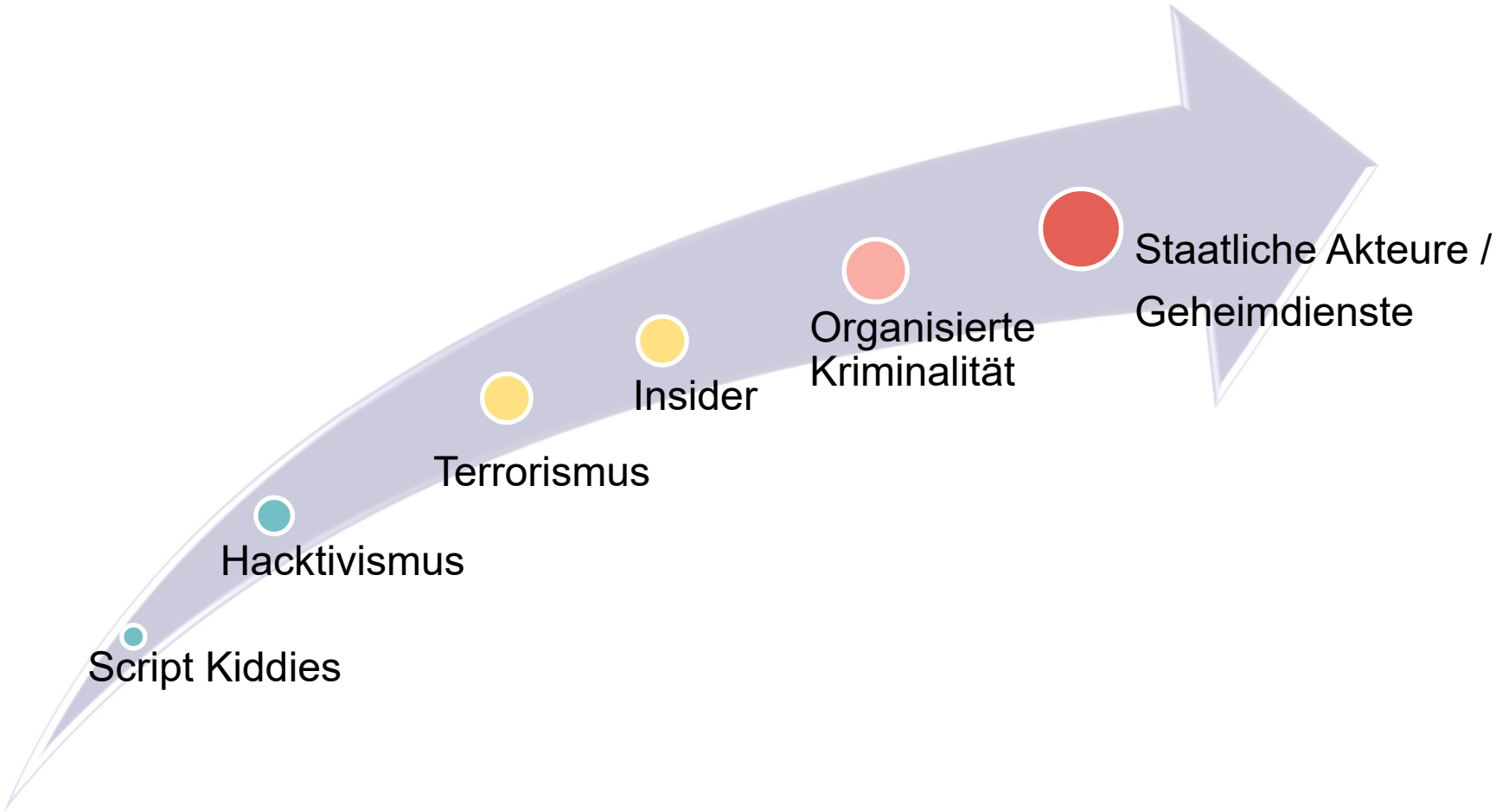
Veränderung der Bedrohungslage

>100 Jahre	Vor 10 Jahren	heute	morgen?
			
derstandard..at	augsburgerallgemeine..de	jdpower..com	fossbytes.com

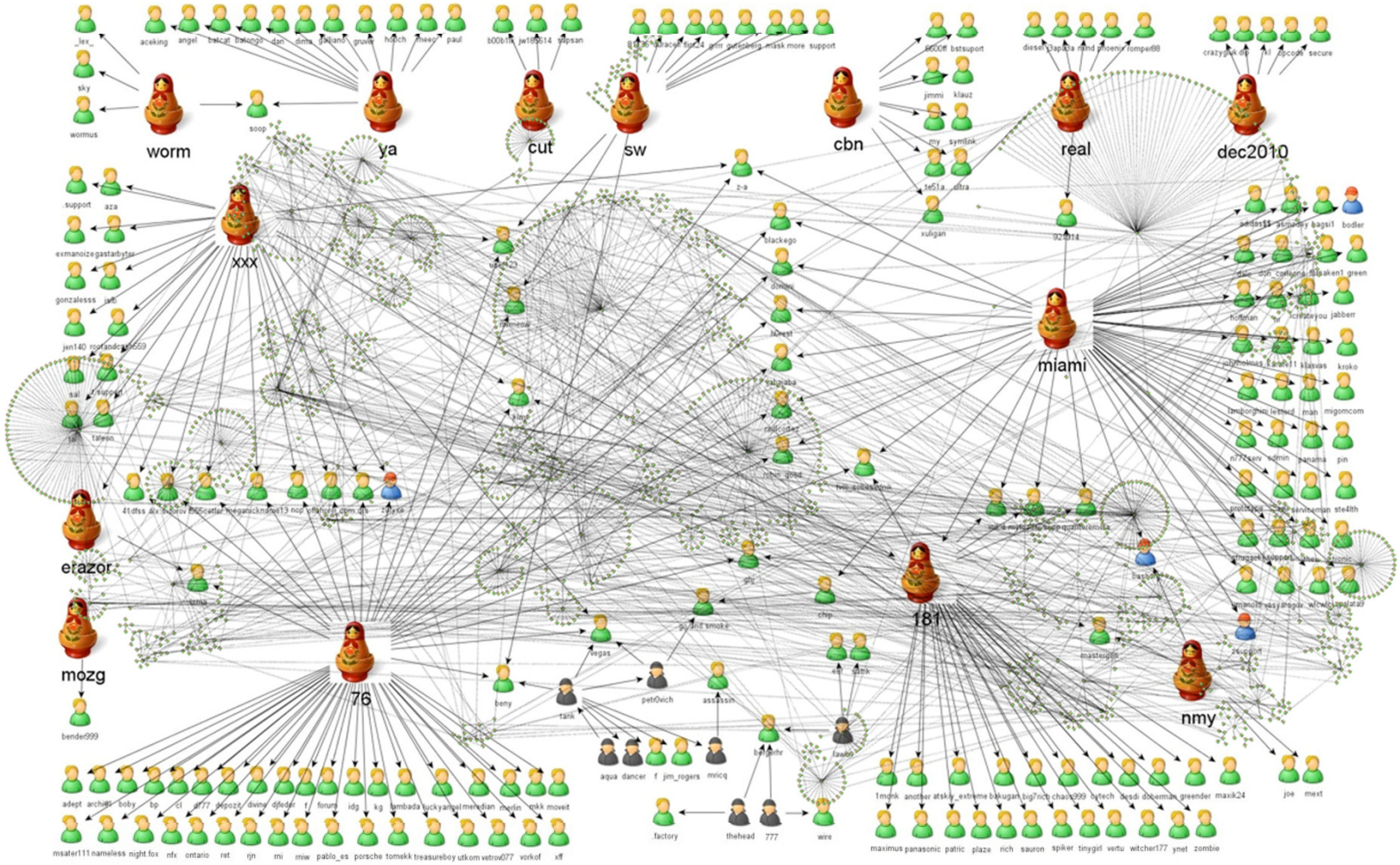
- Modernere Mittel
- Vernetzte Bevölkerung
- Zu geringes Sicherheitsbewusstsein

Aktuelle Bedrohungslage

Akteure


Staatliche Akteure /
Geheimdienste
Organisierte
Kriminalität
Insider
Terrorismus
Hacktivismus
Script Kiddies

Die Arbeitsteilung bei Cyberattacken



Inhalte

1. Melde- und Analysestelle Informationssicherung MELANI

2. Bedrohungslage:
   Veränderung, Lage national/international, Akteure

3. Cyber-Angriffe: Ausgewählte Beispiele

4. Schlussfolgerungen/Empfehlungen

Angriffe heute

Opfer

Internet

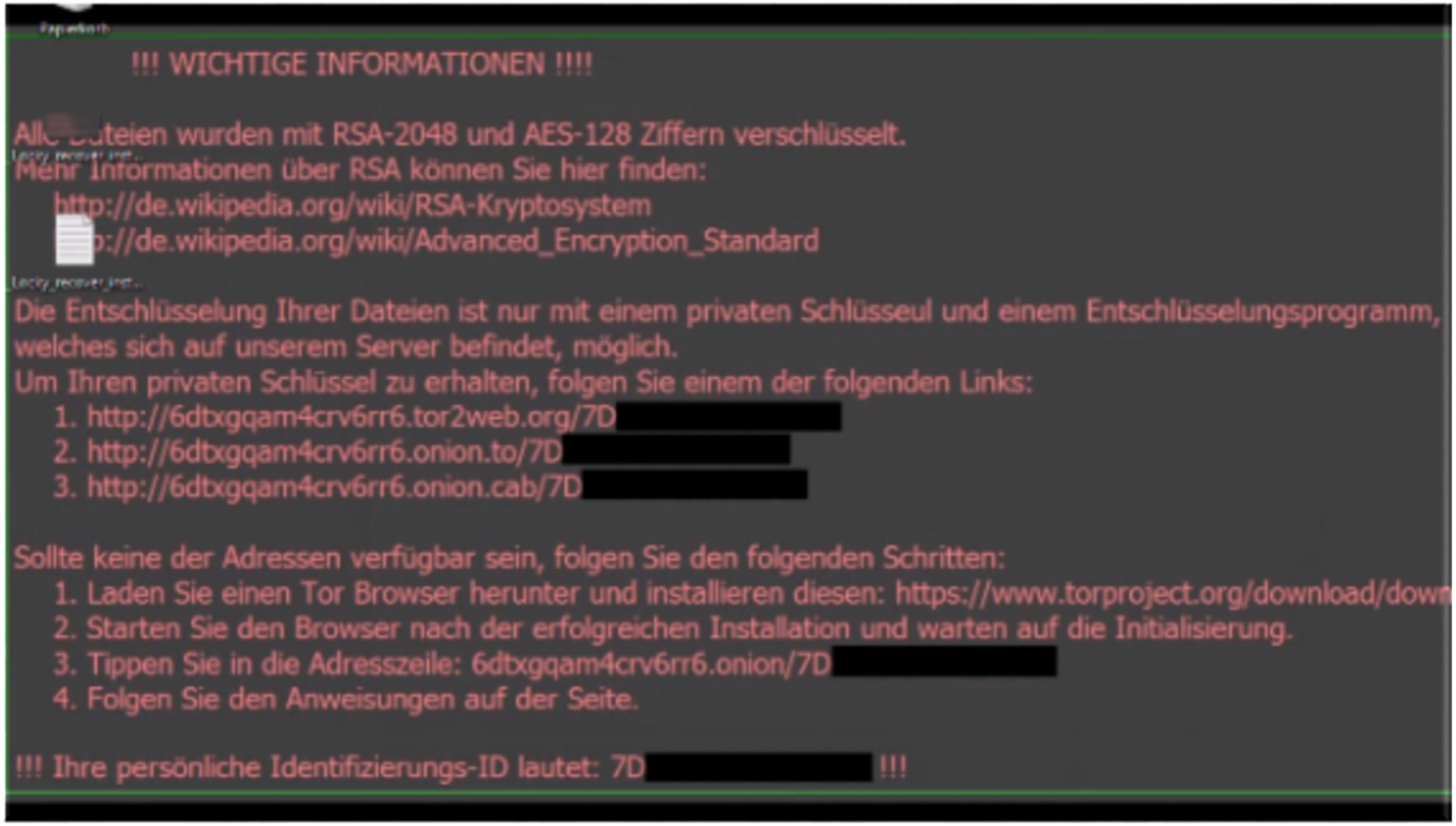
Krimineller

auch ein Krimineller

Erpressung

http://www.trustedwatch.de

Verschlüsselungstrojaner «Locky» (1/2)



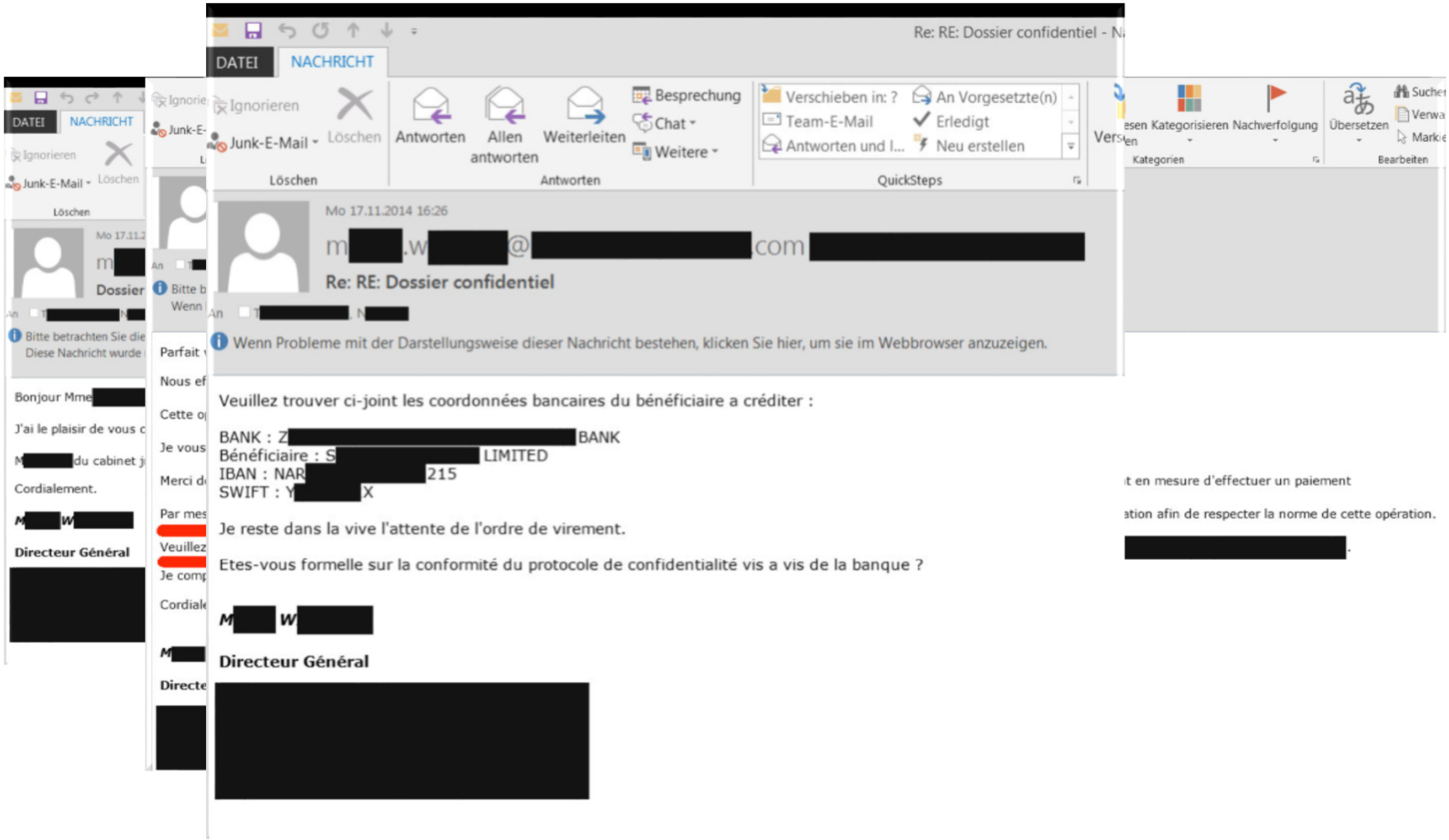
Verschlüsselungstrojaner «Locky» (2/2)

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

CEO Fraud

CEO Fraud


DATEI
NACHRICHT
Re: RE: Dossier confidentiel
Ignorieren
Junk-E-Mail
Löschen
Antworten
Allen antworten
Weiterleiten
Besprechung
Chat
Weitere
Verschieben in: ?
Team-E-Mail
Antworten und l...
An Vorgesetzte(n)
Erledigt
Neu erstellen
QuickSteps
Kategorisieren
Nachverfolgung
Übersetzen
Kategorien
Bearbeiten
Mo 17.11.2014 16:26
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 ?
Directeur Général

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

Inhalte

1. Melde- und Analysestelle Informationssicherung MELANI

2. Bedrohungslage:
   Veränderung, Lage national/international, 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 oft das schwächste Glied in der Kette und wird deshalb meistens angegriffen.

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

Gretchenfrage:
Infizierte Systeme abschotten: ja oder nein?

Auf keinen Fall Lösegeld bezahlen!

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