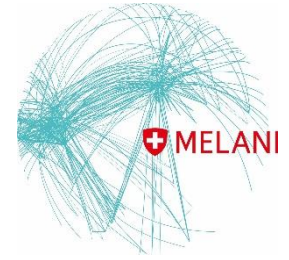




Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB  
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

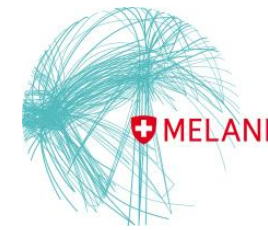


# Cyber-Gefahren: Aktuelle Bedrohungslage für KMU

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



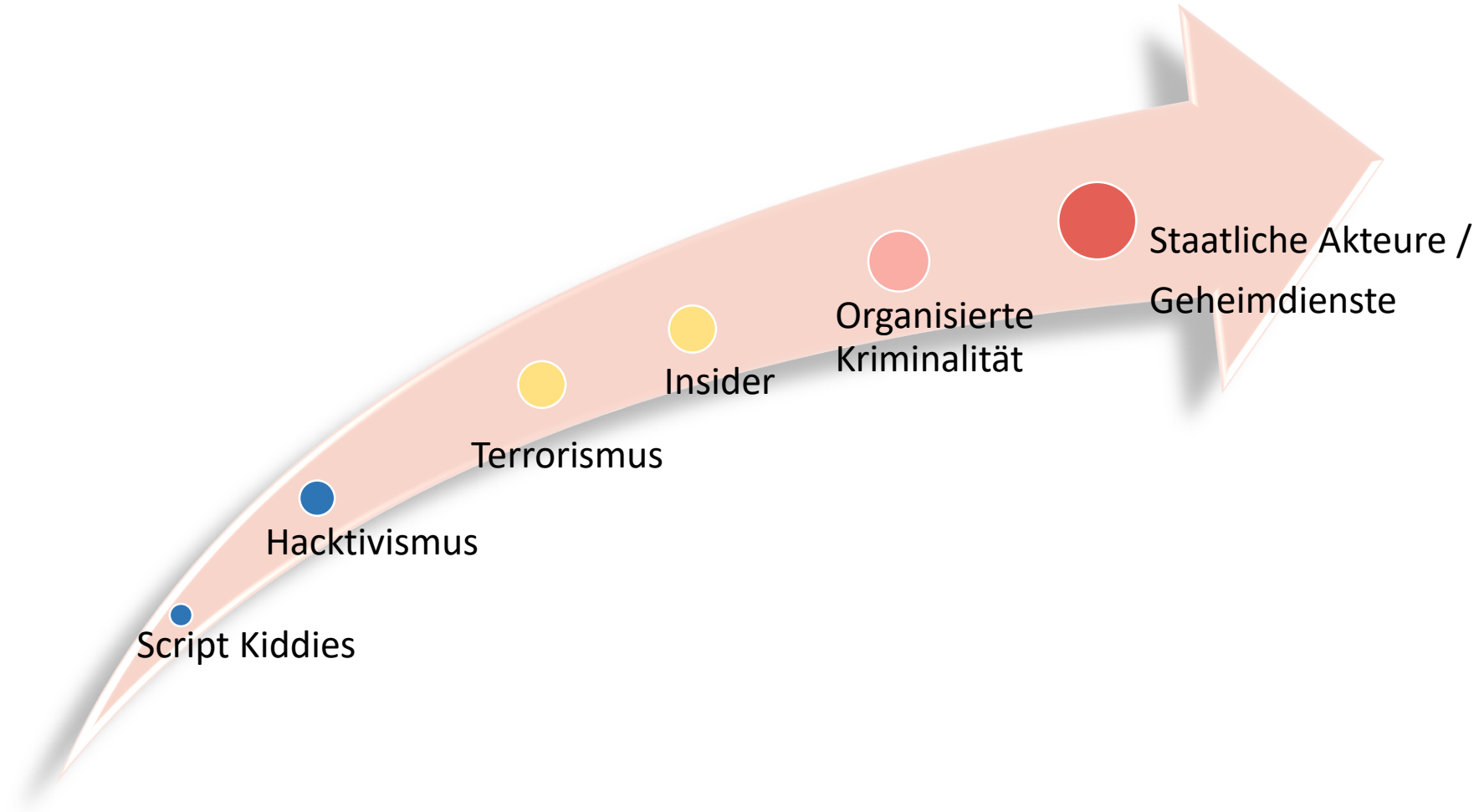
# Inhalte



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

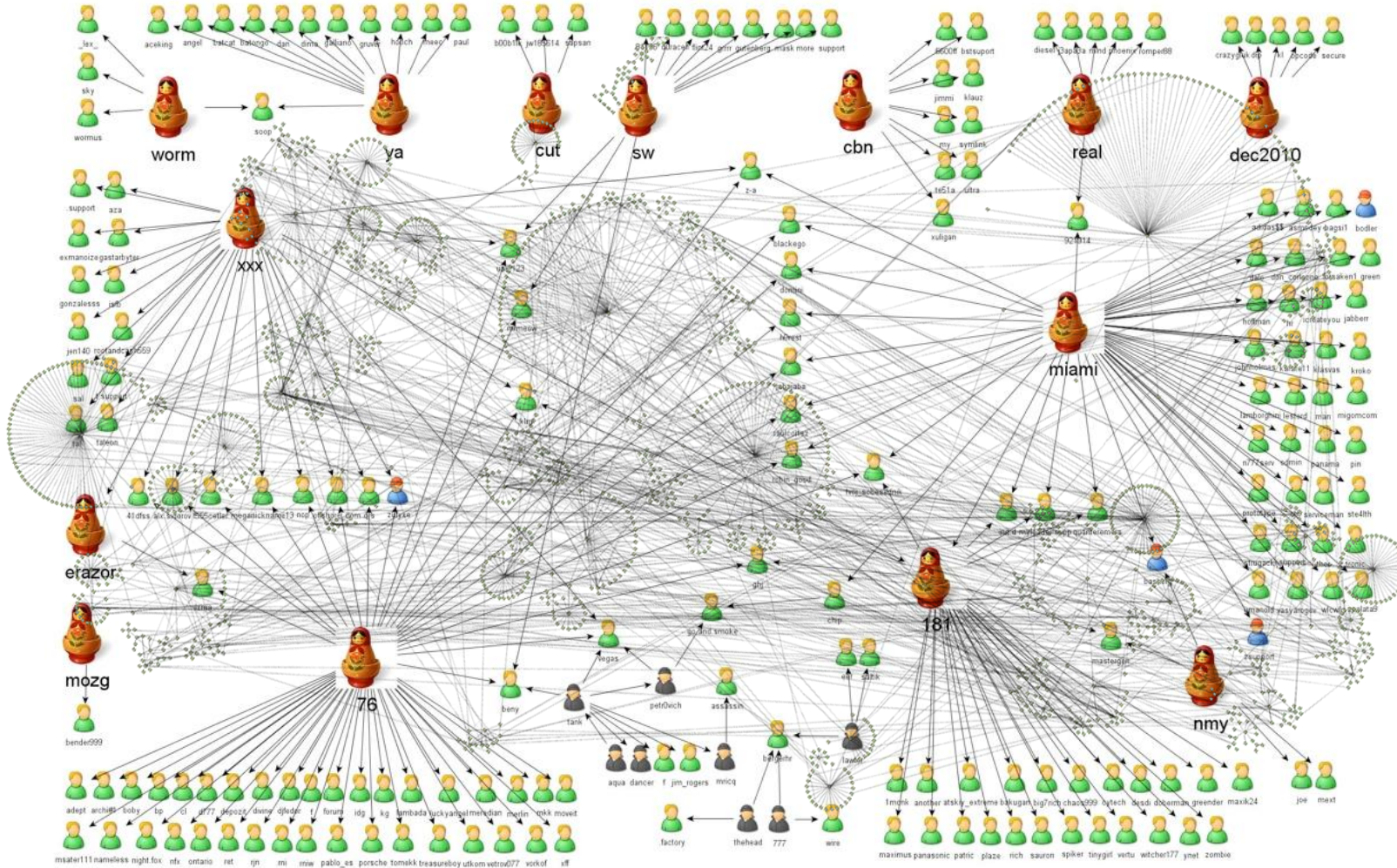


# Akteure





# Die Arbeitsteilung bei Cyberattacken





# Am Anfang fast allen Übels: Social Engineering

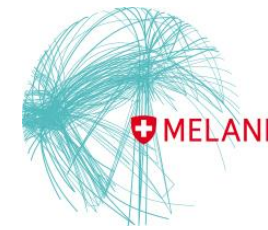


<https://www.youtube.com/watch?v=F7pYHN9iC9I>





# Inhalte



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



# Wie gefährdet sind KMU?

SRF 20 minuten Zürich 12°

Schweiz Ausland Wirtschaft Sport People Entertainment Digital Wissen

News Taschengeldrechner Börse Grow Up

Ihre Story, Ihre Informationen, Ihr Hinweis? [feedback@zominuten.ch](mailto:feedback@zominuten.ch)

Internet-Sicherheit 24. Februar 2017 23:18; Akt: 24.02.2017 23:18

## Hacker greifen KMU mit falschen Bewerbungen an

von K. Wolfensberger - Hacker nutzen einen neuen perfiden Trick: Sie geben sich als Jobbewerber aus, um Sicherheitsmassnahmen von Firmen zu umgehen und Geld zu erpressen.

← VORHERIG STE SENDUNG →

Schw... Krimi... Download Sendetern



Grosse k... sie sich... vieler kl... für zu w

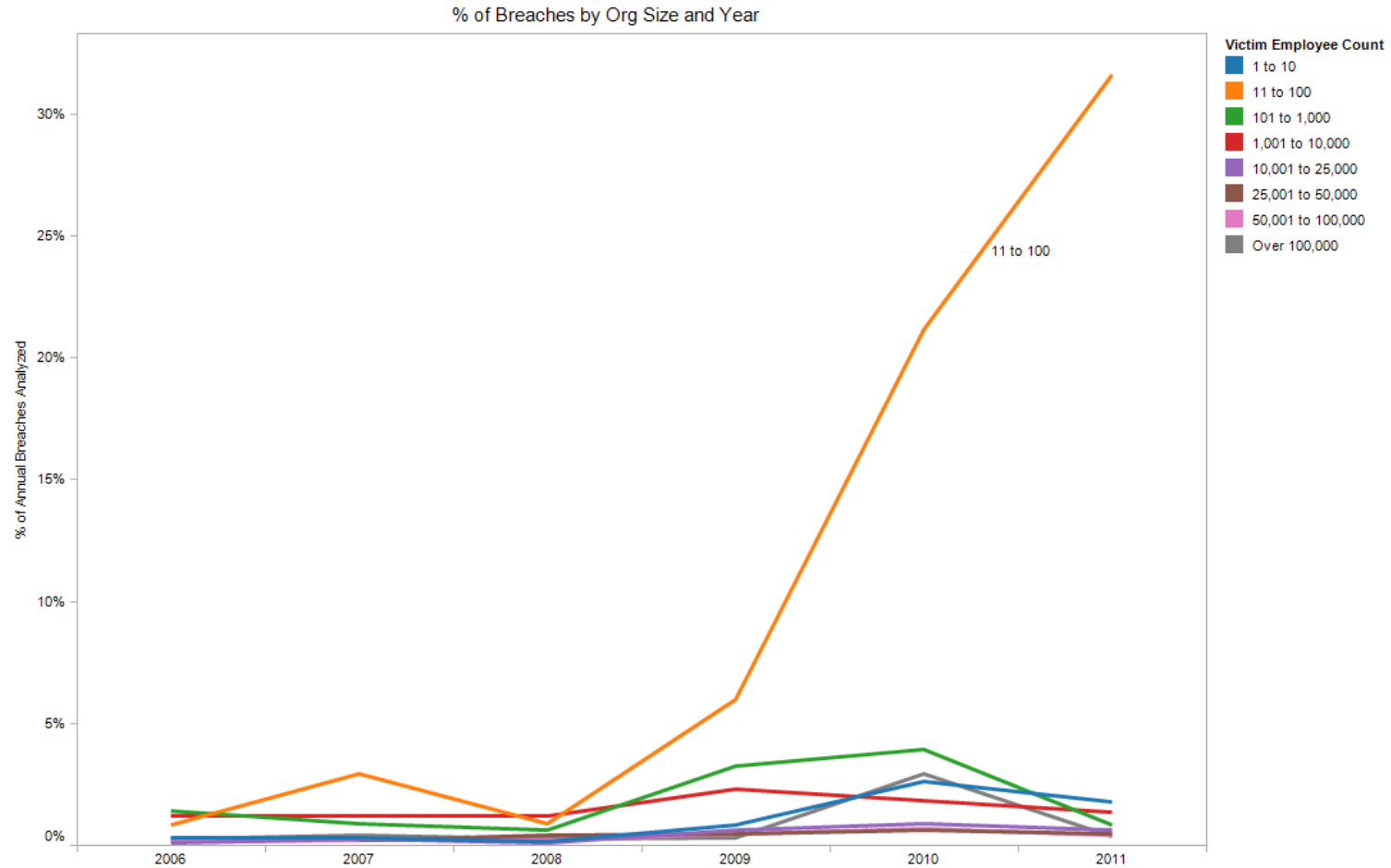
119 In den letzten Wochen haben in der Schweiz Hackerangriffe eines neuen Typs zugenommen.

3 6

5

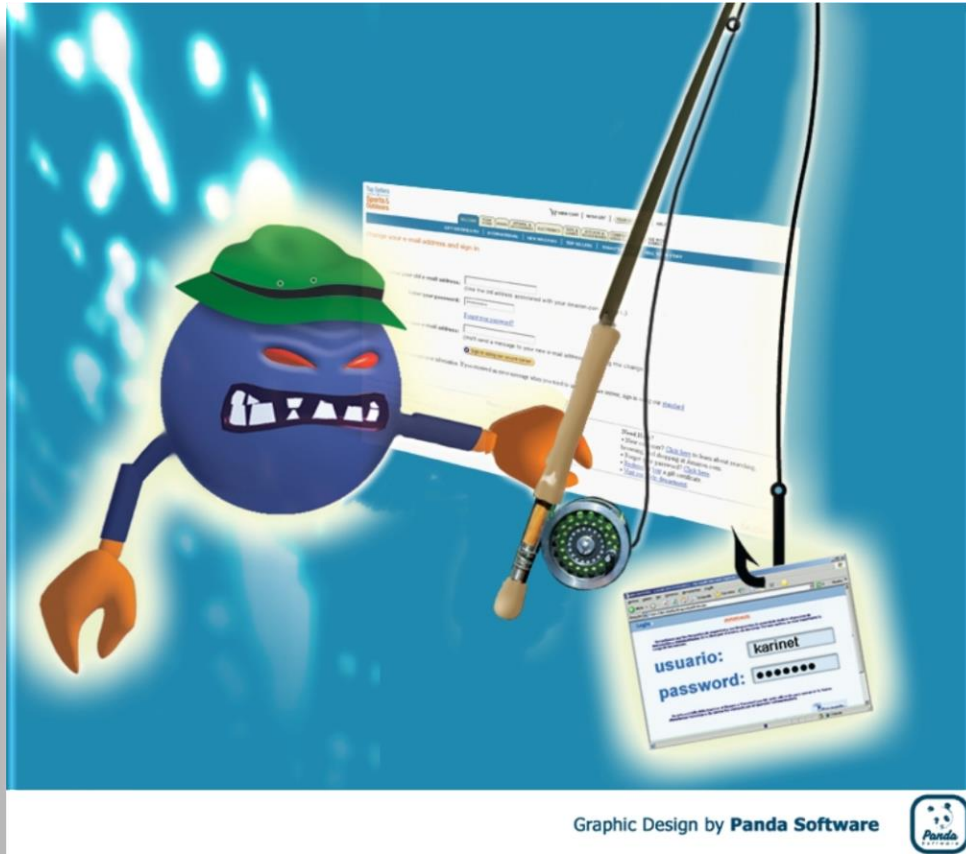


# KMU sind gefährdeter als Grossunternehmen!





# Phishing (Password, Harvesting und Fishing)





# Phishing: Beispiel aus der Schweiz

The screenshot shows a web browser window with the address bar displaying <https://www.postfinance-logout.biz/moro/100/>. The page features the PostFinance logo in a yellow box at the top left and a 'Hilfe und Support' dropdown menu at the top right. The main content area is titled 'Login' and contains a form with the following fields and links:

- E-Finance-Nummer / Benutzername
- Passwort
- [Passwort vergessen / ändern >](#)
- Falls vorhanden:
  - Benutzeridentifikation
- [Weiter](#)

On the right side of the login form, there is a 'Hilfe zum Login' section with the following links:

- [Schritt-für-Schritt erklärt >](#)
- Sie haben noch kein Login?**
- [Werden Sie Online-Kunde >](#)
- [Demo E-Finance >](#)



# 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

```
!!! 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.html
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 !!!
```







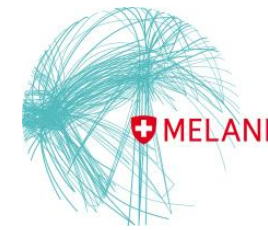
# Verschlüsselungstrojaner: Empfehlungen



- Regelmässige Datensicherung
- Datenträger nach Backup vom PC / Netz trennen
- Qualität der Backups sporadisch überprüfen
- Versuchen Sie, die Daten wiederherzustellen:  
[www.nomoreransom.org](http://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 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

## Unterstützung für KMU:

- Bundesamt für Polizei (fedpol):  
[www.cybercrime.ch](http://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



Max Klaus  
Stv. Leiter Melde- und Analysestelle  
Informationssicherung MELANI

Schwarztorstrasse 59  
3003 Bern

