Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Unité de pilotage informatique de la Confédération (UPIC)
Service de renseignement de la Confédération SRC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

Cyber Threats:
Or forget cyber and think about crown jewels

ACTSR - June 2018

Content

1. What is MELANI
2. Let's think about critical processes
3. Un-targeted and Targeted Attacks
4. A few examples

Federal Council Mandate

- The Reporting and Analysis Centre for Information Assurance
- Active since 2004
- Critical infrastructure protection against abuse and attacks (concept of subsidiarity)
- Early warning and incident handling in information and communications infrastructure

MELANI is based on a Public-Private-Partnership (PPP) approach and voluntary participation of its partners

Our mandate (continued)

- National strategy for Switzerland's protection against cyber risks (2013-2017)
  - Focus on Critical Infrastructure (Closed Circle)

- National strategy for Switzerland's protection against cyber risks 2.0 (2018-2022)
  - SMEs and Citizens

Two videos

- ENISA: Heightened Defences:
  https://www.youtube.com/watch?v=b6i8gc4LbC4

- Jimmy Kimmel : Password Sidewalk
  https://www.youtube.com/watch?v=opRMrEfAIiI

Throwing Cyber out the window

- Different Vectors (physical, tech-based, humans…)
- Different Actors (individuals, organized crime, …)
- Different means and aims (financial, information,…)
- How do we try to make sense of all this?

The CIA Triad : a model to assessing risks

Attacks on:

- Confidentiality (phishing; E-banking viruses, CEO Fraud; APT, ….)
- Availability (DDoS, Ransomware, …)
- Integrity (Sabotage…)

So where are your crown jewels?

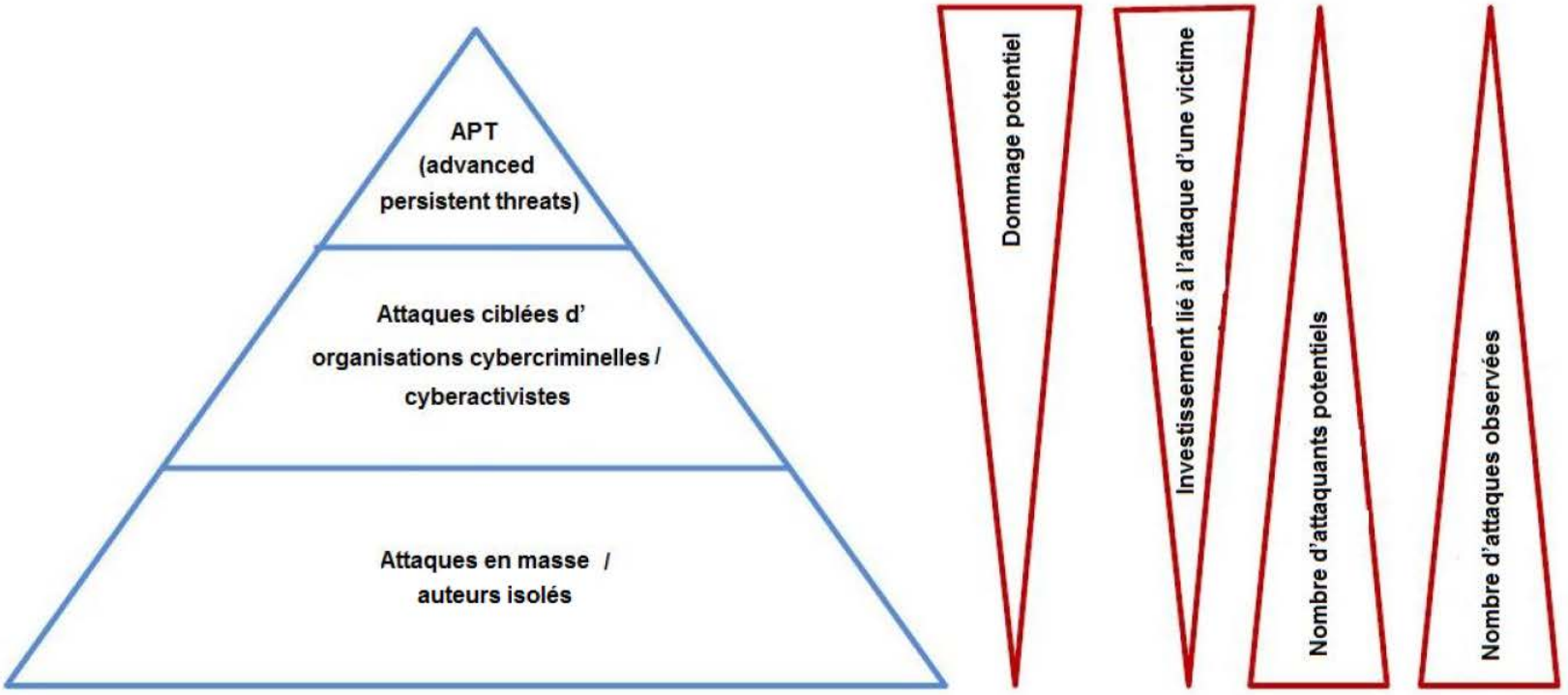
- Is it the Confidentiality?
  - Customer Data? Contractual agreements? Financial Documents? Negotiations? Designs?
- Is it the Availability?
  - Customer Data? Working documents? Workstations? Web shop?
- Is it the Integrity?
  - The functioning of a factory? A medical device? (This last one will get more and more critical)

So how do you manage your Data?

- Is there data more sensitive that other?
- Who has access?
- How are they stored?
- How are they shared?

If there is data that should never be compromised, don't leave it on a connected object…

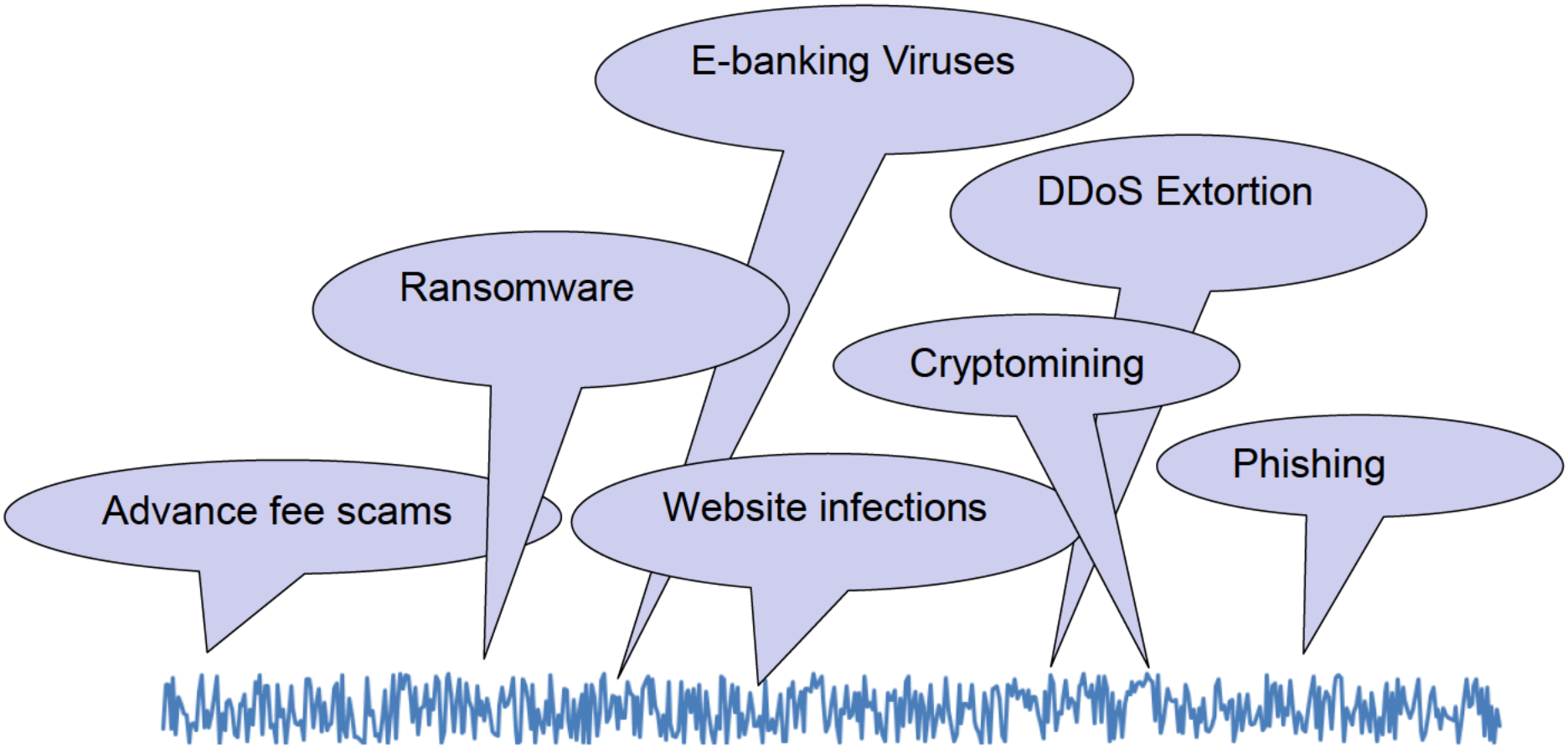
Different Actors have different Aims



Source: Threat Pyramid, adapted from sans.org

So what do we see "in the wild"?

A large amount of Background Noise



In general: Background Noise is Un-targeted

The attacker, typically,:

- Sends out large amounts of emails
- Hoping someone will fall victim to the attack

As a 'defender', you can reduce your threat to a high degree on a organisational level by:

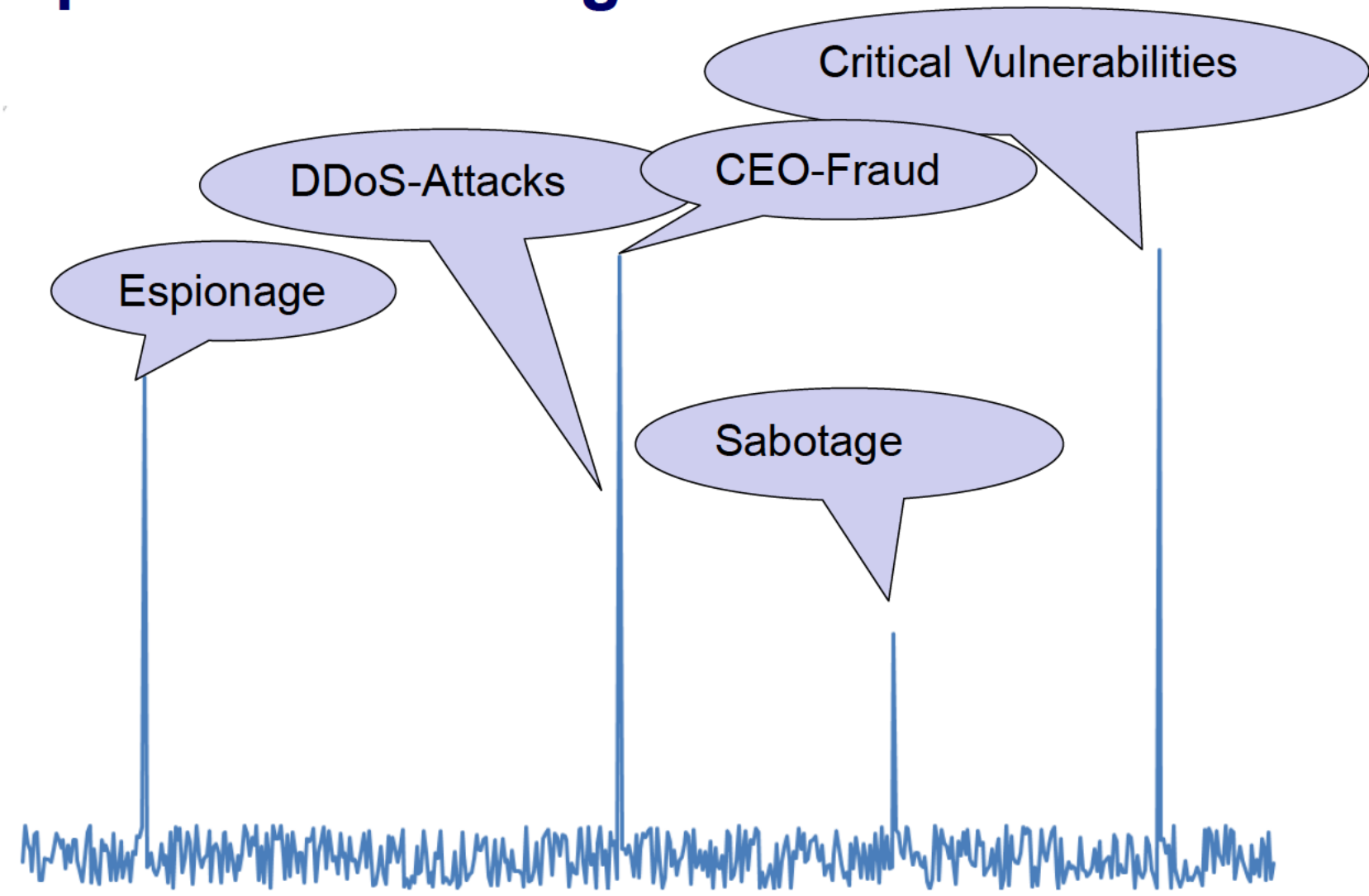
- Creating awareness among your collaborators
- Creating an environment where error can be communicated ("I might have clicked on something…")

Risk Reduction Measures

- Having clear processes (also reaction processes)
- Using up-to-date software (OS, Browser, CMS, etc.)
- Segmenting your network, or isolating your payment machine (or other sensitive appliances)
- Keeping regular backups (disconnected when finished)
- Network Security Monitoring (even very basic)

The objective is to reduce the amount of damage background noise can create.

Spikes and/or targeted



Spikes are much rarer, but:

In the case of a targeted attack, the attacker:

- Has resources (capacity, time and money)
- Will get in your organisation.

In all of these cases, as a 'defender', having defined your critical processes, you should be able to estimate:

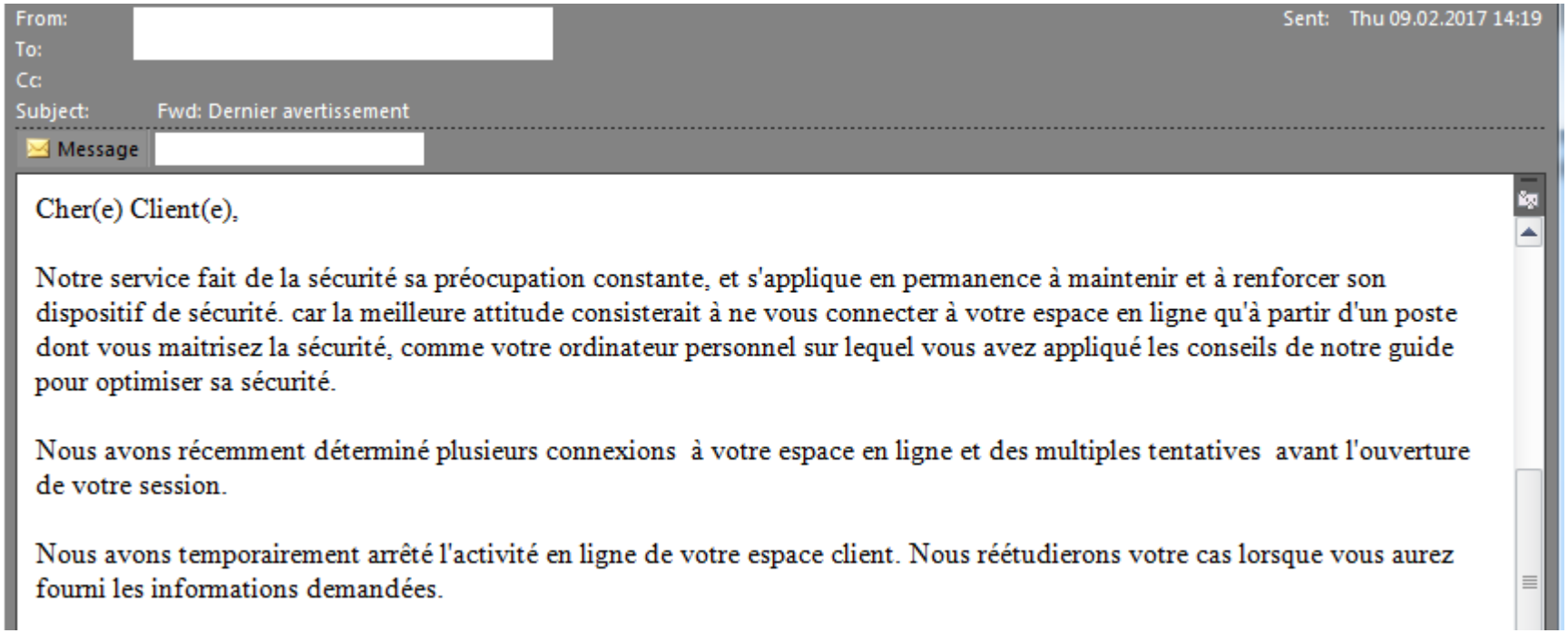
- And know how and where you are at risk.
- What could they be after, if it is targeted

- **Reaction is of the essence, so be prepared.**

Phishing

“Give a man an 0-day and he'll have access for a day,
Teach a man to phish and he'll have access for life.”
- the grugq

Phishing (2)



From:
To:
Cc:
Subject: Fwd: Dernier avertissement
Sent: Thu 09.02.2017 14:19

Message

Cher(e) Client(e),

Notre service fait de la sécurité sa préocupation constante, et s'applique en permanence à maintenir et à renforcer son dispositif de sécurité. car la meilleure attitude consisterait à ne vous connecter à votre espace en ligne qu'à partir d'un poste dont vous maitrisez la sécurité, comme votre ordinateur personnel sur lequel vous avez appliqué les conseils de notre guide pour optimiser sa sécurité.

Nous avons récemment déterminé plusieurs connexions à votre espace en ligne et des multiples tentatives avant l'ouverture de votre session.

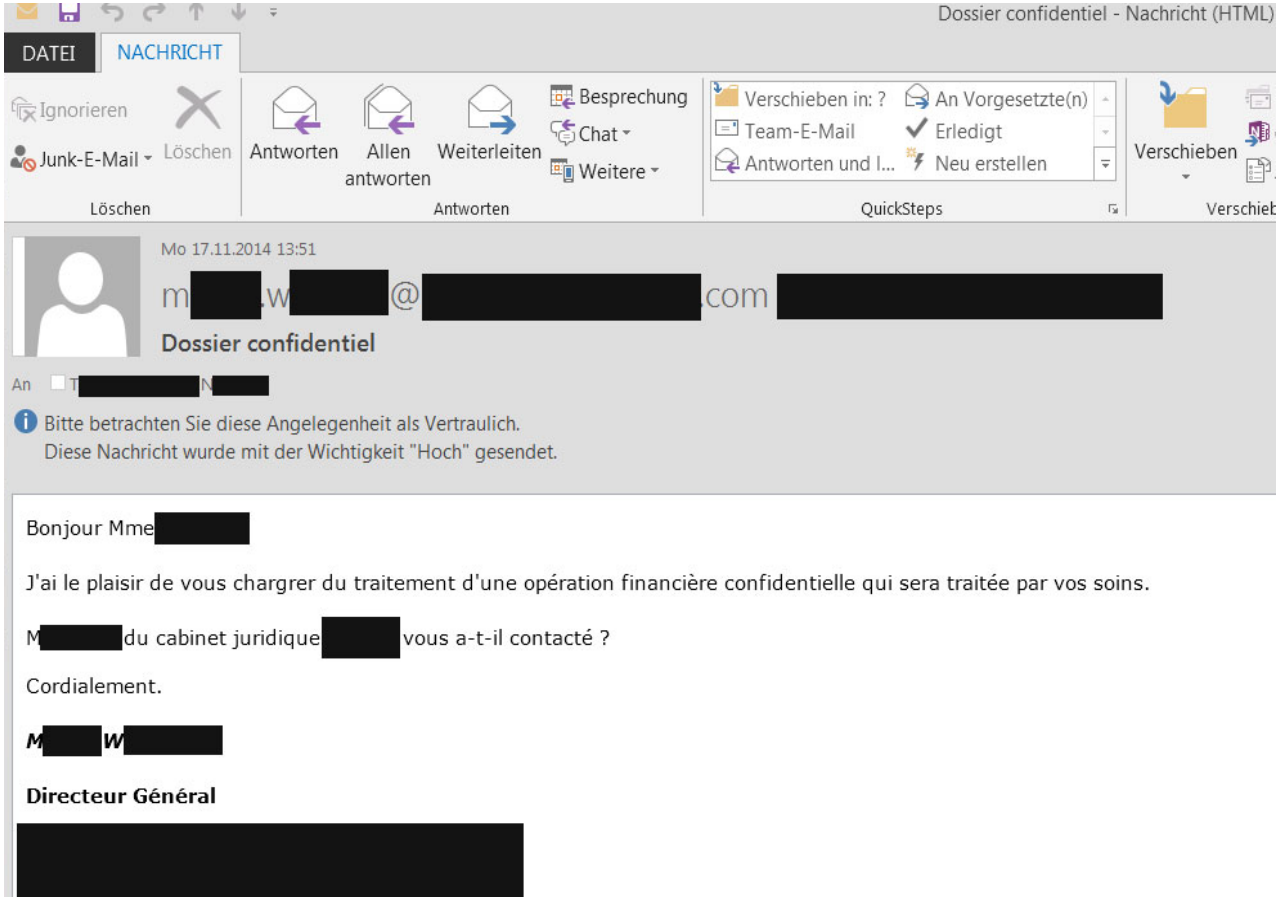
Nous avons temporairement arrêté l'activité en ligne de votre espace client. Nous réétudierons votre cas lorsque vous aurez fourni les informations demandées.

Phishing: General Recommendations

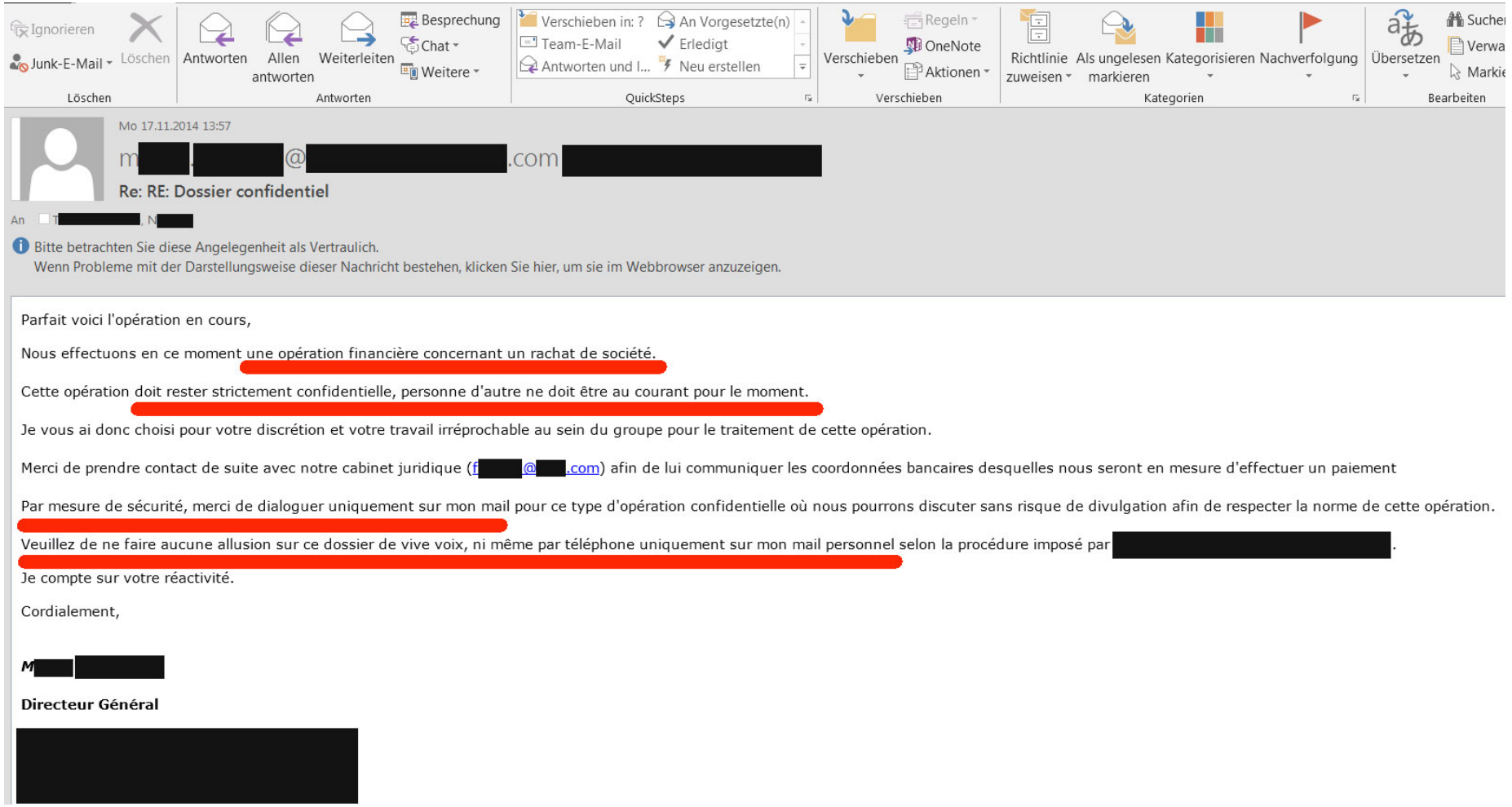
- No financial institution will ever ask you for your login information be it by email or phone
- Distrust emails that require (immediate) action on your behalf and/or threaten you of consequences
- Contact you financial institution if you believe you have revealed your login credentials
- You can announce phishing links at: **antiphishing.ch**

CEO Fraud

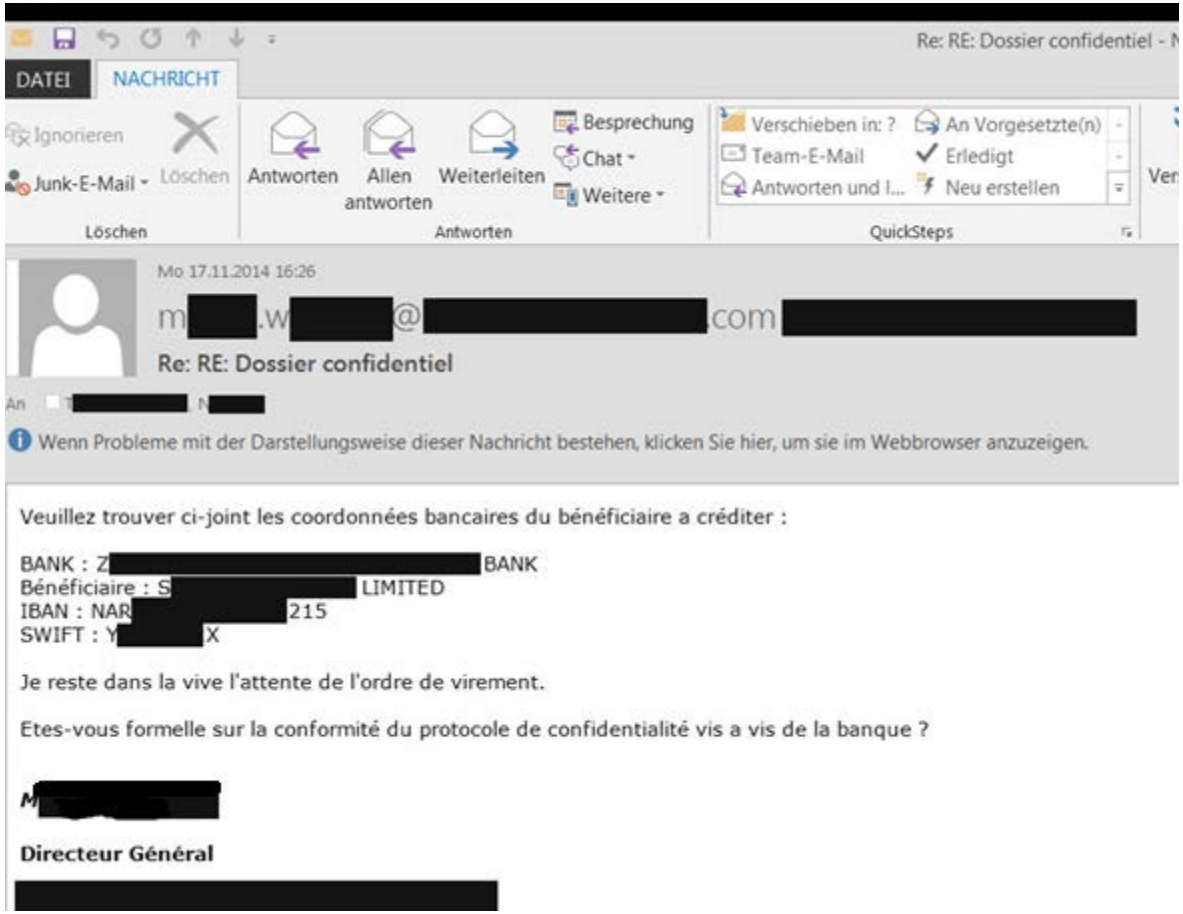
CEO Fraud: a potentially targeted attack



CEO Fraud (2)


Ignorieren
Junk-E-Mail
Löschen
Antworten
Allen antworten
Weiterleiten
Besprechung
Chat
Weitere
Löschen
Antworten
Verschieben in: ?
Team-E-Mail
Antworten und l...
An Vorgesetzte(n)
Erledigt
Neu erstellen
QuickSteps
Verschieben
Regeln
OneNote
Aktionen
Verschieben
Richtlinie zuweisen
Als ungelesen markieren
Kategorisieren
Nachverfolgung
Kategorien
Übersetzen
Suchen
Verwa
Markie
Bearbeiten
Mo 17.11.2014 13:57
m[redacted].com[redacted]
Re: RE: Dossier confidentiel
An T[redacted], N[redacted]
Bitte betrachten Sie diese Angelegenheit als Vertraulich.
Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.
Parfait voici l'opération en cours,
Nous effectuons en ce moment une opération financière concernant un rachat de société.
Cette opération doit rester strictement confidentielle, personne d'autre ne doit être au courant pour le moment.
Je vous ai donc choisi pour votre discrétion et votre travail irréprochable au sein du groupe pour le traitement de cette opération.
Merci de prendre contact de suite avec notre cabinet juridique (f[redacted]@[redacted].com) afin de lui communiquer les coordonnées bancaires desquelles nous seront en mesure d'effectuer un paiement
Par mesure de sécurité, merci de dialoguer uniquement sur mon mail pour ce type d'opération confidentielle où nous pourrons discuter sans risque de divulgation afin de respecter la norme de cette opération.
Veuillez de ne faire aucune allusion sur ce dossier de vive voix, ni même par téléphone uniquement sur mon mail personnel selon la procédure imposé par [redacted].
Je compte sur votre réactivité.
Cordialement,
M[redacted]
Directeur Général
[redacted]

CEO Fraud (3)


Re: RE: Dossier confidentiel - N
DATEI
NACHRICHT
Ignorieren
Junk-E-Mail
Löschen
Antworten
Allen antworten
Weiterleiten
Besprechung
Chat
Weitere
Löschen
Antworten
Verschieben in: ?
Team-E-Mail
Antworten und l...
An Vorgesetzte(n)
Erledigt
Neu erstellen
QuickSteps
Mo 17.11.2014 16:26
m[redacted].w[redacted]@[redacted]com[redacted]
Re: RE: Dossier confidentiel
An T[redacted] N[redacted]
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]
Directeur Général
[redacted]

CEO Fraud: General recommendations

- Reduce the exposition of your organisational processes
- Have clearly defined processes for payments and acquisitions
- Require a four-eye principle with a collective signature
- Facilitate internal communication
- Raise awareness with your collaborators
- If you can, ask your financial institution to whitelist your payment destinations

E-banking Trojans

How are the attacks carried out?

- The main target is almost always a user inside a company
  - Often by means of an email resembling a phishing mail
  - From a company that we tend to trust et with whom we potentially have a relation (Apple, Paypal, CFF/SBB, Swisscom, Post, etc).
  - That requires one or more actions on behalf of the user
  - The infection vector is often a document with Macros enabled or by a link to a malicious site

2017 Dridex Campaign

Von: Swisscom [mailto:sme.contactcenter@bill.swisscom.com]
Gesendet: Mittwoch, 15. Februar 2017 12:31
An:
Betreff: Rechnungskopie

swisscom

Sehr geehrte Kundin, sehr geehrter Kunde
Vielen Dank fur Ihren Auftrag.
Hiermit erhalten Sie die gewunschten Unterlagen.

CHF 863.43 (zahlbar bis 24.01.2017) Rechnung einsehen >

Betroffene Rechnung(en): Januar 2017

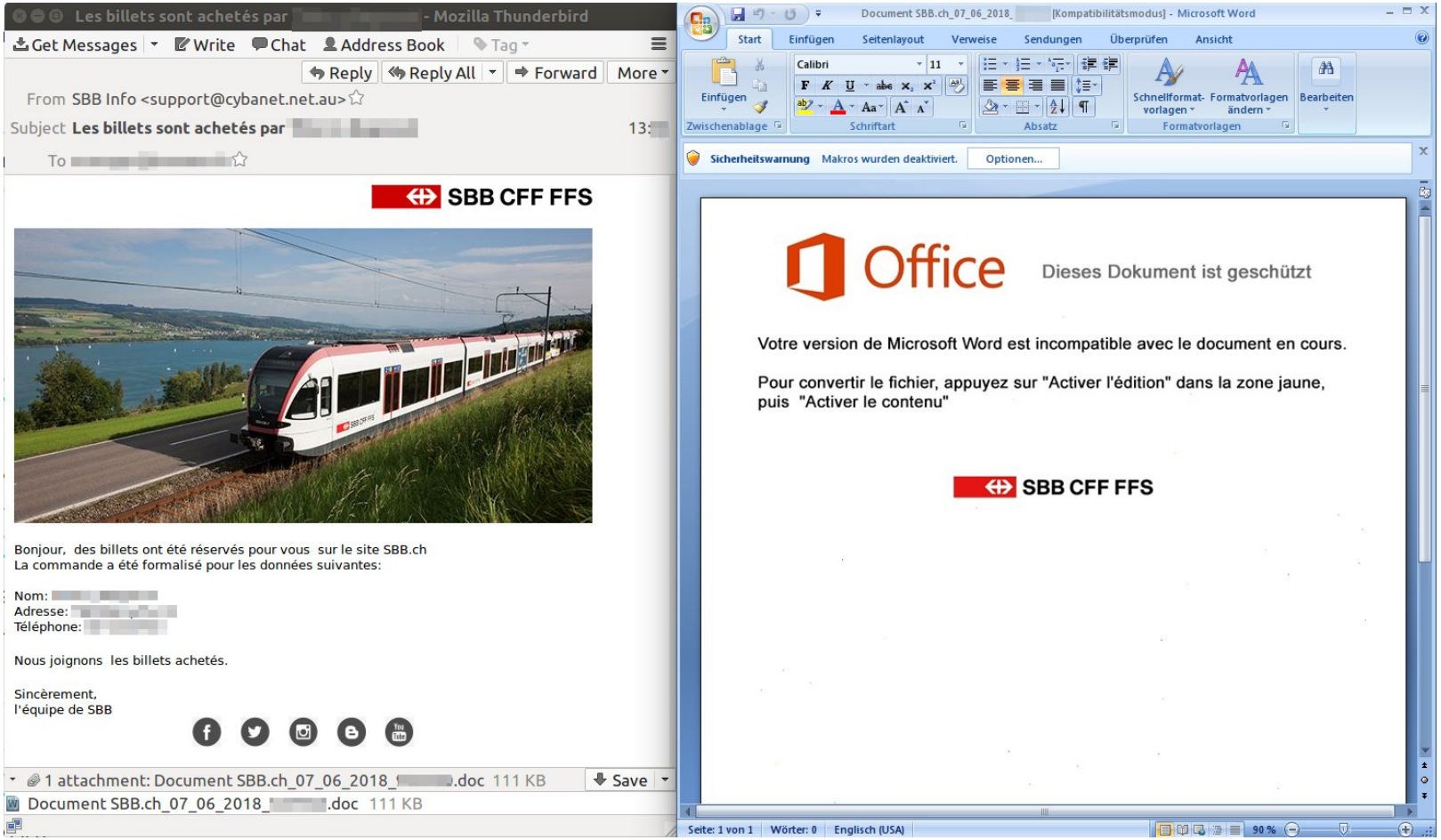
Alles Wissenswerte rund um das Thema Rechnung, Verbindungen & aktuelle Kosten finden Sie in Ihrem personlichen Kundencenter.

Angaben zur papierlosen Bezahlung

Post-Konto:	01-38395-9
Zugunsten von:	Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern
Referenznummer:	788608635814519370390643231
Codierzeile:	0100000549394>788608635814519370390643231+ 010218415>

Falls Sie Ihre Zahlung aus dem **Ausland** tatigen, verwenden Sie bitte folgende Uberweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A.
Ziehen Sie um oder mochten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter konnen Sie Ihre Angaben online anpassen.
Mochten Sie Ihre Rechnung **unkompliziert bezahlen**? Dann registrieren Sie sich fur die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Haben Sie **Fragen** zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer Webseite.
Freundliche Grusse
Ihr Swisscom Team

2018 Retefe


Les billets sont achetés par - Mozilla Thunderbird
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More
From SBB Info <support@cybanet.net.au>
Subject Les billets sont achetés par
To
SBB CFF FFS
Bonjour, des billets ont été réservés pour vous sur le site SBB.ch
La commande a été formalisé pour les données suivantes:
Nom:
Adresse:
Téléphone:
Nous joignons les billets achetés.
Sincèrement,
l'équipe de SBB
1 attachment: Document SBB.ch_07_06_2018_.doc 111 KB
Save
Document SBB.ch_07_06_2018_.doc 111 KB
Document SBB.ch_07_06_2018_ [Kompatibilitätsmodus] - Microsoft Word
Start
Einfügen
Seitenlayout
Verweise
Sendungen
Überprüfen
Ansicht
Sicherheitswarnung
Makros wurden deaktiviert.
Optionen...
Office
Dieses Dokument ist geschützt
Votre version de Microsoft Word est incompatible avec le document en cours.
Pour convertir le fichier, appuyez sur "Activer l'édition" dans la zone jaune, puis "Activer le contenu"
SBB CFF FFS
Seite: 1 von 1
Wörter: 0
Englisch (USA)

E-Banking Trojans in PMEs

Recommendations:

- Use a dedicated Workstation for payments (i.e. don't use it for internet browsing)
- Put the machine on a segmented network if you're doing NSM
- Keep the machine up-to-date

Final Recommendations

- Information security requires an effort by all and a balanced approach between **technical and human aspects**.

- It's not a question of *if* rather of *when* you will get infected.
  - Define your critical processes, or crown jewels and assess their risk
  - Define reaction processes
  - Communicate internally even if mistakes were made

  - The information security risks must be managed by the board (direction)

And if you're "hit"

- Take the appropriate measures to avoid the fraudulent payment(s) of being made (follow the predefined process)
- Announce the incident at MELANI
- File a complaint at the cantonal police.

Thank you for your attention

For more information, consult:

www.melani.admin.ch

David Rüfenacht
Analyst
Reporting and Analysis Centre for Information Assurance Switzerland MELANI