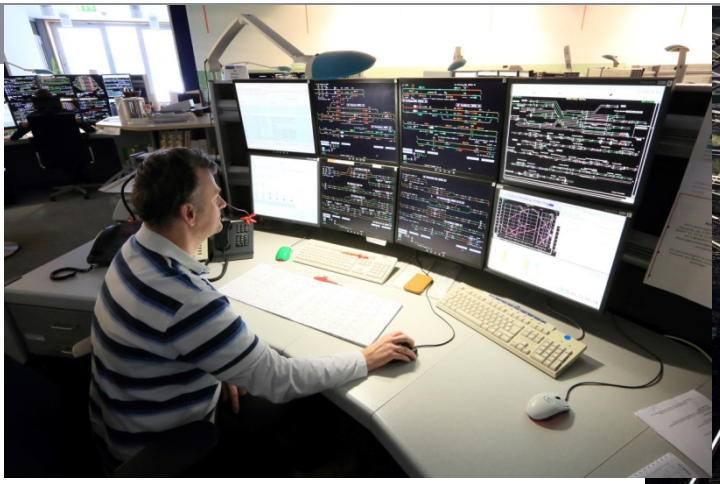
UIC Digital Technology and Railway Security Workshop

Washington 4-5 May 2016



THREATS AND CONSTRAINTS

CRIME SCENE CYBERSPACE AT DB GROUP

With its nine business units DB is active in all segments of the transport market

DB BAHN

Passenger Transport:
Domestic and European-wide mobility services

- **DB Bahn Long Distance**
  Long-distance rail pass. transport[1]
- **DB Bahn Regio**
  Regional/urban pass. transport (GER)
- **DB Arriva**
  Regional/urban pass. transport (EU)[2]

DB SCHENKER

Transportation and Logistics:
Intelligent logistics services via land, air and the sea

- **DB Schenker Rail**
  European rail freight transport
- **DB Schenker Logistics**
  Global logistics services

DB NETZE

Infrastructure:
Efficient and future-oriented rail infrastructure in Germany

- **DB Netze Track**
  Rail network
- **DB Netze Stations**
  Traffic stations
- **DB Netze Energy**
  Traction current

DB Services[3]
Integrated range of services

1 Within Germany as well as cross border traffic; 2 In UK with Arriva-affiliate 'CrossCountry' also long-distance passenger transport;
3 Business unit is assigned to the Infrastructure and Services division

DB is the second biggest provider in the entire European passenger transport market

- **2.7**
  billion passengers per year in trains and buses
- **25,000**
  passenger trains per day
- **260**
  trains are included in ICE fleet of DB
- **9**
  neighboring countries can be reached directly via DB

DB BAHN

DB Bahn Long Distance

DB Bahn Regional

DB Arriva

DB Bahn Sales[1]

Figures on the left side are rounded and exclude Arriva; 1 DB Bahn Sales is a service center within the passenger transport division

DB is the second biggest worldwide provider of transport and logistics services

- **2,000**
  locations in over 140 countries
- **5,000**
  freight trains with more than 1 million tonnes per day through Germany/Europe
- **99**
  million shipments sent per year via European land transport
- **7**
  million square meters of storage space around the world

DB SCHENKER

DB Schenker Rail

DB Schenker Logistics

As of December 31, 2014; Figures are rounded

DB operates the biggest rail network in the heart of Europe

- **5,700**
  train stations serve as railway gateways in Germany
- **33,300**
  km long rail network – three times as long as the German Autobahn network
- **25,000**
  bridges of DB make its way through rivers and valleys
- **5th**
  largest provider of energy in Germany – annual volume of available energy equal to energy consumed by Berlin metropolitan area

DB NETZE

DB Netze Track

DB Netze Stations

DB Netze Energy

DB Netze Projects[1]

As of December 31, 2014; Figures are rounded; 1 DB Netze Projects is a service center within the infrastructure division

What is Cybercrime?

Cybercrime

Cybercrime

Any illegal activity that uses a computer as its primary means of commission.

The U.S. Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence.

Cybercrime – Importance for the DB Group

Mobility Networks Logistics

Phishing

Online-Fraud

Social Engineering

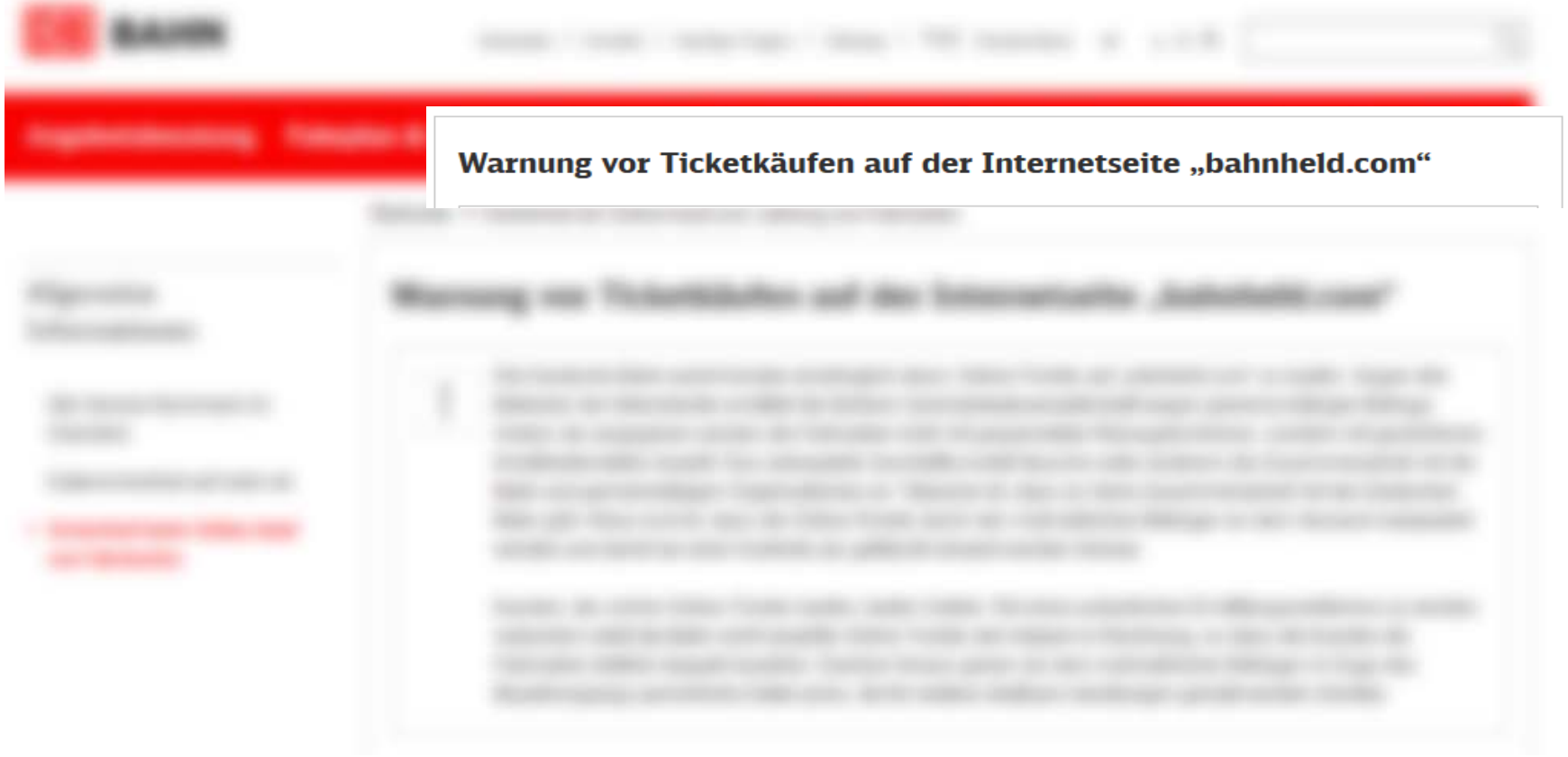
DDos-Attacs

Cybercrime – Importance for the DB Group

Online-Fraud

Cybercrime – Online-Fraud (externally)

- The website „bahnheld.com“ was offering tickets illegally. The tickets had been fraudulently acquired



Warning on DB website

Cybercrime – Importance for the DB Group

DDos-Attacks

DDos-Attack

- Famos crime scene: Ddos-Attack on German parliament network

SPIEGEL ONLINE
15. Mai 2015, 15:28 Uhr

Sicherheitsalarm im Parlament

Cyberangriff auf den Bundestag

Von Maik Baumgärtner, Sven Röbel und Jörg Schindler

Der Bundestag ist nach SPIEGEL-ONLINE-Informationen Ziel eines Cyberangriffs geworden. Unbekannte haben versucht, ins interne Datennetz des Parlaments einzudringen.

Bislang unbekannte Täter haben nach Informationen von SPIEGEL ONLINE das interne Datennetz des Deutschen Bundestags attackiert. Wie Bundestagssprecher Ernst Hebeker am Freitag auf Anfrage bestätigte, seien "die IT-Systeme des Bundestags" Ziel eines elektronischen Angriffs geworden. Hebeker zufolge arbeiteten Experten der Bundestagsverwaltung und des Bundesamts für Sicherheit in der Informationstechnik (BSI) derzeit an der Analyse und Behebung des Problems.

Nach SPIEGEL-ONLINE-Informationen war IT-Spezialisten des Parlaments bereits vor mehreren Tagen aufgefallen, dass Unbekannte versuchten, ins interne Datennetz des Bundestags einzudringen. Offenbar wollten sich die Hacker Zugriff auf Informationen aus dem Computersystem verschaffen. Nahezu zeitgleich bemerkten auch Experten des Verfassungsschutzes im Cyberabwehrzentrum des Bundes den Spähversuch und warnten die Bundestagsverwaltung.

Inwiefern auch Datenspeicher mit hochsensiblen Informationen - etwa von Regierungsmitgliedern - von dem Angriff betroffen sind, war zunächst unklar. Bereits am Freitagvormittag hatten die IT-Abteilungen mehrerer Bundestagsfraktionen ihre Abgeordneten und Mitarbeiter über den "Sicherheitsvorfall" im Datennetz des Parlaments in Kenntnis gesetzt. Sicherheitshalber seien Teile des Bundestagssystems zeitweise heruntergefahren worden. Darunter fallen offenbar auch Laufwerke des Parlamentarischen Untersuchungsausschusses zur Aufklärung der BND/NSA -Spionageaffäre.

Nach Informationen von SPIEGEL ONLINE wird der Vorfall von Spezialisten als schwerwiegend bezeichnet, auch Mitarbeiter des BSI seien vor Ort. Über die Urheber des Cyberangriffs lagen zunächst keine Erkenntnisse vor.

URL:

http://www.spiegel.de/netzwelt/netzpolitik/cyber-angriff-auf-den-deutschen-bundestag-a-1033984.html

Cybercrime – Importance for the DB Group

Phishing

Phishing - Example

Faked Email-adress

Von: Katja Ebering <katja.ebering.deutsc[redacted]@outlook.com>
An: "Klaus.Kemme@deutschebahn.com[redacted]aus.kemme@deutschebahn.com>
Datum: 09.05.2014 11:18
Betreff: Bitte um Ihre Unterlagen/Information

Hallo Herr Kemme,

im Auftrag von Frau D[redacted]el, Leiterin Entgeltabrechnung & HR-Services, bin ich dabei, relevante Daten unserer Mitarbeiter/innen nach zu prüfen.

Hintergrund ist folgender: Nach dem Upgrade der Konzern HR-Systeme haben wir festgestellt, dass manche Mitarbeiterdaten in der Datenbank inkonsistent sind. Wir sind nicht sicher, ob Ihre bisherige Daten noch aktuell sind. Daher möchte ich Sie bitten, Ihre aktuelle Informationen bis zum nächsten Montag, den 12ten mir zukommen zu lassen. Ich werde dies dann an die entsprechende Stelle leiten, damit Ihre Daten rechtzeitig überprüft und aktualisiert werden:

-Fotokopie Ihres Personalausweises oder Reisepasses
-Ihr Aktuelles Gehaltskonto u.a. Bankverbindung

Asking for ID-copy/bank account details

Vielen Dank und viele Grüsse!

Katja Ebering
HR C&B and Services
HR Hauptverwaltung Berlin

Deutsche Bahn AG
Potsdamer Platz 2, 10785 Berlin
Tel. 030 3017-4678, intern 9481-4678, Fax 030 297-57894
Mobil: 0160 90114025

Phishing – Prevention

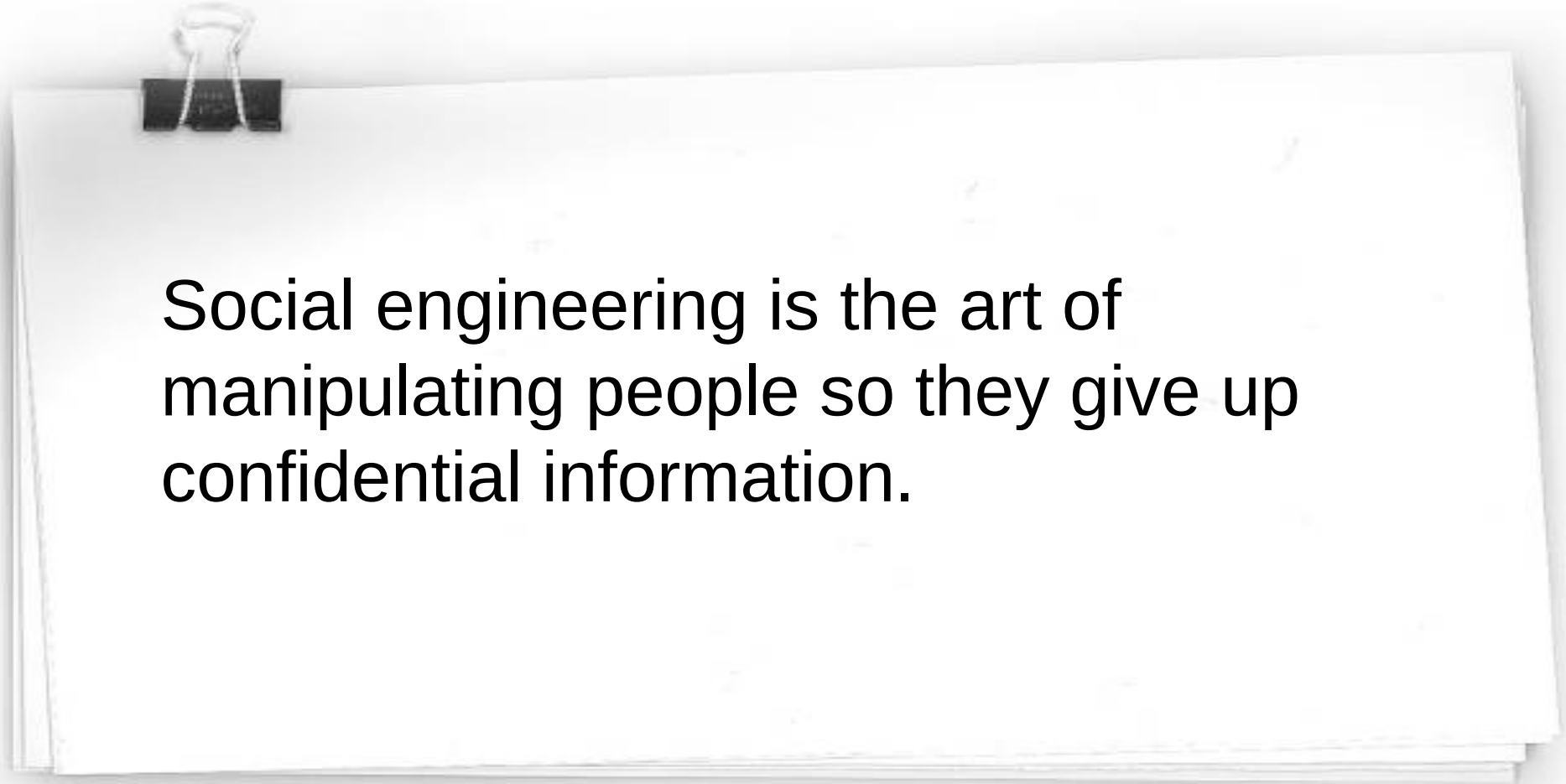
Sensitization concerning

- Grammar-misstakes
- Personal form of addressing is missing („Dear User“)
- Request for personal data (PIN, TAN, …)
- Request to follow a link

Cybercrime – Importance for the DB Group

Social Engineering

Social Engineering – Definition



Social engineering is the art of manipulating people so they give up confidential information.

Social Engineering – Examples

Corporate Security Alert June, 24th 2014

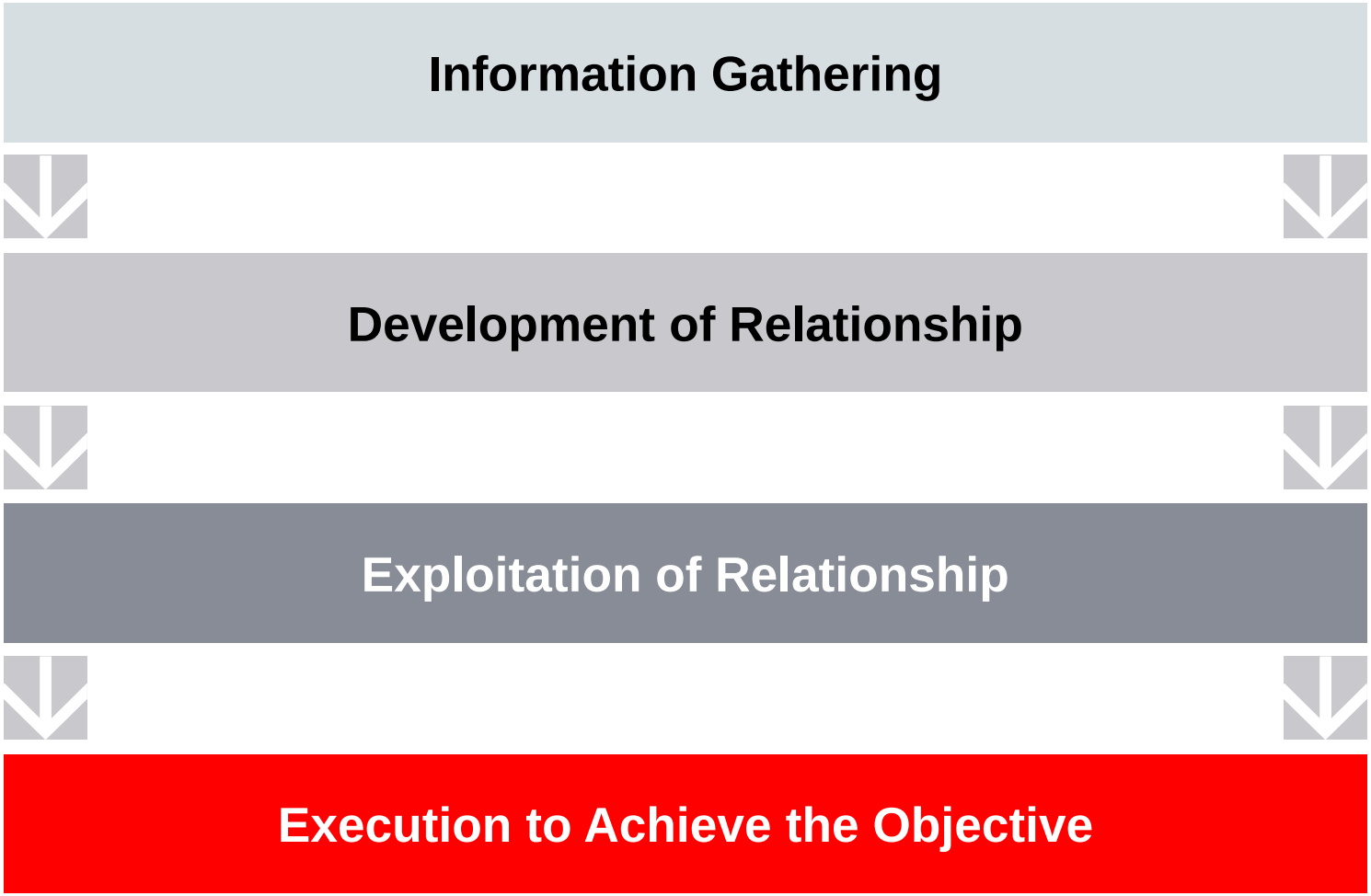
- The Israeli fraudsters impersonate a trusted partner of the company. They contact employees (useful to achieve their imposture) to gather any kind of information.
- The contact may be established by phone calls (imitating the voice) or emails (imitating the email address).
- Using all gathered information the fraudster impersonates a group executive (e.g. CEO, CFO) and contacts a specific employee to set up a urgent, but secret transaction.
- The requested money shall be transfered to foreign accounts in China oder other (European) countries; finally the money will be tranfered to Israel.

Social Engineering – Examples

- A unknown person impersonating a DB Group employee tries to gather invoice documents from the construction company Max Bögl. Therefore the fraudster contacts a Max Bögl employee telling him about a supposed data crash at DB Group and a loss of all open invoice documents. The fraudster appoints a fax number.

- DB Group employees got an E-Mail from a supposed HR-employee. They were asked about their bank account information and a copy of their ID-documents.

Social Engineering - Mechanism



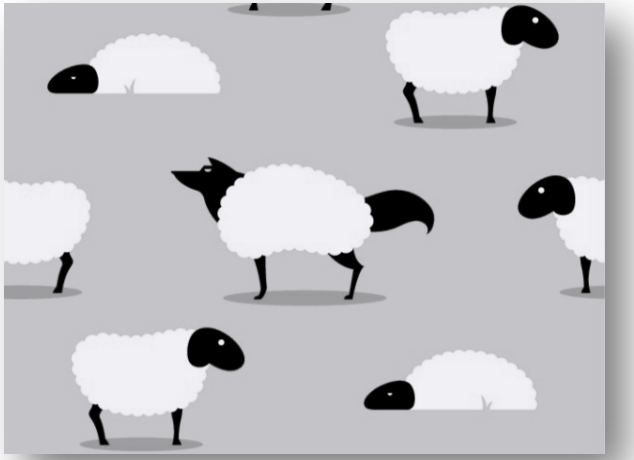
Social Engineering – „How to be convincing“

The fraudster will use a combination of the following elements:

- **Use of authority**:
  “It is an order to do this”
- **Secrecy:**
  “This project is still secret and its success depends on this transaction”
- **Valorization:**
  “I count on you for your efficiency and discretion”
- **Pressure:**
  “The success of the project rests on your shoulders”

Social Engineering – Prevention

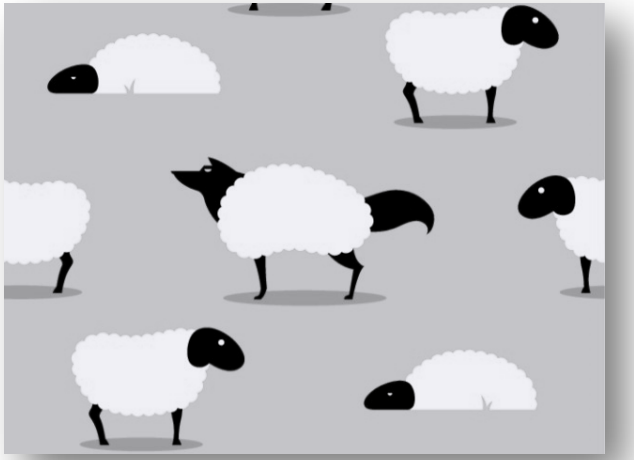
„Don’t become a victim“



- **Slow down.** Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
- **Research the facts.** Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company’s site, or a phone directory to find their phone number.

Social Engineering – Prevention

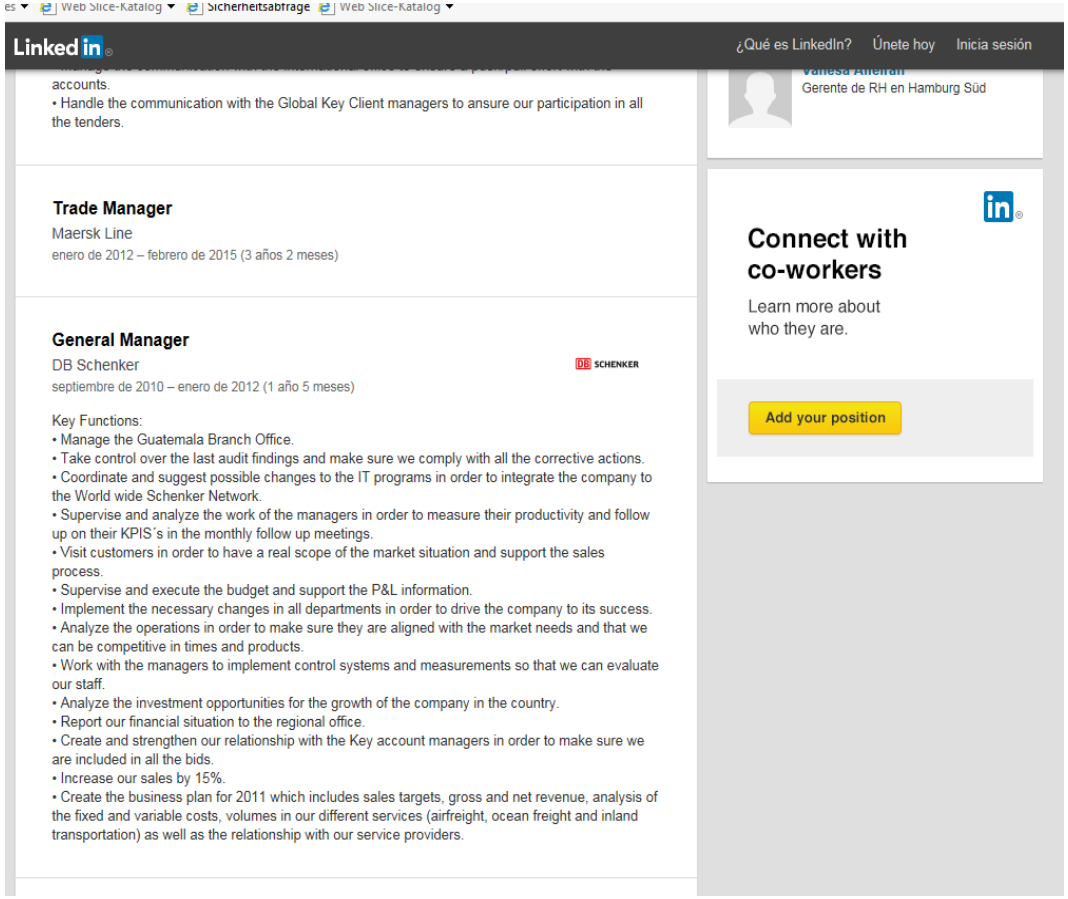
„Don’t become a victim“



- **Delete any request for financial information or passwords.** If you get asked to reply to a message with personal information, it’s a scam.
- **Beware of any download.** If you don’t know the sender personally AND expect a file from them, downloading anything is a mistake
- **Be aware**. No transaction is too secret that nobody is talking about it (4-eyes-principle.

Social Engineering – Prevention

Social media



- **Beware of publishing internal data/information**

Open linked-in-profile former Schenker-employee

Defense of cyber attacks

Actual Activities:

Cloud-Policy

Implementation of IT-Security-Law

Cyber Defense measures

Thank you for your attention