ZKI Frühjahrstagung 2016

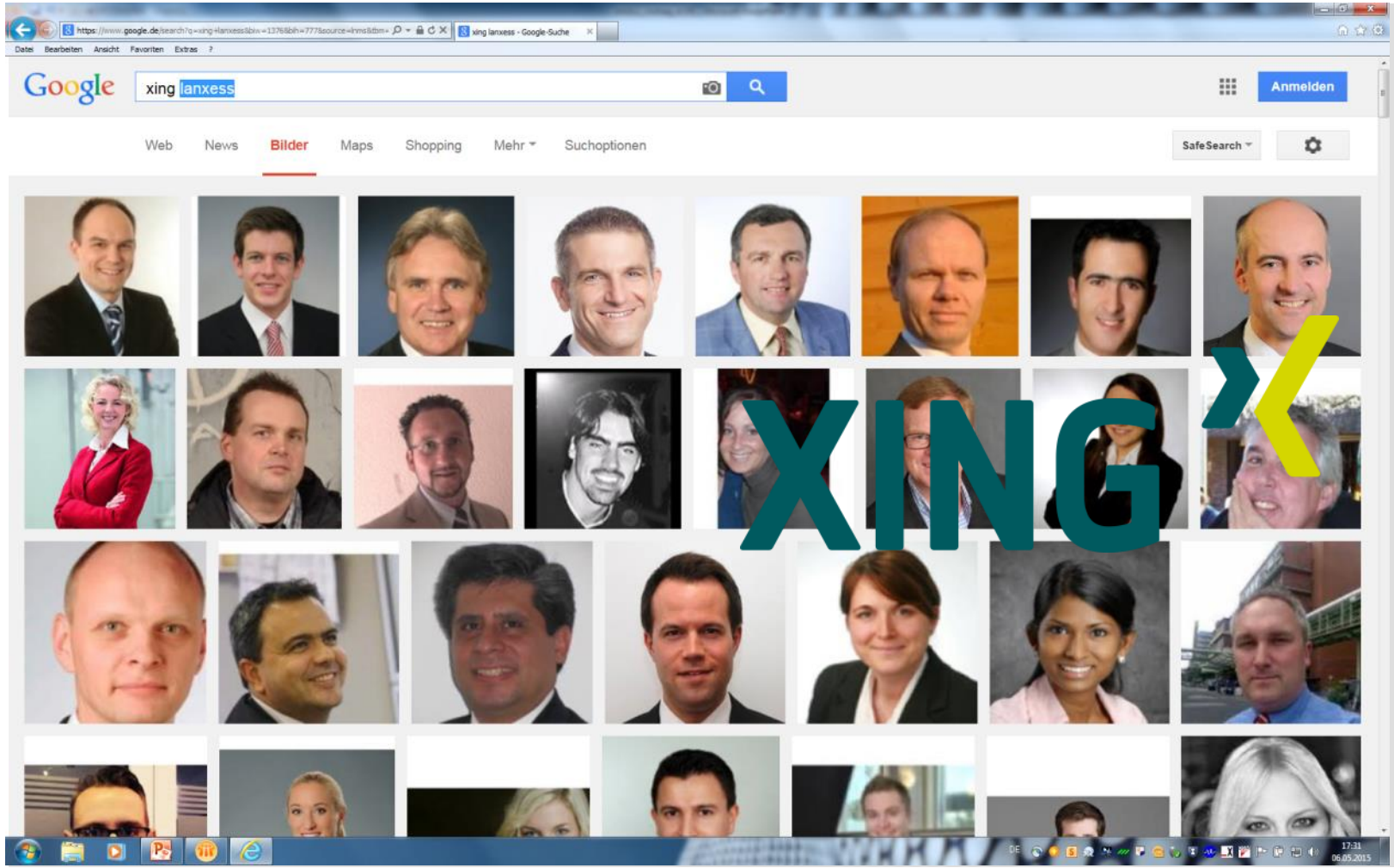
Der Feind in deinem Netz
Oder: Warum wir die Probleme mit der IT nicht mit der IT lösen können!

Dirk Fleischer (M.A.),
Frankfurt (Oder), 08. März 2016

LANXESS
Energizing Chemistry

Es war einmal……

Spear-Phishing



- Ca. 250 namentlich angeschriebene Mitarbeiter(innen)
- 25 Mitarbeiter(innen) reagierten.
- Alle erwähnten Personen sind im Unternehmen tatsächlich präsent.
- Mind. -2- weitere DAX Konzerne wurden mit dem gleichen Modus angegriffen.
- **Und wie kam man auf LXS?**

LANXESS

CEO Fraud

Dear Mrs O'Connor,

As explained by Mr Pontzen ,Lanxess about to close an acquisition very soon.
We decided to request your financial help for the acquisition will stay undisclosed.
The target company is in Hungary.
Will you be able to proceed to a transfer of seven hundred and eighty thousand Euros (780 000 Euros) today?
Let me know so that I can send you the bank details of the company.

Kind Regards,

Liza Kalmann
+41.22.548.34.90

On 5/11/2015 4:19 PM, kim.oconnor@lanxess.com wrote:

I have been referred to you by our global CFO , Michael Pontzen . I understand as a step in this process we will need to acquire locally in the UK the bank details of the target company .

I would be much obliged to you if you could forward same .

Rollenverteilung bei organisierten IT Angriffen (v.a. Fraud)

- **Coders or programmers** write the malware, exploits, and other tools necessary to commit the crime.
- **Distributors or vendors** trade and sell stolen data, and vouch for the goods provided by the other specialties.
- **Technicians** maintain the criminal infrastructure and supporting technologies, such as servers, ISPs, and encryption.
- **Hackers** search for and exploit vulnerabilities in applications, systems, and networks in order to gain administrator or payroll access.
- **Fraud specialists** develop and employ social engineering schemes, including phishing, spamming, and domain squatting.
- **Hosts** provide “safe” facilities of illicit content servers and sites, often through elaborate botnet and proxy networks.
- **Cashers** control drop accounts and provide those names and accounts to other criminals for a fee; they also typically manage individual cash couriers, or “money mules.”
- **Money mules** transfer the proceeds of frauds which they have committed to a third party for further transfer to a secure location.
- **Tellers** assist in transferring and laundering illicit proceeds through digital currency services and between different national currencies.
- **Executives of the organization** select the targets, and recruit and assign members to the above tasks, in addition to managing the distribution of criminal proceeds.

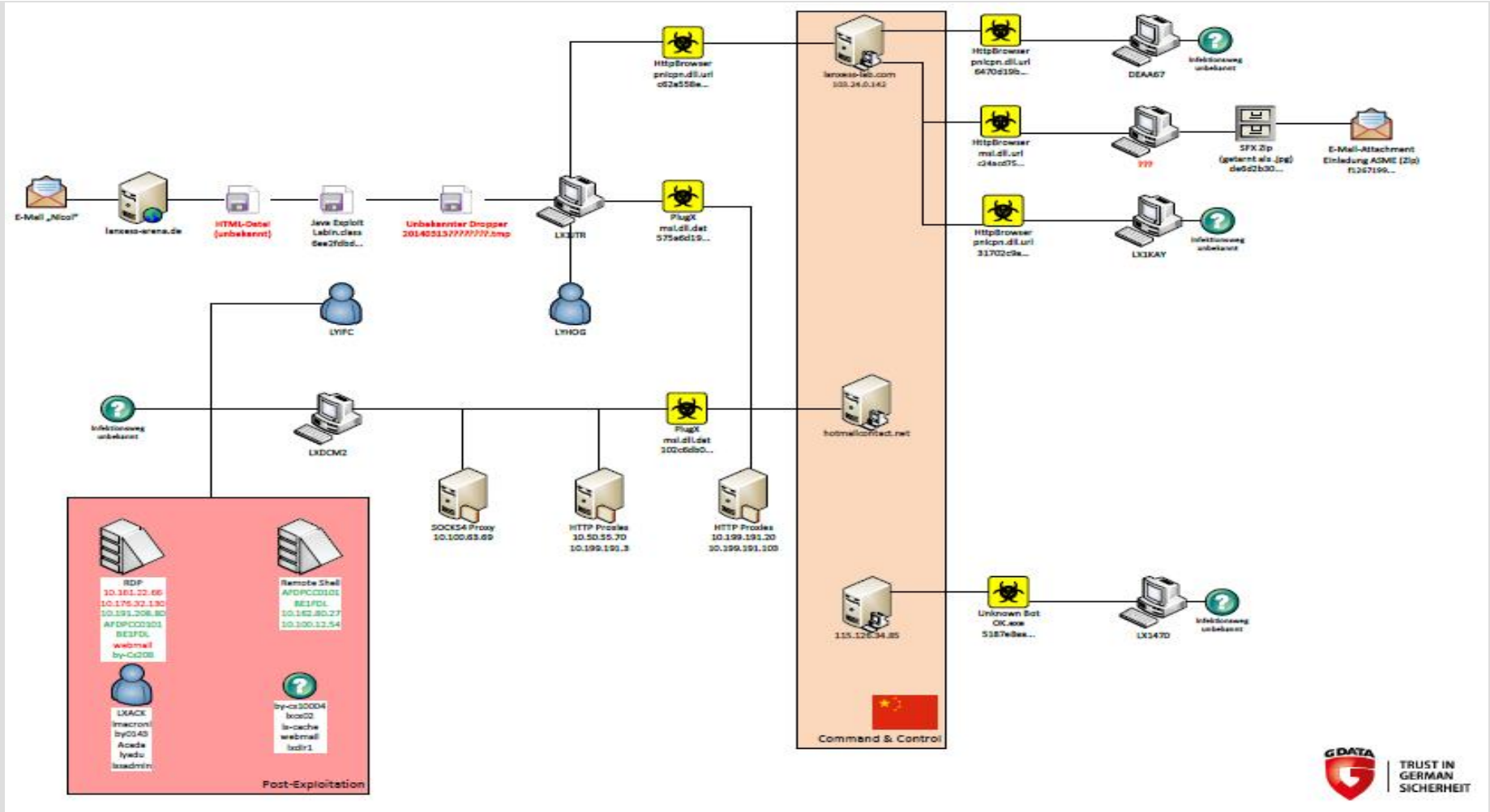
LANXESS

Waterhole Plot und Joint Venture Szenario

Modul	Funktionalität
DISK	Suche von Dateien, Beliebige Manipulationen im Dateisystem (inkl. Ausleitung sowie Upload von Dateien)
KeyLogger	Keylogger
Nethood	Netzwerkverbindungen anzeigen
Netstat	Laufende TCP- und UDP-Verbindungen anzeigen und beenden
Option	Host sperren/herunterfahren/rebooten
PortMap	Port-Mappings durchführen
Process	Prozesse auflisten, erstellen und beenden
Regedit	Beliebige Manipulationen in der Registry
Screen	Screenshots und Videos erstellen
Service	Beliebige Manipulationen installierter Dienste
Shell	Remote-Shell öffnen
SQL	Mit SQL-DB verbinden und dort Befehl ausführen
Telnet	Telnet-Server öffnen

LANXESS

Visualisierung der bekannten Angriffsvektoren



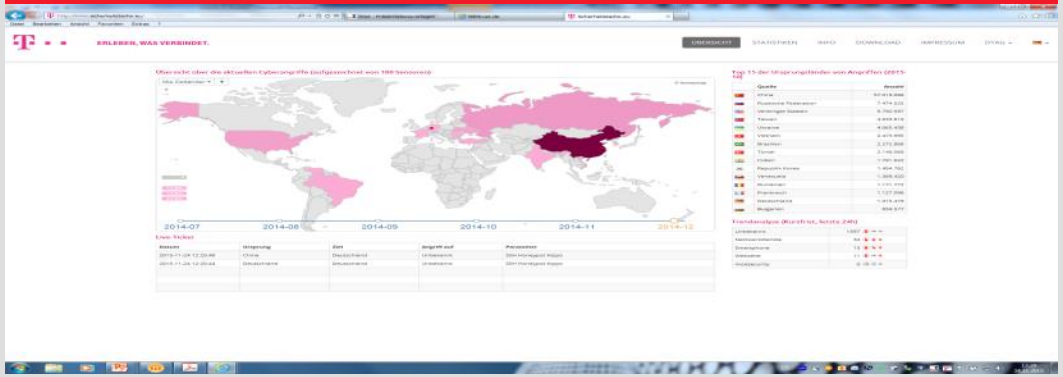
Unterschiedliche Delikte bedingen unterschiedlicher Erklärungsansätze

Routine Activity Theory nach Cohen/Felson

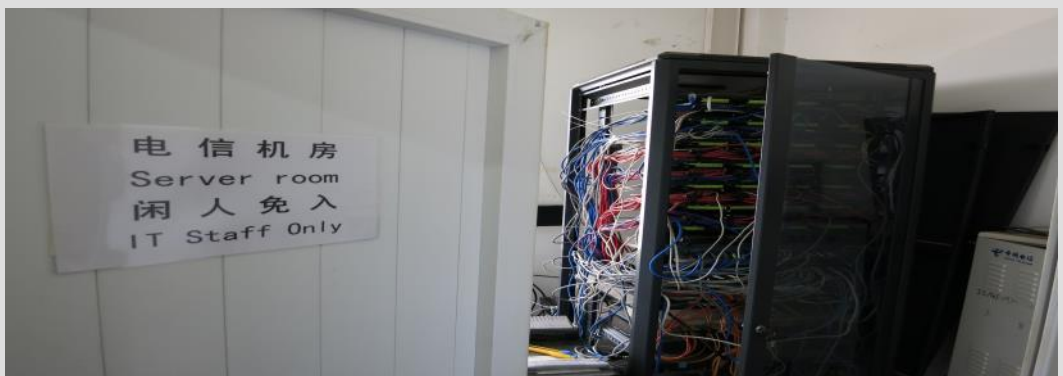
LANXESS

Die Potentiale der IT Risiken ergeben sich aus unterschiedlichen Quellen und Ursachen

Threats



Controls



Vulnerabilities

Ergebniszwischenbericht
Erweiterte Sicherheitsanalyse (Pentest)
30.07.2014

Lanxess

Consequences

Einige Kernthesen

Einige wenige Schlüsselprobleme, die es für die Unternehmen, im Rahmen der Lagebewältigung zu lösen gilt.

Herausforderungen

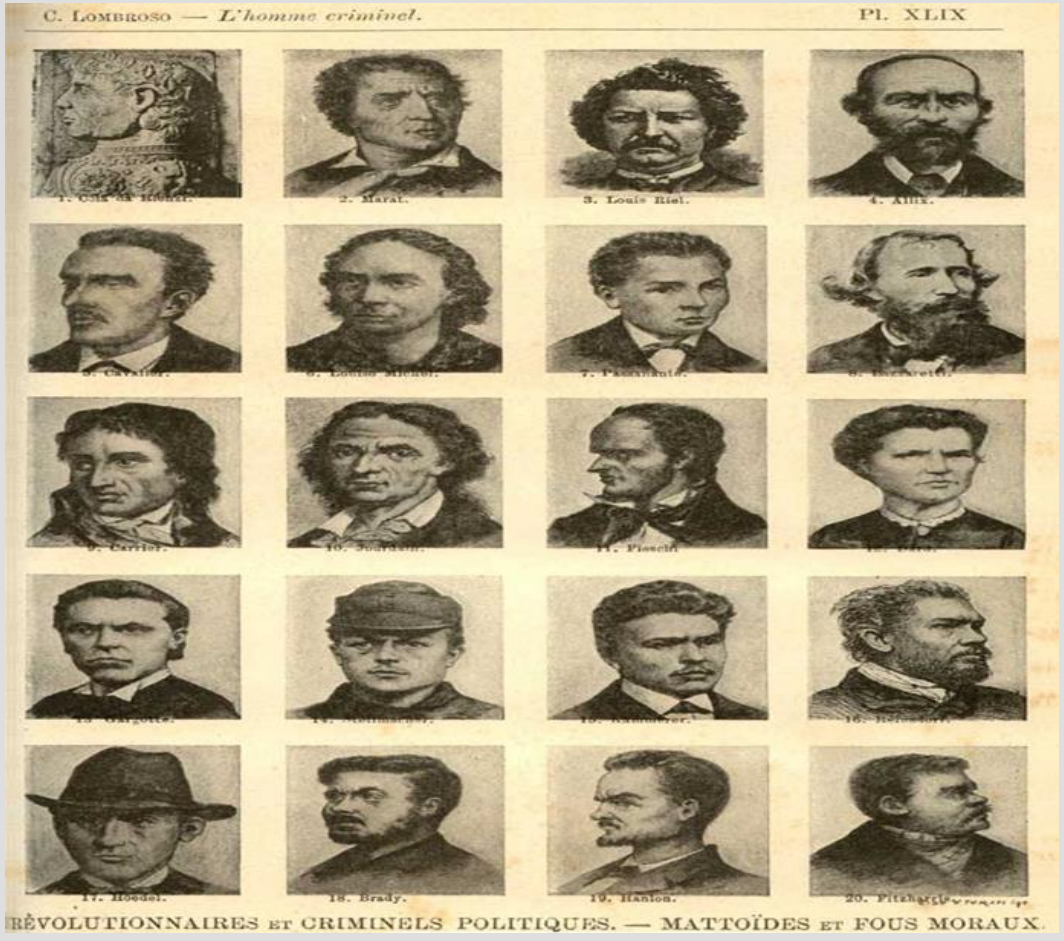
- **Wann weiß das Unternehmen wann, wo und mit welchen Methoden es angegriffen wurde?**
  - **Die Potenz und Zielstrebigkeit der Angreifer** vs. der Verfügbarkeit von Experten.
  - Die fortwährende **Mutation der eingesetzten Angriffsmittel** (Viren, Trojaner etc.)
  - Der gigantische **Rechercheaufwand, um weitere Angriffsvektoren zu schließen**.
  - Insgesamt eine **hoch dynamische Sicherheitslage**.
- **Der Sachverhalt findet in einem vitalen und komplexen Netzwerk bei laufendem Betrieb statt.**
  - **Gewachsene IT Infrastrukturen** in global agierenden Konzernen und Unternehmen.
  - **Fremdbestimmung der Unternehmen** durch Hard- und Softwarehersteller.
  - Eine unüberschaubare **Fragmentierung von internen und externen Kommunikationsschnittstellen**, die bedacht werden müssen.
- **Auf ein IT Problem kann man nicht nur mit neuer und „besserer“ IT reagieren**, wenn das **unternehmerische Mindset** nicht auf allen Ebenen das notwendige Risikobewusstsein und die Handlungskompetenzen entwickelt.

LANXESS

Es gibt keine kriminellen Computer

Lessons learned …

- **Hinter jedem IT Angriff steckt ein Mensch!**
- Jeder **IT Angriff** wird durch die **Nachlässigkeit der Anwender** unterstützt, voraussichtlich sogar **ermöglicht!**
- **Die IT versucht IT Probleme mit IT zu lösen.**
- **Welche Motivation sollte eine IT Abteilung haben die eigenen Defizite mitzuteilen?**
- **Wer ist** für die Sicherheit im Konzern **verantwortlich?**
- Ob ein **Reputationsschaden bilanzierbar** entsteht, ist bisher **wissenschaftlich nicht nachgewiesen** worden**.**



Cybercrime ist klassische Kriminalität mit neuem modus operandi

Lessons learned …

- **Innentäter** als phänomenologische Besonderheit
- Keine kompetierenden, sondern **kooperierende Sicherheitsabteilungen**.
- Komplexe Erfahrungen verlangen oftmals **externe Expertise**…..auch **staatlicher** Expertise!
- Vor allem für **interne Ermittler** ergibt sich das Problem der Ansehensschädigung („*Schnüffler*“)
- **Ermittlungskompetenzen und –befugnisse** werden weiterhin **streitig** diskutiert. („*Keine StPO für Unternehmen*“); auch **BDSG**
- „*Jeder ungeregelte Zustand wird grundsätzlich zu Lasten des Unternehmens ausgelegt*.“

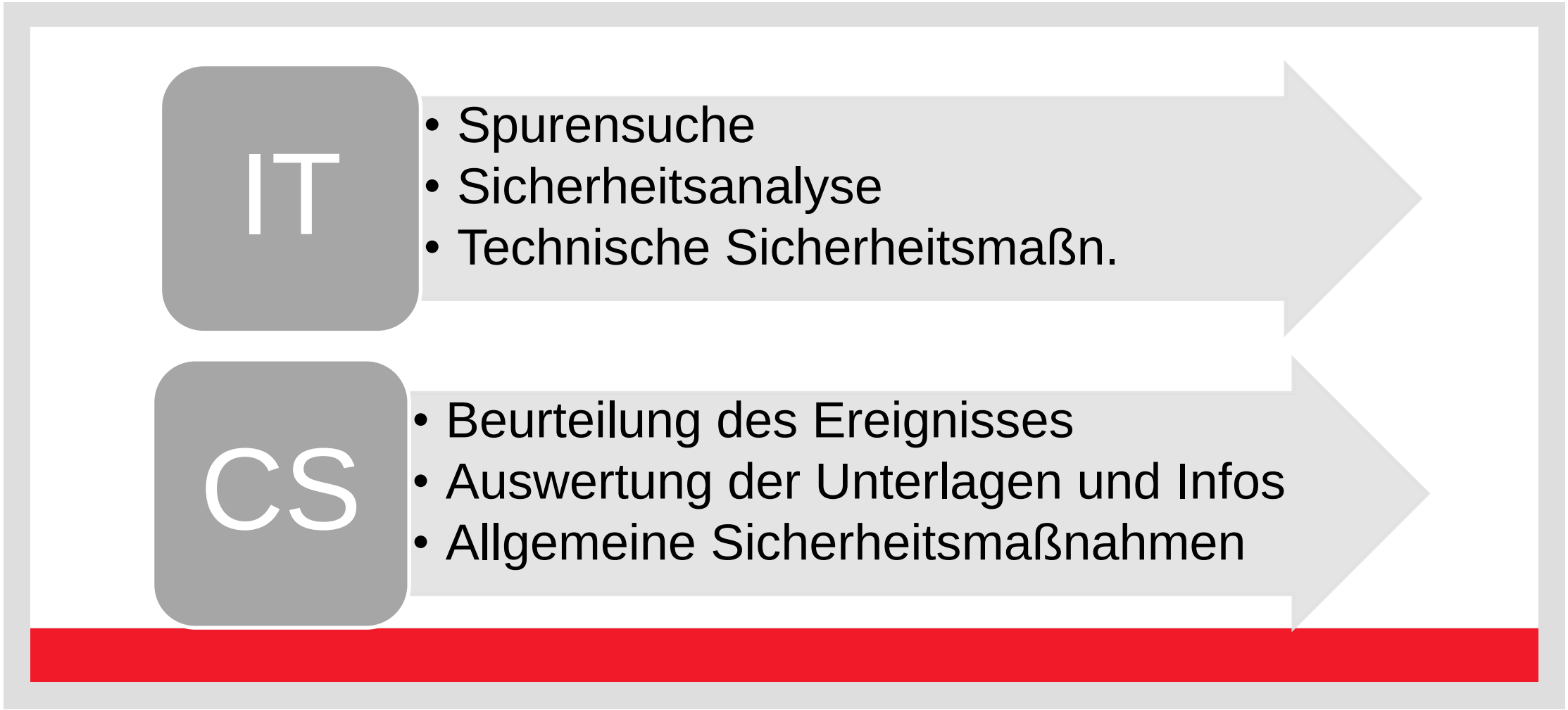
Egal ob Industriespionage oder Konkurrenzausspähung….niemand kennt das Hellfeld

Lessons learned…

- **Bewusstsein und die Fähigkeit von Mitarbeitern** sind zentral. (Awareness vs. Capability)
- **Social Engineering** stellt die Unternehmen vor Herausforderungen, die **mit der IT nicht gelöst** werden können.
- Die Gefahr liegt in der Kombination von **OSINT – SIGNINT – HUMINT**.
- Die **Grenzen zw. Konkurrenzausspähung und Industriespionage** verschwimmen. Dies gilt auch für die **rechtliche Bewertung**.
- Die Anforderung an die **Kooperationsbereitschaft der unternehmensinternen Abteilungen** ist extrem hoch.

Konsequenzen

Aufgabenverteilung innerhalb der Organisation



Das ISC soll unternehmensweite strategische und operative IT Sicherheitsfragen beantworten

Strategische Aufgaben

- Weiterentwicklung der IT Security und Informationssicherheitsrichtlinien
- Etablierung eines wirksamen Industriestandards zur Informationssicherheit (analog DIN 27000 ff.)
  - Risk Assessment
  - Verantwortlichkeiten und Rollen
  - Monitoring auf der Grundlage definierter KPI
- Etablierung eines Standards für die Sicherheit von Produktionsnetzwerken
- Unternehmensweite Awarnessmaßnahmen

Operative Aufgaben

- Vorbereitung von Beschlüssen zu unternehmensweiten Informationsschutz- und IT-Sicherheitsmaßnahmen
- Nachbereitung und Analyse von IT Security Incidents und sonstigen relevanten Cybervorfällen
- Auswertung der Ergebnisse von IT Sicherheitsaudits und erweiterten Sicherheitsanalysen (v.a. Pentesting)

LANXESS

In einem unternehmensweiten Information Security Committee sollen alle relevanten Aspekte beleuchtet werden.

Information Security Committee (ISC)

Aufgaben:

- Bereichsübergreifendes Riskassessment der Cyberrisiken
- Etablierung eines unternehmensweiten ISMS Systems
- Entscheidung über IT Sicherheitsmaßnahmen einschl. Maßnahmenmonitoring
- Reporting an der Corporate Risk Committee (CRC)

Mitglieder:

- Leitung: LEX - Corporate Security; Vertretung: Leitung IT-SGC
- Ständige Mitglieder: IT-SGC-QRM, LEX-IA, Datenschutzbeauftragter, PTSE-PLC, CON-, TAX, ACC, BU XY, BU ABC, GPL
- Erweiterte Mitglieder: COM, HR

Tagungsintervall:

- Das ISC tagt mit den ständigen Mitgliedern zunächst monatlich und mit den erweiterten Mitliedern einmal im Quartal; das Reporting in CRC erfolgt halbjährlich

Vielen Dank für Ihre Aufmerksamkeit?

Kontakt: Dirk.Fleischer@lanxess.com

LANXESS
Energizing Chemistry


LANXESS
Energizing Chemistry