

Cyberisiko und Threat Intelligence

Breakout Session – Kleinbankensymposium vom 14. Januar 2019

14. Januar 2019

Agenda

- **Cyberisiko**
 - Was versteht die FINMA darunter?
 - Wie ist die Regulierung aufgebaut?
- **Threat Intelligence**
 - Vorstellung Konzept
 - Wesentliche Aspekte: Bedrohungen, Schwachstellen, "Crown Jewels"
 - Auswertung der Selbstbeurteilung bei Kategorie 2 bzw. 3 Banken
- **CEO Fraud**
 - Praxisbeispiel
 - Lessons learned

Cyberisiko

Yves Obrist

Was versteht die FINMA unter Cyberrisiko?

Definition "Cyber-Attacken" gemäss FINMA RS 08/21 "Operationelle Risiken – Banken", **Fussnote 19**:

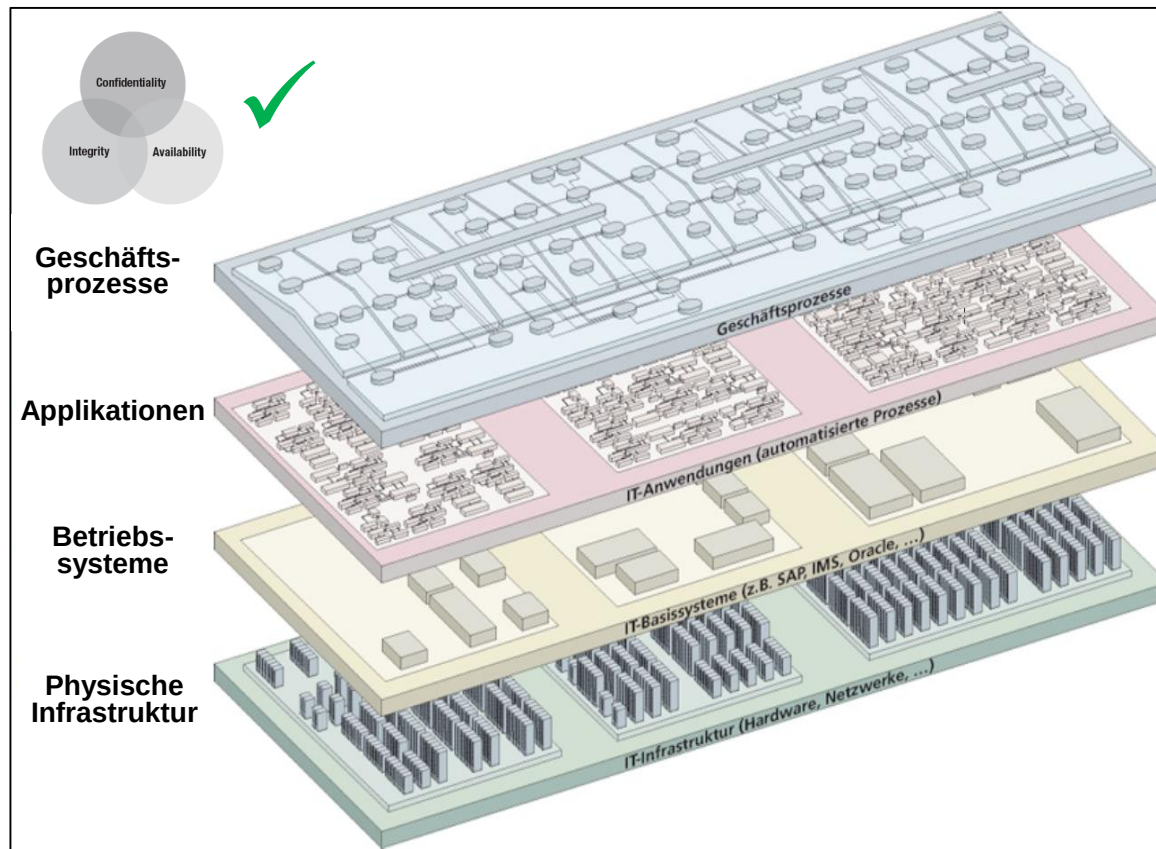
Sind Angriffe aus dem **Internet** und **vergleichbaren Netzen**, auf die **Integrität**, die **Verfügbarkeit** und die **Vertraulichkeit** der **Technologieinfrastruktur**, insbesondere in Bezug auf **kritische und/oder sensitive Daten** und **IT-Systeme**.



Vertraulichkeit bedeutet Schutz vor unbefugtem Zugriff, während **Integrität** Schutz vor unbefugter Änderung und **Verfügbarkeit** Schutz vor Zugriffsstörungen bedeutet.

Was versteht die FINMA unter Cyberrisiko?

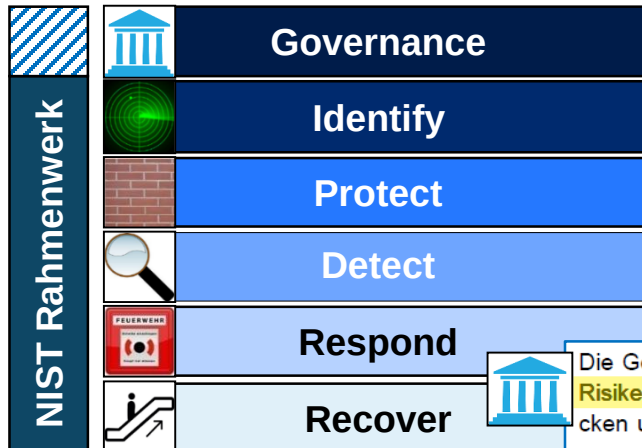
Definition "Technologieinfrastruktur" gemäss FINMA RS 08/21
"Operationelle Risiken – Banken", **Fussnote 15**:



Technologieinfrastruktur bezeichnet den **physischen** und **logischen** (elektronischen) **Aufbau** von IT- und Kommunikationssystemen, die einzelnen Hard- und Softwarekomponenten, die Daten und die Betriebsumgebung.

Quelle: ISACA Chapter Schweiz

Wie ist die Regulierung aufgebaut?



FINMA RS 2008/21 "Operationelle Risiken – Banken"

Die Geschäftsleitung hat zudem ein **Risikomanagement-Konzept für den Umgang mit Cyber-Risiken**¹⁷ zu implementieren. Dieses Konzept hat mindestens die folgenden Aspekte abzudecken und eine effektive Umsetzung durch **geeignete Prozesse** sowie eine eindeutige Festlegung von **Aufgaben, Rollen und Verantwortlichkeiten** zu gewährleisten:

135.6*



Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken¹⁹, insbesondere in Bezug auf kritische und/oder sensitive Daten und IT-Systeme,

135.7*



Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyber-Attacken, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen und/oder sensitiven Daten und IT-Systeme,

135.8*



Zeitnahe **Erkennung** und Aufzeichnung von Cyber-Attacken auf Basis eines Prozesses zur systematischen Überwachung der Technologieinfrastruktur,

135.9*



Reaktion auf Cyber-Attacken durch zeitnahe und gezielte Massnahmen sowie bei wesentlichen, die Aufrechterhaltung des normalen Geschäftsbetriebs bedrohenden Cyber-Attacken in Abstimmung mit dem BCM, und

135.10*



Sicherstellung einer zeitnahen **Wiederherstellung** des normalen Geschäftsbetriebs nach Cyber-Attacken durch geeignete Massnahmen.

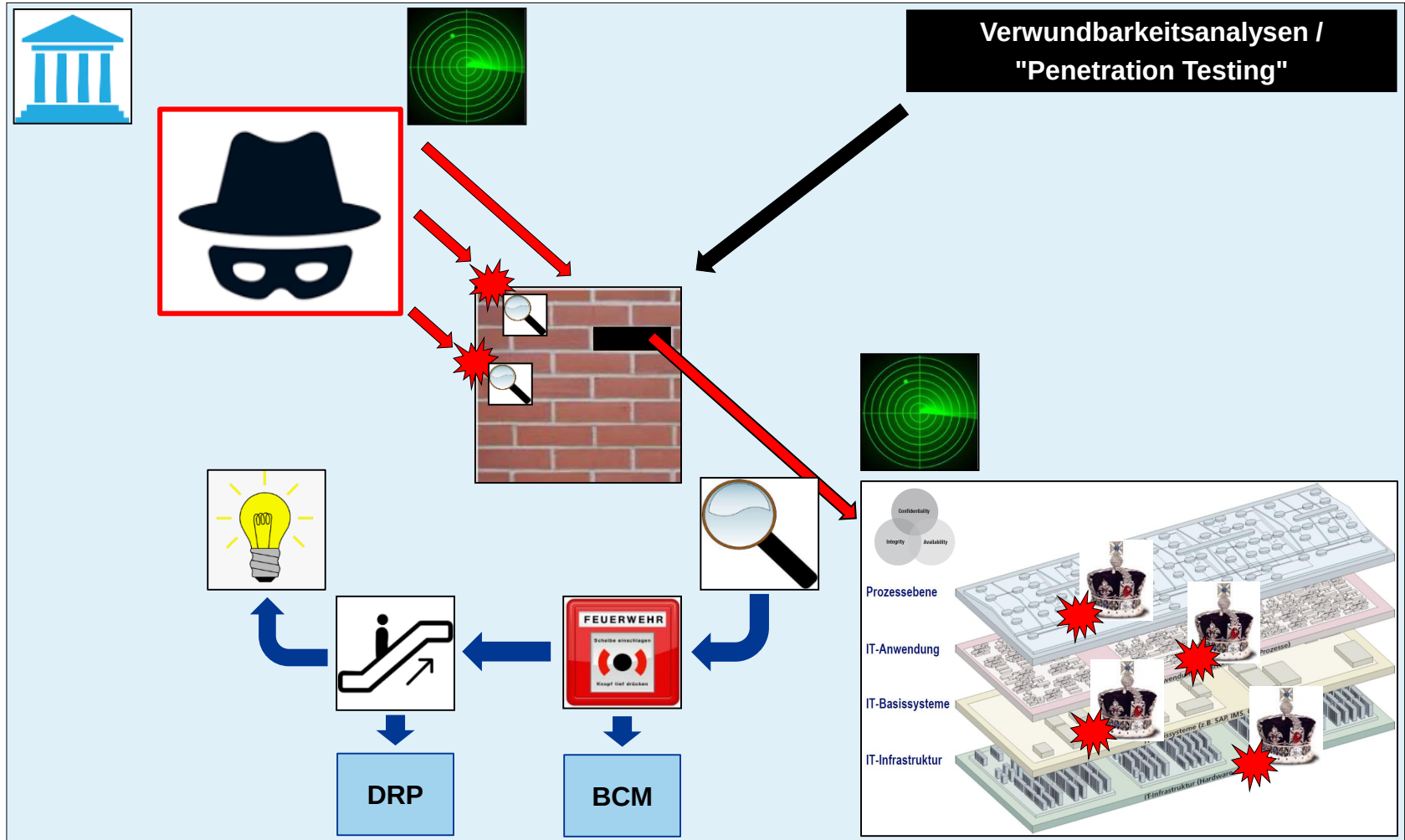
135.11*



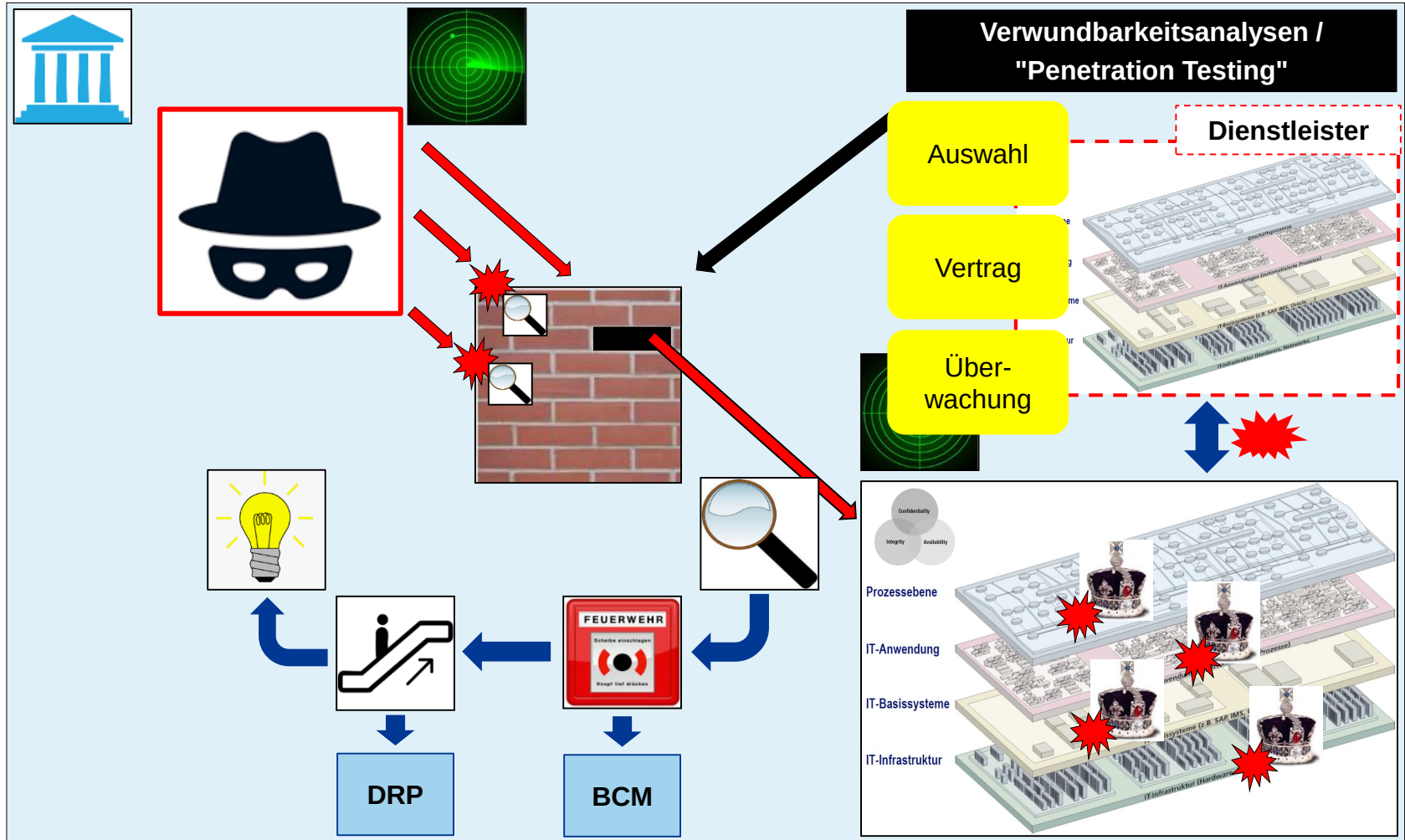
Die Geschäftsleitung lässt zum Schutz der kritischen und/oder sensitiven Daten und IT-Systemen vor Cyber-Attacken regelmässig **Verwundbarkeitsanalysen**²⁰ und **Penetration Testings**²¹ durchführen. Diese müssen durch qualifiziertes Personal mit angemessenen Ressourcen durchgeführt werden.

135.12*

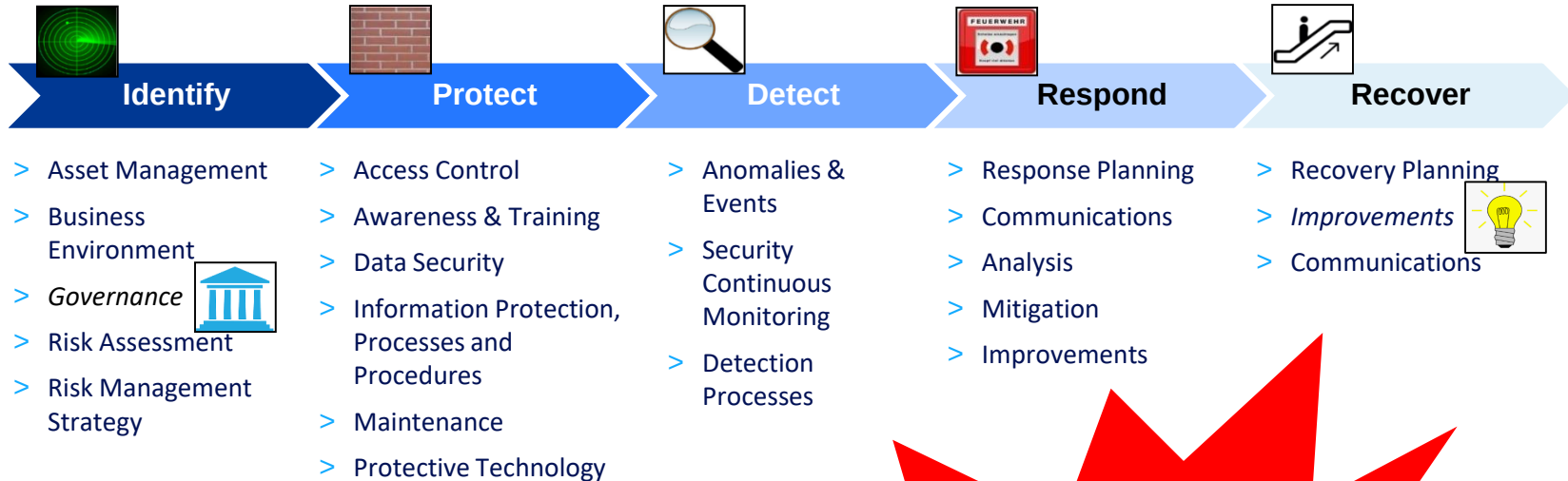
Wie ist die Regulierung aufgebaut?



Wie ist die Regulierung aufgebaut?



Wie ist die Regulierung aufgebaut?



Anwendung
Proportionalitäts-
prinzip

Bewusstsein schaffen!

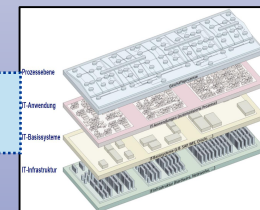
Awareness

Kunden



Awareness

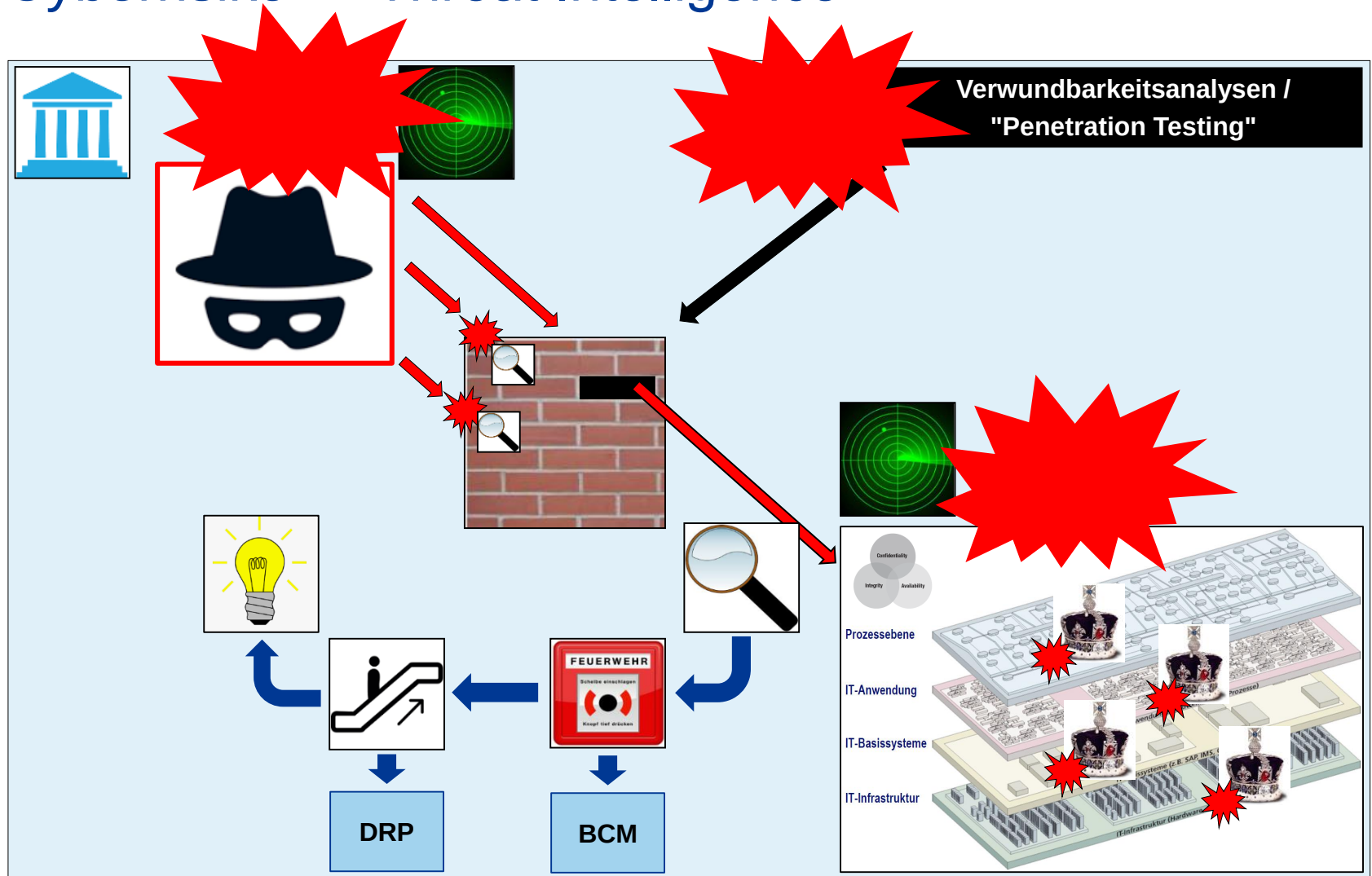
Bank



"Social Engineering"

Cyberattacken gegen Technologieinfrastruktur

Cyberrisiko → Threat Intelligence



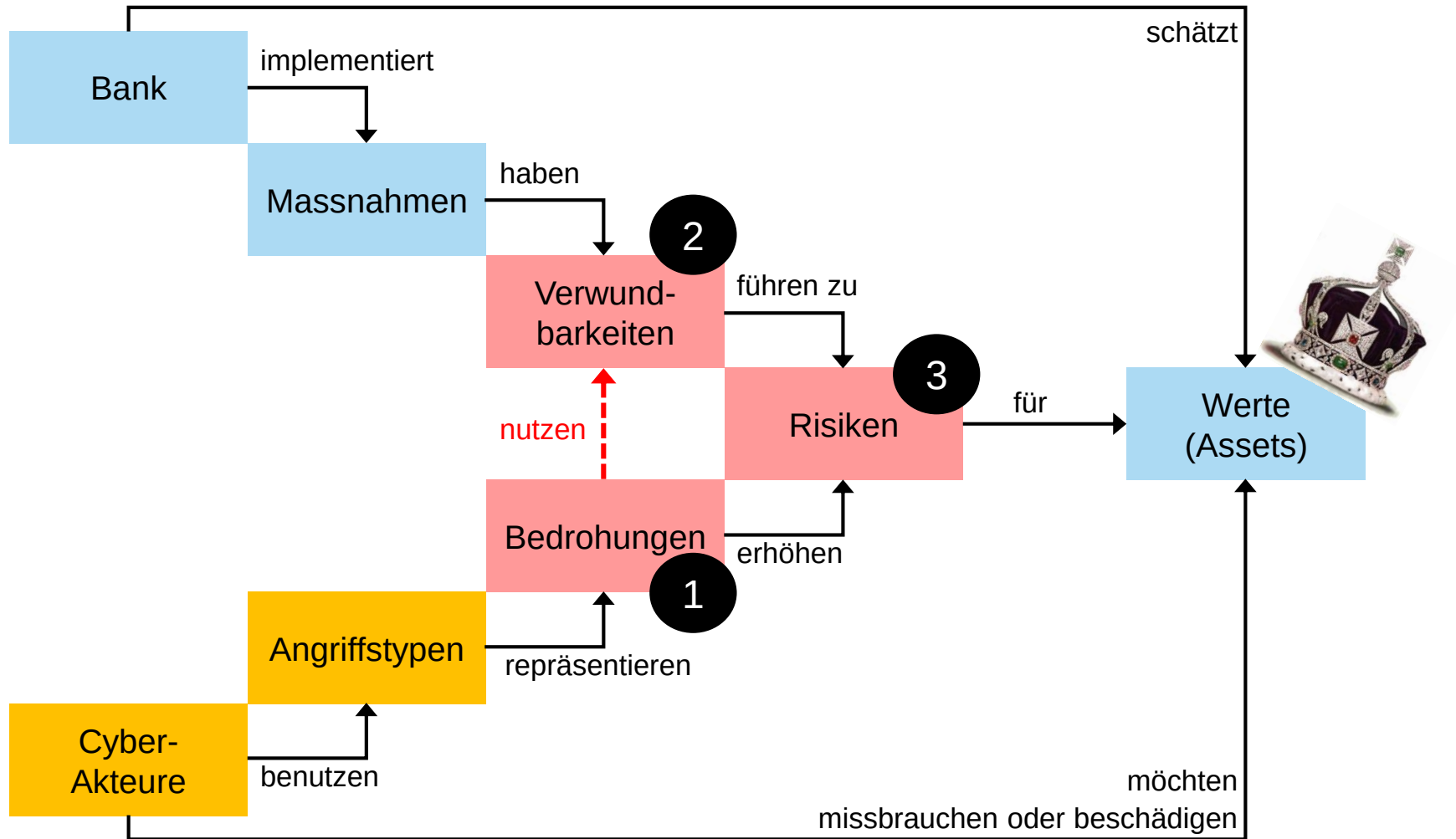
Threat Intelligence

Christian Steffen

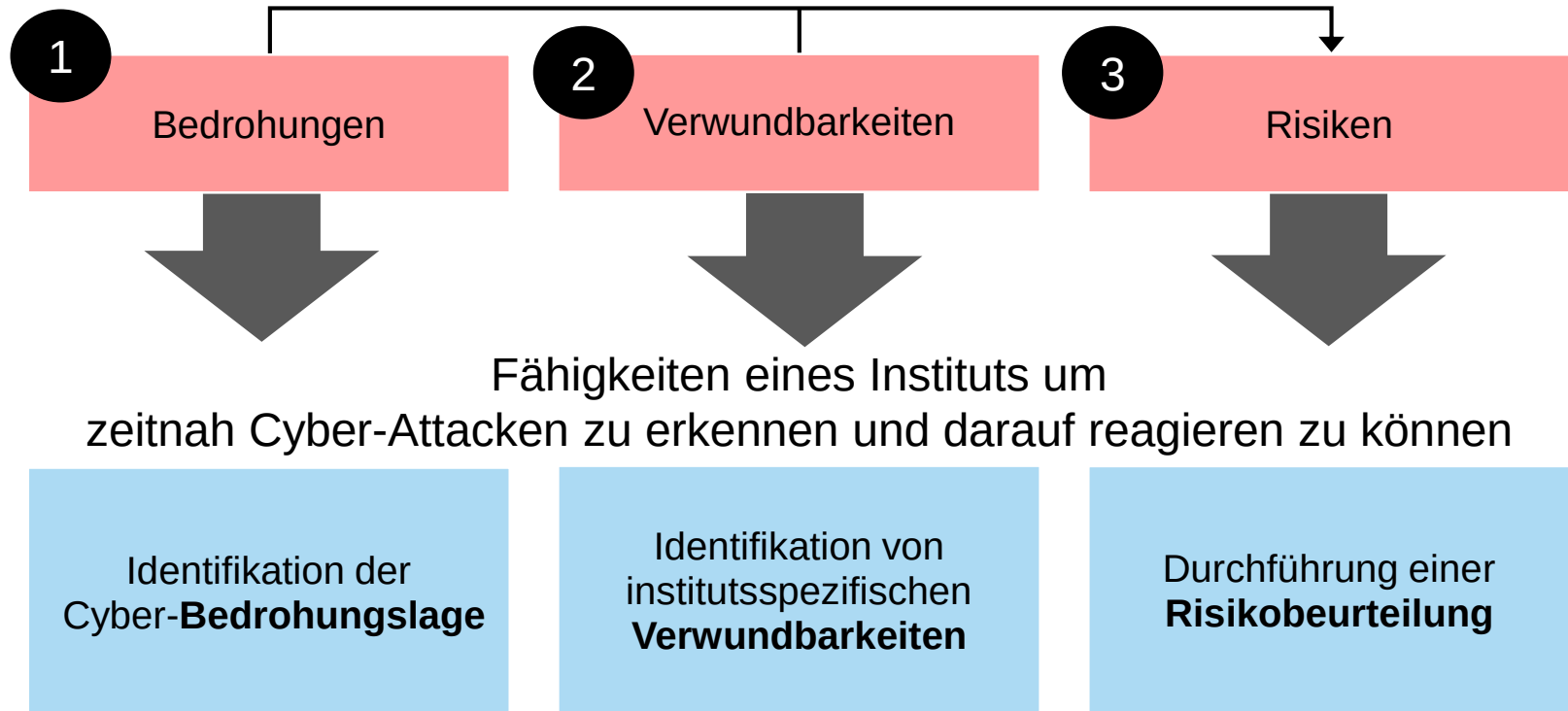
Selbstbeurteilung 2018

- Die FINMA erachtet "Threat-Intelligence" als **wichtige Disziplin** einer **effektiven Abwehr** von Cyber-Attacken.
- Die FINMA hat im Sommer 2018 **die Kat. 2 und 3 Banken** eingeladen, an der **Selbstbeurteilung** über den Umgang mit "Threat-Intelligence" teilzunehmen (*Teilnahme: 3 Kategorie 2-Banken; 23 Kategorie 3-Banken*)
- Die **aufsichtsrechtliche Grundlage** für den Umgang mit "Threat Intelligence" besteht dabei prinzipienbasiert im Rahmen des **FINMA-RS 2008/21** "Operationelle Risiken – Banken", Grundsatz 4: Technologieinfrastruktur
- Bei den Aspekten gemäss Fragenkatalog handelt es sich allgemein nicht um explizite aufsichtsrechtliche Anforderungen. Jedoch erachtet die FINMA diese Aspekte als **wichtige Best Practices** an.

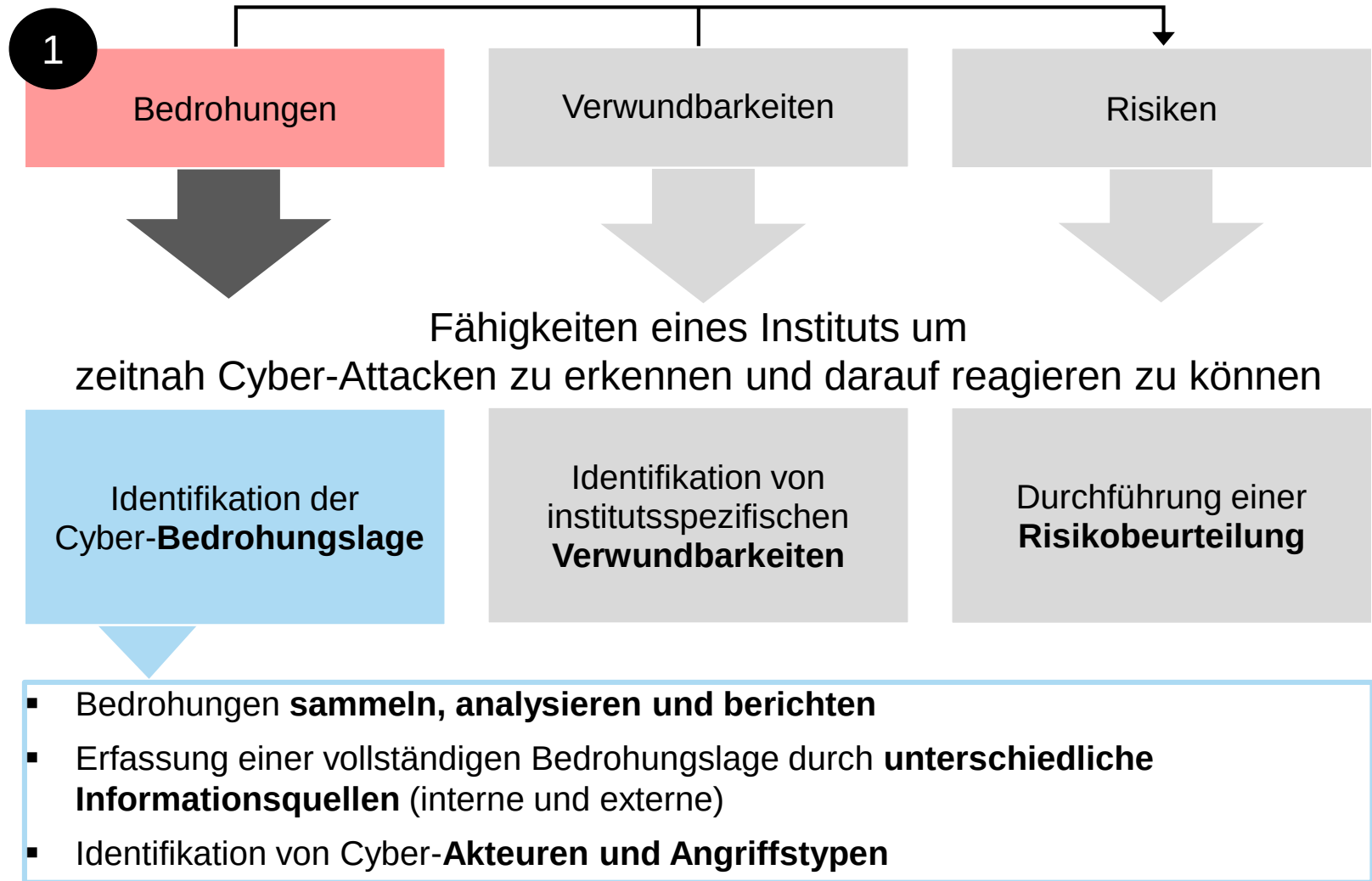
Die wesentlichen Aspekte



Erkennung von Cyber-Attacken

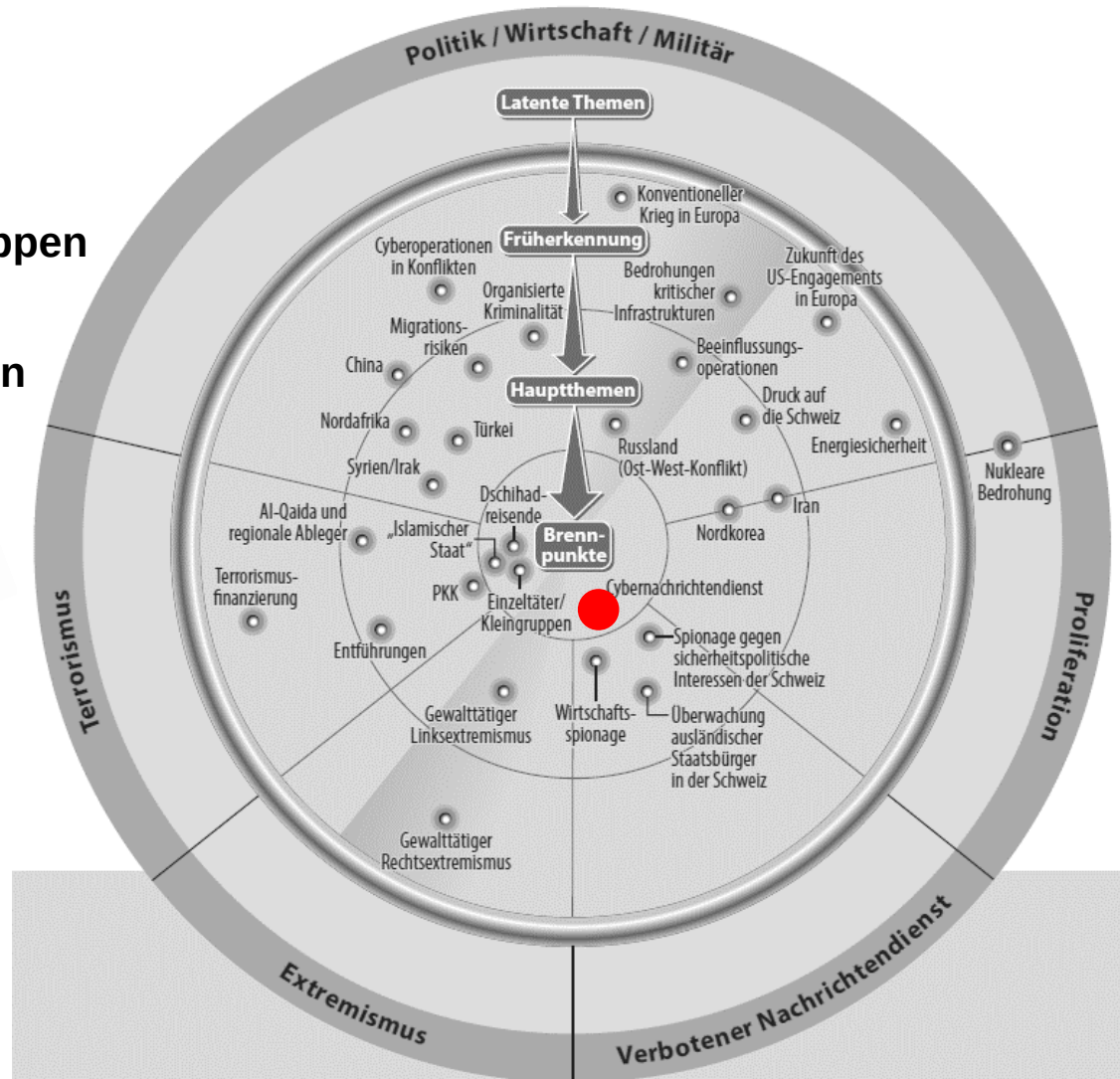


Erkennung von Cyber-Attacken

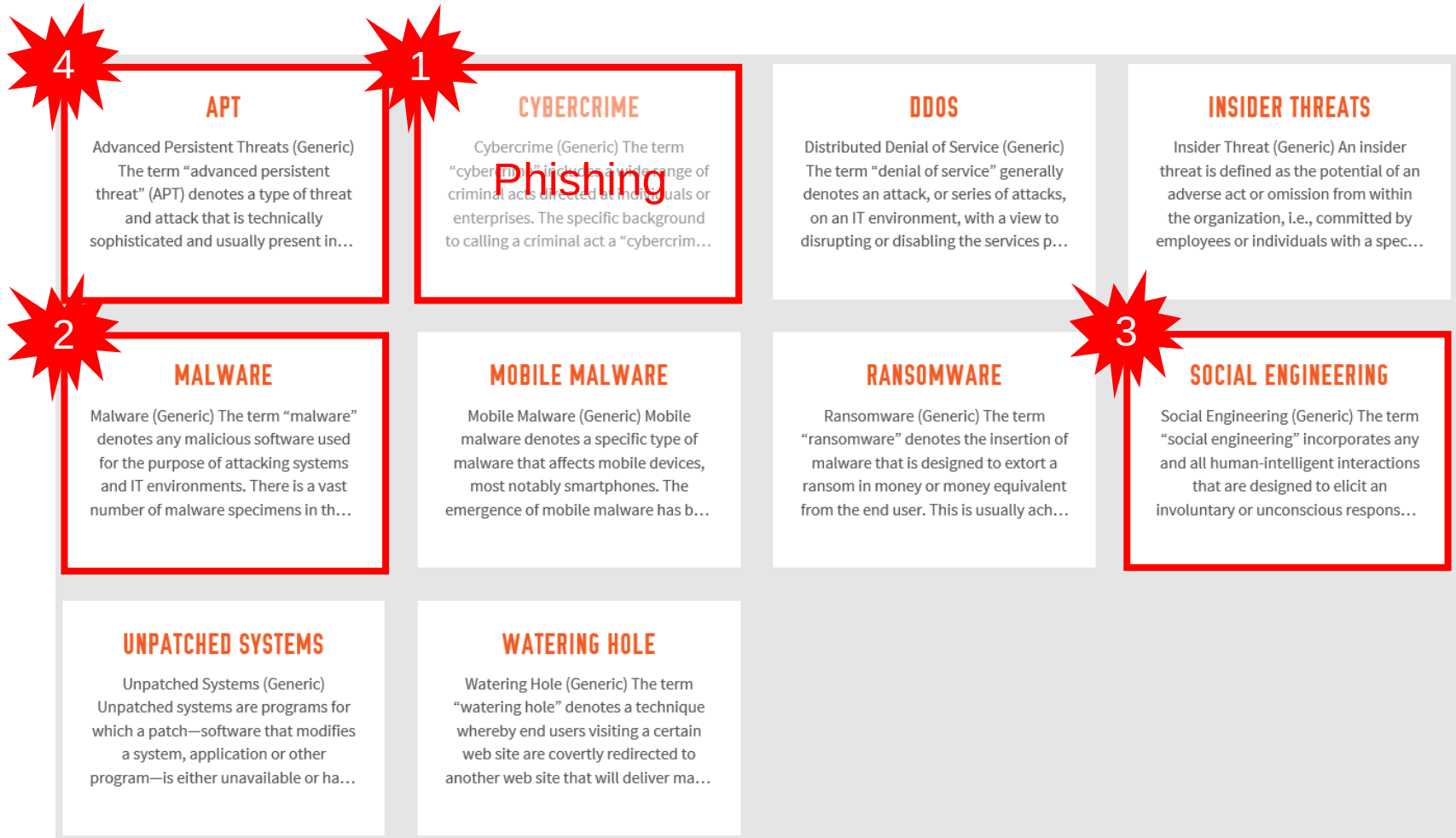


Bedrohungslage – Wer sind die Cyber-Akteure?

- Staatlich finanzierte Gruppen
- Kriminelle Organisationen
- Interne Mitarbeiter
- Isolierte Hackers
- Script Kiddies



Mit welchen Cyber-Bedrohungen sind Banken in der Schweiz konfrontiert?

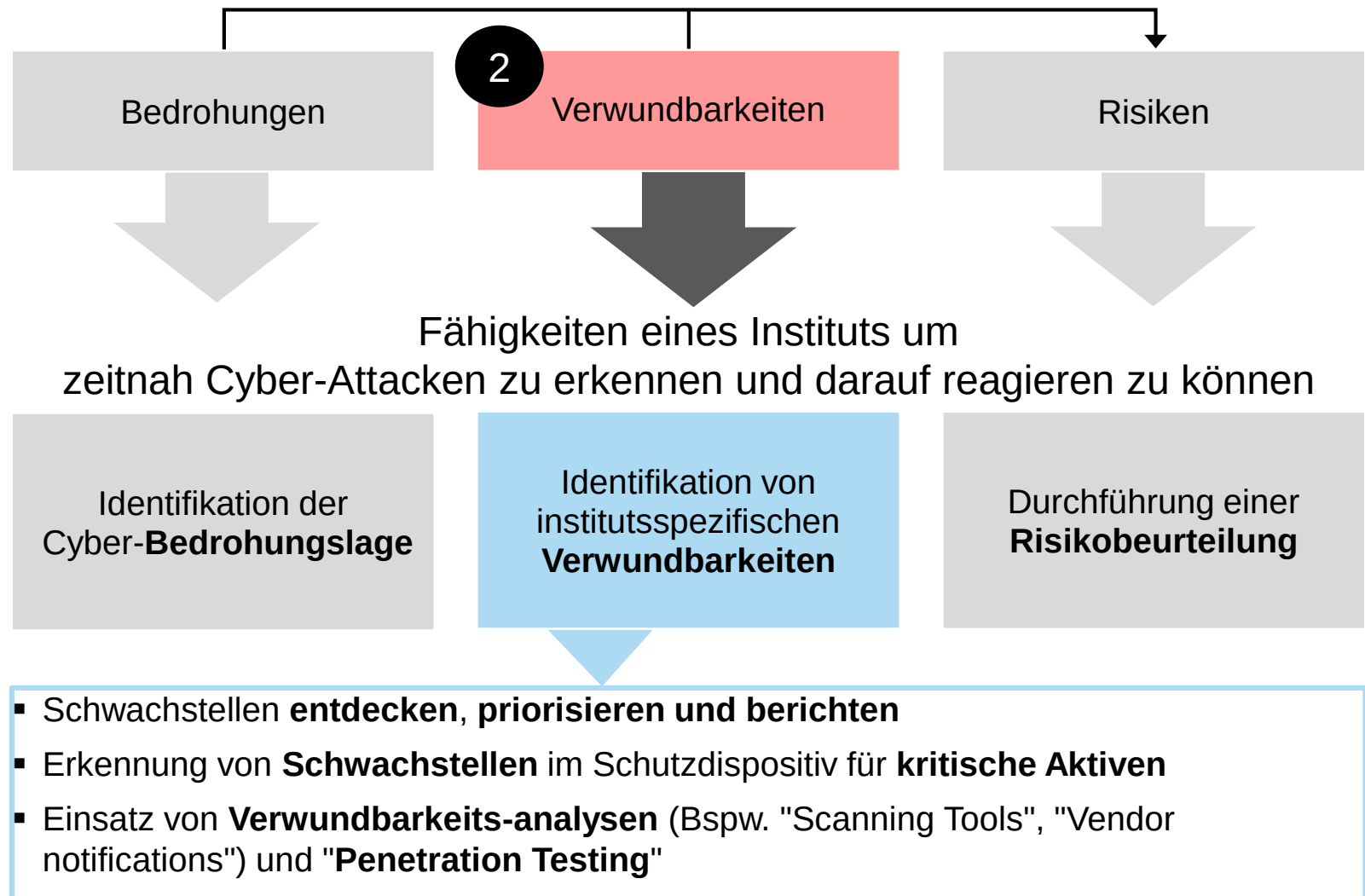


Selbstbeurteilung 2018

1. Identifikation von institutsspezifischen Bedrohungspotenzialen

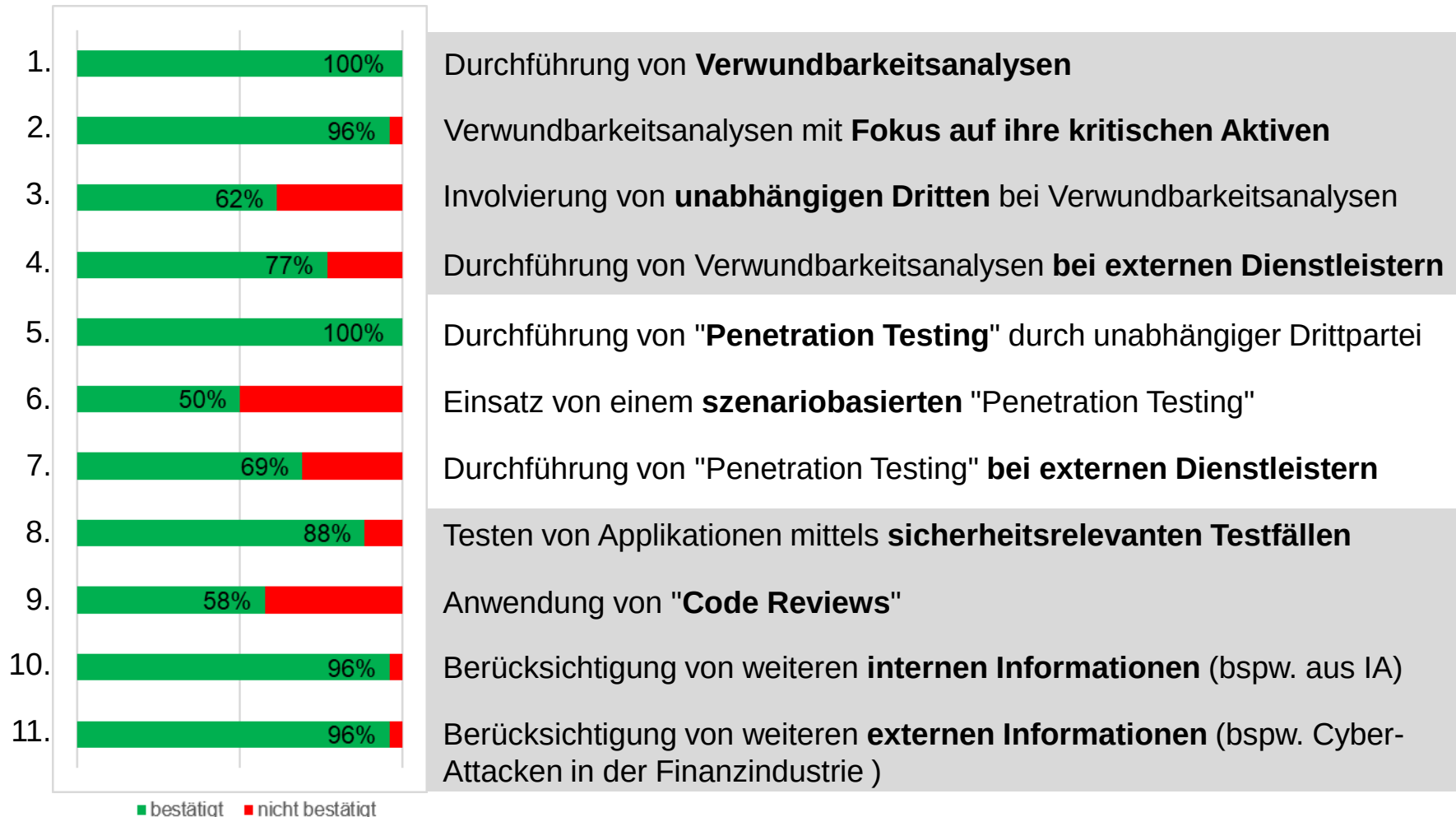


Erkennung von Cyber-Attacken

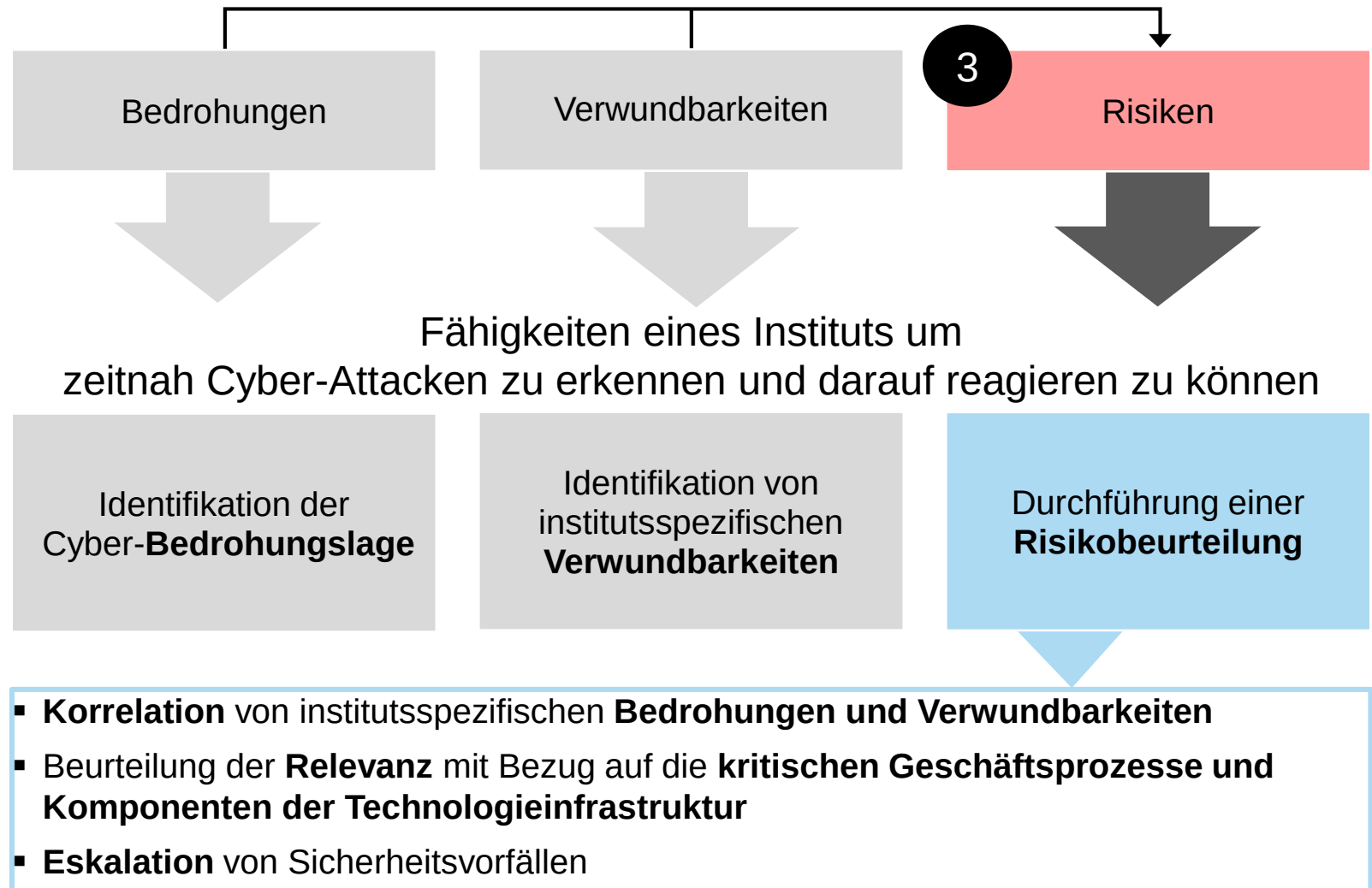


Selbstbeurteilung 2018

2. Identifikation von institutsspezifischen Verwundbarkeiten



Erkennung von Cyber-Attacken



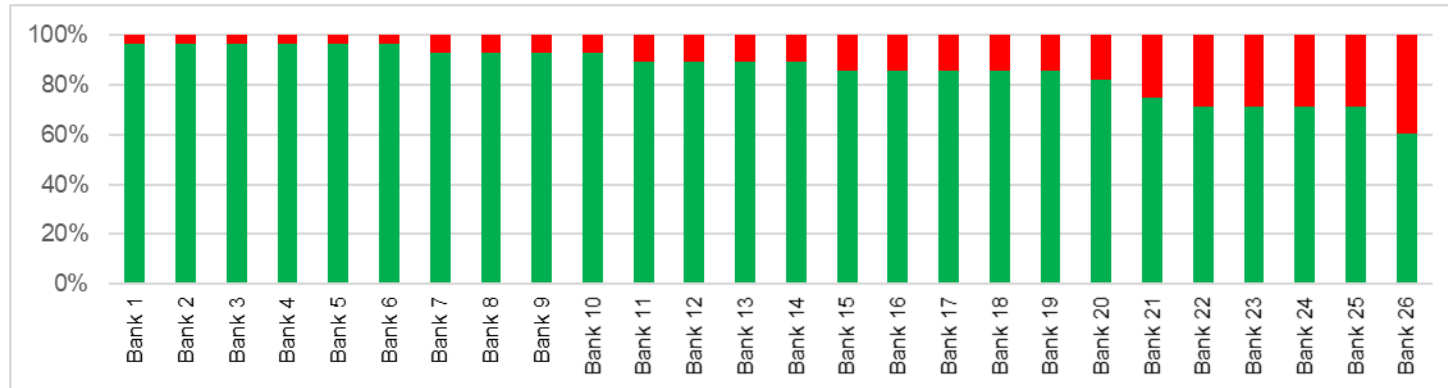
Selbstbeurteilung 2018

3. Durchführung einer Risikobeurteilung



Selbstbeurteilung 2018

Vergleich über die teilnehmenden Institute



Dabei entspricht 100% der Bestätigung einer vollständigen Adressierung aller kritischen Aspekte gemäss Fragenkatalog.

Schlussfolgerung der FINMA

- Grundsätzlich hat die Auswertung der Antworten der **teilnehmenden Institute** aufgezeigt, dass sich diese der Thematik **bewusst** sind **und grösstenteils Massnahmen umgesetzt** haben.
- Nichtsdestotrotz weisen einzelne Institute noch **Verbesserungspotenzial** in der Adressierung der kritischen Aspekte gemäss Fragenkatalog auf.
- Die Auswertung hat insbesondere gezeigt, dass die Institute bei der **Identifikation von Verwundbarkeiten** noch nicht in allen Bereichen "Best Practice"-Grundsätze erreicht haben.

CEO Fraud

Christophe Monigadon - CISSP

golem.de IT-NEWS FÜR PROFIS
HOME TICKER VIDEO AUDIO FORUM
TOP-THEMEN: 35C3 Raumfahrt 5G Security IT-Jobs Auto

CEO-FRAUD Autozulieferer Leoni um 40 Millionen Euro betrogen

Mit dem sogenannten Chef-Trick erbeuten Kriminelle oft Millionenbeträge von Unternehmen. Mit fingierten **E-Mails** und Zahlungsanweisungen werden illegale Geldtransfers eingeleitet. Jetzt hat es einen großen deutschen Automobilzulieferer getroffen.

Der deutsche Automobilzulieferer Leoni ist um rund 40 Millionen Euro betrogen worden, wie das Unternehmen am **Dienstag selbst bekanntgegeben hat**. Die Angreifer nutzten dabei offenbar eine als Chef-Trick oder CEO-Fraud bekannte Masche, um sich Zugriff auf die Zahlungen zu sichern.

Kantonspolizei Aargau

CEO-Betrüger treiben nun auch im Aargau ihr Unwesen

Mittwoch, 19.09.2018, 11:21 Uhr

- Die neue Masche heisst «CEO-Fraud». Man erhält vom (angeblich) eigenen Chef ein Mail mit der Anweisung, Bargeld ins Ausland zu überweisen.
- Die Kantonspolizei Aargau hat Kenntnis von mehreren derartigen Fällen.
- Adressaten der kriminellen Mails sind vor allem Vereine.

Sie habe am Dienstag von mehreren Betrugsversuchen erfahren, teilt die Kantonspolizei Aargau mit. Unbekannte Absender von E-Mails hätten die Empfänger aufgefordert, für die Firma eine dringende Überweisung zu machen. Das Geld sei ins Ausland zu überweisen. Die Täter hätten sich als vorgesetzte Personen ausgegeben. Ob tatsächlich Geld überwiesen worden sei, weiss die Polizei noch nicht.

• In einem Fall haben Büromitarbeiter den Kriminellen über 100'000 Franken überwiesen.

20 minuten de fr it
Schweiz Ausland Wirtschaft Sport People Entertainment
Zürich Bern Basel Zentralschweiz Ostschweiz

Gefälschtes Mail 16. August 2018 14:17; Akt: 16.08.2018 17:18

Sekretärin fällt auf CEO-Masche herein

Im Mai haben unbekannte Betrüger mit der Masche CEO-Betrug rund 80'000 Euro ergaunert. Die Kantonspolizei Thurgau mahnt zur Vorsicht.

Eine Sekretärin einer Thurgauer Firma hat Betrügern einen Betrag von 80'000 Euro überwiesen. (Bild: Keystone/Martin Ruetschi)

Abonnemente
Menü Startseite Panorama Unglücksfälle und Verbrechen

Neue Zürcher Zeitung Falsche Chefs täuschen Millionen und erbeuten Millionen

Sie geben sich als Direktoren oder Firmen-Anwälte aus, imitieren deren E-Mail-Adressen und beauftragen dann Angestellte mit Transaktionen in Millionenhöhe auf ausländische Konten. Dieser «CEO-Betrug» hat Westschweizer Firmen 2015 Millionen gekostet.

27.1.2018, 14:02 Uhr
(sda) Die Täter gehen dabei äusserst professionell vor, wie die Koordinationsstelle zur Bekämpfung der Internetkriminalität (Kobik) auf ihrer Website schreibt: Angestellte werden zuerst telefonisch in einen fiktiven, dringlichen internationalen Unternehmenskauf im Ausland eingeweiht.

Sechs Millionen Franken Schaden in Genf

Am meisten betroffen von derartigen Betrugsfällen war im vergangenen Jahr der Kanton Genf. Dort gab es rund dreissig entsprechende Klagen mit einer Schadenssumme von sechs Millionen Franken, wie Marc Zingg von der Finanzabteilung bei der Genfer Kantonspolizei sagte. Er bestätigte damit eine Meldung der Zeitung «Le Matin Dimanche».

Weniger bekannt ist das Phänomen in der Deutschschweiz: Der Kanton Bern registrierte 2015 ein Dutzend CEO-Betrugsversuche für einen Gesamtbetrag von gegen zehn Millionen Franken, wie der Sprecher der Kantonspolizei, Nicolas Kessler, auf Anfrage sagte. In zehn Fällen waren die Täter erfolgreich und erbeuteten insgesamt rund 400'000 Franken.

Das Vorgehen kennt man auch im Kanton Genf, wo im vergangenen Jahr rund siebzig ähnliche Fälle bekannt wurden. Die Deliktsumme beläuft sich dabei auf rund 800'000 Franken. Gemäss Zingg werden den Genfer Behörden jede Woche ein bis zwei neue derartige Fälle gemeldet.

Home News Schweiz

Mails von falschem «Chef» im Umlauf

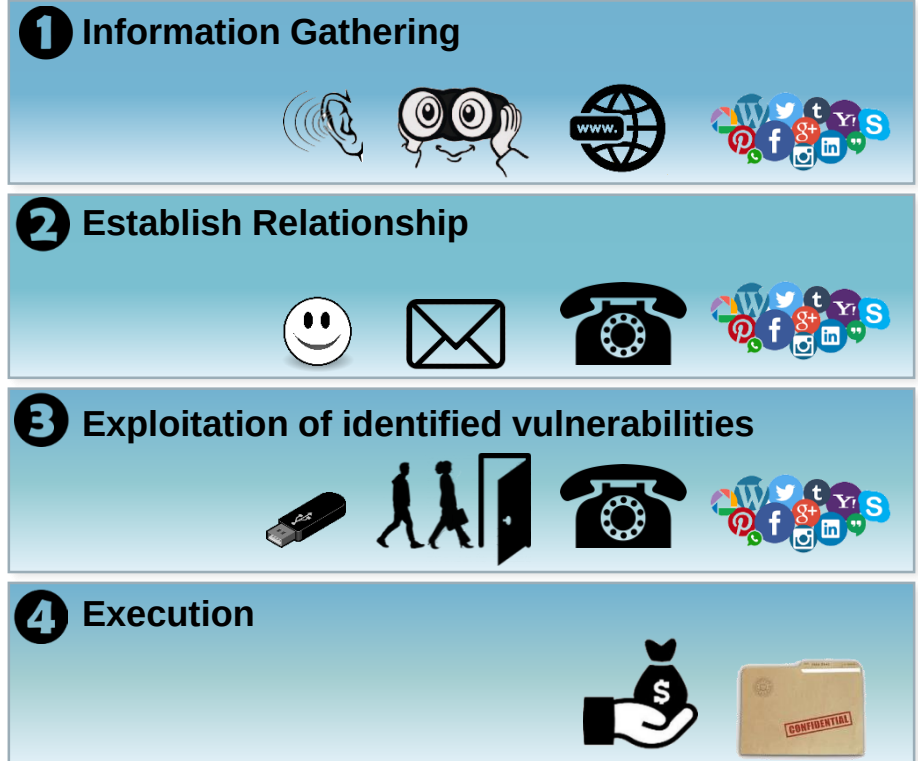
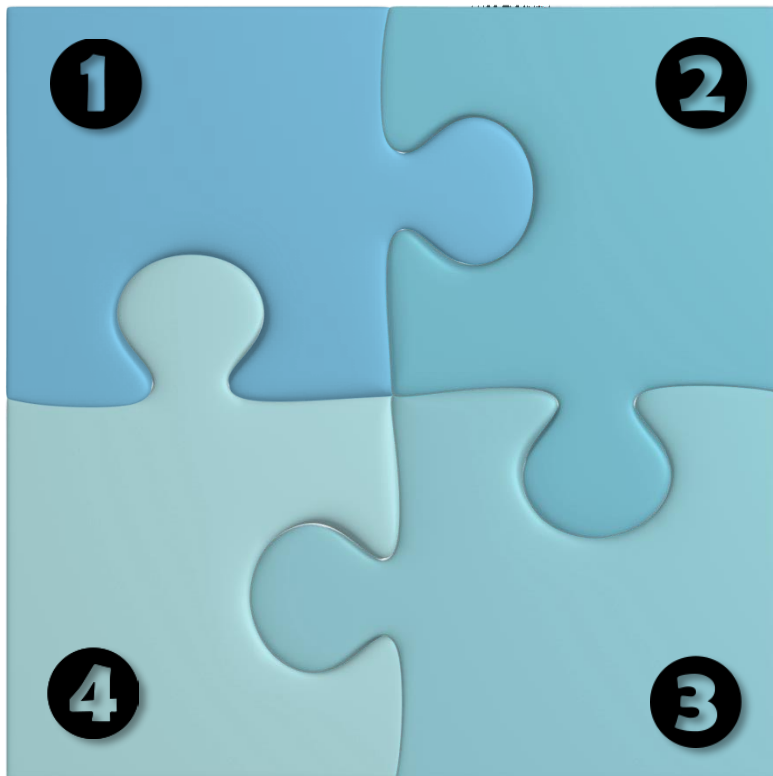
Luzerner Arbeitnehmer aufgepasst: In den vergangenen Wochen sind mehrere Fälle von so genanntem «CEO Fraud» bekannt geworden. Dabei werden Mitarbeiter mit gefälschten Mails gebeten, eine Zahlung auszulösen.

- <https://www.golem.de/news/ceo-fraud-autozulieferer-leoni-um-40-millionen-euro-betrogen-1608-122741.html>
- <https://www.srf.ch/news/regional/aargau-solothurn/kantonspolizei-aargau-ceo-betrueger-treiben-nun-auch-im-aargau-ihr-unwesen>
- <https://www.20min.ch/schweiz/ostschweiz/story/Mit-CEO-Masche-betrogen-22194934>
- <https://www.nzz.ch/panorama/ungluecksfaelle-und-verbrechen/falsche-chefs-taueschen-angestellte-und-erbeuten-millionen-1.18684623>

Social Engineering

Definition: *The act of manipulation by one person to another to accomplish goals that may or may not be in the “target’s” best interest*

Social Engineering follows 4 steps:



CEO Fraud / CEO Impersonation

Definition: *CEO fraud involves impersonation of senior business managers, using social engineering to persuade employees to transfer their business money under the auspice of acceptable business intent and trust.*



KEY TARGETS:

Mid-level employees in financial or procurement services



HIGHLY ATTRACTIVE CRIME:

Large profits and low risk of detection



HIGH FINANCIAL IMPACT FOR TARGETED COMPANIES:

Losses up to several millions (€, \$, CHF, £ ...)



DIRECT HUMAN COSTS:

Shame, sanctions, loss of employment

PSYCHOLOGICAL TRICKS



GAIN THE TRUST OF THE TARGET:

Using stories with legitimate-seeming background



TIME PRESURE:

Create a situation where the “victim” does not have enough time to make a proper decision



HACKING:

Exploit weaknesses in email systems



PHISHING:

Send emails with stolen credentials



EMAIL SPOOFING – PHONE SPOOFING:

Disguising a communication from an unknown source as being from a known, trusted source



TYPOSQUATING:

use similar internet or e-mail addresses

How CEO Fraud works



Information Gathering

- OSINT, Website, Social Media, Phone, Dumpster diving,...



Establish Relationship

- A fraudster calls posing as a high ranking figure of the company (e.g. CEO or CFO)
- Requires an urgent transfer of funds and absolute confidentiality
- Invokes a sensitive situation (e.g. tax control; merger; acquisition)



Exploitation

- Pressures the employee not to follow the regular authorisation procedures
- Instructions on how to proceed are given later by a third-person or via e-mail



Execution

- The employee transfers funds to an account controlled by the fraudster.
- The money is re-transferred to accounts in multiple jurisdictions

Praxis Beispiel: Der Fall "Lasertech"



Wilhelm Gross
Präsident des
Verwaltungsrats



Bruno Meier
Geschäftsführer



Franz Müller
Leiter Finanz-und
Rechnungswesen



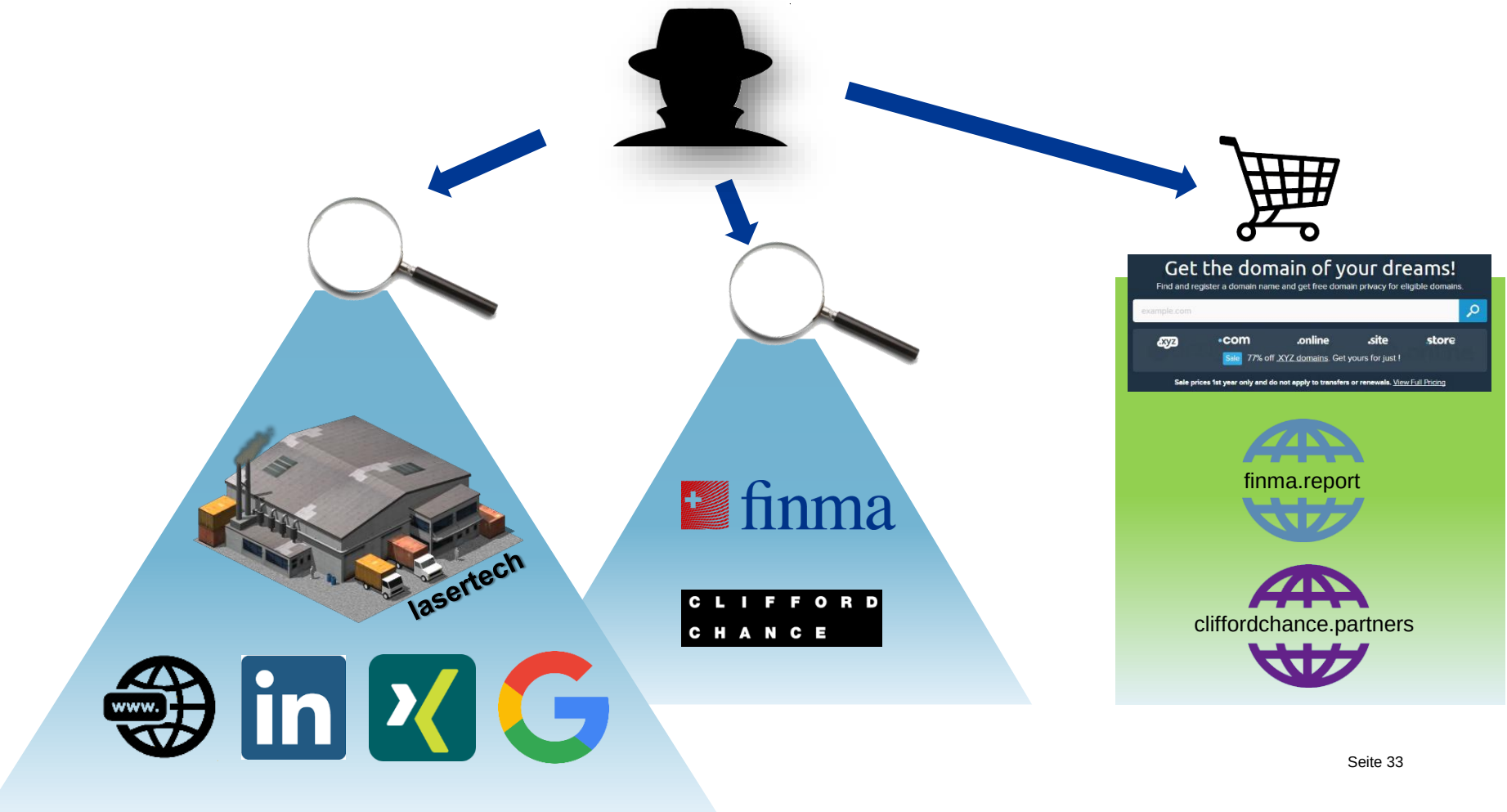
Dr. Alex Riley
externer
Rechtsanwalt

Step 1 - Information Gathering



Information Gathering

- OSINT, Website, Social Media, Phone, Dumpster diving,...



Step 2 - Establish Relationship

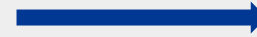
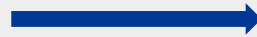


Establish Relationship

- A fraudster calls posing as a high ranking figure of the company (e.g. CEO or CFO)
- Requires an urgent transfer of funds and absolute confidentiality
- Invokes a sensitive situation (e.g. tax control; merger; acquisition)



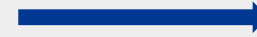
Dr. Riley



Franz Müller



Wilhelm Gross



Franz Müller

Step 2 - Establish Relationship

Von: Wilhelm Gross <wilhelm.gross@lasertech.org>;

Gesendet: Dienstag, 26. November 2017 12:12

An: Müller Franz <franz.mueller@lasertech.org>

Cc: Dr. Alex Riley <alex.riley@cliffordchance.partners>

Betreff: FWD: RB GT9382

Wichtigkeit: Hoch

Guten Tag, Herr Müller

Hat Sie Dr. Riley bereits kontaktiert?

Ich würde Ihre Mitarbeit in einer Angelegenheit von Herrn Meier benötigen.

Wie flexibel sind Sie heute?

Mit freundlichen Grüßen

Wilhelm Gross

Präsident des Verwaltungsrats

Sent from my iPhone



Anfang der weitergeleiteten Nachricht:

Von: "Dr. Alex Riley" <alex.riley@cliffordchance.partners>

Betreff: RB GT9382

Datum: November 25, 2016 17:44:06 AM GMT+01:00

An: "Wilhelm Gross" <wilhelm.gross@lasertech.org>; <protokoll@finma.report>

Sehr geehrter Herr Gross,

Vielen Dank für die Benachrichtigung bezüglich Ihres Zeitfensters.

Um dieses einzuhalten, sollten wir folgende Punkte, vorrangig hinsichtlich der FINMA Richtlinien, die Sorgfältigkeitspflichten beachten:

Wie bereits erörtert, muss sämtliche Kommunikation im Rahmen der Buyer's Due Diligence und Data Room Vorgaben stattfinden.

d.h.:

- ausnahmslose Diskretion gegenüber allen Unbeteiligten dieser Übernahme (auch innerhalb der mitwirkenden Gesellschaften)
- interne digitale Kommunikation ausschliesslich schriftlich (E-Mail & Fax)
- protokollierter, lückenloser und chronologischer Kommunikationsverlauf (mich & die FINMA stets im CC der E-Mails verankern; respektive stets bei Antworten auf "Allen Antworten" klicken)
- vorherige Absprache beim Hinzuziehen weiterer Personen (mit Namens-, Status-, Kontaktangaben)

Dies sollte bis zur öffentlichen Bekanntmachung Ihrerseits durchgängig eingehalten werden.

Für die weiteren Schritte würden wir dringend einen Nachweis über die Transaktion benötigen, sodass wir das Vorkaufsrecht sichern können.

Optimal hierfür wäre die Transaktionsbestätigung: **SWIFT MT103**

Da ich weiterhin in Brüssel bin, können Sie mich in dringenden Notfällen weiterhin mobil erreichen.

Mit freundlichen Grüßen

DR. Alex RILEY

Rechtsanwalt

Partner Mergers & Acquisitions

Clifford Chance, Frankfurt

Step 3 - Exploitation

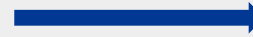


Exploitation

- Pressures the employee not to follow the regular authorisation procedures
- Instructions on how to proceed are given later by a third-person or via e-mail



Wilhelm Gross



Franz Müller

Step 3 - Exploitation

Von: Wilhelm Gross <wilhelm.gross@lasertech.org>; <protokoll@finma.report>

Gesendet: Dienstag, 26. November 2017 14:10

An: Müller Franz <franz.mueller@lasertech.org>

Cc: Dr. Alex Riley <alex.riley@cliffordchance.partners>

Betreff: Re: RB GT9382



Sehr geehrter Herr Müller

Wie sie vielleicht aus dem Anhang entnehmen konnten, bereiten wir mit Hilfe von Dr. Riley von Clifford Chance eine Übernahme vor.

Genau aus diesem Grund, waren Sie intern noch nicht informiert. Viele weitere aus unserem Hause sind es und sollten es auch bis zur öffentlichen Bekanntmachung auch nicht werden.

Beachten Sie bitte, dass einige Richtlinien der FINMA eingehalten werden müssen.

Erwartet wird absolute Diskretion (auch innert der Gesellschaft) und lückenloser Nachweis über unsere Kommunikation (stets "Allen Antworten", sodass auch Dr. Riley und das Protokoll beachtet werden.

Um ein Vorkaufsrecht zu sichern, müssen wir eine Zahlung ins Ausland i.d.H. von EURO

1'172'000.00 tätigen.

Welches wäre der einfachste und effektivste Weg, dies am heutigen Tage abzuwickeln, sodass wir eine Zahlungsbestätigung einreichen können?

Mit freundlichen Grüßen

Wilhelm Gross
Präsident des Verwaltungsrats

Sent from my iPhone

Step 4 - Execution



Execution

- The employee transfers funds to an account controlled by the fraudster. The money is re-transferred to accounts in multiple jurisdictions



Franz Müller



Dr. Alex Riley



Franz Müller



finma



Lessons learned

at the company level:

- Be aware of the risks and spread the information within the company.
- Avoid sharing sensitive information on the company's hierarchy, security or procedures.
- Have robust funds transfer processes
- Finding out who owns a Internet domain similar to yours
- Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.
-

as an employee:

- Be careful when using social media: by sharing information on your workplace and responsibilities you increase the risks of becoming a target.
- Always carefully check e-mail addresses when dealing with sensitive information/money transfers.
- Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure.
- In case of doubt on a transfer order, always consult a colleague even if you were asked to use discretion.
-