LKA 543
Hamburg

Cybercrime

Aktuelle Phänomene und Handlungsempfehlungen der Polizei Hamburg

Agenda

- Vorstellung / Einleitung ins Thema
- CEO-Fraud / Mailkompromittierung
- Malware spez. Ransomware
- DDoS-Angriffe
- Weitere Angriffsfelder
- Incident Response / Polizei
- Fazit

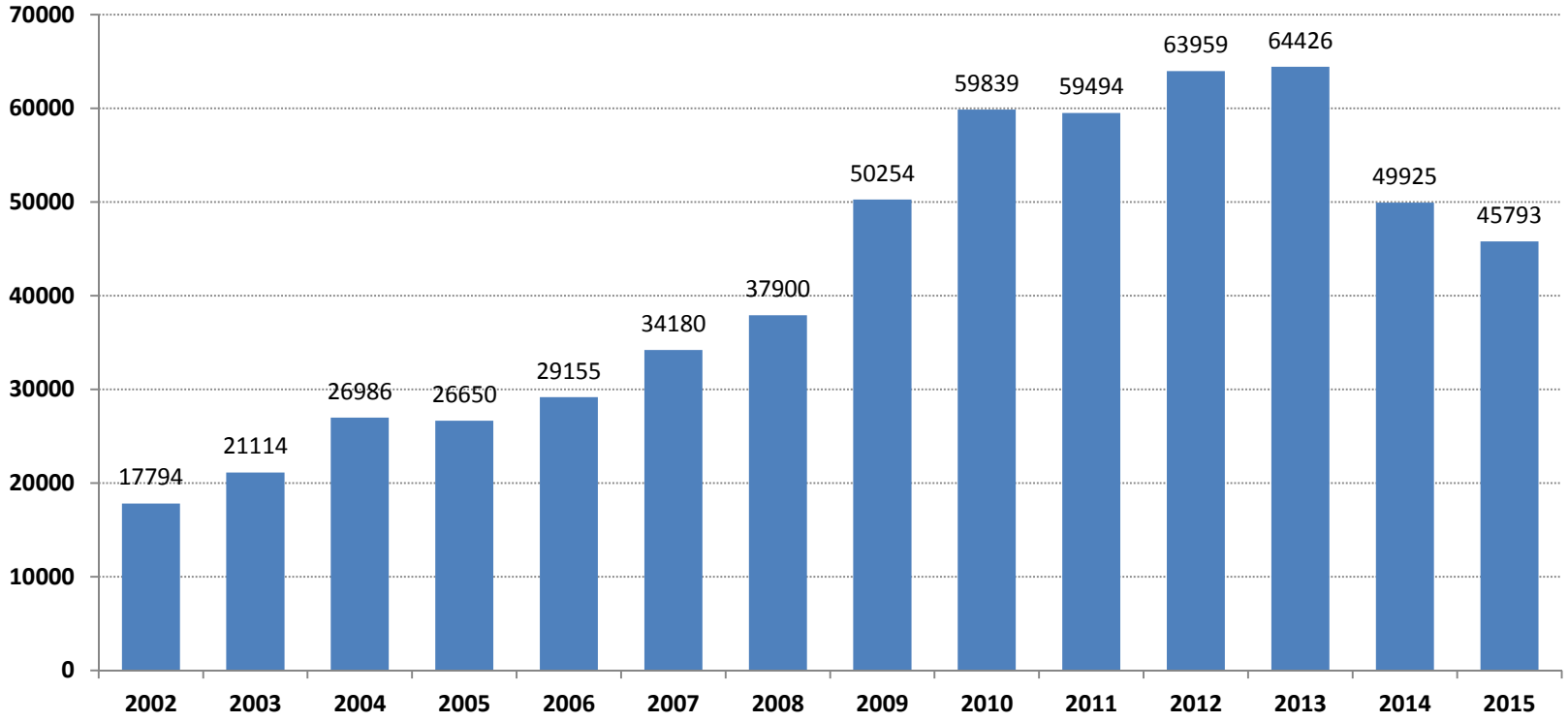
- LKA 541

- LKA 542

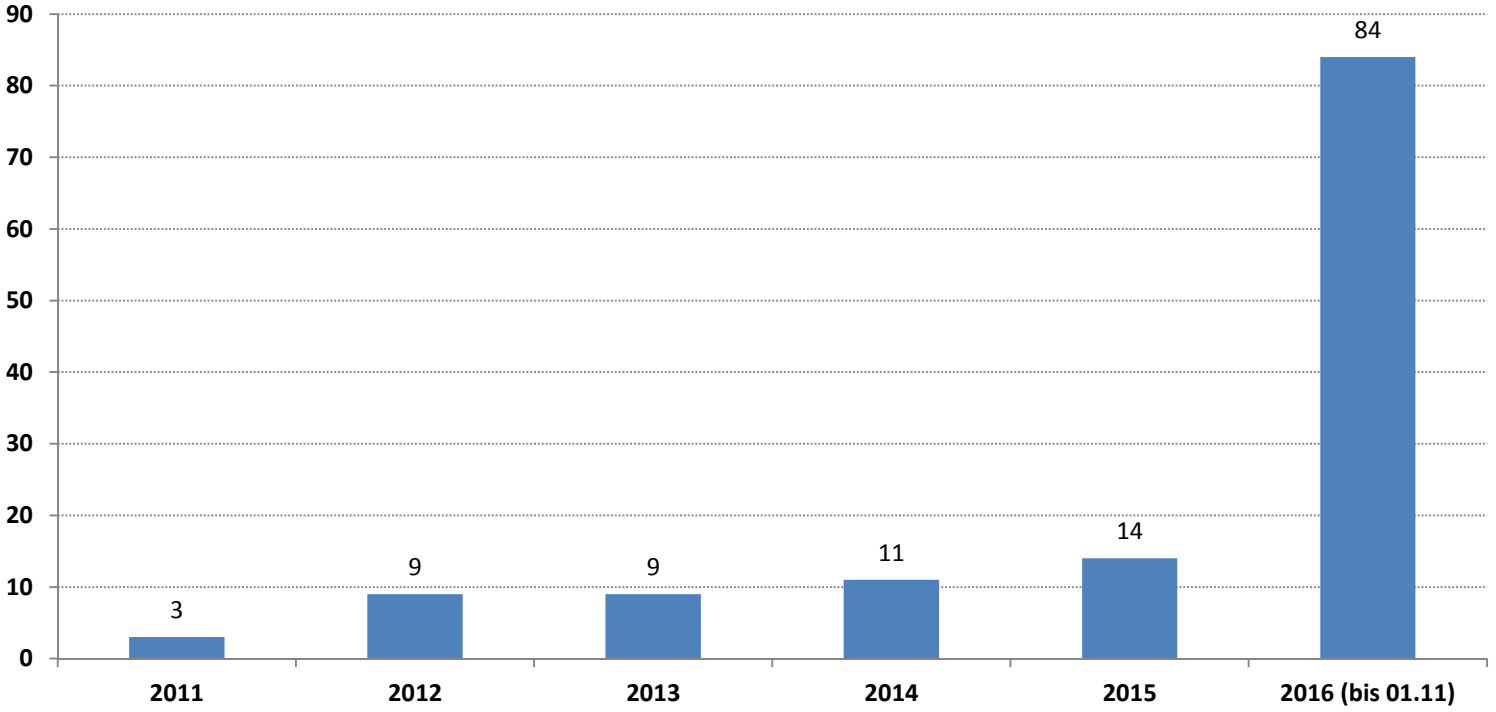
- LKA 543

Statistik

Entwicklung von Cybercrime?



Entwicklung CEO-Fraud in Hamburg



Tätertypen

CEO-Fraud

Sehr geehrte Frau M.,

ich kann doch in einer streng vertraulichen Finanzangelegenheit auf Ihre Unterstützung zählen. Unser Unternehmen plant eine Expansion in den asiatischen Geschäftsraum und wird hierzu eine existierende Firma übernehmen. Wie Sie sicher verstehen können, ist diese Transaktion streng geheim. Aus diesem Grunde und zu Dokumentationszwecken für die Bafin darf die gesamte Kommunikation mit mir ausschließlich per Mail erfolgen.

Mit der Abwicklung wurde das Schweizer Notariat E. betraut. Der Rechtsanwalt und Notar Dr. E. wird sich morgen telefonisch bei Ihnen bezüglich der Details melden.

Bitte bereiten Sie alles für eine entsprechende Auslandsüberweisung vor.

Ich weiß, dass ich mich auf Sie verlassen kann.

Mit freundlichen Grüßen

Dr. W., CEO

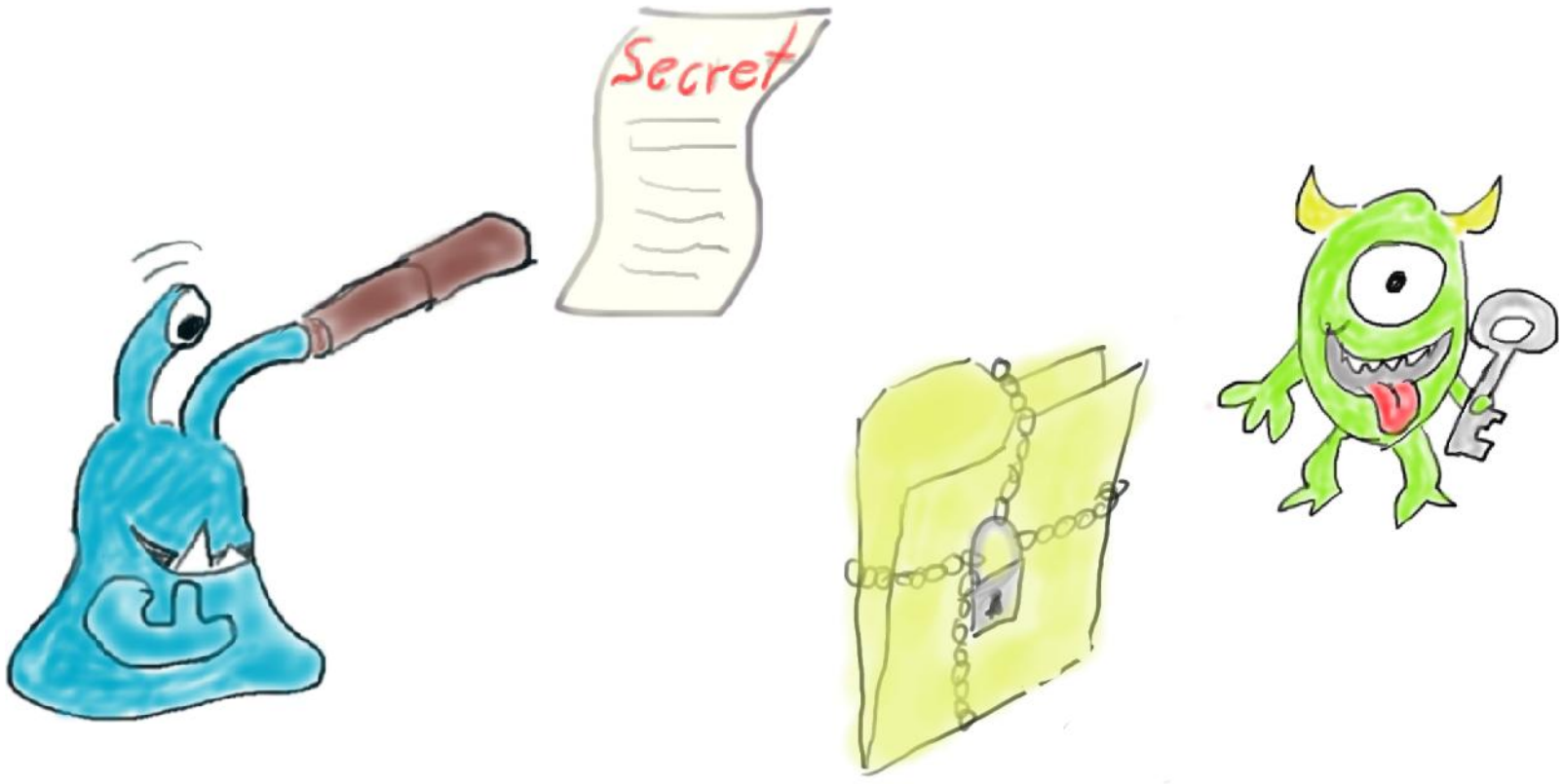
Mail-Kompromittierung

Informationsbeschaffung

Maßnahmen

- Awarenessmaßnahmen bei den Mitarbeitern
  - Betroffenen Personenkreis definieren (externe Dienstleister?)
  - Art der Maßnahme (Persönliche Schulung, Warnzettel, Webschulung)
  - Überprüfung der Durchführung und des Erfolgs der Maßnahmen
  - Regelmäßige Wiederholung der Maßnahmen
- Technische Möglichkeiten
  - Mailserverkonfiguration optimieren
    - Überprüfung interne/externe Mail
    - Bei externer Mail Überprüfung auf relevante Namen und Domains
    - ggf. Marker [CEO-FRAUD] setzen
  - Signaturen
- Klare Abläufe definieren
  - Keine Überweisung auf neue Konten ohne Rückfrage auf zweitem Weg (nicht per Mail!!!)
  - Regeln durch Geschäftsführung
    (z.B. Vieraugenprinzip, Stichwort für Überweisungen)

Malware



Malware

Ein Angestellter der Fa. L. erhält zunächst auf seinem privaten Smartphone eine Email mit einem Dateianhang, welchen er nicht öffnen kann. Diese enthält einen Anhang mit der Bezeichnung Rechnung. Er loggt sich vom Firmenrechner aus in seinem privaten Email-Konto ein und öffnet den Dateianhang, wodurch eine Schadsoftware auf dem Rechner installiert wird. Von dem Rechner verbreitet sich die Verschlüsselungssoftware durch interne Netzwerkfreigaben auf dem gesamten Serversystem des Unternehmens (ca. xx angeschlossene Server). Die betroffene Datenmenge hat einen Umfang von rund x,x TB Daten.

Es kommt zum Totalausfall der Produktion wodurch pro Tag ein Schaden im hohen 6-stelligen Bereich anzunehmen ist.

Die genaue Schadenshöhe derzeit noch unklar, da die Systemwiederherstellung derzeit noch mit Problemen verbunden ist, da Backupdateien von der Infektion betroffen sind.

Seitens des Unternehmens wurden zwei Zahlungen in Höhe von jeweils xxx,-Euro in Bitcoins vorgenommen. Daraufhin konnte ein Encoder zur Entschlüsselung geladen werden.

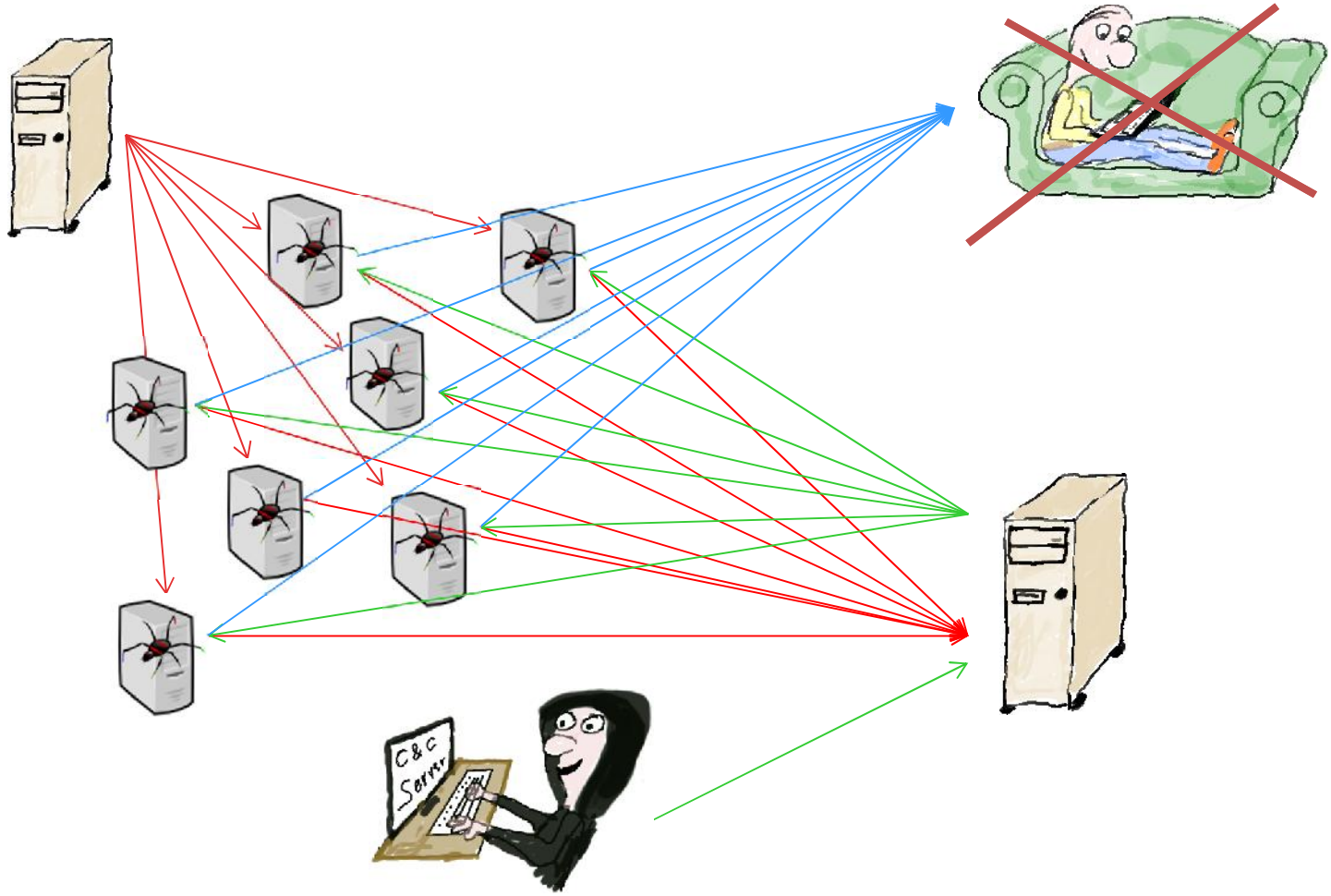
Wann die Produktion wieder gestartet werden kann, ist momentan noch unklar.

Maßnahmen

- Awarenessmaßnahmen bei den Mitarbeitern
  - Problem „Gutgläubigkeit“
  - Problem „Vertrauen in die IT“
- Regelmäßige Datensicherungen (Archivierung?)
- Regelmäßiges Einspielen von Updates
- Monitoring von Prozessen
- Application Whitelisting
- Antivirensoftware auf allen Systemen

DDoS

DDoS



DDoS

Hi!

If you dont pay 5 bitcoin until 1. february you will be hardly ddosed!
Our attacks are super powerfull (Mirai botnet). And if you dont pay until 1. february ddos attack will start and price to stop will double!
We are not kidding and we will do small demo now on just one of your servers xxx.xx.xxx.xxx to show we are serious. It will not be strong, we dont want damage now we hope you cooperate, just small flood to show we are not hoax.
Pay and you are safe from us forever. Ignore, you go down longtime and price go up.
OUR BITCOIN ADDRESS: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Dont reply, we will ignore!
Pay and we will be notify you payed and you are safe.

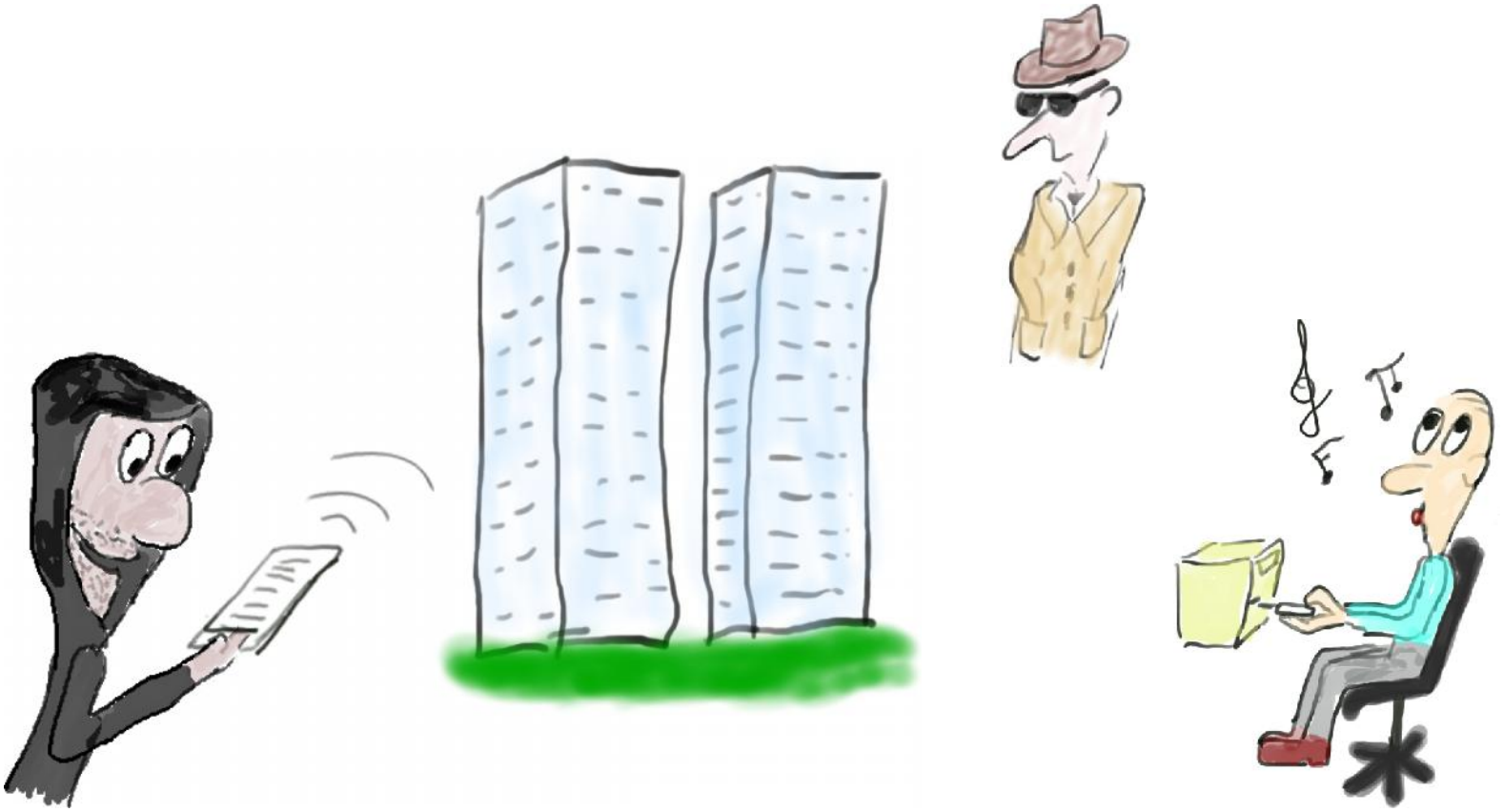
Cheers!

Maßnahmen

- Risikobewertung
  - ggf. betroffene Geschäftsbereiche?
  - Verluste (z.B. Onlineshops)
- Kontaktaufnahme mit ISP
- ggf. Beratung durch speziellen Anbieter

Bitcoin

Weitere Angriffsfelder



Maßnahmen

- Informationsarmut
- Einschlägige Sicherheitsmaßnahmen
  - Firewall
  - Monitoring
  - AV-Lösungen
  - ggf. (H|N)IDS, ISMS
- Rechtemanagement
- Awareness auch/gerade auf Führungsebene
- Regelungen bei Mitarbeiterwechsel

Polizei

Ermittlungsmöglichkeiten

- CEO-Fraud
  - E-Mailadresse?
  - IP-Adresse aus Header?
  - ggf. Rufnummer?
  - ggf. Bankverbindung?

- Ransomware / DDoS
  - E-Mailadresse?
  - IP-Adresse aus Header?
  - Bitcoin-Adresse?

Gründe für Cybercrime

Ursachen für Erfolge der Täter

- IT-Sicherheit als Zustand betrachten
- Unzureichende Awarenessmaßnahmen
- Updates nicht eingespielt
- Kostenfaktor IT-Sicherheit
- Komplexität der Unternehmensstruktur
- Komplexität der Software
- Gewachsene Systeme
- Unzureichendes Rechtemanagement
- Unklare Abläufe bei Abgang von Mitarbeitern

Incident Response

Planen Sie den Sicherheitsvorfall bevor er passiert!

- Machen Sie eine Risikoanalyse!
- Verantwortliche(n) im Vorwege benennen!
- Woher bekommt man Bitcoins?
- Analyse des Angriffs (Kosten/Nutzen)?
- Polizei einschalten: ja / nein?
- Sicherung von Beweismitteln vs. Produktivität
- Umgang mit Medien / Presse
- ggf. Umgang mit Kunden
- usw.

Ermittlungen 2025?

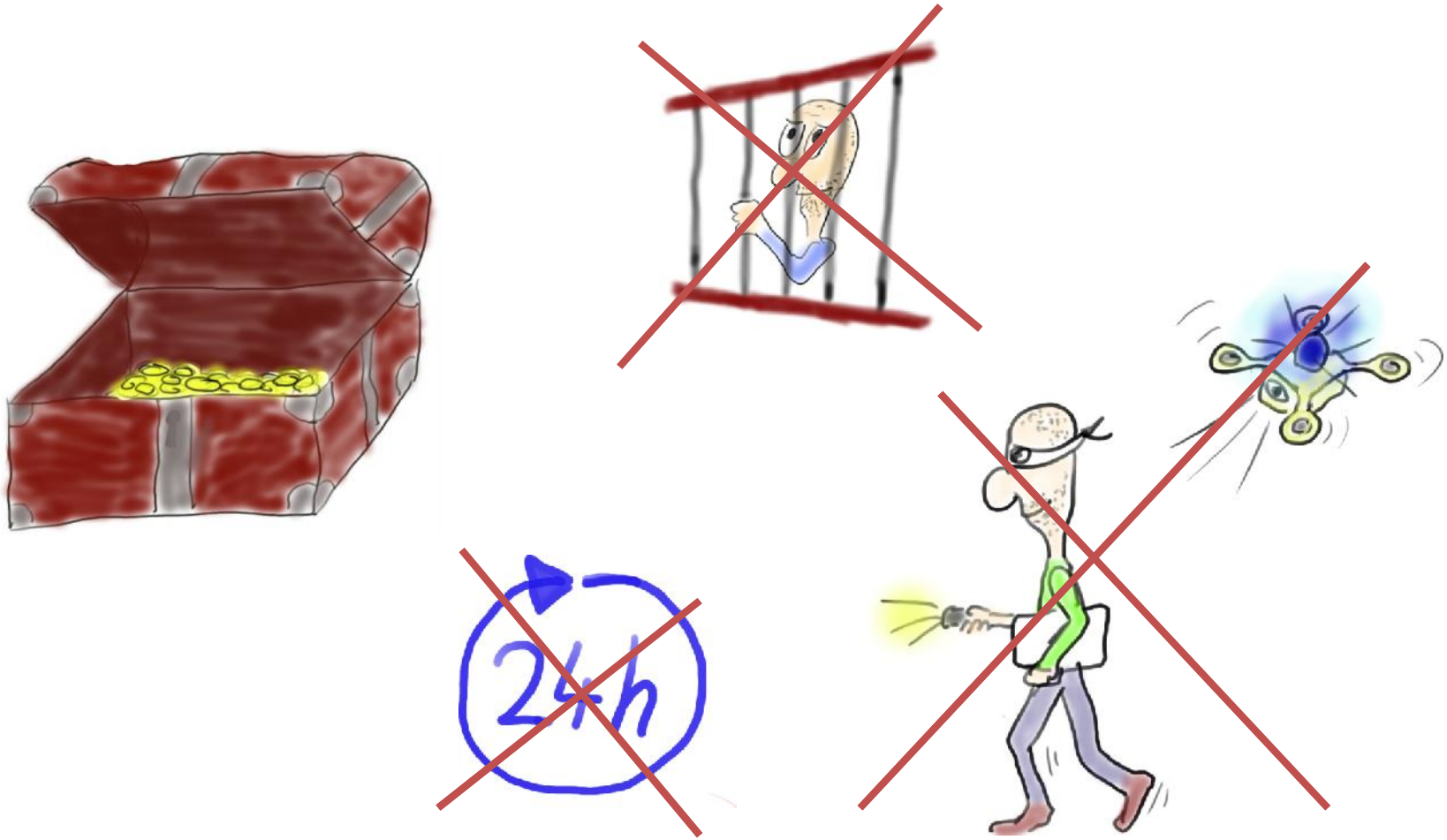
- Neue Kriminalitätsfelder
  - Industrie 4.0
  - Smart Home
  - weitere Verlagerung bestehender Kriminalität
- Weniger Ermittlungsmöglichkeiten
  - Verschlüsselung von Geräten
  - Verschlüsselung von Kommunikation
  - Verschlüsselung von Webseiten
- Neue Rechtsgrundlagen?

Ermittlungen 2025?

Wünsche

- Politik
  - Ehrlicher Umgang mit dem Problem
- Unternehmen
  - Besseres Monitoring / Reaktionsschnelligkeit
- Hersteller
  - Höhere Qualität / langfristigen Support

Kriminologie



Gewinne bei Cybercrime

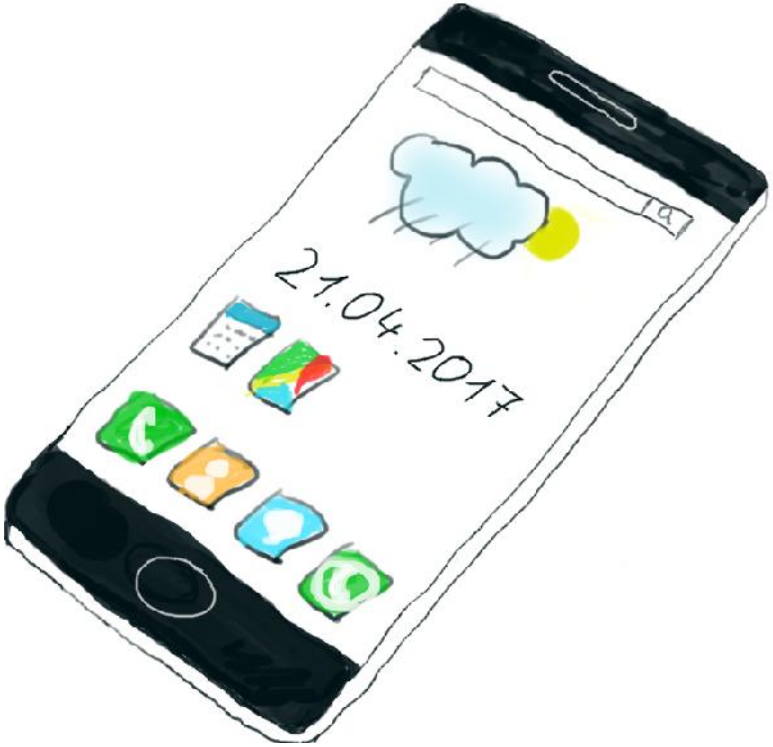
Straftat/Gewinn		Ursache
CEO-Fraud	→	User
Malware	→	User
Betrug	→	User
DDoS	→	User

Stichwort: User-Prävention!

Entwicklung 1987 - 2017

Kommunikation 1987

Entwicklung 1987 - 2017



Kommunikation 2017

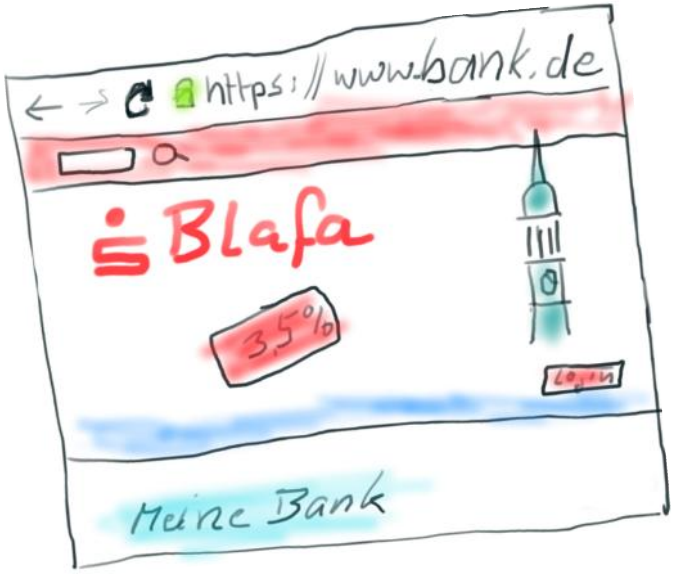
Entwicklung 1987 - 2017

Geld und Waren 1987

Entwicklung 1987 - 2017

amazon

ebay

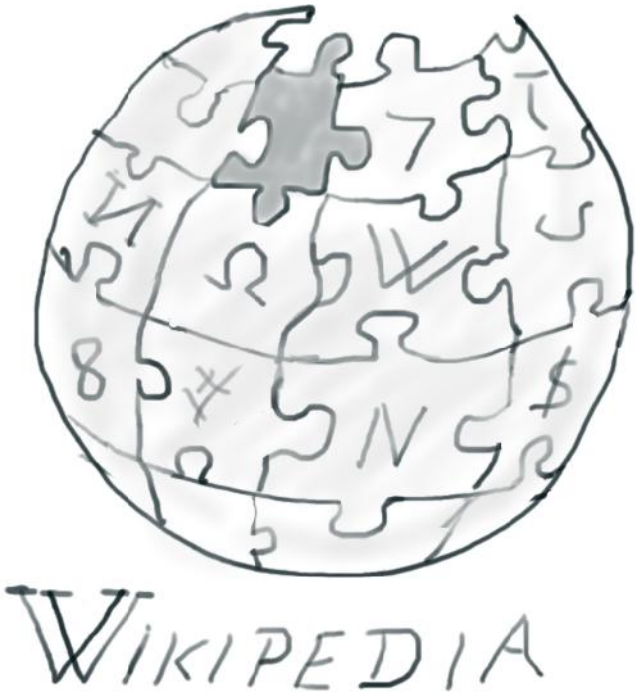


Geld und Waren 2017

Entwicklung 1987 - 2017

Referat vorbereiten 1987

Entwicklung 1987 - 2017



Referat vorbereiten 2017

Entwicklung 1987 - 2017

Informatikpflichtstunden 1987

(in Hamburg)

0

Entwicklung 1987 - 2017

Informatikpflichtstunden 2017

(in Hamburg)

0

zum Vergleich (Klasse 5-10): Theater: 76

Musik und Kunst je: 152, Sport: 684

Bildung

Die Medienerziehung, die Erziehung zur Medienmündigkeit und zu einem vernünftigen Umgang mit Medien, muss in den Elternhäusern stattfinden.

Josef Kraus, Präsident Deutscher Lehrerverband,
Interview in der Tagesschau vom 19.04.2017

Fazit

Es wird nicht besser!

Vielen Dank für Ihre Aufmerksamkeit

Polizei Hamburg
LKA 543
Bruno-Georges-Platz 1
22297 Hamburg
Tel: +49(0)40 4286-75455
Fax: +49(0)40 4279-99141
E-Mail: zac@polizei.hamburg.de