LKA 543
Hamburg

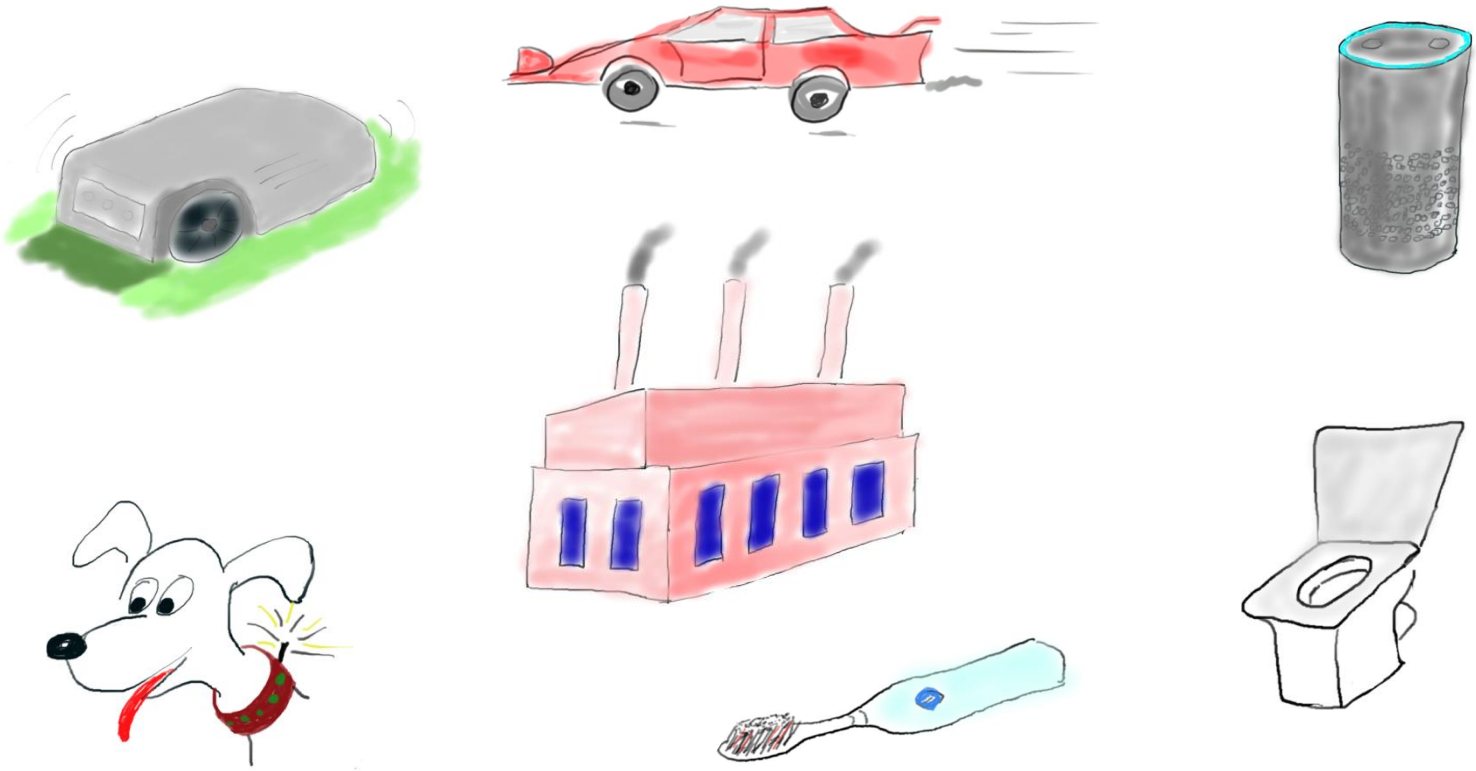
Cybercrime

Aktuelle Phänomene und Handlungsempfehlungen der Polizei Hamburg

Agenda

- Einleitung ins Thema
- CEO-Fraud / Payment Diversion Fraud
- Malware spez. Ransomware
- DDoS und weitere Angriffsfelder
- Polizei / Ermittlungen
- Maßnahmen
- Fazit

Digitalisierung



Exponentielle Entwicklung

Technologischer Fortschritt	Dauer
1900 - 1970	70 Jahre
1970 - 2000	30 Jahre
2000 - 2010	10 Jahre
2010 - 2014	4 Jahre

Tätertypen

CEO-Fraud

CEO-Fraud 2015/2016

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

CEO-Fraud 2017/2018

Guten Marion,

Was ist unser Bankguthaben?

Können wir heute 70T bezahlen?

Gruß

Thomas Meier

Geschrieben von iPhone

CEO-Fraud 2017/2018

OK. Bitte zahlen

Account Name: xxxx

Bank Name: xxxx

IBAN: xxxx

Bank Address: xxx

Zweck der Bezahlung: Neuer technischer Maschinenkauf

69.359,- Euro

Senden Sie mir eine Zahlungsbestätigung

Gruß

Thomas Maier

Gesendet von iPhone

Payment Diversion Fraud

E-Mailmanipulation

Thomas Meier thomas.meier@meinewelten.de

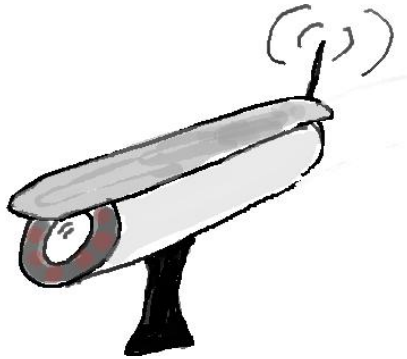
Thomas Meier thomas.meier@meinewelten.com

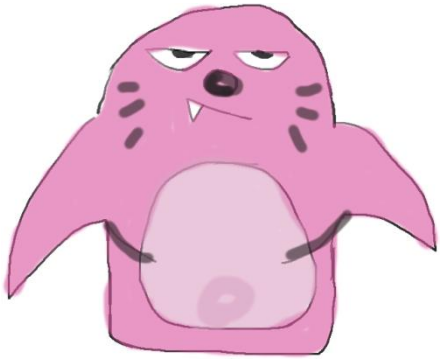
Thomas Meier thomas.meier@meinewellen.de

Thomas Meier thomas.meier@rneinewelten.de

Thomas Meier thomas.meier@meineweiten.de

Informationsbeschaffung

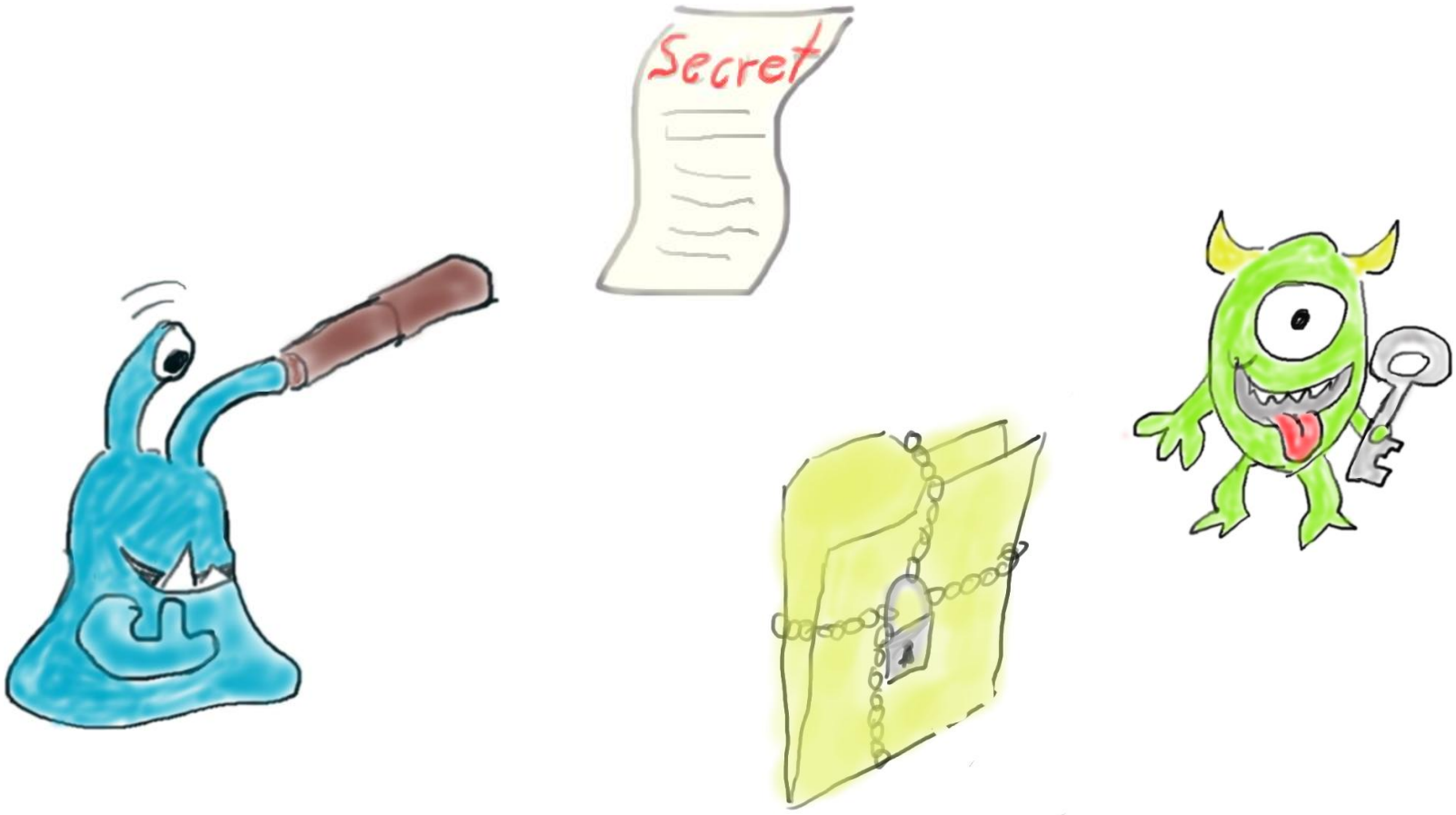




Maßnahmen

- Awarenessmaßnahmen bei den Mitarbeitern
- Technische Maßnahmen / Passwortsicherheit
- Klare Abläufe definieren
- Strategien der Geschäftsführung

Malware



Malware

Fall 1

Ein Angestellter öffnet eine Bewerbungsmail auf seinem Arbeitsplatz-PC. Aufgrund eines mangelhaften Rechtemanagements kann die enthaltene Schadsoftware sämtliche Netzwerkfreigaben und das Backup des Unternehmens verschlüsseln. Die Firma ist gezwungen das Lösegeld zu zahlen, da ansonsten das Fortbestehen gefährdet ist.

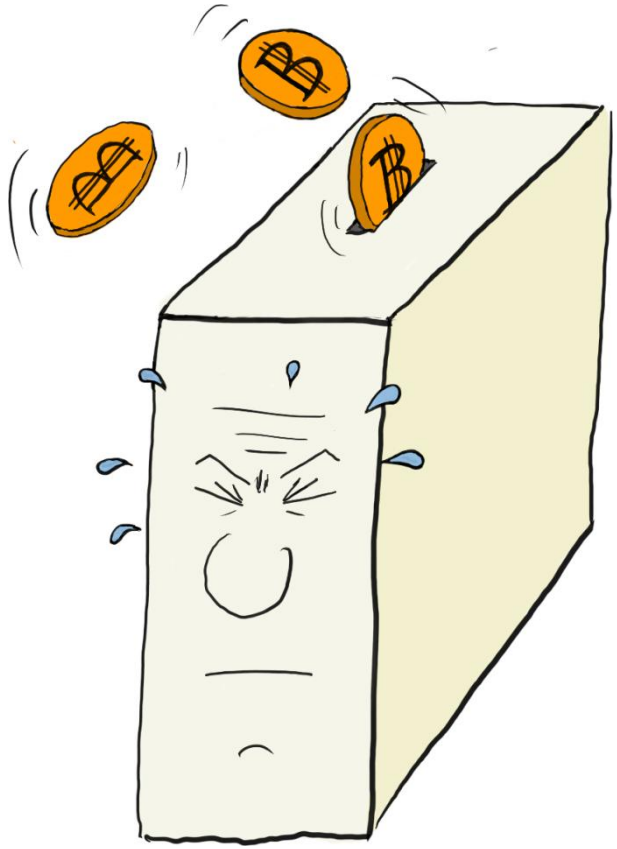
Fall 2

Ein Angestellter erhält auf seinem privaten Smartphone eine Email mit einem Dateianhang, welchen er nicht öffnen kann. Er loggt sich vom Firmenrechner aus in seinem privaten Email-Konto ein und öffnet den Dateianhang. Von dem Rechner verbreitet sich die im Anhang enthaltene Verschlüsselungssoftware auf dem gesamten Serversystem des Unternehmens. Es kommt zum Totalausfall der Produktion wodurch pro Tag ein Schaden im hohen 6-stelligen Bereich anzunehmen ist.

Fall 3

Über einen Updateprozess wird eine Schadsoftware auf einem Unternehmenscomputer eingespielt. Diese verbreitet sich unter Ausnutzung von Sicherheitslücken auf allen erreichbaren Rechnern im gesamten Firmennetzwerk und verschlüsselt zu einem vordefinierten Zeitpunkt sämtliche Systeme.

Krypto-Mining-Trojaner

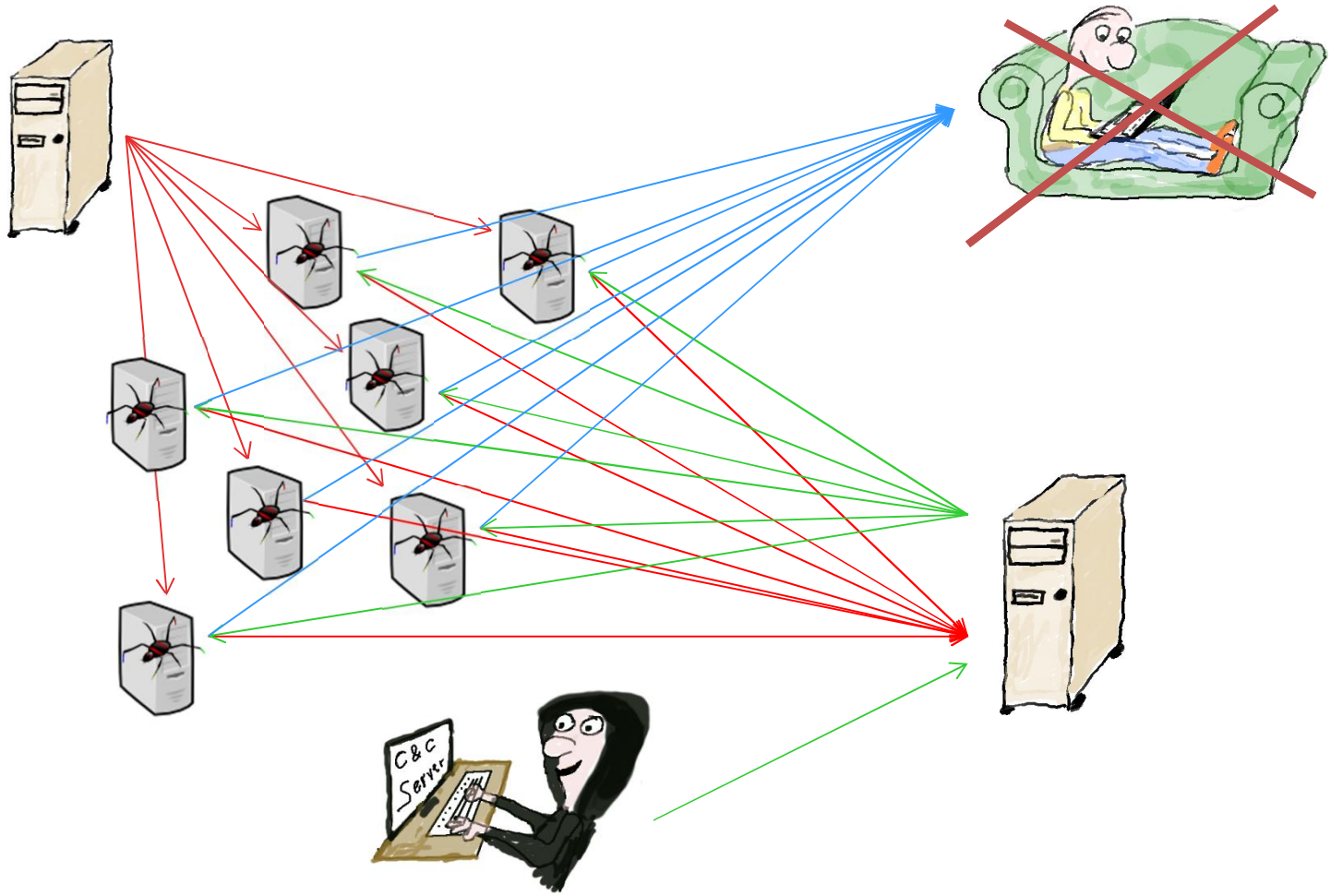


Maßnahmen

- Awarenessmaßnahmen
- Regelmäßige Datensicherungen
- (vernünftiges) Rechtemanagement
- Updates und Antiviren-Software

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.

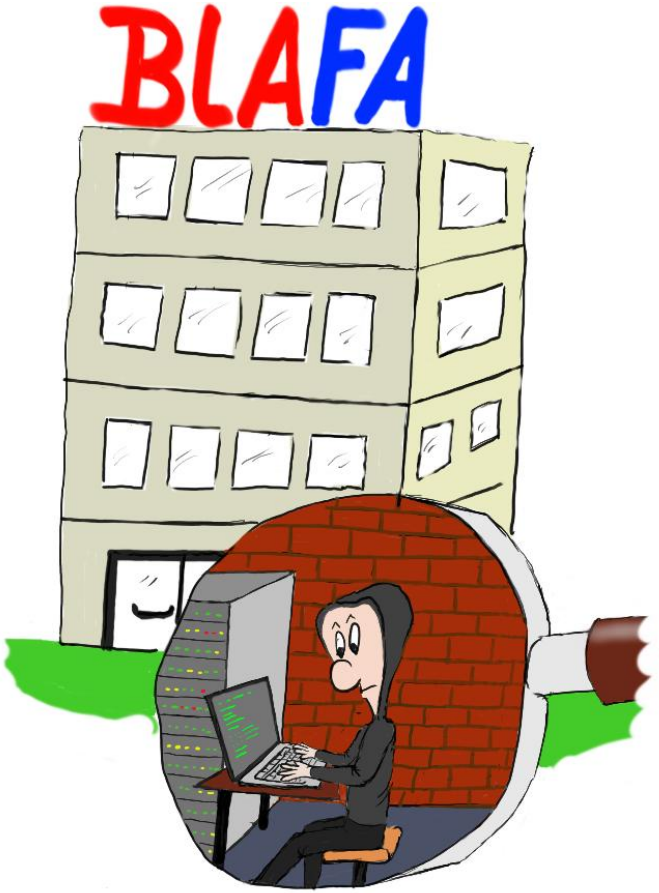
Cheers!

Webseitenangriffe

Phreaking

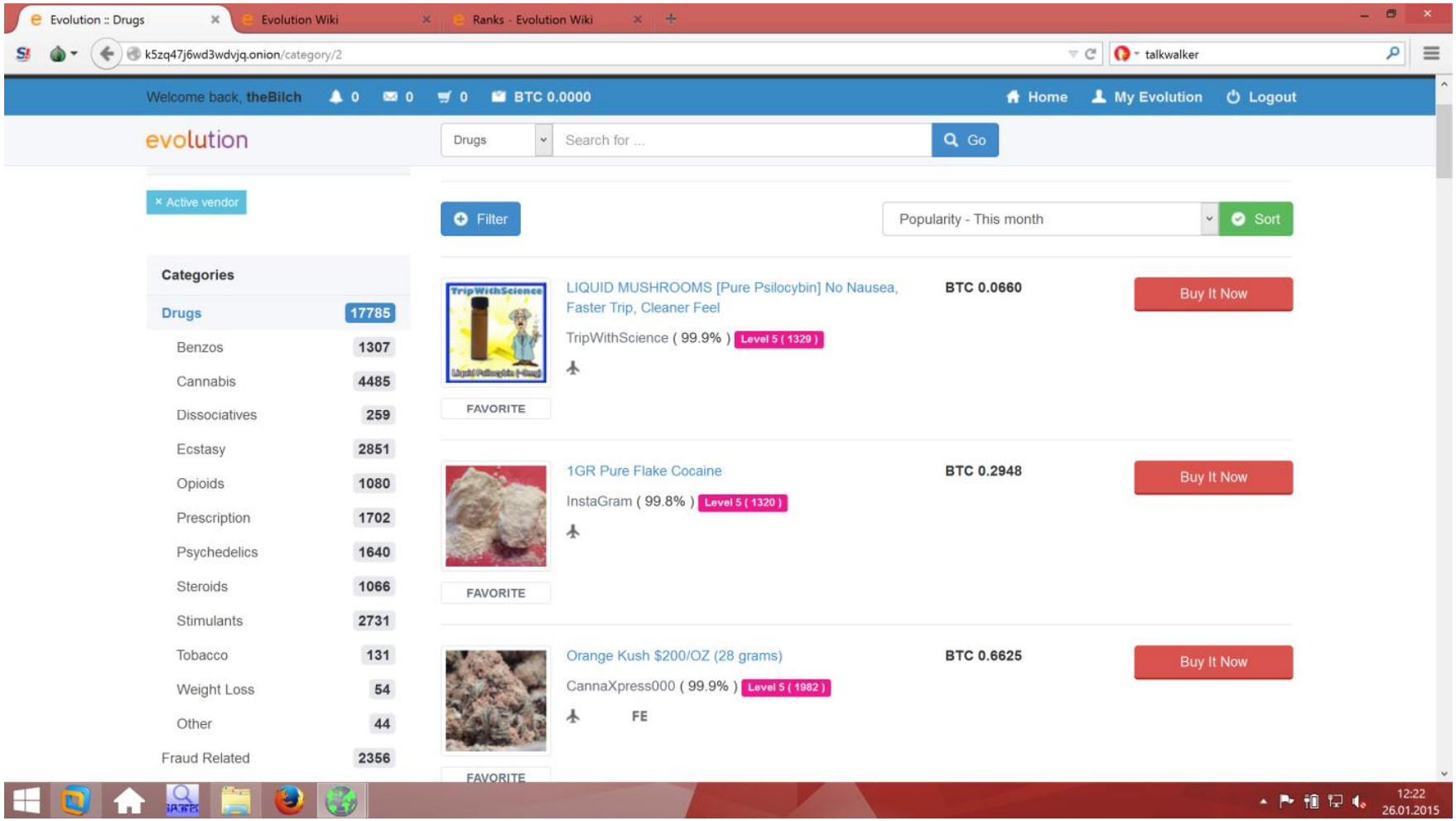
(Spear)-Phishing

APT-Angriffe



Bitcoin

Darknet


Evolution :: Drugs
Evolution Wiki
Ranks - Evolution Wiki
k5zq47j6wd3wdvjq.onion/category/2
talkwalker
Welcome back, theBilch 0 0 0 BTC 0.0000
Home
My Evolution
Logout
evolution
Drugs
Search for ...
Go
× Active vendor
Filter
Popularity - This month
Sort
Categories
Drugs 17785
Benzos 1307
Cannabis 4485
Dissociatives 259
Ecstasy 2851
Opioids 1080
Prescription 1702
Psychedelics 1640
Steroids 1066
Stimulants 2731
Tobacco 131
Weight Loss 54
Other 44
Fraud Related 2356
LIQUID MUSHROOMS [Pure Psilocybin] No Nausea, Faster Trip, Cleaner Feel
BTC 0.0660
Buy It Now
TripWithScience (99.9%) Level 5 (1329)
FAVORITE
1GR Pure Flake Cocaine
BTC 0.2948
Buy It Now
InstaGram (99.8%) Level 5 (1320)
FAVORITE
Orange Kush $200/OZ (28 grams)
BTC 0.6625
Buy It Now
CannaXpress000 (99.9%) Level 5 (1982)
FE
FAVORITE
12:22
26.01.2015

Polizei

LKA 54

- LKA 541

LKA 54

- LKA 542

LKA 54

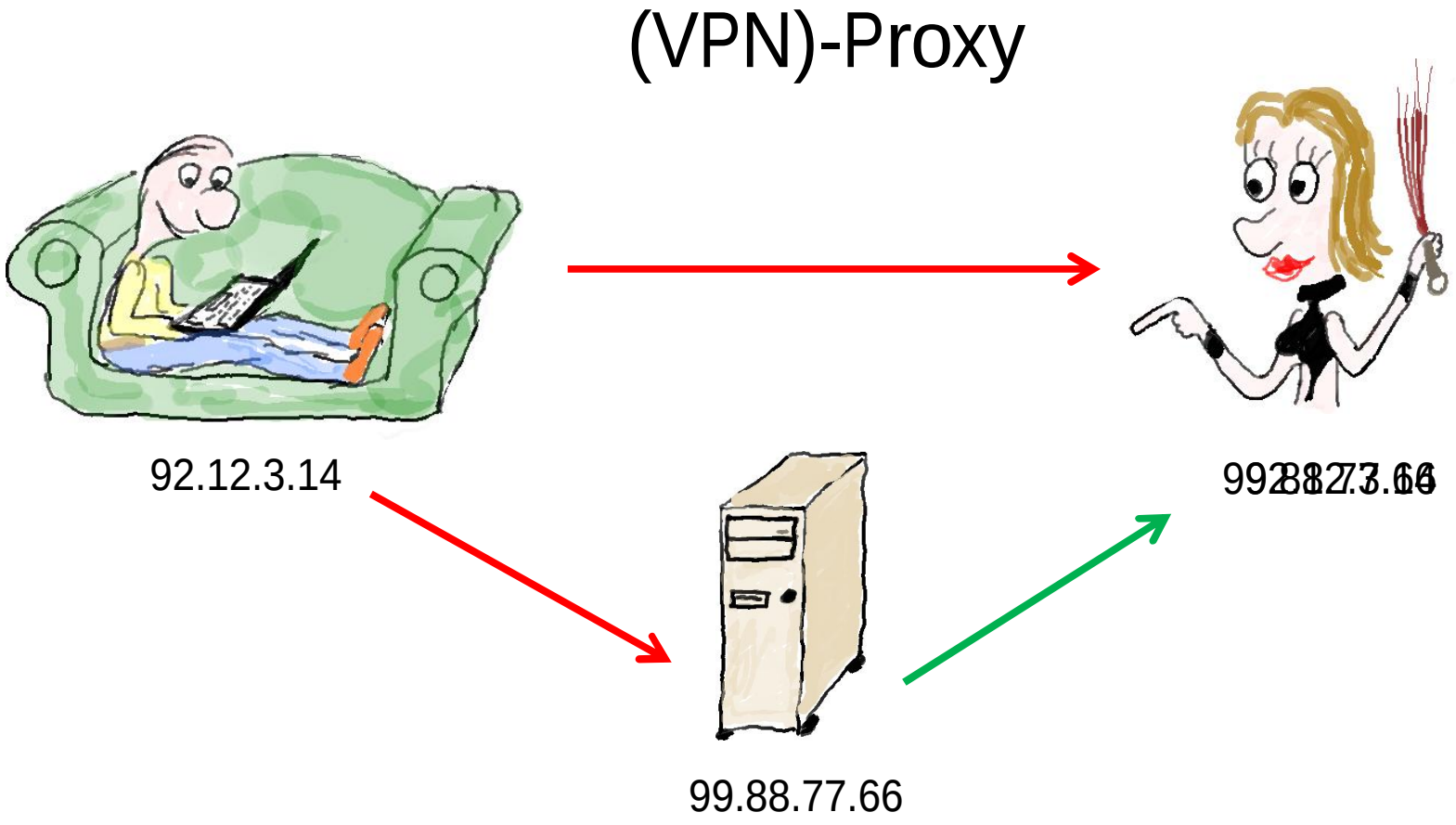
- LKA 543

Ermittlungsmöglichkeiten

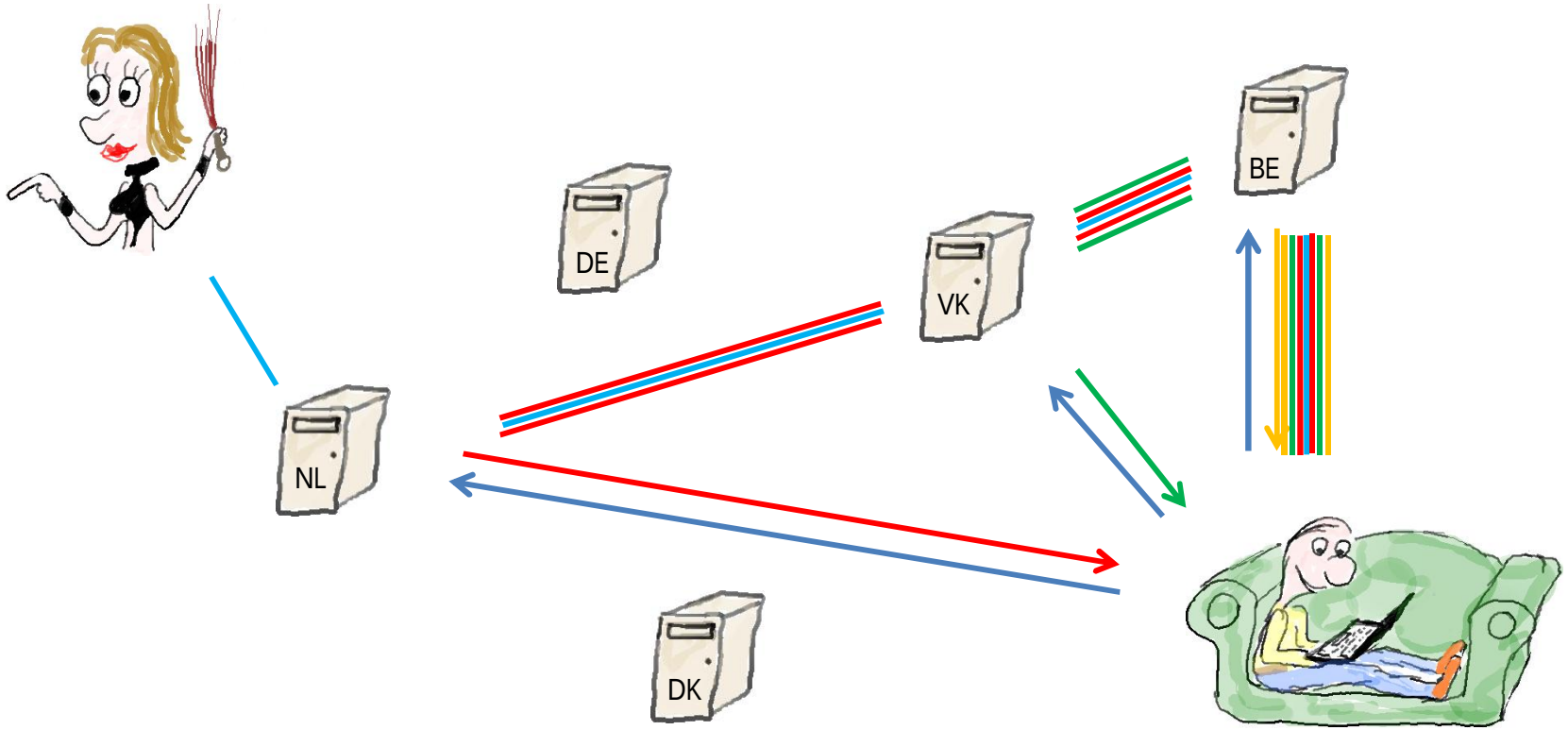
- CEO/Payment-Diversion-Fraud
  - E-Mailadresse?
  - IP-Adresse aus Header?
  - ggf. Rufnummer?
  - ggf. Bankverbindung?

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

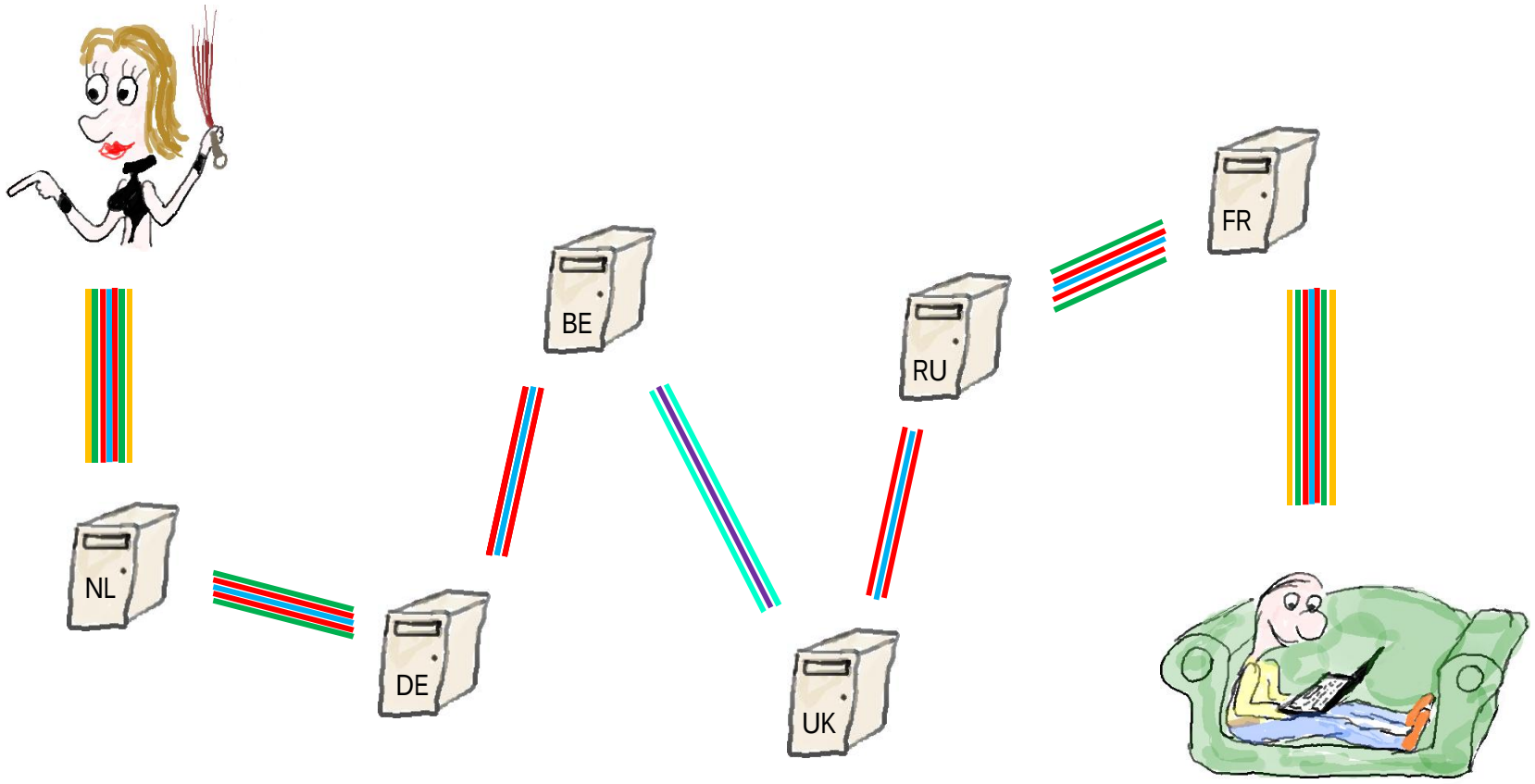
Anonymisierung



Tor Onion Routing



Tor Hidden Services



Datenmengen

Ein aktueller „Discounter-Computer“ hat
eine Festplatte von 3 TB (Terabyte)

Der Text wie vieler Jahrgänge der

„Hamburger Morgenpost“

könnten hierauf gespeichert werden?

(Eine Mopo enthält 50 Din-A4-Seiten a 3000 Zeichen.
Ein Zeichen entspricht einem Byte.)

Zeiten mit Papierbezug ;-)

um 1780 Erfindung der Kopierpresse

um 1455 Erfindung des Buchdrucks

um 350 Erfindung des Buches

um 50 v. Chr. Erfindung des Papiers

um 3.100 v. Chr. Erfindung von Schrift

um 30.000 v. Chr. Erste Höhlenmalerei

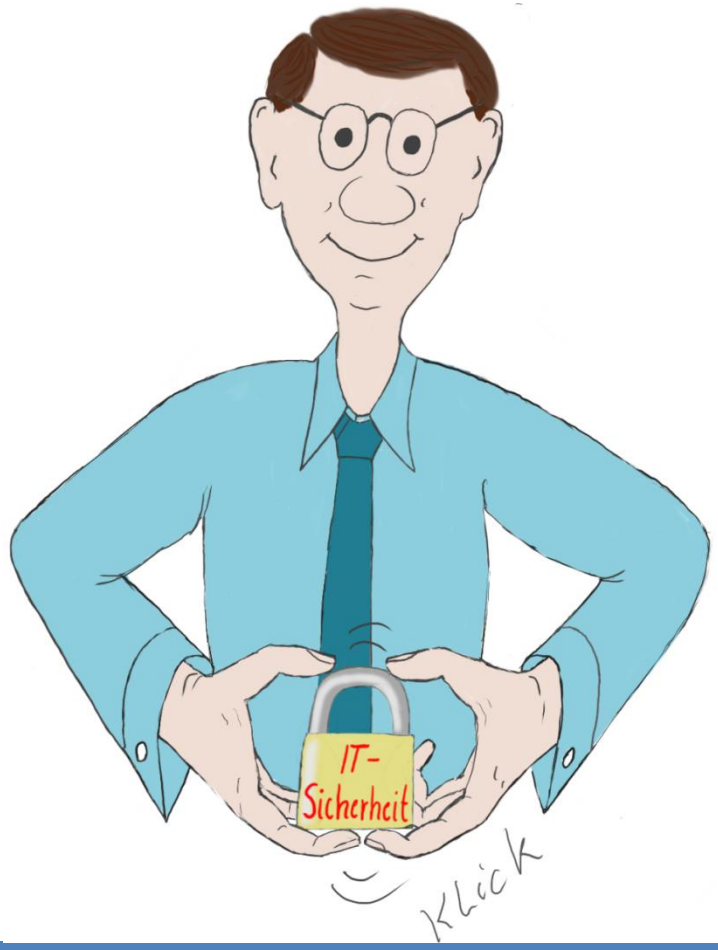
um 55.000 v. Chr. erste MOPO-Ausgabe

um 200.000 v. Chr. Entstehung Homo Sapiens

Ermittlungen 2020?

- Weitere Kriminalitätsfelder
  - Stetig neue Business-Modelle
  - „Smart“ City / Car / Home usw.
  - weitere Verlagerung klassischer Kriminalität
- Weniger Ermittlungsmöglichkeiten
  - Verschlüsselung von Geräten
  - Verschlüsselung von Kommunikation
  - Weitere Professionalisierung der Täter

IT-Sicherheit thematisieren!



IT-Sicherheitsrisiko

Schadenshöhe im Angriffsfall

x

Eintrittswahrscheinlichkeit

–

getroffene Maßnahmen

Gedankenfehler

- IT-Sicherheit nach dem Prinzip Hoffnung
- IT-Sicherheit als Zustand betrachten
- IT-Sicherheit beginnt beim Mitarbeiter

Faktor Mensch

IT-Sicherheitsanalyse

- Sachstand erfassen
  - Welche Daten besitzen wir?
  - Was sind unsere wichtigsten Daten?
  - Welche Maßnahmen wurden bereits getroffen?
  - usw.
- Maßnahmen erörtern und umsetzen
  - Maßnahmen klassifizieren und gewichten
  - Festlegung welche Maßnahmen wann umgesetzt werden sollen
  - usw.
- Erfolg kontrollieren
  - Wurden die Maßnahmen korrekt umgesetzt?
  - Dokumentation der Maßnahmen
  - usw.

IT-Dienstleister

Incident Response

Planen Sie den Sicherheitsvorfall bevor er passiert!

- Dokumentieren Sie Ihre IT-Struktur.
- Wer ist der verantwortliche Ansprechpartner?
- Woher bekommt man Bitcoins?
- Analyse des Angriffs (Kosten/Nutzen)?
- Polizei einschalten: ja / nein?
- Umgang mit Medien / Presse
- ggf. Umgang mit Kunden
- Meldepflichten?
- usw.

Home Sweet Home

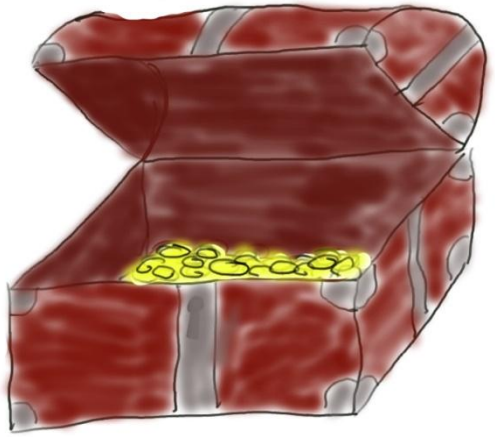
Heimnetzwerke sind heutzutage oftmals sehr komplex:

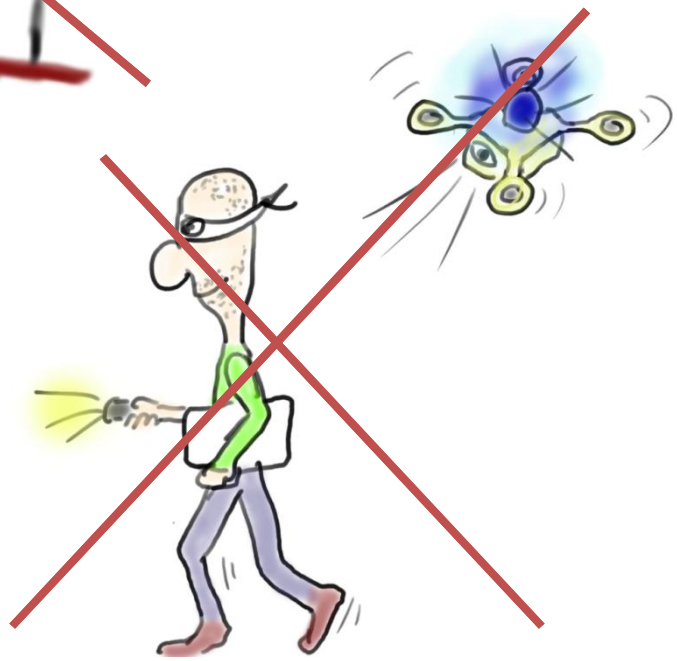
- Router, Repeater, Switche, Laptops, PCs, Tablets,
- Smartphones, Alexa, Philips Hue, IP-Cameras, NAS,
- SmartHome, Fernseher, Spielekonsolen usw.

Und die Sicherheit?

- Wer darf in IHR Heimnetzwerk?
- Wie sicher sind die Geräte Ihrer Angehörigen?
- Dürfen auch Freunde Ihrer Kinder in Ihr Netzwerk?
- Ändern Sie ggf. Ihr WLAN-Passwort?
- Wann haben Sie das letzte Backup erstellt?
- Ist Ihr Router auf dem aktuellen Softwarestand?
- usw.

Kriminologie





Gewinne bei Cybercrime

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

Stichwort: User-Prävention!

Entwicklung 1988 - 2018

Kommunikation 1988

Entwicklung 1988 - 2018

Kommunikation 2018

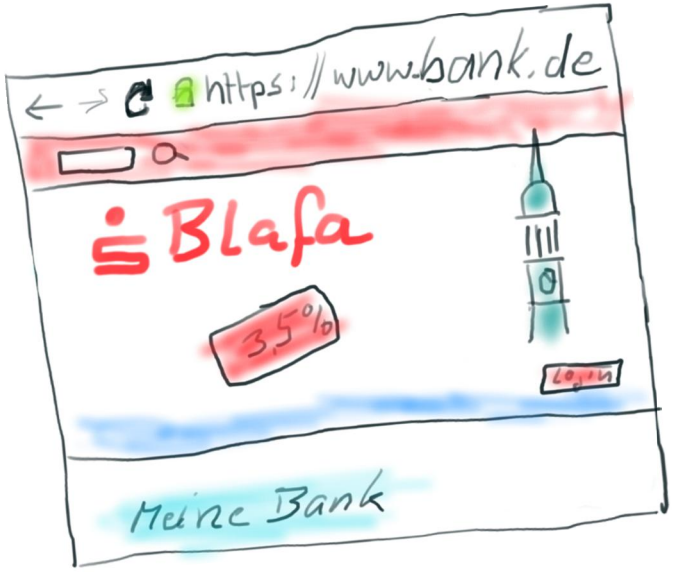
Entwicklung 1988 - 2018

Geld und Waren 1988

Entwicklung 1988 - 2018

amazon

ebay



Geld und Waren 2018

Entwicklung 1988 - 2018

Informatikpflichtstunden 1988

(in Hamburg)

0

Entwicklung 1988 - 2018

Informatikpflichtstunden 2018

(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, 1987-2017 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