LKA 543
Hamburg

Cybercrime

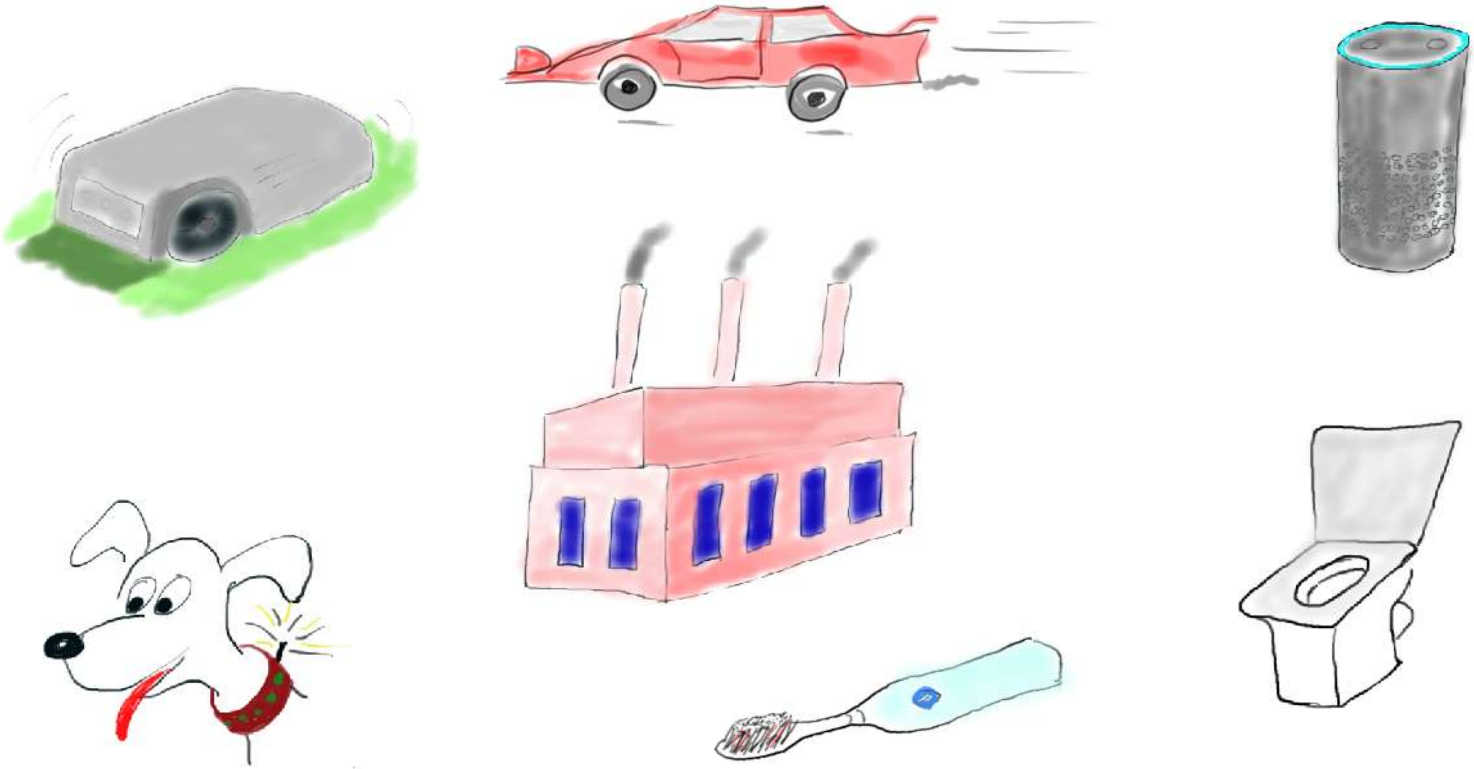
Aktuelle Phänomene und
Handlungsempfehlungen
der Polizei Hamburg

Steckbrief

Agenda

- Einleitung ins Thema
- CEO-Fraud / Payment Diversion Fraud
- Malware spez. Ransomware
- 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?

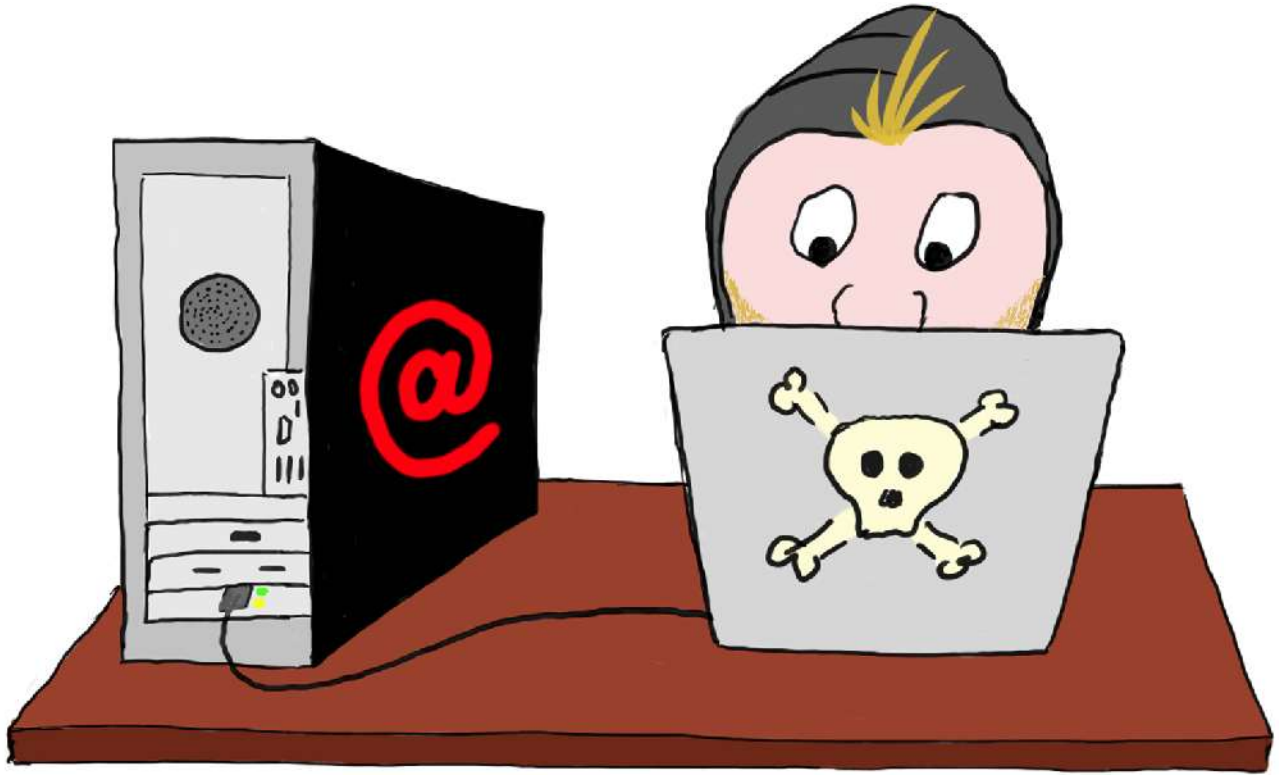
Können wir heute 70T bezahlen?

Gruß

Thomas Meier

Geschrieben von iPhone

Payment Diversion Fraud



E-Mailmanipulation

Thomas Meier thomas.meier@meinewelten.de

Thomas Meier thomas.meier@meinewelten.com

Thomas Meier thomas.meier@meinewellen.de

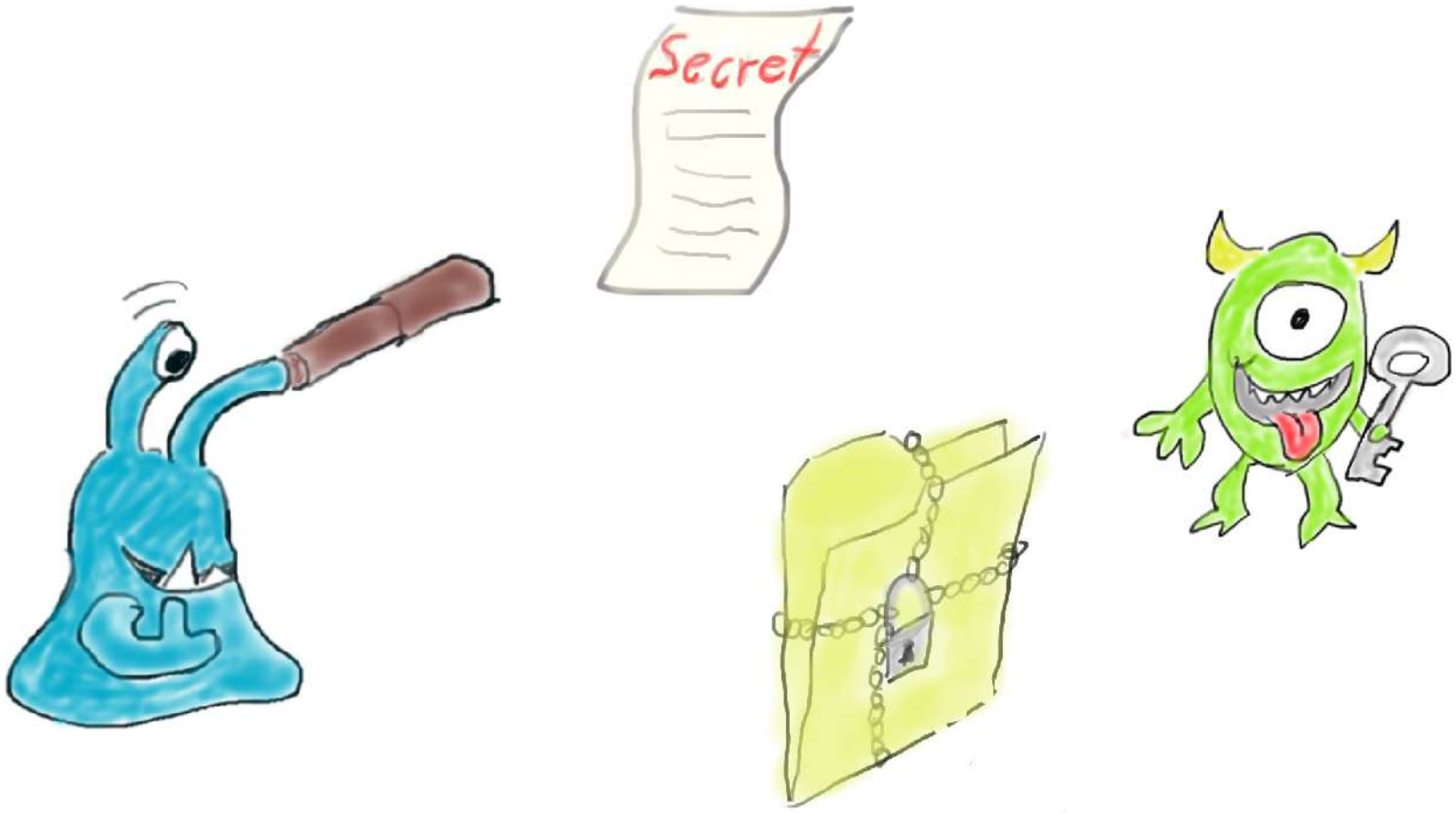
Thomas Meier thomas.meier@rneinewelten.de

Thomas Meier thomas.meier@meineweiten.de

Maßnahmen

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

Malware



Verschlüsselung

Klartext:

Nachstehend wurde dieser Text mit einem symmetrischen Schlüssel verschlüsselt. Eine symmetrische Verschlüsselung unterscheidet sich von einer asymmetrischen Verschlüsselung dadurch, dass bei der symmetrischen Verschlüsselung der gleiche Schlüssel zum Ver- und Entschlüsseln verwendet wird, bei der asymmetrischen Verschlüsselung hingegen zwei Schlüssel verwendet werden.

Schlüssel: „q2R#ki7Gg89p“

Geheimtext:

jA0ECQMCb8dO0fkRXjXn0sA8ATLaULYSsr1j25lu+d6nE2B7DfKkgH8Gs8bmwa+hWBVyfkS74AE0d/xXeJm4hP
F/7IUq/jw+Gjm/pFz7kfzqEjO0d5GwwPzAwy1viJmVjJPUEvL7Ku2r5fQBCX7dh2ePKGRGnTs0uM+4coX7BQ79S
WKtEZdWylC4Eevdq5+QLkb5cMzjgPQYj+fMYP35uM9orvZlZLdRjYB5wtJ3Oiq3ABnZheX7Gkf+ttbYQvnXuFW
AEIG7ds5vAcN3FVxVJKO8Wf5BFhjjK3juYnrfzt7rqDo10mUINJ1qZ35cOoHYPsGClg9KJ+DIi3NM8l85od550P5k
XLEguyS2ecQC=FdKr

Verschlüsselung

128 Bit Schlüssel = 2^{128} verschiedene Schlüssel:

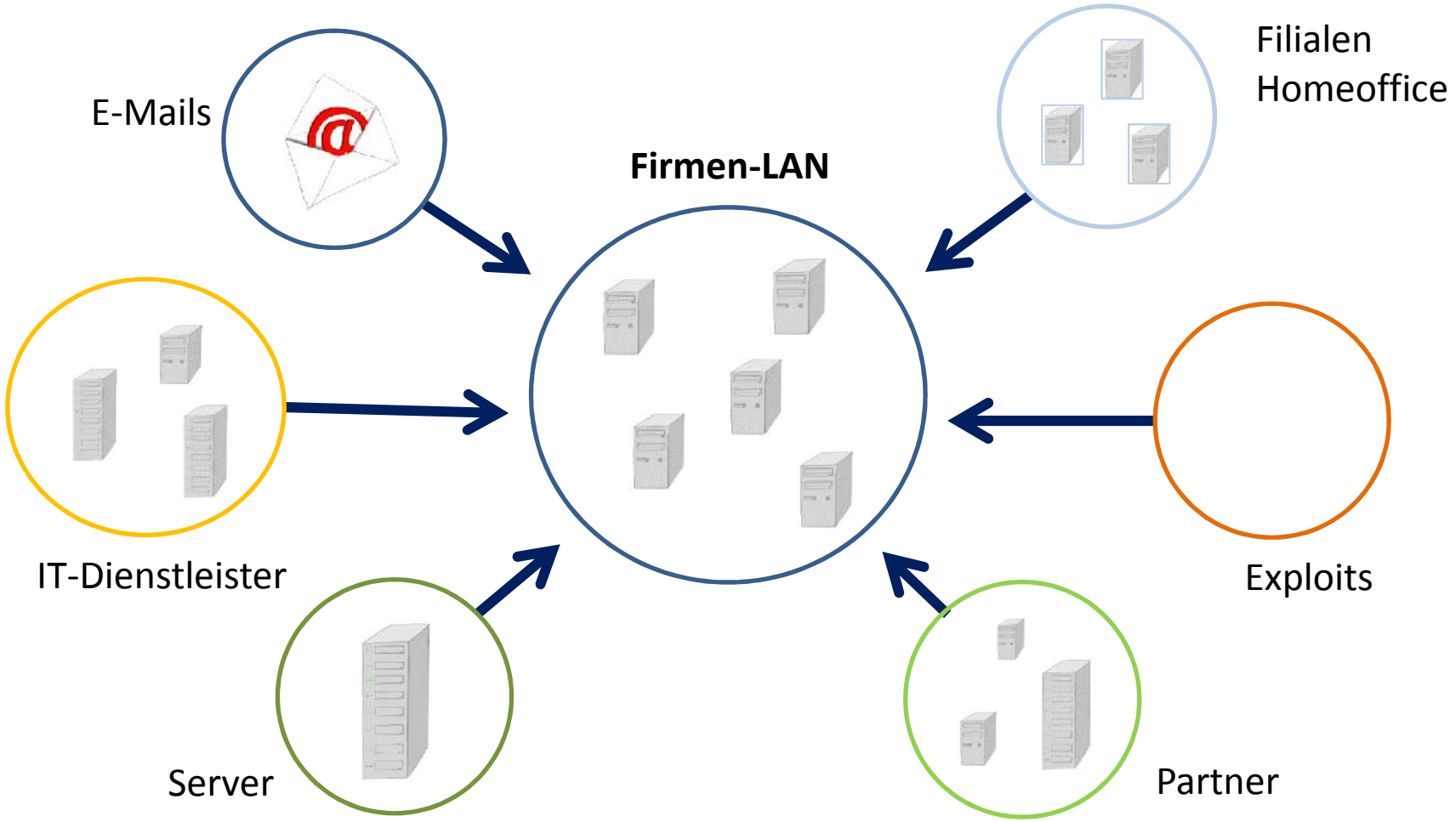
340.282.366.920.938.463.463.374.607.431.768.211.456

Zeitdauer des Durchprobierens aller möglichen Schlüssel:
(8 Milliarden Menschen mit PC probieren 10 Millionen Schlüssel pro Sekunde)

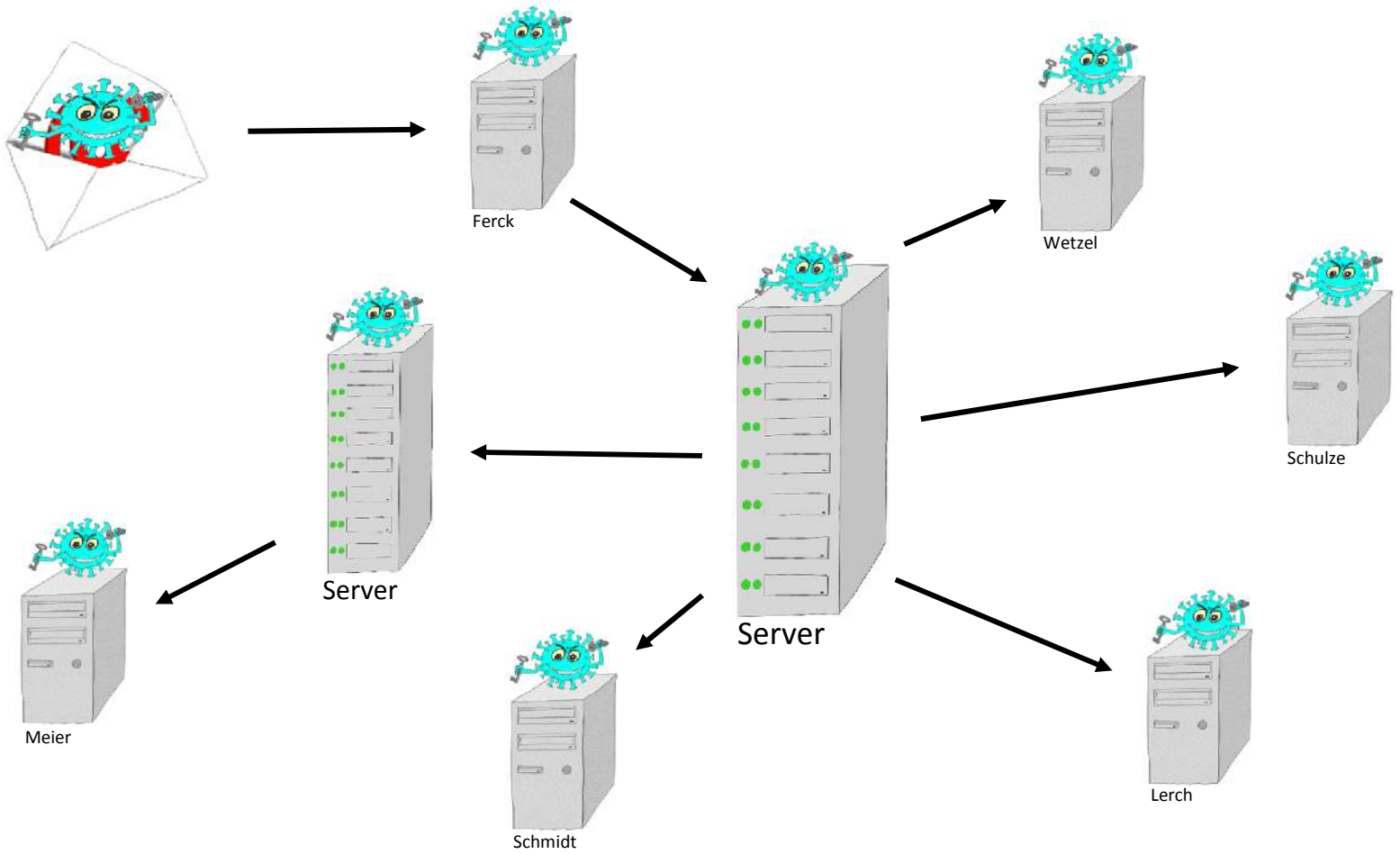
134.878.538.385.075 Jahre

Ziele der Schadsoftware

Infektionswege



Interne Verbreitung



Reale Beispiele

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.

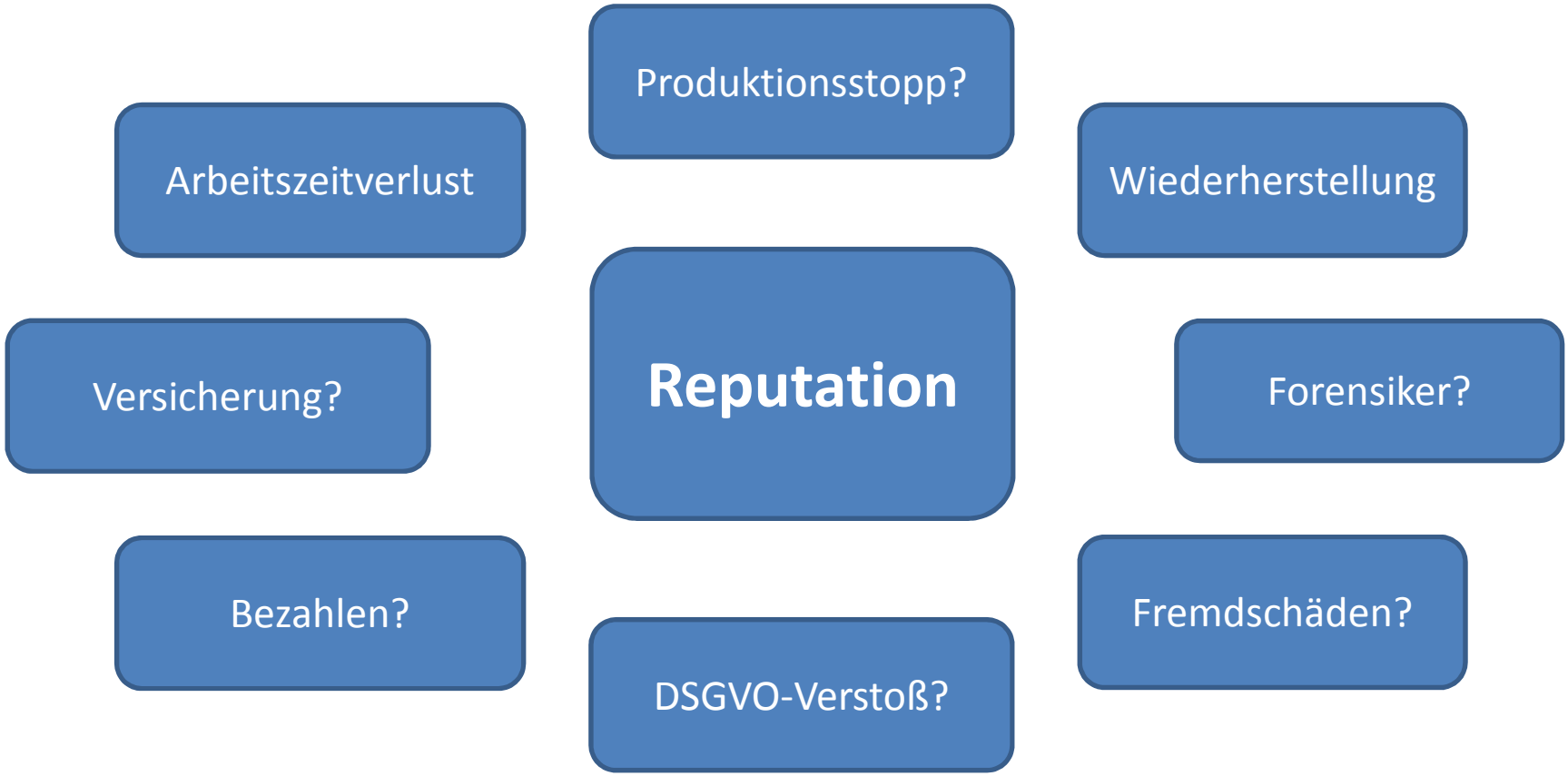
Fall 2

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.

Schäden / Kosten



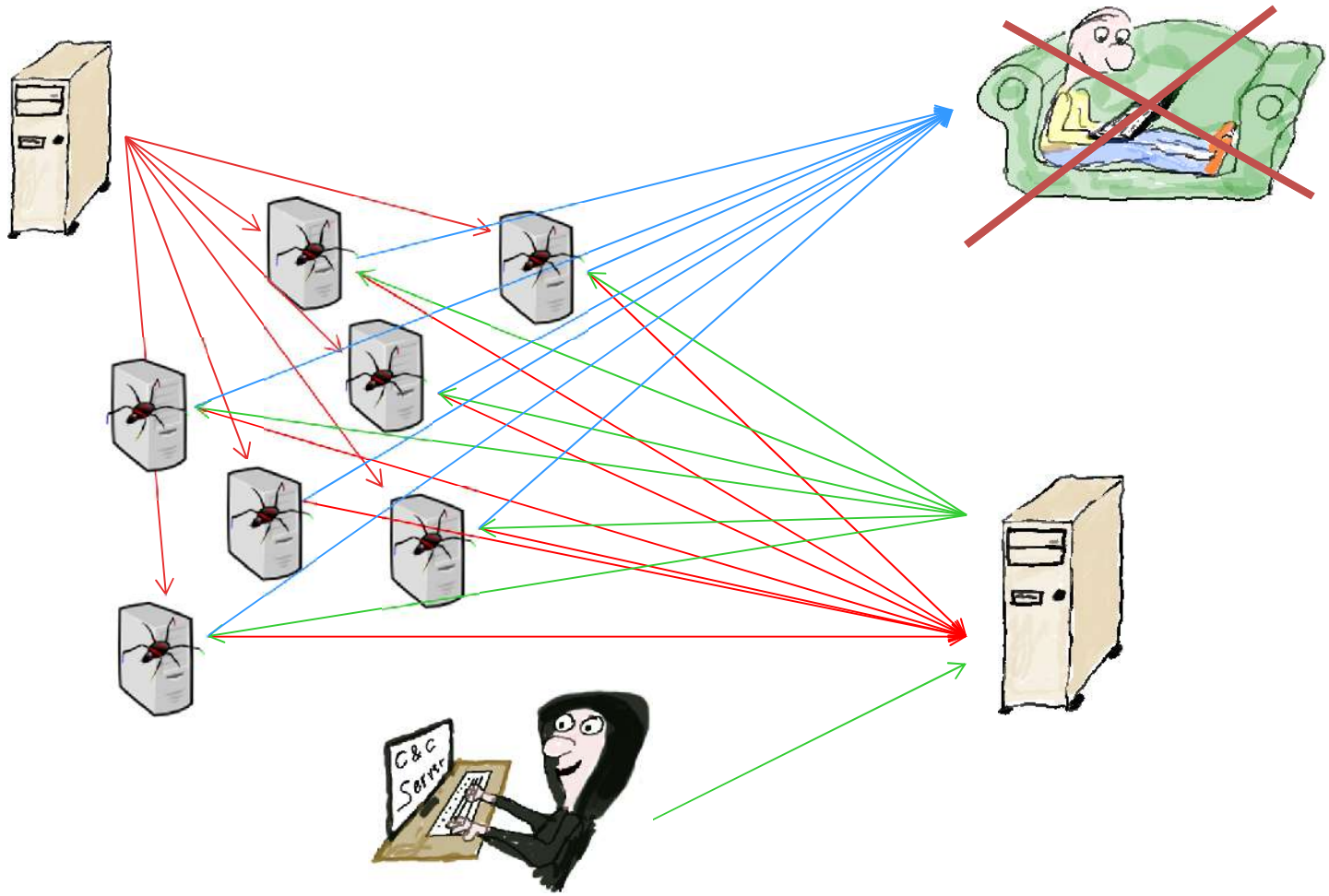
Maßnahmen

- Awarenessmaßnahmen
- Durchdachtes Datensicherungskonzept
- (vernünftiges) Rechtemanagement
- Updates und Antiviren-Software
- usw.

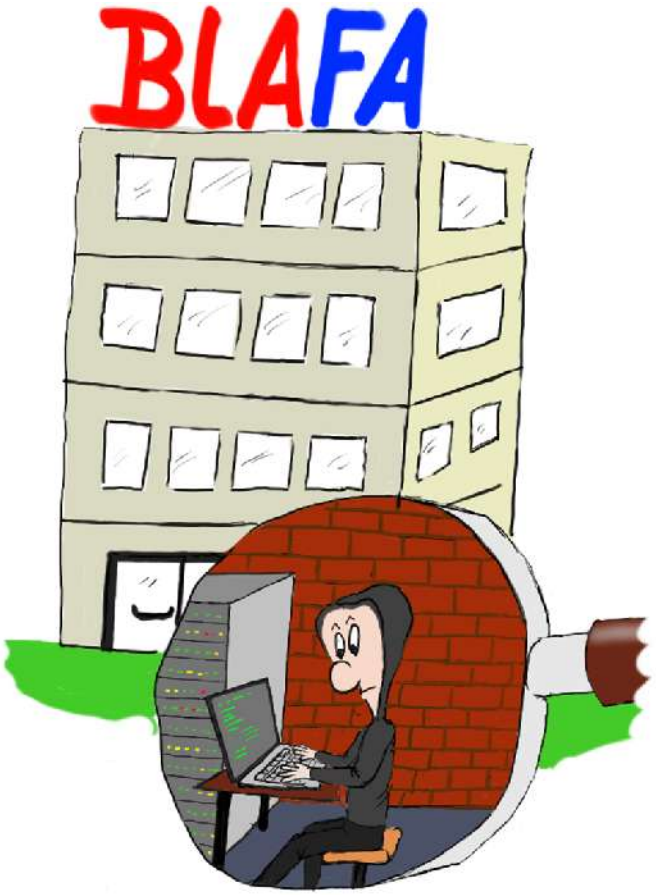
Webseitenangriffe

DDoS

DDoS



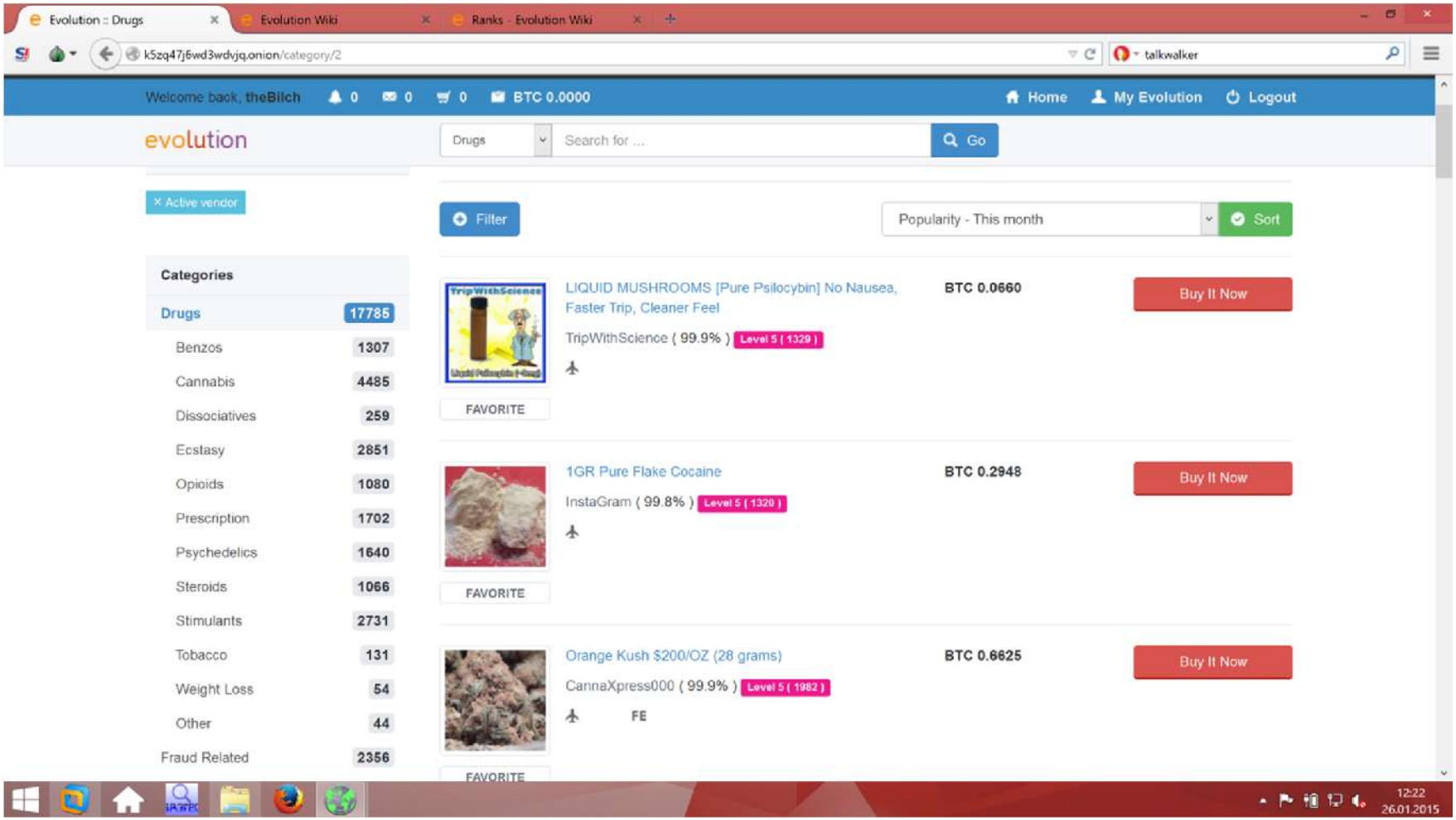
APT-Angriffe



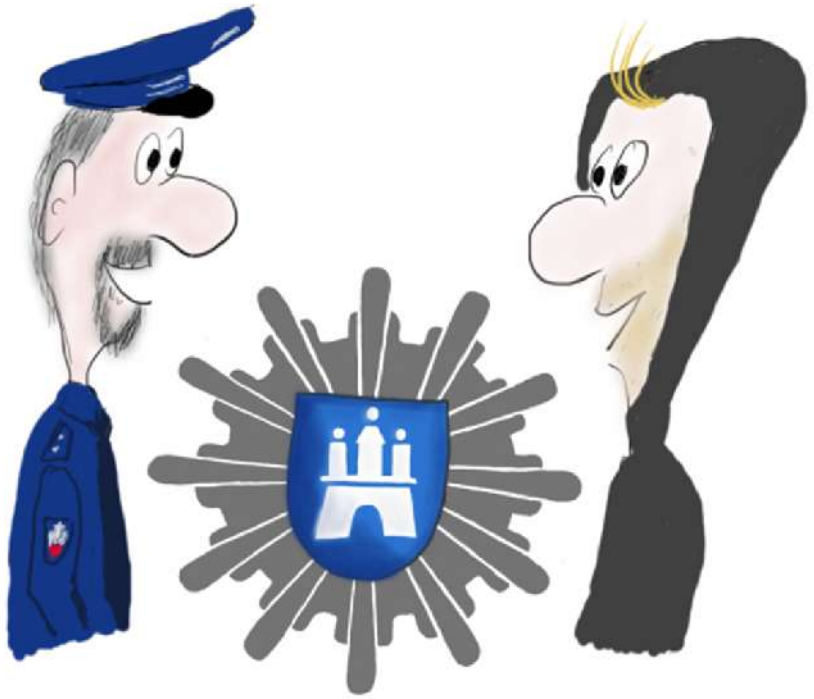
(Spear)-Phishing

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



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?

IT-Sicherheit thematisieren!

Gedankenfehler

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

Faktor Mensch

IT-Dienstleister

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.

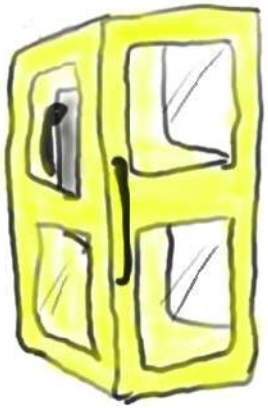
Private „Angriffe“

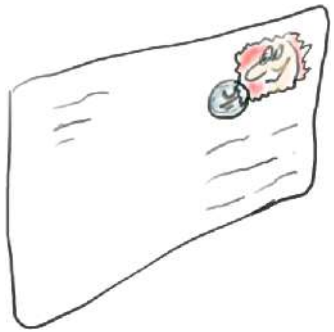
Gewinne bei Cybercrime

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

Stichwort: User-Prävention!

Entwicklung 1987 - 2020





1987

Entwicklung 1987 - 2020

amazon

ebay

2020

Entwicklung 1987 - 2020

Informatikpflichtstunden 1987

(in Hamburg)

0

Entwicklung 1987 - 2020

Informatikpflichtstunden 2020
(in Hamburg)

0

zum Vergleich (Klasse 5-10): Theater: 76
Musik und Kunst je: 152, Sport: 684

Fazit

Ihre Mitarbeiter sind der wichtigste Teil Ihrer Firewall!

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