
大成 DENTONS
it's.BB
IHK Berlin
Cybercrime
Neue Verteidigungsstrategien
16. September 2021
Object Security
M&H
HISOLUTIONS

Agenda

1. EMOTET – eine Erfolgsgeschichte
2. Cyberangriffe – Neue Verteidigungsstrategie

   Praxisfall – Was ist nach einem Cyberangriff zu tun?
   - Organisatorisch, aus IT-Sicht
   - Schadensbegrenzung vs. Beweissicherung
   - IT-Forensik
   - Zusammenarbeit mit den Strafverfolgungsbehörden
   - Lösegeldzahlungen
3. Melde- und Dokumentationspflichten
4. Die weiteren Folgen
5. Neue Ausrichtung bei der Cybercrime-Bekämpfung

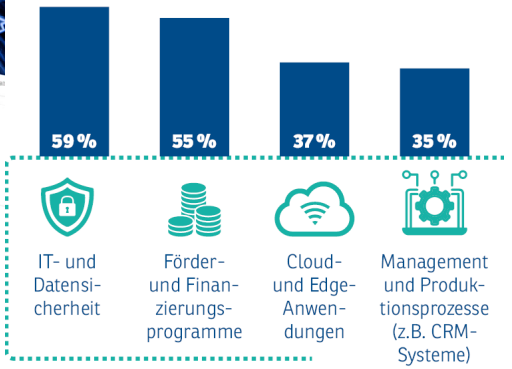
Über it‘s.BB e.V.

Ziele des Netzwerks

- Sensibilisierung des Bewusstseins für IT-Sicherheit in der Region Berlin-Brandenburg (BB)
- Umdenken in Prozessen und Systemen anstoßen
- Kompetenznetzwerk (POC) und vertrauenswürdiger Ansprechpartner
- Zusammenarbeit der IT Sicherheitsbranche in BB
- Einbeziehung weiterer Wirtschaftsbereiche der Region / Austausch mit Startup-Szene in BB
- Kooperation von Wissenschaft und Wirtschaft
- Entwicklung von Fachkräften für die Branche fördern
- Akquisition gemeinsamer Projekte zur IT-Sicherheit

Die Netzwerkmitglieder

IHK Berlin



Bedarf für Informations- und Beratungsangebote

Quelle: IHK Digitalisierungsumfrage Dez. 2020

Wissen, was schützt: Angebote der IHK Berlin

Informieren | Sensibilisieren | Vernetzen

Veranstaltungen

- Sicherheit zum Frühstück
- **IT-Sicherheitssprechstunde mit LKA Berlin 28.09.**
- Digitale Awareness-Reihe (mit it‘s.BB) **heute**
- **IT- Sicherheitstag Mittelstand 23.09.**
- Seminar EU-Datenschutz-Grundverordnung

www.ihk-berlin.de/sicherheitsveranstaltungen

Weitere Kanäle

- Online Informationsseite
- **Newsletter: „Unternehmenssicherheit: Tipps aus Berliner Expertenkreisen“ 23.09.**
- Transferstelle IT-Sicherheit im Mittelstand
- **Sec-O-Mat (Tool für IT-Sicherheitsbedarf)**
- Sicherheitspartnerschaft mit dem Land Berlin

www.ihk-berlin.de/cybersicherheit
www.ihk-berlin.de/nl-sicherheit

www.tisim.de/
www.sec-o-mat.de
www.ihk-berlin.de/sipa

EMOTET

Der König ist tot … lang lebe der König!

Emotet – was ist das?

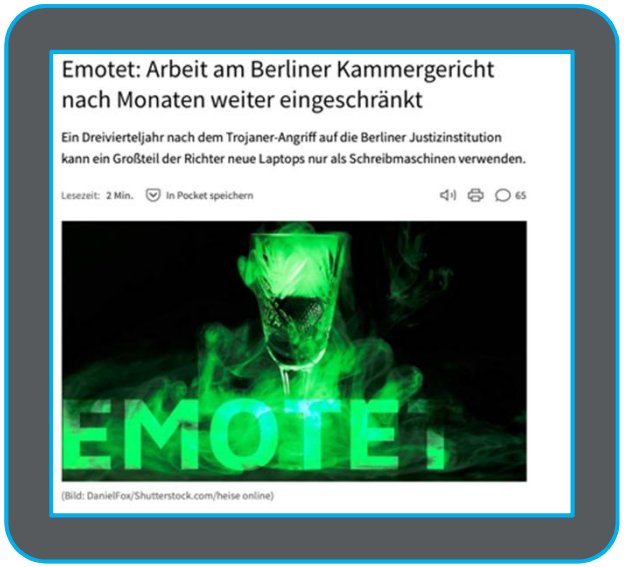
Emotet war eine **Schadsoftware**…ein Stück „**bösartige**“ Software!

Emotet hat **persönliche Daten** gestohlen!

Emotet infizierte Computersysteme … **weltweit**!

Perfide! Emotet hat andere Malware, insbesondere **Ransomware**, nachgeladen!

Infektionen mit Emotet



Die “Gute Seite der Macht”

Und was macht die Strafverfolgung so?

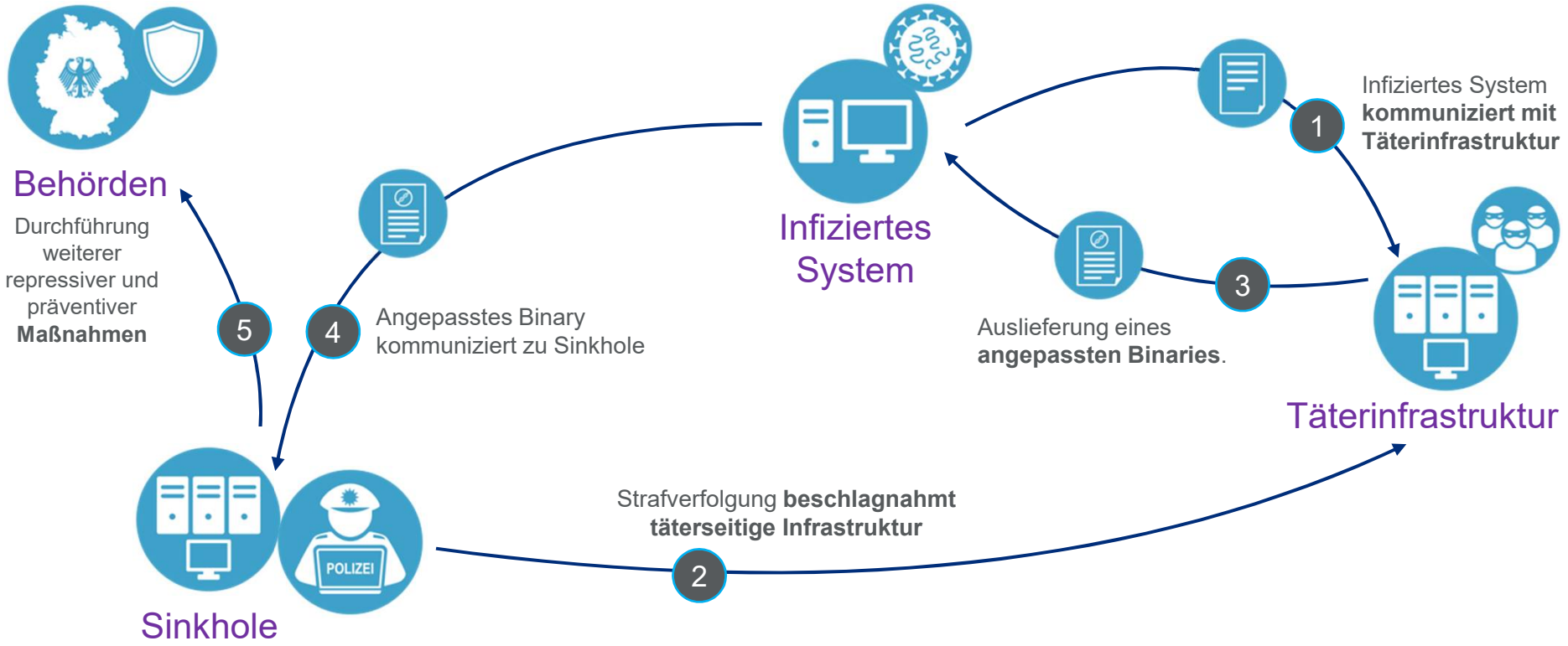
Durchführung umfangreicher **strafprozessualer Maßnahmen**…

Zentrale Ermittlungen!

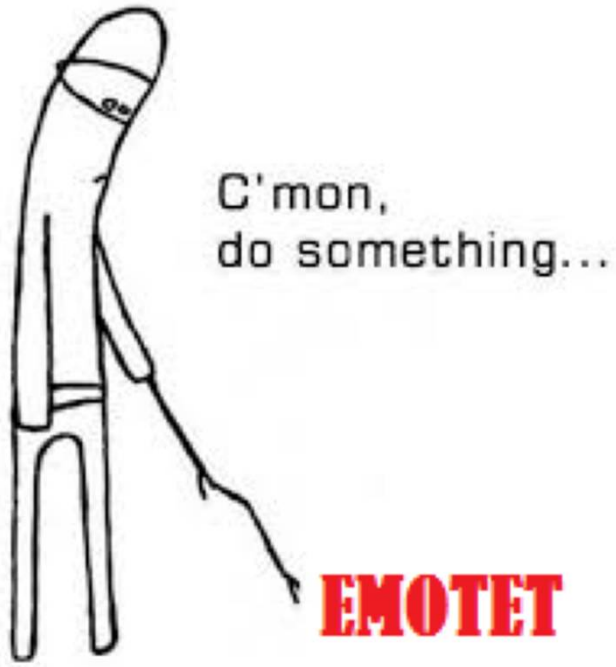
Versuch der **Identifizierung von Tatverdächtigen**

Planung von **Takedown-Maßnahmen**

Take ‘em down!


Behörden
Durchführung weiterer repressiver und präventiver **Maßnahmen**
5
4
Angepasstes Binary kommuniziert zu Sinkhole
Infiziertes System
1
Infiziertes System **kommuniziert mit Täterinfrastruktur**
3
Auslieferung eines **angepassten Binaries**.
Täterinfrastruktur
POLIZEI
Sinkhole
Strafverfolgung **beschlagnahmt täterseitige Infrastruktur**
2

Und nun?



Lessons learned

Der Kampf gegen **Windmühlen** macht so ganz alleine keinen Spaß!

Erfolge sind **möglich**!

Die Zusammenarbeit mit der **Privatwirtschaft** ist absolut notwendig!

Eine **Schwalbe macht noch keinen Frühling**!

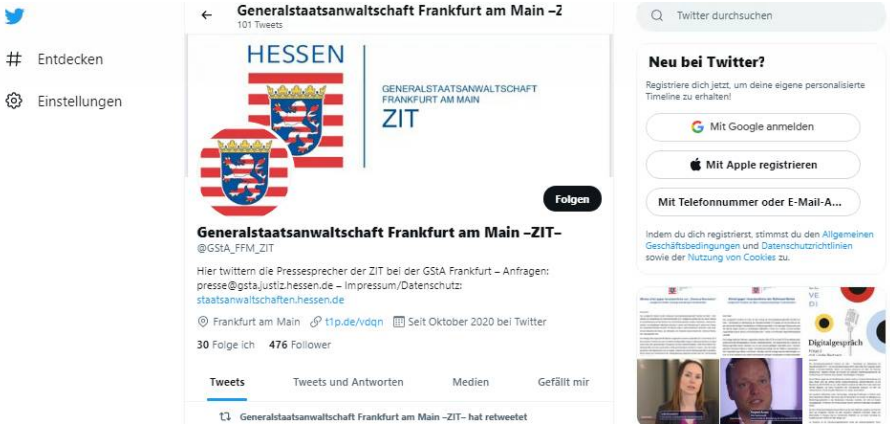
Cyberangriffe

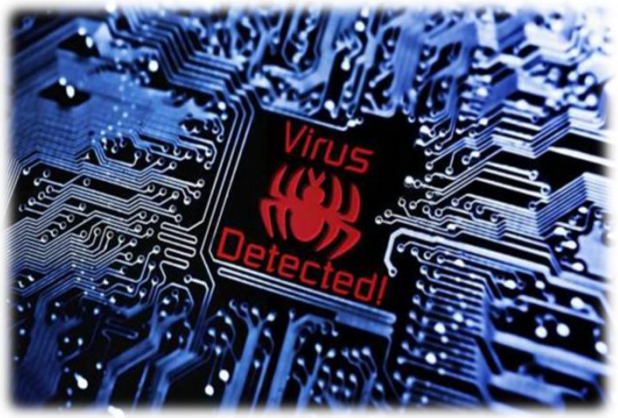
Neue Verteidigungsstrategien

Zentralstelle zur Bekämpfung der Internetkriminaliät (ZIT)

Generalstaatsanwaltschaft Frankfurt am Main

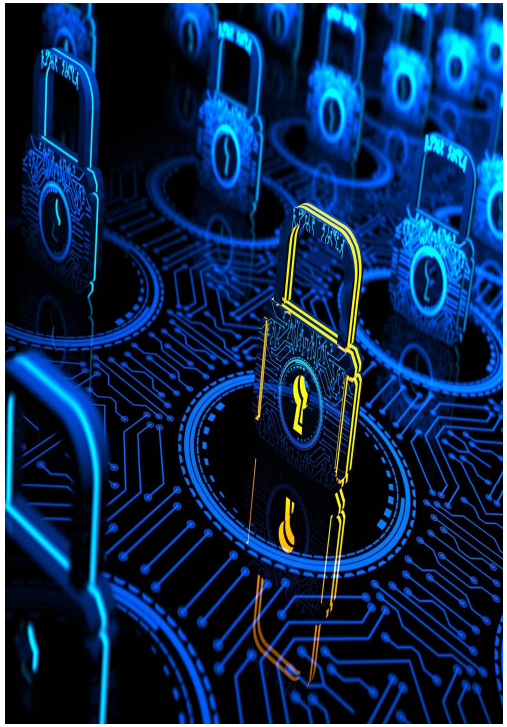
- 4 Teams
- 14 Staatsanwälte
- (k)eine normale Staatsanwaltschaft



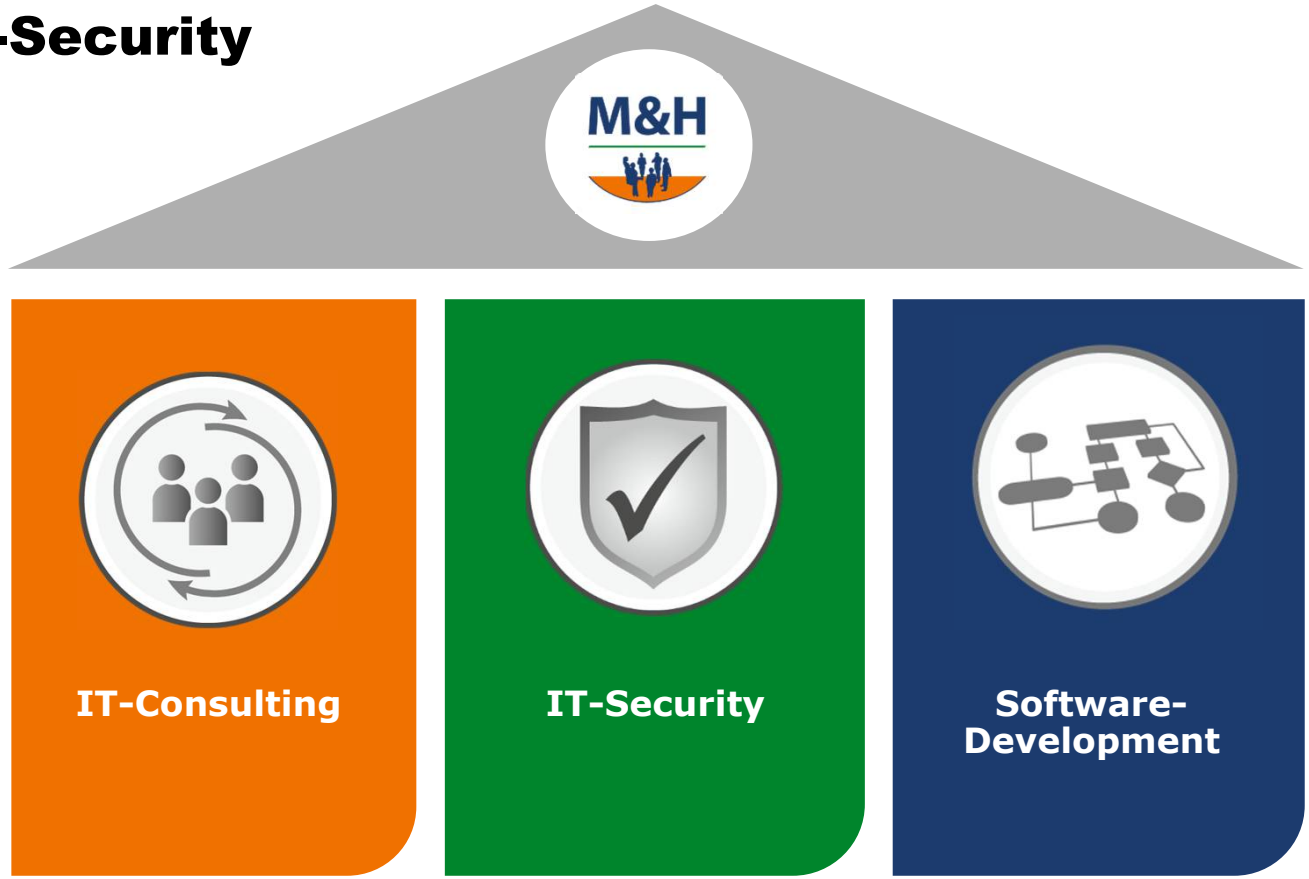


HiSolutions

- Produktneutrales Beratungs- und Dienstleistungsunternehmen mit Sitz in Berlin
- Mit 250 Mitarbeitern bearbeiten wir Themen aus den Bereichen Digitalisierung und Cybersicherheit
- Wir helfen bei der Prävention: Von der Strategie über das Sicherheits-konzept bis hin zur Planung und Umsetzung von Sicherheitsmaßnahmen
- Wir prüfen das erreichte Sicherheitsniveau: vom technischen Penetra-tionstest bis hin zur Zertifizierung des Sicherheitsmanagementsystems
- Wir bewältigen Cyberangriffe durch Unterstützung im Cyber-Krisenmanagement und in der technischen Behandlung und Aufklärung (IT-Forensik)
- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat uns als Anbieter zertifiziert.

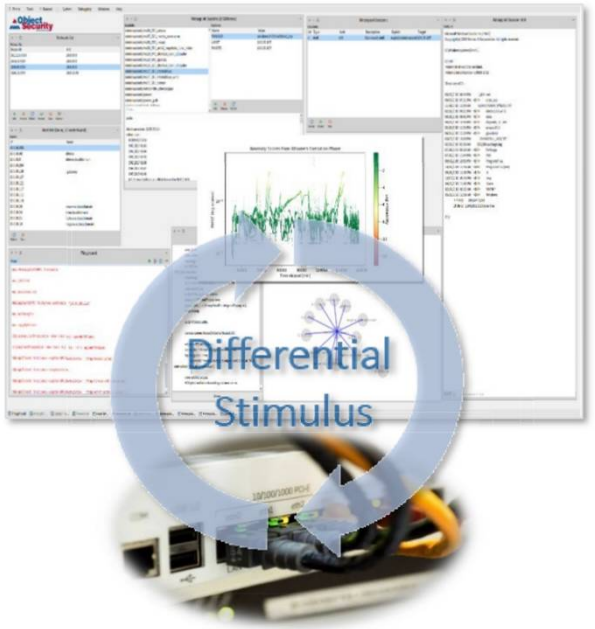


M&H IT-Security



ObjectSecurity

- Standorte in Falkensee und San Diego (CA), 20 Mitarbeiter
- Fokus: Risikomanagement in komplexen Systemen (Infrastruktur, Industrie, Verkehr, Automotive, Verteidigung, 5G, Lieferketten, KI)
- Spezieller Ansatz: Automatisierung
  - Modellierung/Regelbasiert
  - Artificial Intelligence/Machine Learning
- Entwicklung/Anwendung spezieller Werkzeuge
  - Penetration Tests/Schwachstellenanalyse
  - Anomalies Detection
  - Reverse Engineering
  - Forensik komplexer Systeme
- Umsetzung von Zero Trust Architectures
  - Zugriffskontrolle



Dentons Team der Daten- und Cyber-Experten

大成 DENTONS

Praxisfall: SECPORT (1/4)

SECPORT, ein *hidden champion* der deutschen Industrie ist Weltmarktführer innovativer Cloud-basierter Schließsysteme.

Der erste Erfolg wurde durch Kombination von Sensoren und mechanischen Verschlusssystemen erreicht: Vor 10 Jahre stattete SECPORT Banken und Behörden mit biometrischen Sensoren zur Erkennung von Fingerabdrücken, der Iris und schließlich auch Stimmen aus. Eine zentrale Speicherung biometrischer Daten erlaubt schnelle Anpassungen und höchste Sicherheit gegen lokal Eingriffe.

Neuestes Produkt ist eine *nearfield*-Kommunikation über *bluetooth*, die durch Verschlüsselungsalgorithmen jedes Handy zum perfekten Schlüssel macht.

Ferner bietet SECPORT seinen Kunden im Notfall an, Schließsysteme vollständig oder in Teilen über besondere Internet-Zugriffe freizuschalten.

Praxisfall: SECPORT (2/4)

Den ganzen Tag über erscheint das IT-System der Verwaltung „lahm“.

Bei der IT-Abteilung gehen Beschwerden über Schwierigkeiten bei Serverzugriffen ein, ein Mitarbeiter beschwert sich über die ständigen Festplattengeräusche seines (alten) Laptops und das „Einfrieren“ des Bildschirms.

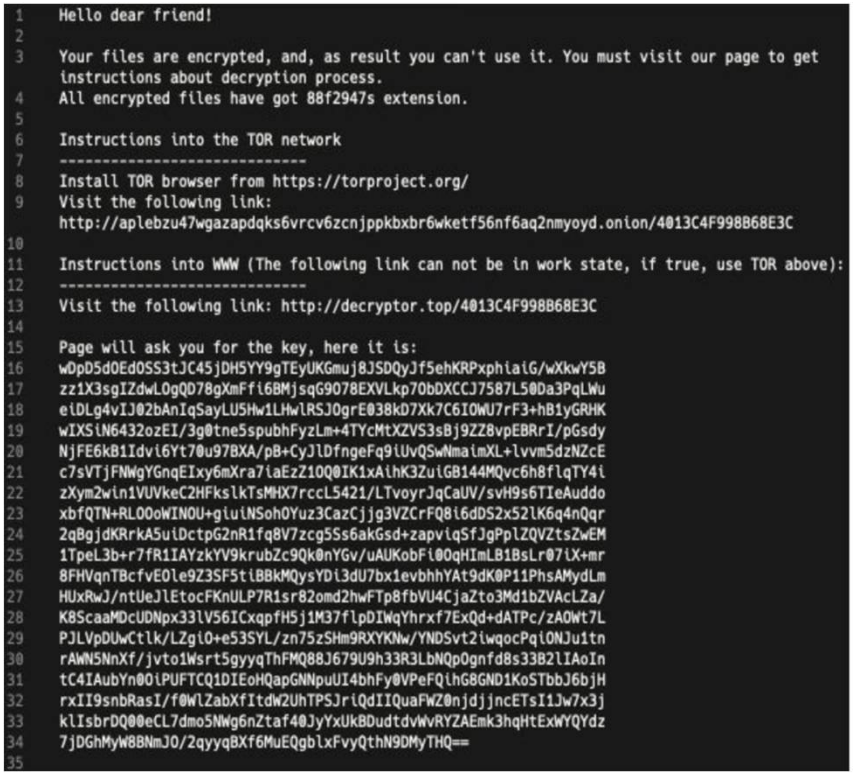
Läuft gerade ein Windows-Update? Das war doch erst letzte Woche …

Der Leiter IT wundert sich und hat einen schrecklichen Verdacht, hätte man doch in mehr IT-Sicherheit investiert …

Was ist jetzt zu tun?

- ✓ Nichts, das kann alle möglichen Ursachen haben!
- ✓ Bei der IT nachfragen, ob andere auch dieselben Probleme haben oder ob nur der eigene Rechner betroffen ist.
- ✓ IT dazu auffordern, die Systeme ordnungsgemäß herunter zu fahren.
- ✓ IT dazu auffordern, sofort die Systeme vom Netz trennen.
- ✓ Sofort den Strom abschalten!
- ✓ Die Polizei benachrichtigen und weitere Meldungen vorbereiten.

Praxisfall: SECPORT (3/4)



```
Hello dear friend!

Your files are encrypted, and, as result you can't use it. You must visit our page to get
instructions about decryption process.
All encrypted files have got 88f2947s extension.

Instructions into the TOR network
-----------------------------
Install TOR browser from https://torproject.org/
Visit the following link:
http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/4013C4F998B68E3C

Instructions into WWW (The following link can not be in work state, if true, use TOR above):
-----------------------------
Visit the following link: http://decryptor.top/4013C4F998B68E3C

Page will ask you for the key, here it is:
wDpD5dOEdOSS3tJC45jDH5YY9gTEyUKGmuj8JSDQyJf5ehKRPxphiaiG/wXkwY5B
zz1X3sgIZdwLOgQD78gXmFfi6BMjsqG9O78EXVLkp7ObDXCCJ7587L50Da3PqLWu
eiDLg4vIJ02bAnIqSayLU5Hw1LHwlRSJOgrE038kD7Xk7C6IOWU7rF3+hB1yGRHK
wIXSlN6432ozEI/3g0tne5spubhFyzLm+4TYcMtXZVS3sBj9ZZ8vpEBRrI/pGsdy
NjFE6kB1Idvl6Yt70u97BXA/pB+CyJlDfngeFq9iUvQSwNmaimXL+lvvm5dzNZcE
c7sVTjFNWgYGnqEIxy6mXra7iaEzZ1OQ0IK1xAihK3ZuiGB144MQvc6h8flqTY4i
zXym2win1VUVkeC2HFkslkTsMHX7rccL5421/LTvoyrJqCaUV/svH9s6TIeAuddo
xbfQTN+RLOOoWINOU+giuiNSohOYuz3CazCjjg3VZCrFQ8i6dDS2x52lK6q4nQqr
2qBgjdKRrkA5uiDctpG2nR1fq8V7zcg5Ss6akGsd+zapviqSfJgPplZQVZtsZwEM
1TpeL3b+r7fR1IAYzkYV9krubZc9Qk0nYGv/uAUKobFi0OqHImLB1BsLr07iX+mr
8FHVqnTBcfvEOle9Z3SF5tiBBkMQysYDi3dU7bx1evbhhYAt9dK0P11PhsAMydLm
HUxRwJ/ntUeJlEtocFKnULP7R1sr82omd2hwFTp8fbVU4CjaZto3Md1bZVAcLZa/
K8ScaaMDcUDNpx33lV56ICxqpfH5j1M37flpDIWqYhrxf7ExQd+dATPc/zAOWt7L
PJLVpDUwCtlk/LZgiO+e53SYL/zn75zSHm9RXYKNw/YNDSvt2iwqocPqiONJu1tn
rAWN5NnXf/jvto1Wsrt5gyyqThFMQ88J679U9h33R3LbNQpOgnfd8s33B2lIAoIn
tC4IAubYn0OiPUFTCQ1DIEoHQapGNNpuUI4bhFy0VPeFQihG8GND1KoSTbbJ6bjH
rxII9snbRasI/f0WlZabXfItdW2UhTPSJriQdIIQuaFWZ0njdjjncETsI1Jw7x3j
klIsbrDQ00eCL7dmo5NWg6nZtaf40JyYxUkBDudtdvWvRYZAEmk3hqHtExWYQYdz
7jDGhMyW8BNmJO/2qyyqBXf6MuEQgblxFvyQthN9DMyTHQ==
```

Der Assistent der Geschäftsführung ist in Eile. Seine Chefin will schnell auf eine Veranstaltung über Cyber-Sicherheit und braucht dringend noch eine Unternehmens-präsentation. Er will gerade die neueste Version ausdrucken, als der Bildschirm schwarz wird …

… der Leiter IT hat es geahnt!

Was ist jetzt zu tun?

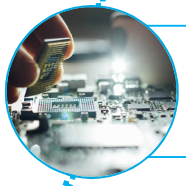
- ✓ IT dazu auffordern die Systeme ordnungsgemäß herunter zu fahren.
- ✓ IT dazu auffordern, sofort die Systeme vom Netz trennen.
- ✓ Sofort den Strom abschalten!
- ✓ IT-Spezialisten einschalten!
- ✓ Die Polizei beachrichtigen.
- ✓ Geschäftspartner auf Bedrohung aufmerksam machen.

Das ist jetzt zu tun …

IT-Spezialisten einschalten!

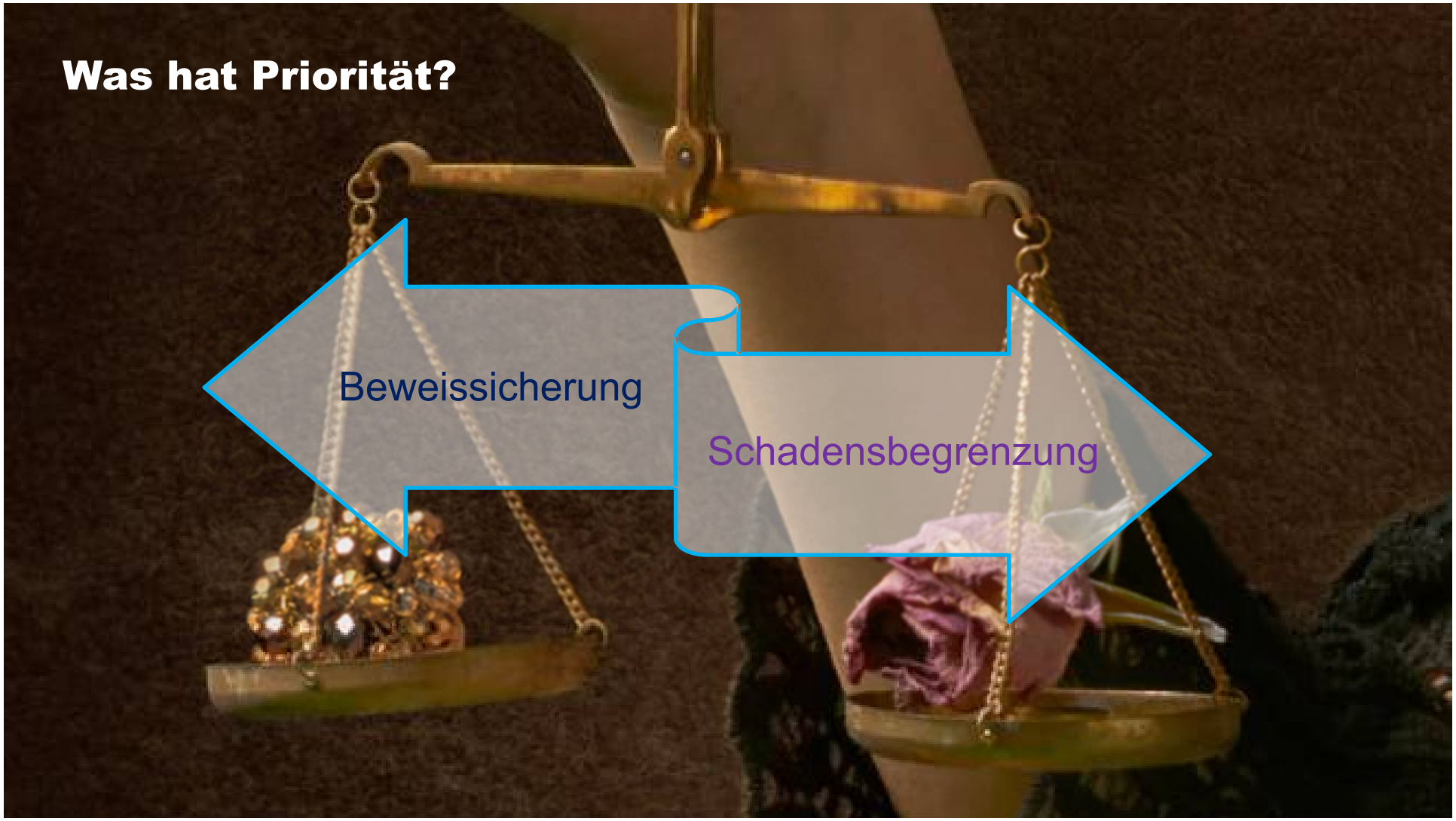
- HiSolutions bietet eine Hotline an, die direkt mit dem Experten verbindet (kein Callcenter).

Notfall-Experten nehmen den Sachverhalt auf und empfehlen geeignete Sofortmaßnahmen und Untersuchungsschritte zur Auswahl.



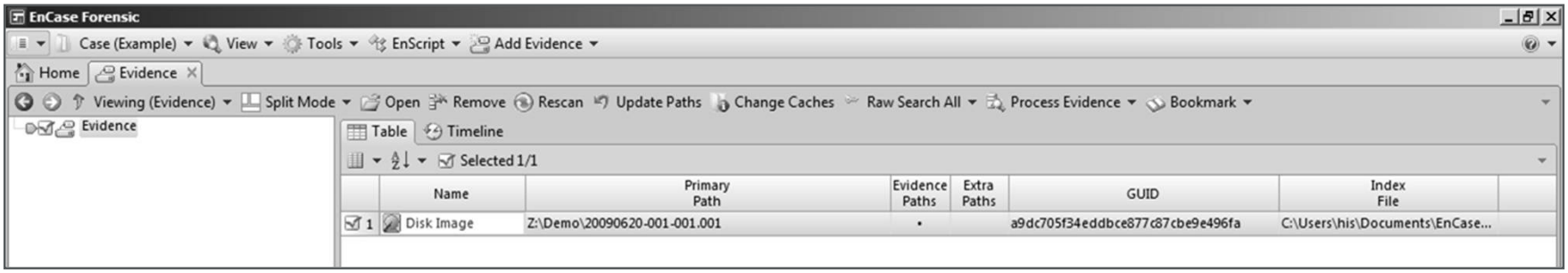
Entscheidungen zu (i) Schadensbegrenzung, (ii) Beweissicherung und (iii) Wiederherstellung der befallenen Systeme

Wiederholung des Vorfalls muss verhindert werden


Was hat Priorität?
Beweissicherung
Schadensbegrenzung

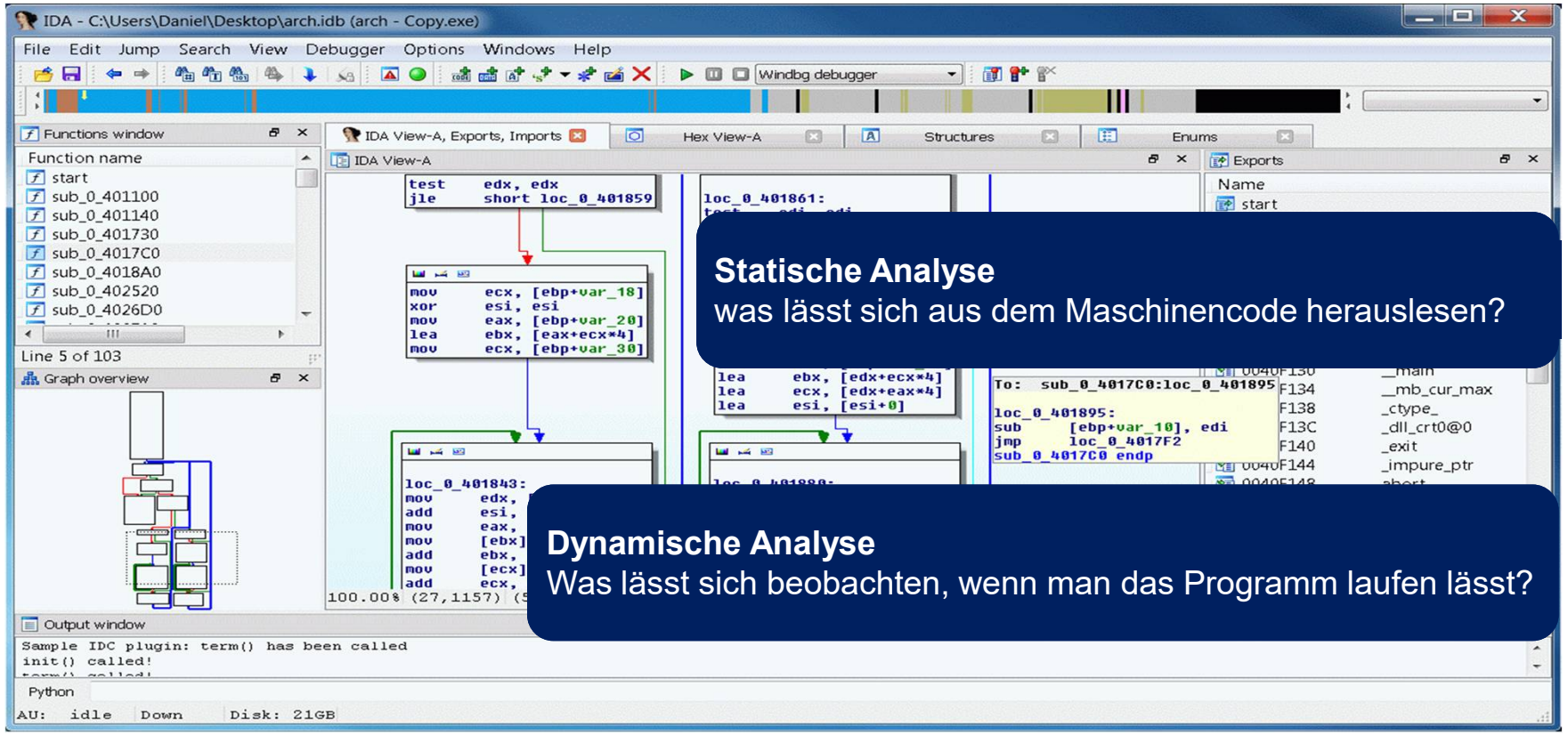
Elektronische Spurensicherung (IT-Forensik)

Datenanalyse



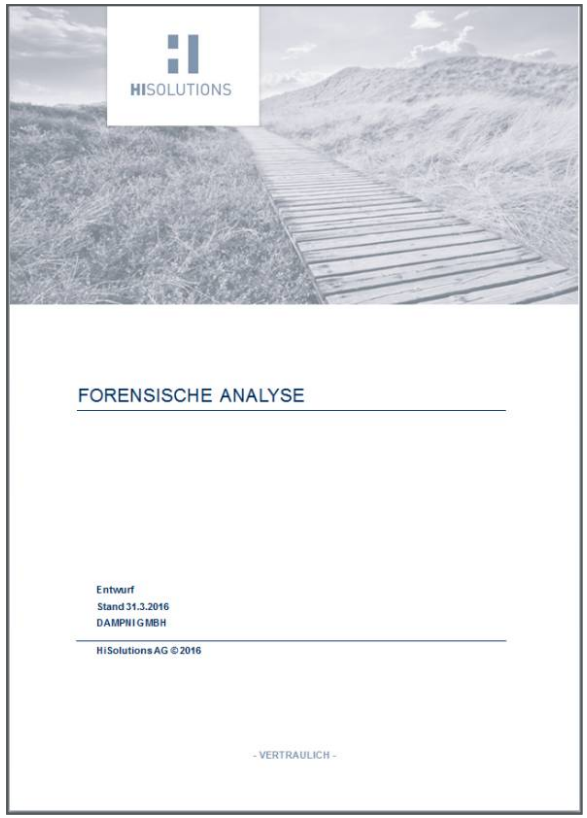
- Komplexe Suchanfragen über ganzen Datenträger
- Wiederherstellung gelöschter Dateien aus Datenspuren
- Zeitreihen zur Nachverfolgung von Angriffswegen
- und viele andere Möglichkeiten…

Reverse Engineering



Dokumentation

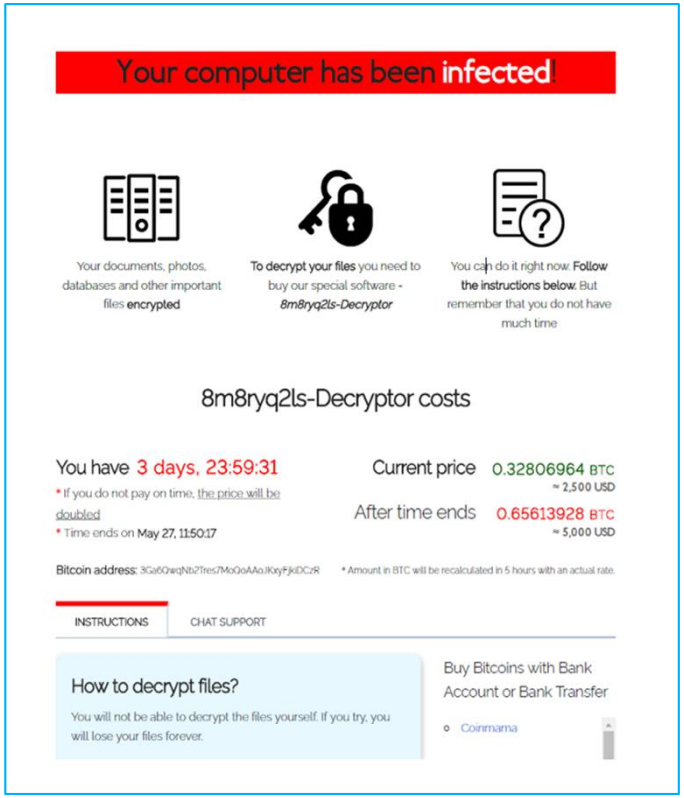
- Alle Untersuchungsschritte werden bei Bedarf in einem forensischen Bericht genau dokumentiert.
- Die erkannten Sachverhalte werden dargestellt und belegt.
- Daraus werden Erkenntnisse über den Tathergang abgeleitet.
- Auf dieser Grundlage können
  - Maßnahmen abgeleitet werden, um vergleichbare Angriffe künftig zu verhindern.
  - (arbeits-)rechtliche Schritte gegen den oder die Täter ergriffen werden.
  - Ermittlungsbehörden einbezogen werden.



Praxisfall: SECPORT (4/4)

Die Veranstaltung muss leider ohne SECPORT auskommen, die Geschäftsführerin hat gerade anderes zu tun.

Schade, leider verpasst sie so entscheidende Tipps zur Cyber-Sicherheit, die sie gerade jetzt gebrauchen könnte, denn auf dem Bildschirm erscheint folgende seltsame Nachricht:



Was ist jetzt zu tun?

- ✓ Technische Untersuchung fortsetzen.
- ✓ Lösegeld zahlen.
- ✓ Wenn noch nicht getan: Polizei einschalten!
- ✓ Oder gleich sofort die Staatsanwaltschaft beim ZIT?
- ✓ Geschäftspartner warnen!
- ✓ Eine Meldungen an das BSI ist erforderlich!
- ✓ Die 72h-Frist läuft ab – die Datenschutzbehörde muss benachrichtigt werden!

Zusammenarbeit mit den Strafverfolgungsbehörden

Die Behörden empfehlen, Strafanzeige zu erstatten

- Abschreckungswirkung für die Zukunft
- Zusätzliche Ermittlungshilfe
- Rechts-/Amtshilfemöglichkeit der Behörden
- Erfolgreiche Bekämpfung von Cybercrime wird erheblich eingeschränkt

Nur ca.11,9 % der Unternehmen erstatten Strafanzeige

- Lange Dauer von Ermittlungsverfahren
- Angst vor Reputationsschäden (Presse)
- Unsichere Erfolgsaussichten
- Angst vor negativen Auswirkungen unter Wettbewerbsgesichtspunkten
- Erfolglosigkeit von Ermittlungsverfahren
- Sicherstellung von Hardware
- Angriff letztlich abgewehrt
- Angst vor eigener Verfolgung

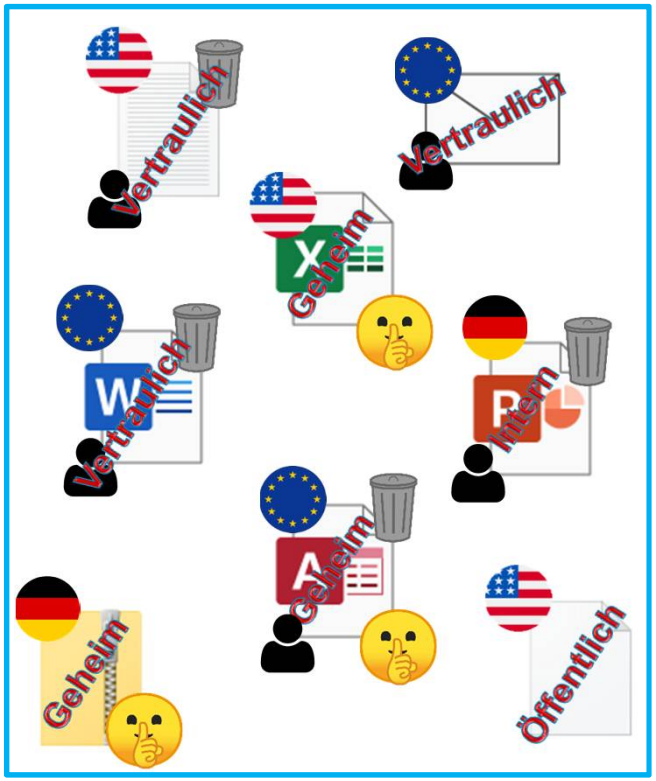
Lösegeldzahlung

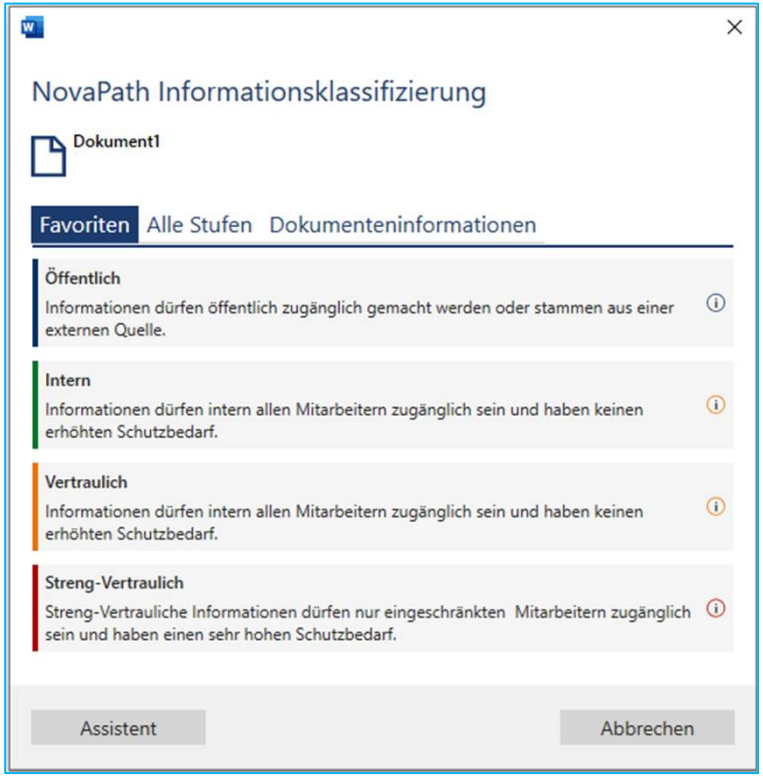
Mache ich mich selbst strafbar, wenn ich Lösegeld zahle?

Wie soll ich vorgehen, wenn ich Lösegeld zahlen möchte? Strafverfolgungsbehörden einbeziehen?

Woher weiß ich, ob die Angreifer meine Daten tatsächlich entschlüsseln und nicht zum Verkauf anbieten?

Informationsklassifizierung





Potentielle Auswirkungen?

- Direkter Angriff gegen IT-Systeme zur Verwaltung von Banken, Behörden und Unternehmen
- Welchen anderen (technischen) Assets sind noch betroffen?
  - Fertigung? Zulieferer?
  - Kundenservices/Kundendaten?
  - Fernwartung? Gebäudetechnik?
- Folgen
  - Juristisch?
    - Geheimhaltungspflichten / Datenschutz
    - Vertragspflichten?
  - Haftung?
    - Schliessysteme bei Kunden
    - Angriffe auf Kunden über Fernwartung
  - Reputation?

Risiko und Komplexität

- Komplexe IT/OT-Systeme in Unternehmen
- Abschätzung der Risiken schwierig, vor allem im Notfall (fehlende Dokumentation)
- Einsatz automatischer Werkzeuge
  - Netzwerktopologie
  - Kommunikationsanalyse
  - Log/Audit-Analyse
- Wenn SECPORT seine Hausaufgaben gemacht hat, dann
  - sind nur Unternehmensverwaltung betroffen,
  - ist F&E komplett getrennt,
  - ist die Fertigung durch Umsetzung von IEC 65443 geschützt,
  - hätte bei Kundenservices in der Cloud der Angriff keine Auswirkungen auf Schliessysteme!

Melde- und Dokumentationspflichten

72h

Art. 33 DSGVO

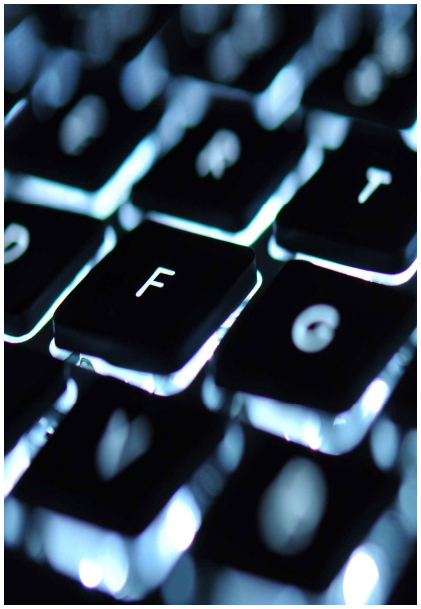
Meldung der Verletzung an die datenschutzrechtliche Aufsichtsbehörde

Art. 34 DSGVO

Benachrichtigung der betroffenen Person von der Verletzung

Art. 33 Abs. 5 DSGVO

Dokumentation von Verletzungen des Schutzes personenbezogener Daten



§ 8b Abs. 4 BSIG

Meldepflicht für KRITIS-Betreiber

§ 8c Abs. 3 BSIG

Meldepflicht für digitale Diensteanbieter

§ 8f Abs. 7, 8 BSIG

Meldepflicht für Unternehmen von besonderem öffentlichen Interesse

Geldbußen bis zu EUR 20 Mio. oder 4 % des Vorjahresumsatzes
Haftung auf Schadensersatz

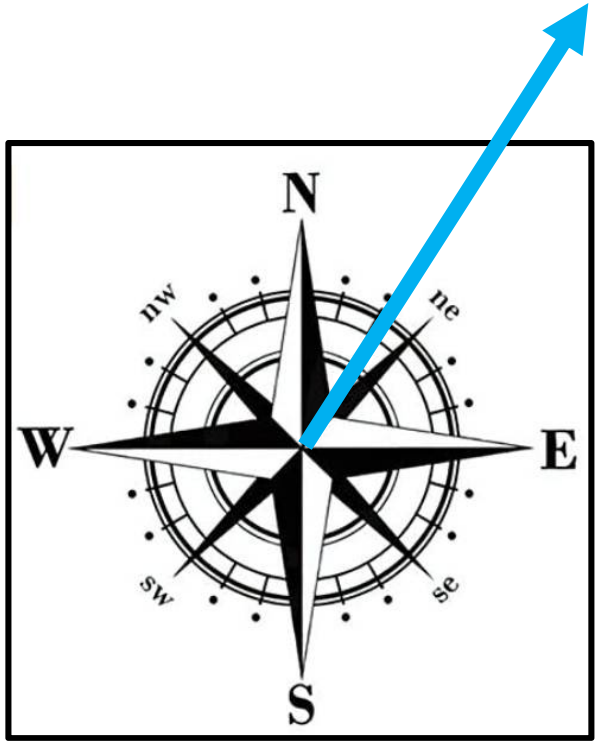
Bei Nichteinhaltung der Meldepflichten drohen Geldbußen bis zu einer Höhe von EUR 500.000.

Ausblick: Neuausrichtung in der Bekämpfung der Cybercrime – eine Vision der ZIT

Systemangelegte Probleme

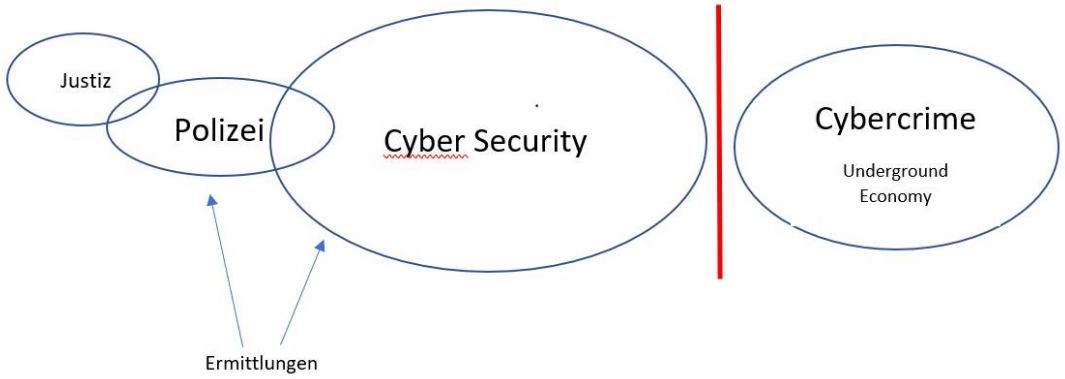
Lösungsansätze

Neuausrichtung

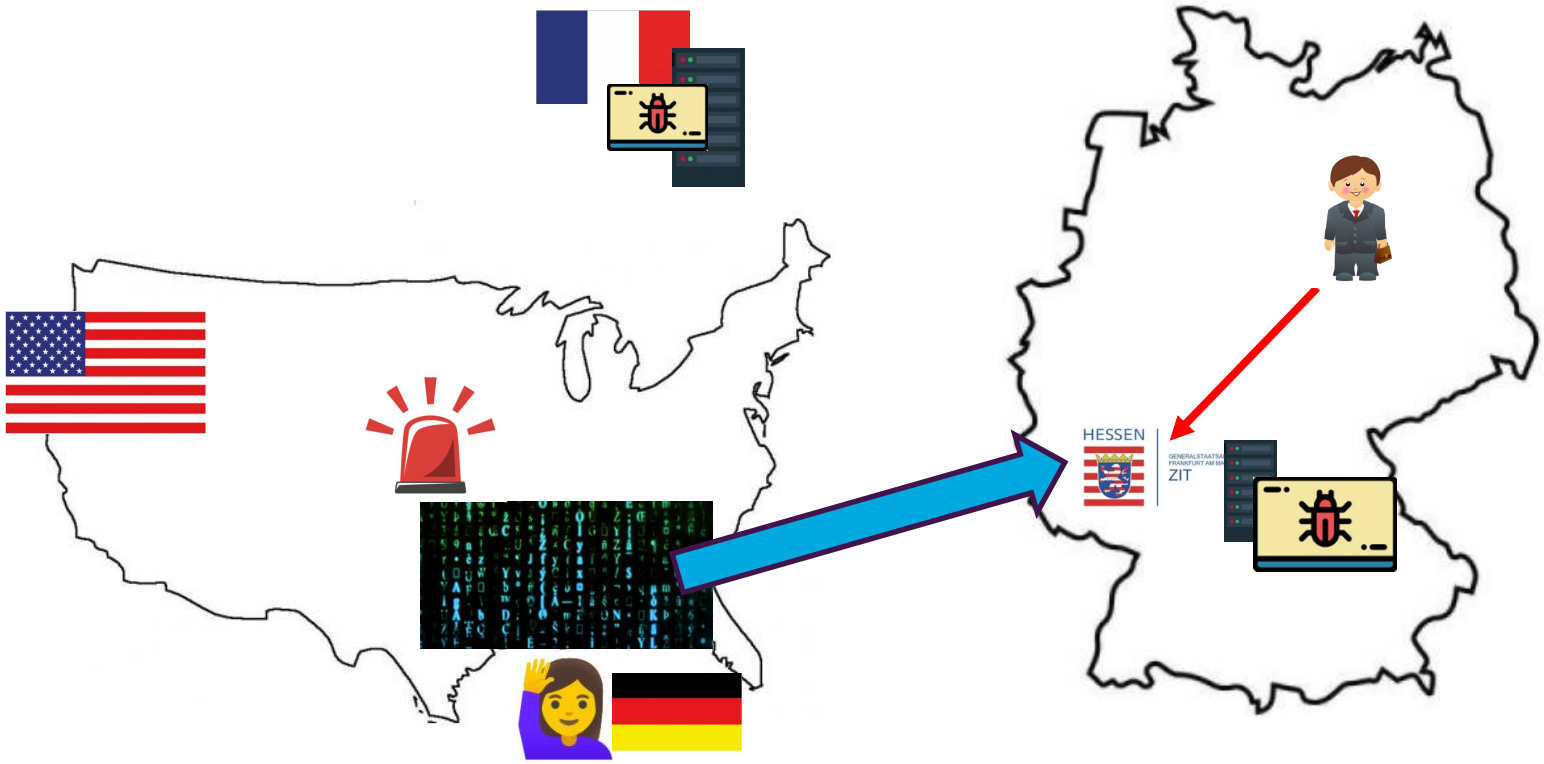


Haben wir ein systemisches Problem bei der Bekämpfung von CC?

- „Business Model“ / Kosten-Nutzen-Rechnung der Cyberkriminellen
- Finden alles in der UE (CaaS)
- Ermittlungserfolge machen die Täter besser
- Zwischenergebnis: Systemirrelevanz der Ermittlungsbehörden für die Täter?
- Wer ist wie relevant?



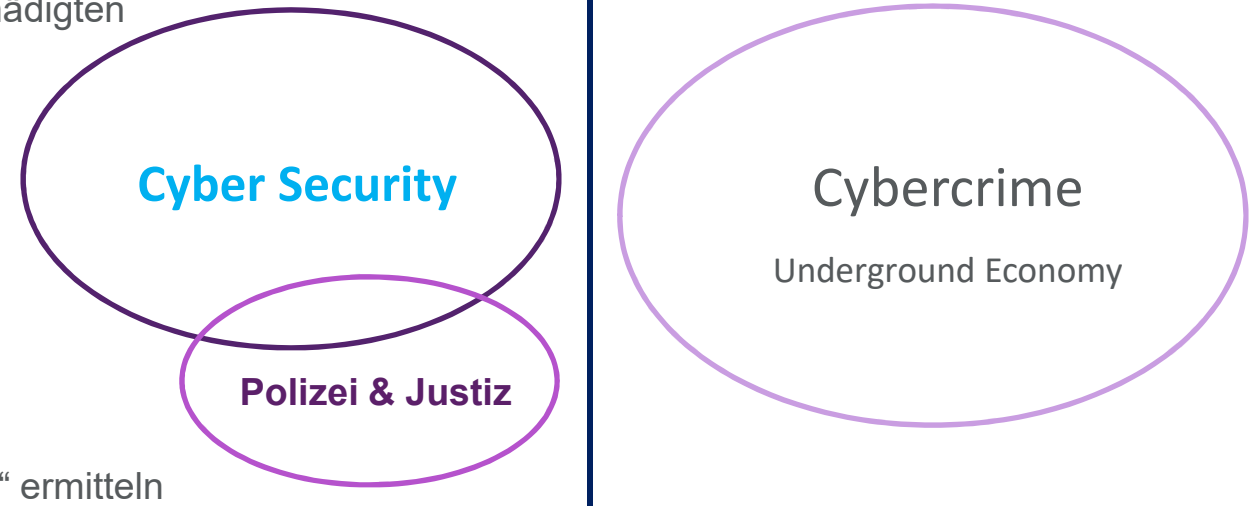
Ein neues Modell der Zusammenarbeit?



Die Vision – Strafverfolgung von morgen?

Cyber Security

- Erstzugriff / Analysemöglichkeiten
- Kenntnis der Opfersysteme
- Enger Kontakt zu Geschädigten



Polizei & Justiz

- „Hinter dem Gartenzaun“ ermitteln
- IT-Infrastruktur herunternehmen
- Daten erheben, wo Freiwilligkeit und Käuflichkeit aufhören