

大成 DENTONS

it's.BB



Cybercrime

Neue Verteidigungsstrategien

16. September 2021



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



Kriminalität verlagert sich ins Internet

Unternehmen vermehrt Ziel von Hackerangriffen

Mehr als 28 Prozent der Unternehmen in Berlin und Brandenburg sind im Jahr 2018 Opfer einer Cyberattacke geworden. Das geht aus dem jüngsten Kriminalitätsbarometer der Industrie- und Handelskammer von Berlin und Brandenburg hervor, das am Donnerstag vorgestellt wurde. Die Zahl der Hackerangriffe ist demnach in den vergangenen Jahren deutlich gestiegen: 2010 seien es noch zehn Prozent gewesen. Insgesamt wurden fast zwei Drittel der Berliner Unternehmen im vergangenen Jahr Opfer einer Straftat, und die wenigsten erstatten Anzeige bei der Polizei.

Selbst bei schweren Delikten wie Einbruchsdiebstahl wird nicht einmal jede zweite Straftat angezeigt, bei Vandalis-

mus und Diebstahl sind es nur 30 Prozent. Bei Hackerangriffen erstatten die Betroffenen nur zu 6,5 Prozent Anzeige. Es wurden 1624 Unternehmen verschiedener Branchen und Größen in den **IHK-Bezirken** Berlin, Cottbus, Ostbrandenburg und Potsdam befragt.

Damach folgt das Verbrechen dem Geschäft – und verlagert sich genau wie dieses zusehends ins Internet. Die Kriminalitätszahlen zeigen nur die berühmte Spitze des Eisbergs. Laut polizeilicher Kriminalstatistik wurden im Jahr 2018 fast 32.000 Fälle von Cyberkriminalität erfasst, das von der ganz überwiegende Teil Betrugsdelikte. 63 Prozent der Unternehmen schätzen die Cyberkriminalität als „bedrohlich“ oder „schwer bedrohlich“ ein, zugleich halten weniger als die Hälfte der Unternehmen ihre eigenen Sicherheitsmaßnahmen für „gut“ oder „sehr gut“.

Laut **IHK-Umfrage** wurden nur 15,5 Prozent der Betrugsfälle angezeigt. Daraus folgt, dass die realen Zahlen viel höher als die in der PKS erstatten sein müssen: noch deutlicher ist dies bei den Hackerangriffen. „Wir wollen die Unternehmen aktivieren, Taten anzuzeigen“, sagte der stellvertretende Hauptgeschäftsführer der **IHK Berlin, Christoph Jergusch**. Die Anzeigebereitschaft sei seit Jahren rückläufig. „Es handelt sich um ein wachsendes Kriminalitätsfeld“, so Jergusch. „Die Unternehmen werden digitaler, die Kriminalität ebenfalls, also muss auch die Strafverfolgung digitaler werden.“ Offenbar hätten die Unternehmen kein allzu großes Vertrauen in die Effektivität der Strafverfolgung.

66 Prozent der befragten Unternehmen waren 2018 von Kriminalität betroffen, ein Drittel davon durch Diebstahl, ein Viertel durch Betrug. Die größten Schäden werden bisher durch Diebstahl und Einbruchsdiebstahl angerichtet. Maschineller Klauspiel besonders im Baugewerbe eine Rolle. 65 Prozent der befragten Unternehmen des Baugewerbes wurden im vergangenen Jahr bestohlen; auf Baustellen herrschte massiver Schwund an Maschinen und Material. Hier müssen die Unternehmen über Selbstschutz nachdenken, so das **IHK**.

FATINA KEILANI

„Wir kennen nur die Spitze des Eisbergs“

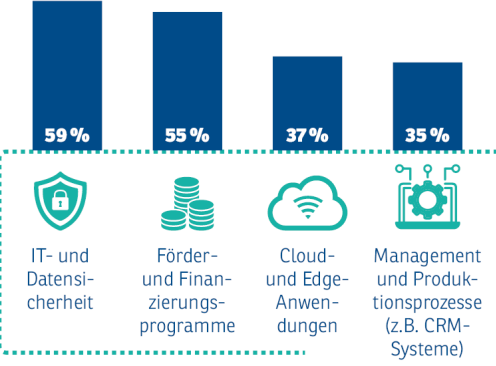
Laut **IHK** wird in Berlin und Brandenburg nur jede 15. Hackerattacke auf Unternehmen angezeigt

Von Ina-Christin Böhler (Text) und Anja-Gabriele Gatzert (Bilder)

Kriminalität verlagert sich ins Internet. Mehr als 28 Prozent der Unternehmen in Berlin und Brandenburg sind im Jahr 2018 Opfer einer Cyberattacke geworden. Das geht aus dem jüngsten Kriminalitätsbarometer der Industrie- und Handelskammer von Berlin und Brandenburg hervor, das am Donnerstag vorgestellt wurde. Die Zahl der Hackerangriffe ist demnach in den vergangenen Jahren deutlich gestiegen: 2010 seien es noch zehn Prozent gewesen. Insgesamt wurden fast zwei Drittel der Berliner Unternehmen im vergangenen Jahr Opfer einer Straftat, und die wenigsten erstatten Anzeige bei der Polizei.

Selbst bei schweren Delikten wie Einbruchsdiebstahl wird nicht einmal jede zweite Straftat angezeigt, bei Vandalis-

Bedarf für Informations- und Beratungsangebote



Quelle: IHK Digitalisierungsumfrage Dez. 2020

<https://www.itsbb.net/mitglieder/>

Wissen, was schützt: Angebote der IHK Berlin

Informieren

Sensibilisieren

Vernetzen

Veranstaltungen

- Sicherheit zum Frühstück
- **IT-Sicherheitsprechstunde 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/cybsersicherheit

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

Emotet: Arbeit am Berliner Kammergericht nach Monaten weiter eingeschränkt

Ein Dreivierteljahr nach dem Trojaner-Angriff auf die Berliner Justizinstitution kann ein Großteil der Richter neue Laptops nur als Schreibmaschinen verwenden.

Leszeit: 2 Min. [In Pocket speichern](#) 🔊 🔄 65



(Bild: Danielfox/Shutterstock.com/heise online)

Emotet: Angreifer wollten Bundeswehr-Fuhrparkservice erpressen

Der Bundeswehr-Fahrdienst, der auch Bundestagsabgeordnete befördert, wurde Opfer der Ransomware Emotet. An Daten hatten die Angreifer wohl kein Interesse.

Leszeit: 1 Min. [In Pocket speichern](#) 🔊 🔄 74



(Bild: PORTRAIT IMAGES ASIA BY NONWARIT/Shutterstock.com)

Auch Klinikum Fürth wurde Opfer des Trojaners Emotet

Freitag, 20. Dezember 2019

[f](#) [t](#) [in](#) [📄](#) [🔍](#) [🌟](#)



Bild vergrößern...

Picture alliance, Jens Büttner, ab

Die "Gute Seite der Macht"



Und was macht die Strafverfolgung so?



Durchführung umfangreicher **strafprozessualer Maßnahmen...**



Zentrale Ermittlungen!

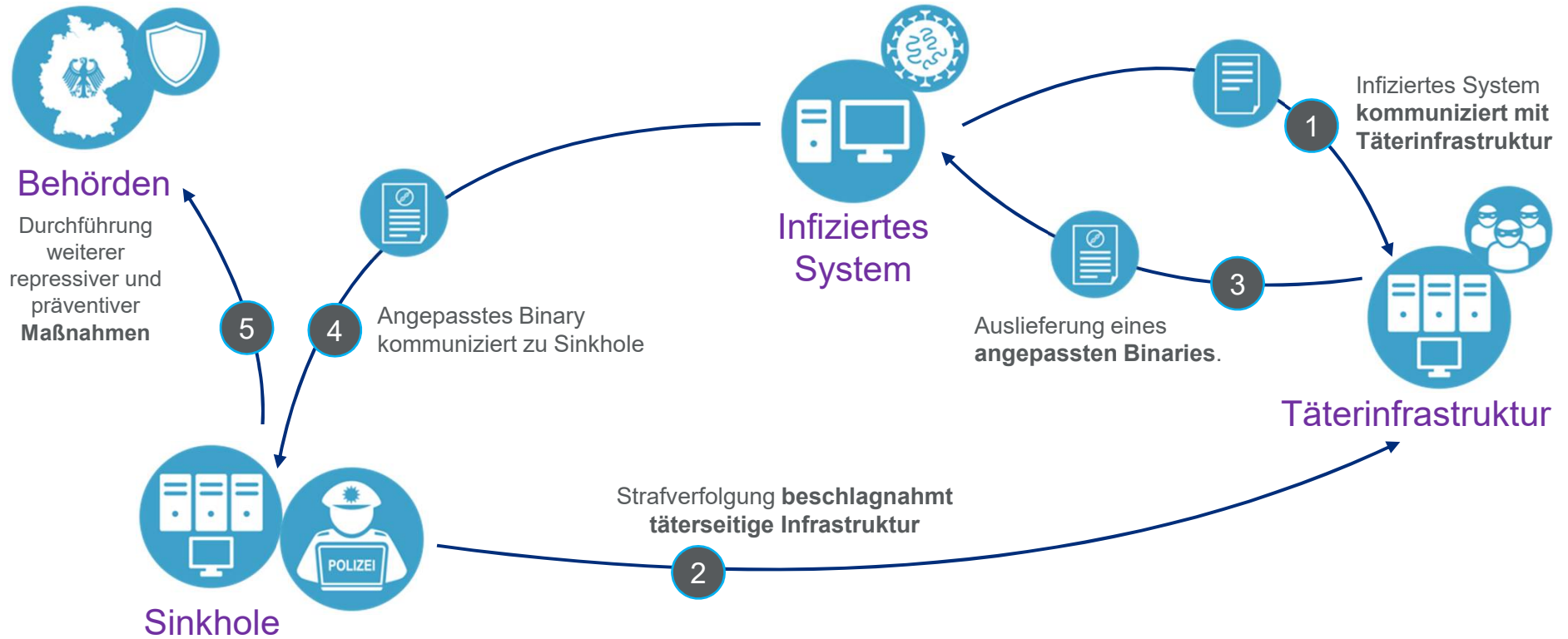


Versuch der **Identifizierung von Tatverdächtigen**



Planung von **Takedown-Maßnahmen**

Take 'em down!



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 Internetkriminalität (ZIT)

Generalstaatsanwaltschaft Frankfurt am Main

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



Generalstaatsanwaltschaft Frankfurt am Main - ZIT
101 Tweets

Entdecken
Einstellungen

Neu bei Twitter?
Registriere dich jetzt, um deine eigene personalisierte Timeline zu erhalten!

Mit Google anmelden
Mit Apple registrieren
Mit Telefonnummer oder E-Mail-A...

Indem du dich registrierst, stimmst du den Allgemeinen Geschäftsbedingungen und Datenschutzrichtlinien sowie der Nutzung von Cookies zu.



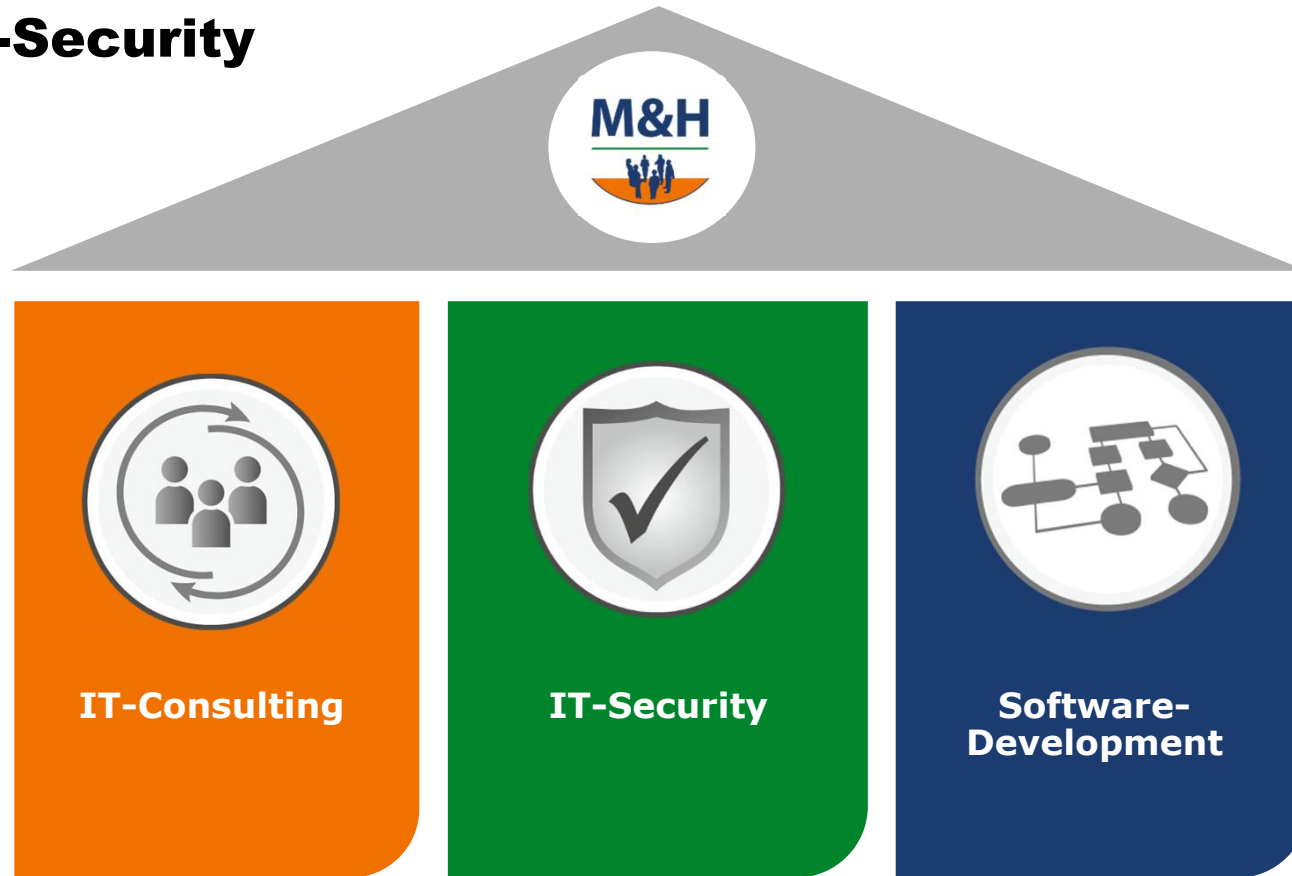
HiSolutions



- 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 Sicherheitskonzept bis hin zur Planung und Umsetzung von Sicherheitsmaßnahmen
- Wir prüfen das erreichte Sicherheitsniveau: vom technischen Penetrationstest 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.

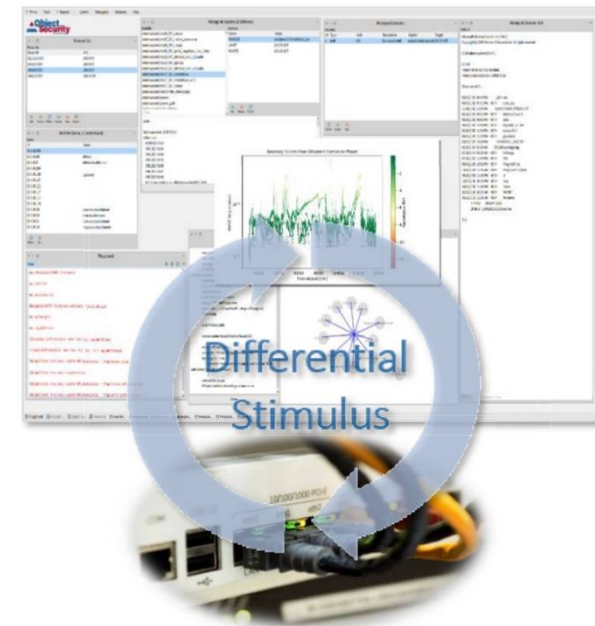


M&H IT-Security



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)

```
1 Hello dear friend!
2
3 Your files are encrypted, and, as result you can't use it. You must visit our page to get
  instructions about decryption process.
4 All encrypted files have got 88f2947s extension.
5
6 Instructions into the TOR network
7 -----
8 Install TOR browser from https://torproject.org/
9 Visit the following link:
  http://aplebzu47wgazapdqks6vrcv6zcnjppkxbr6wketf56nf6aq2nmyoyd.onion/4013C4F998B6E3C
10
11 Instructions into WWW (The following link can not be in work state, if true, use TOR above):
12 -----
13 Visit the following link: http://decryptor.top/4013C4F998B6E3C
14
15 Page will ask you for the key, here it is:
16 wDpD5d0Ed0S53tJC45jDHSYY9gTEyUKGmuJ8JSDQyJf5ehKRPxphlaIG/wXkwY5B
17 zz1X3sgIZdwL0gQD78gXmFf16BMjsqG9078EXVLkp70bDXCCJ7587L50Da3PqLWu
18 eLDLg4vIJ02bAnIqSayLU5Hw1LHwLR5J0grE038k07Xk7C6IOWU7rF3+hB1yGRHK
19 wIXSIN6432ozEI/3g0tne5spubhFyzLm+4TYCmTXZVS3sBj9ZZ8vpEBRrI/pGsdY
20 NjFE6k81Idvi6Yt70u97BXA/pB+CyJlDfngFq9lUvQSwLmaImXL+lvvm5dzNZcE
21 c7sVTjFNWgYGnqEixy6mXra7IaEzZ10Q0IK1xAIhK3ZuLGB144MQvc6h8fLqTY4l
22 zXym2wln1VUVKkeC2HFkslKtsMHX7rccL5421/LTvoyrJqCaUV/svH9s6TIEAuddo
23 xbfQTH+RL00wIN0U+giuINSoh0Yuz3CazCjJg3VZCrFQ8l6dDS2x52LK6q4nQqr
24 2q8gjdKRrKA5uIdctpG2hR1fq8V7zcg5Ss6akGsd+zapvLqSfJgPpLZQVZtsZwEM
25 1TpeL3b+r7fR1IAYzkYV9krubZc9Qk0nYGV/uAUKobF100qHImLB1BsLr07LX+mr
26 8FHVqnTbcfvE01e9Z3SF5tIbBkMQysYDi3dU7bx1evbhYAt9dK0P11PhsAmydLm
27 HUxRwJ/ntUeJlEtocFKnULP7R1sr82omd2hwFTp8fbVU4CjaZto3Md1bZVAcLZa/
28 K8ScaamDcUDNpx33LV56ICxqpfH5j1M37flpDIWqYhrxf7ExQd+dATPc/zAOWt7L
29 PJLVpDUwCtLk/LZgl0+e53SYL/zn75zSHm9RXYKw/YNDSvt2lwqocPq1ONJJu1tn
30 rAWNSnXf/jvto1wsrt5gyyqThFMQ88J679U9h33R3LbNq0gnfd8s33B2LIAoIn
31 tC4IAubYn0lPUFTCQ1DIEoHQapGNpuUI4bhFy0VPeFQhG8GND1KoSTbbJ6bjH
32 rxI9sbnRasI/f0wLZabXfItw2UhtPSJrIqDIQuaFWZ0njdjncETsI1Jw7x3j
33 kLI5brDQ0eCL7dmo5NWg6nZtaf40JyYxUkBDudtdvWVRYZAEmk3hqHtExWYQYdz
34 7jDGhMyW8BnmJ0/2qyyqBXf6MuEQgbLxVvyqthN90MyTHQ==
35
```

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 ...

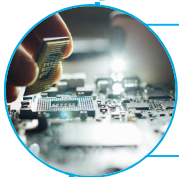


IT-Spezialisten einschalten!

- 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

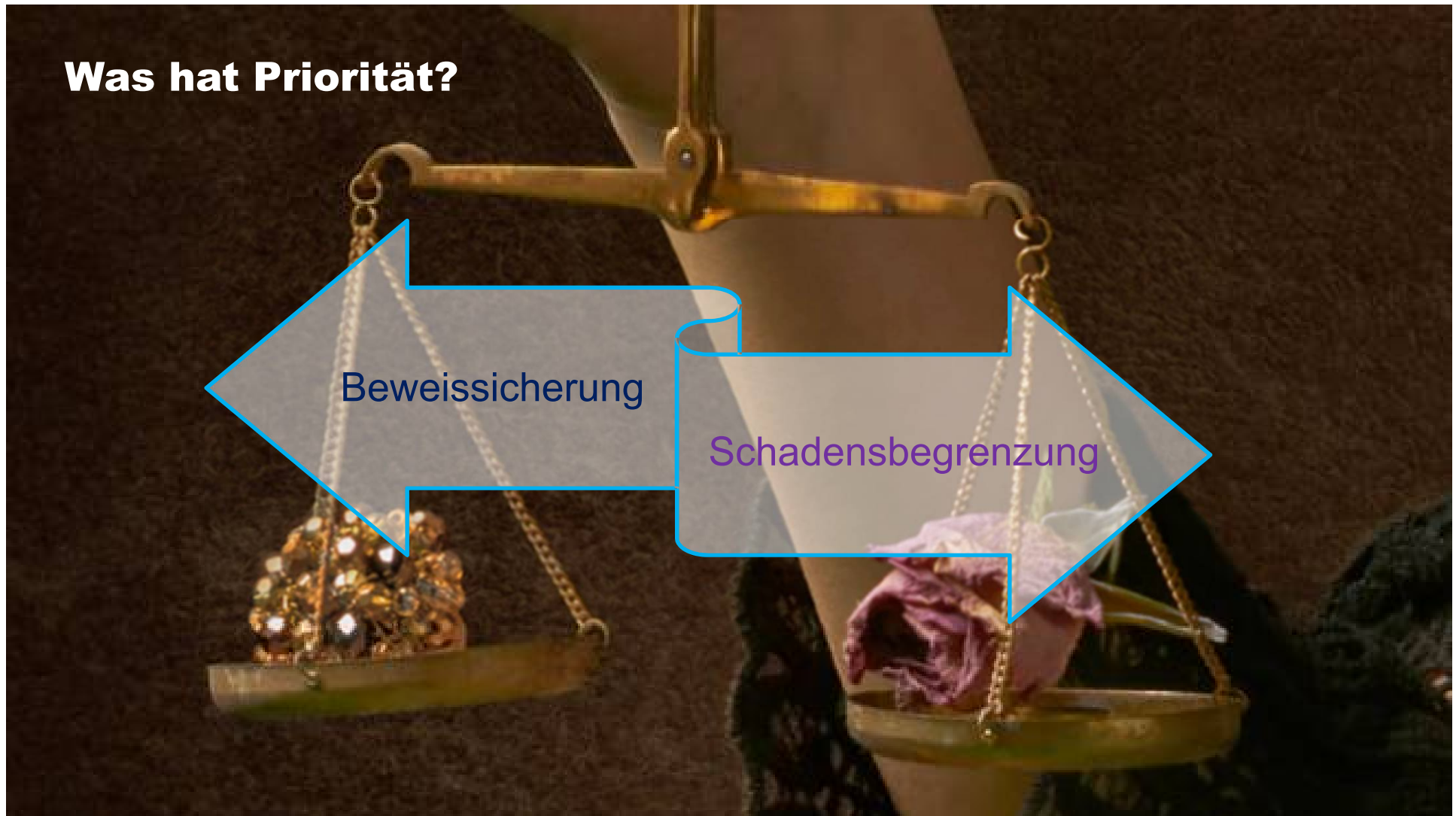


Wiederholung des Vorfalles muss verhindert werden

Was hat Priorität?

Beweissicherung

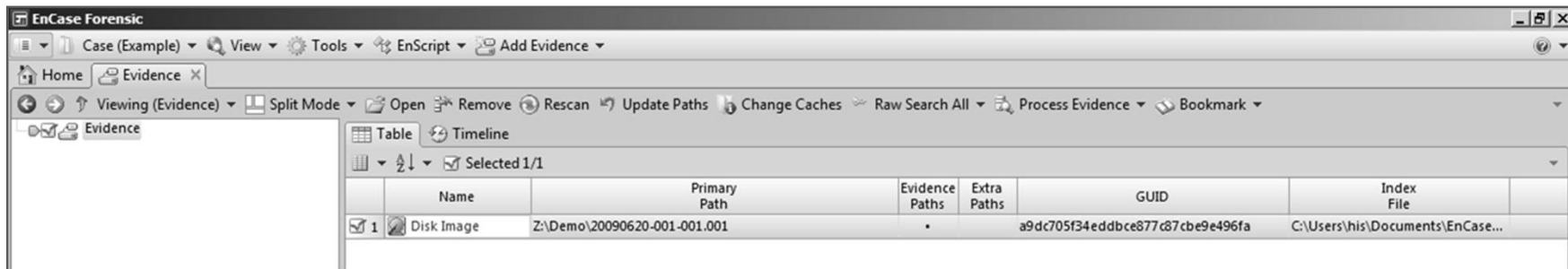
Schadensbegrenzung



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

The screenshot shows the IDA Pro interface with the following components:

- Functions window:** Lists functions such as `start`, `sub_0_401100`, `sub_0_401140`, `sub_0_401730`, `sub_0_4017C0`, `sub_0_4018A0`, `sub_0_402520`, and `sub_0_4026D0`.
- Graph overview:** A control flow graph showing the relationship between different code blocks.
- IDA View-A:** Displays assembly code for `loc_0_401859` and `loc_0_401843`.

```
loc_0_401859:
test  edx, edx
jle   short loc_0_401859

loc_0_401843:
mov   ecx, [ebp+var_18]
xor   esi, esi
mov   eax, [ebp+var_20]
lea   ebx, [eax+ecx*4]
mov   ecx, [ebp+var_30]
```
- Exports window:** Lists exported symbols like `start`.
- Output window:** Shows log messages: `Sample IDC plugin: term() has been called`, `init() called!`, `term() called!`.

Two blue callout boxes are overlaid on the screenshot:

- Statische Analyse**
was lässt sich aus dem Maschinencode herauslesen?
- Dynamische Analyse**
Was lässt sich beobachten, wenn man das Programm laufen lässt?

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:

Your computer has been infected

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - **8m8ryq2ls-Decryptor**

You can do it right now. Follow the instructions below. But remember that you do not have much time

8m8ryq2ls-Decryptor costs

You have **3 days, 23:59:31**

Current price **0.32806964 BTC**
≈ 2,500 USD

After time ends **0.65613928 BTC**
≈ 5,000 USD

* If you do not pay on time, the price will be doubled
* Time ends on May 27, 11:50:17

Bitcoin address: 3Gx5QwqNz7res7MsQoAAoIKyF9jDCR * Amount in BTC will be recalculated in 5 hours with an actual rate.

INSTRUCTIONS | CHAT SUPPORT

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

Buy Bitcoins with Bank Account or Bank Transfer

o Coinmama

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 Meldung 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?

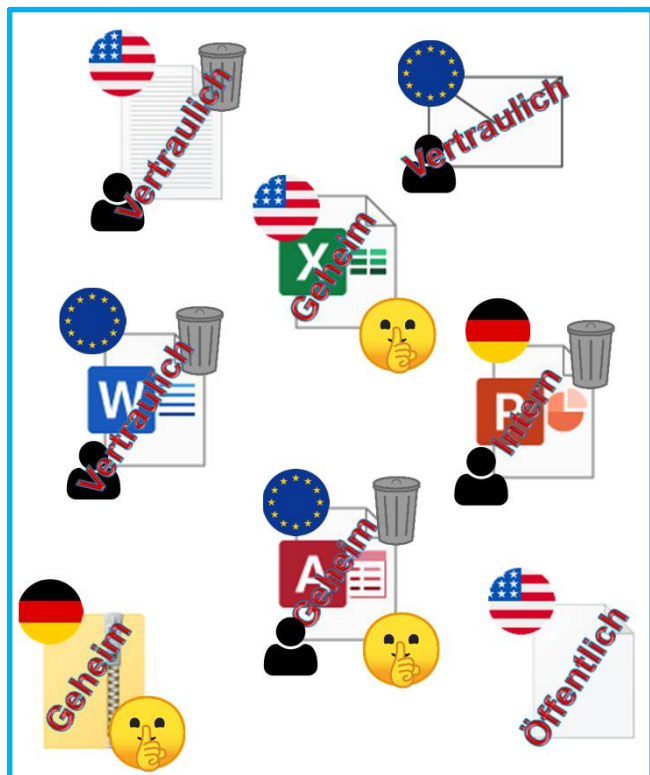


Wie soll ich vorgehen, wenn ich Lösegeld zahlen möchte?
Strafverfolgungsbehörden einbeziehen?



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

Informationsklassifizierung



NovaPath Informationsklassifizierung

Dokument1

Favoriten | Alle Stufen | Dokumenteninformationen

- Öffentlich**
Informationen dürfen öffentlich zugänglich gemacht werden oder stammen aus einer externen Quelle.
- Intern**
Informationen dürfen intern allen Mitarbeitern zugänglich sein und haben keinen erhöhten Schutzbedarf.
- Vertraulich**
Informationen dürfen intern allen Mitarbeitern zugänglich sein und haben keinen erhöhten Schutzbedarf.
- Streng-Vertraulich**
Streng-Vertrauliche Informationen dürfen nur eingeschränkten Mitarbeitern zugänglich sein und haben einen sehr hohen Schutzbedarf.

Assistent | Abbrechen

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

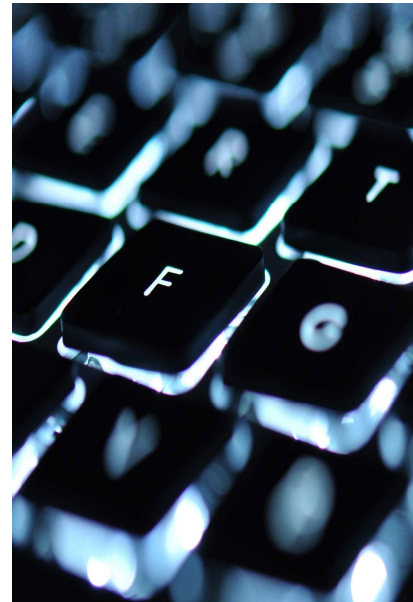
Meldung der Verletzung an die datenschutzrechtliche Aufsichtsbehörde

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**

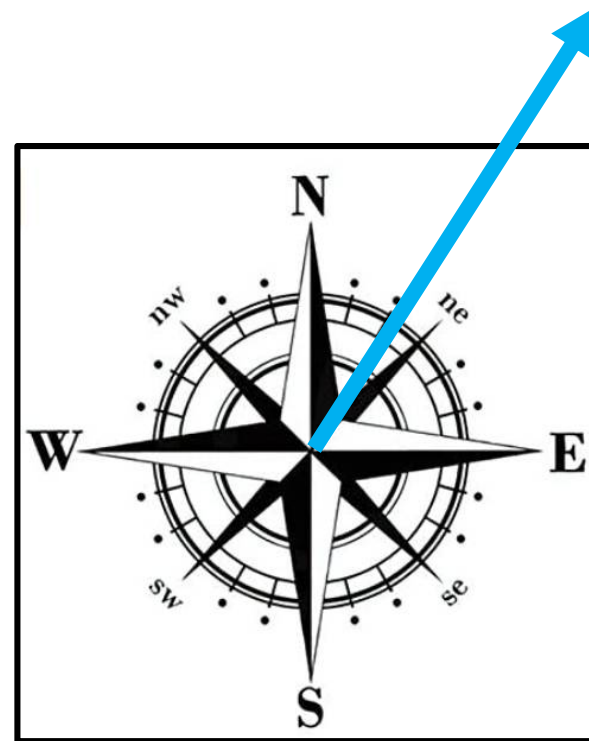
Bei Nichteinhaltung der Meldepflichten drohen Geldbußen bis zu einer Höhe von EUR 500.000.

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

Systemangelegte Probleme

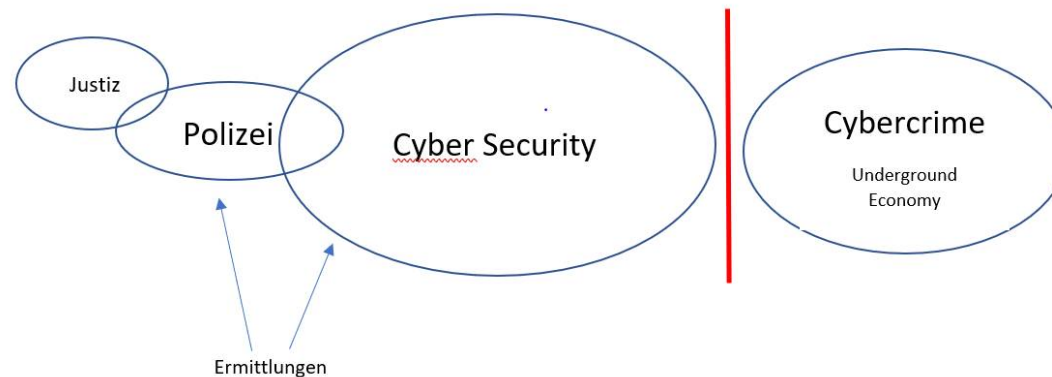
Lösungsansätze

Neuausrichtung

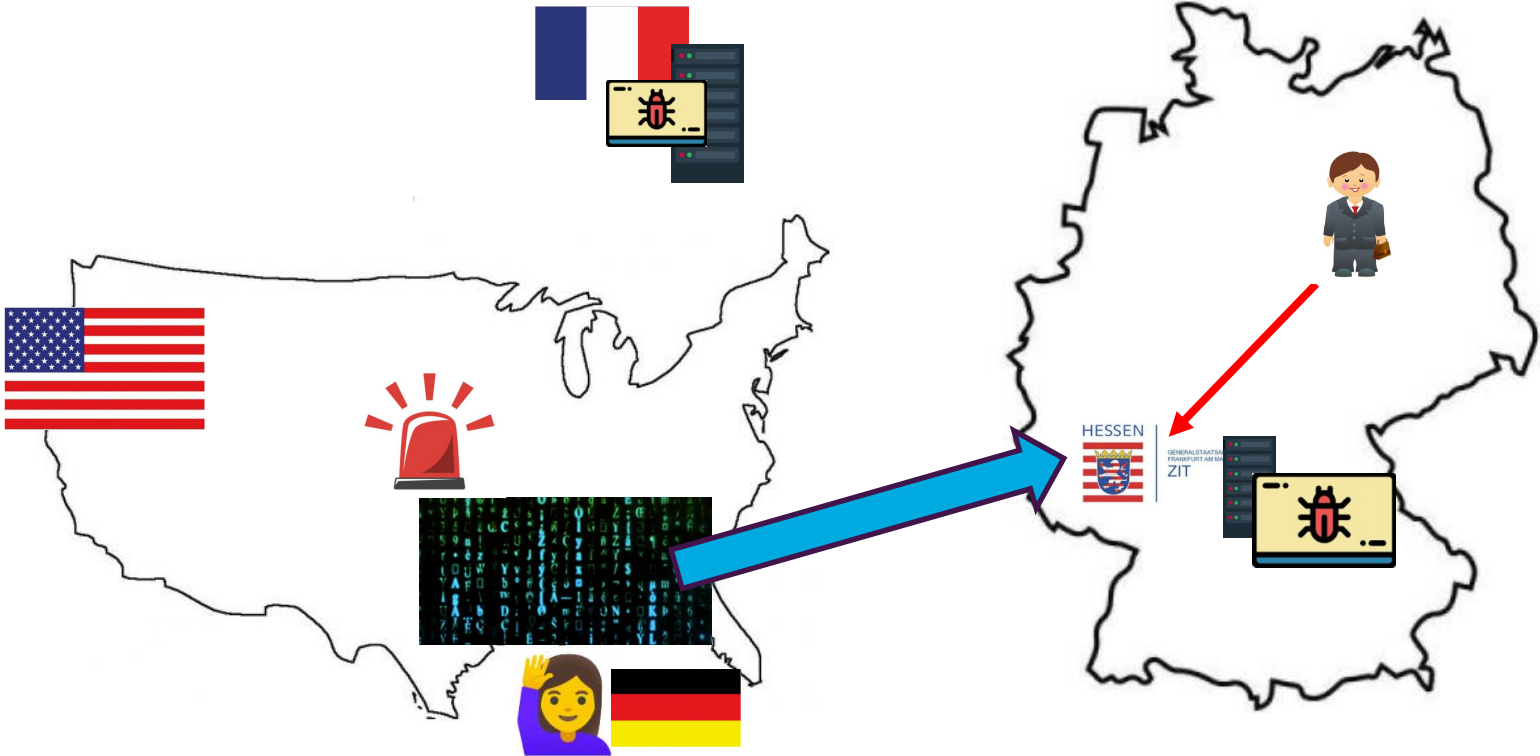


Haben wir ein systemisches Problem bei der Bekämpfung von CC?

- „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?



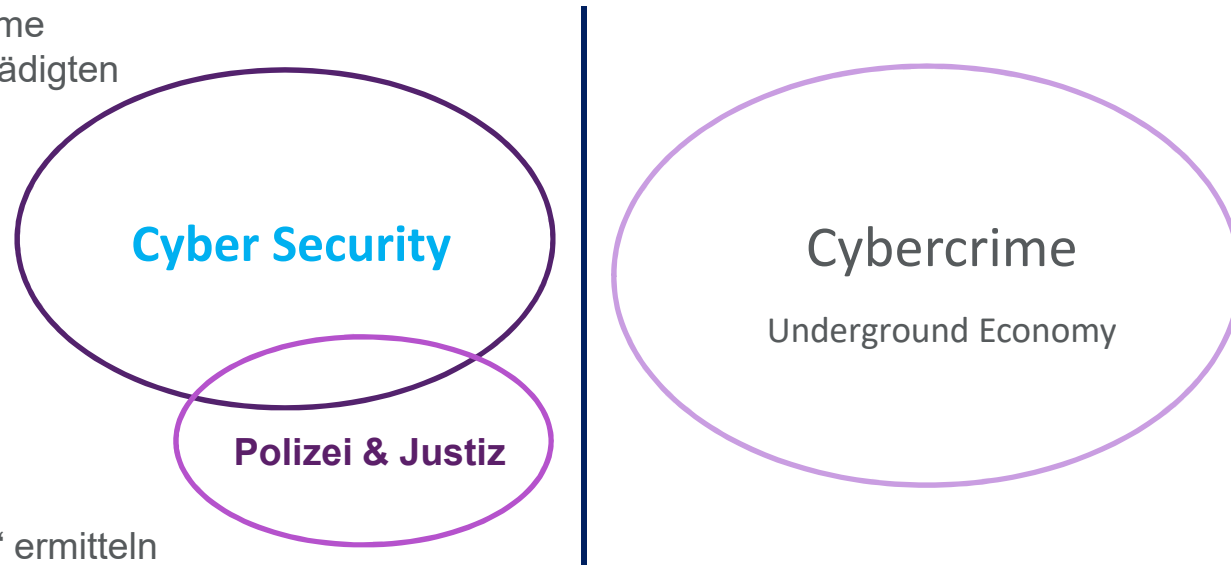
Ein neues Modell der Zusammenarbeit?



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

© Dentons. Dentons ist eine globale Wirtschaftskanzlei, die durch ihre Mitglieder und Partnerfirmen weltweit Beratungsleistungen für Mandanten erbringt. Dieses Dokument stellt weder rechtliche noch anderweitige Beratung dar und sollte nicht als solche verstanden werden. Auf Grundlage seines Inhaltes sollten daher weder Maßnahmen oder Handlungen ergriffen noch unterlassen werden. Ergänzend verweisen wir auf die rechtlichen Hinweise (Legal Notices) auf www.dentons.com.

© Dentons. Dentons is a global legal practice providing client service worldwide through its member firms and affiliates. This publication is not designed to provide legal advice and you should not take, or refrain from taking, action based on its content. Please see www.dentons.com for Legal Notices.

