Wirtschaftsbeirat Bayern, 05.Nov.2019
„Digitale Risiken in den Griff bekommen – Wie es in der Praxis funktionieren kann“

Cyber-Bedrohungen gestern, heute und morgen

Dr. Kai Buchholz-Stepputtis
Principal Security Consultant G4C

vorher 25 Jahre Commerzbank, die letzten 10 Jahre
Head of Information Security Consulting & Research

G4C – German Competence Centre against Cybercrime e.V.

Deutschland steht im Fokus von Cyber-Kriminellen

Chinesicher Hacker greifen DAX-Konzerne an

Die mutmaßlich im Auftrag chinesischer Behörden handelne Hackergruppe "Winnti" versuchte mindestens sechs DAX-Konzerne auszuspähen, darunter Siemens und BASF.

24.07.2019, 06:00 Uhr

Hackerangriffe auf DAX-Konzerne: Auch Siemens betroffen

Eine mutmaßlich chinesische Hackergruppe mit dem Namen "Winnti" hat über Jahre hinweg Konzerne ausspioniert. Recherchen von BR und NDR ergeben, dass ihr Schwerpunkt auf Deutschland lag. Sicherheitsbehörden beobachten die Hacker mit großer Sorge.

Datendiebstahl und Doxing bei Politikern und Prominenten

Ein Schüler sammelte persönliche Daten von rund 1.000 Politiker und anderen Personen des öffentlichen Lebens in Deutschland und stellte sie ins Netz.

REGIERUNG LÖST CYBER-ALARM AUS

Behörden wussten schon im Dezember vom Hacker-Angriff

+++ BKA und Geheimdienst ermitteln ++ Knapp 1000 Datensätze veröffentlicht ++ Merkel-Sprecherin: „Sehr, sehr ernster Vorfall“

Betriebsunterbrechung bei Krauss-Maffei nach Cyber-Angriff

Fertigung und Montage beim Wehrtechnik-Unternehmen KraussMaffei waren nach einem Ranswomware-Angriff zeitweise unterbrochen.

Cyber-Angriff auf Krauss-Maffei-Group: Mitarbeiter arbeiten jetzt eingeschränkt

Aktualisiert: 23.11.18 - 08:39

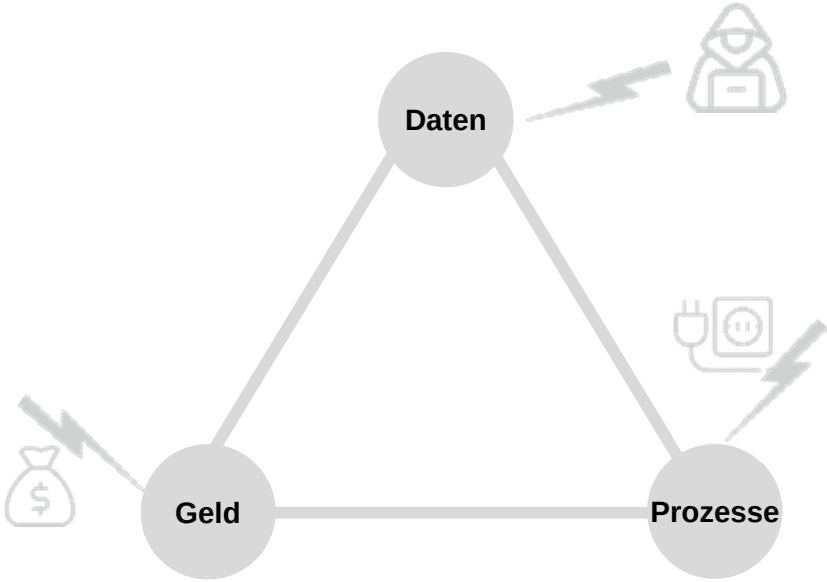
Cyber-Risiken für Unternehmen

Unternehmen im Fokus von Cyber-Kriminalität

- Cyber-Kriminalität ist laut Global Risk Report 2019 des World Economic Forum eines relevantesten Risiken auf globaler Ebene und das größte unmittelbare Risiko für Unternehmen.
- Dieses Risiko nimmt zu, was sowohl an der steigenden Zahl der Vorfälle als auch an deren Qualität sowie den erzeugten Schäden liegt.
- Das Gesamtvolumen der in den kommenden fünf Jahren erwarteten Schäden wird vom World Economic Forum auf acht Billionen USD geschätzt.
- Sowohl die Organisierte Kriminalität als auch Staaten und Innentäter treten als Akteure in Erscheinung

Risiken für Unternehmen

- Exfiltration von Daten
- Denial of Services/Betriebsunterbrechung (Sabotage, Erpressung etc.)
- Cyber-Diebstahl/Erpressung



Lagebilder

Bei Bedarf an weiteren Informationen, anbei Verweise auf die aktuellen (deutschen) Lagebilder dazu, z.B.:

BSI „Die Lage der IT-Sicherheit in Deutschland 2019“ (BSI, 17.10.2019)
https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html

BKA „Bundeslagebild Cybercrime“ (2018 wird ganz in Kürze erscheinen ...)
https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

Aber auch aus dem benachbarten (deutschsprachigen) Ausland, z.B.:

Halbjahresbericht 2019/1 MELANI (Schweiz, 29.10.2019)
(Melde- und Analysestelle Informationssicherung)
https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2019-1.html

Bericht Cyber-Sicherheit (Österreich, 28.06.2019)
https://www.onlinesicherheit.gv.at/service/publikationen/sicherheitsberichte/447940.html?2

Cyber-Bedrohungen gestern, heute und morgen
Ein Versuch, das etwas zu „sortieren“

1. Was bedeutet „Cyber-Bedrohungen“
2. Cyber-Security, Cyber-Crime, Cyber-Activism, Cyber-Spionage, Cyber-Sabotage/Terrorism, Cyber-War
3. Branchenübergreifende Cyber-Bedrohungen, z.B. CEO-Fraud, Ransomware
4. Branchenspezifische Cyber-Bedrohungen, z.B. Financial Cyber-Crime, Intellectual Property, „Kritische Infrastrukturen“, sonstige Branchen, ...
5. Was kann konkret und effizient getan werden ?

Cyber-Bedrohungen und Cyber-Security ganz allgemein

- Informationen und Assets von Unternehmen und Institutionen liegen zunehmend in (nur noch) rein digitaler Form vor, auch die Datenmengen nehmen ständig zu

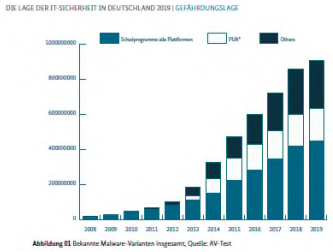


Abbildung 01 Bekannte Malware-Varianten insgesamt, Quelle: AV-Test

- Die digitale Vernetzung (Anzahl Systeme und Schnittstellen) steigt stetig, sowohl intern, als auch in der Lieferkette und zu Partnern/Kunden

- Die Komplexität nimmt dabei automatisch ebenfalls permanent zu

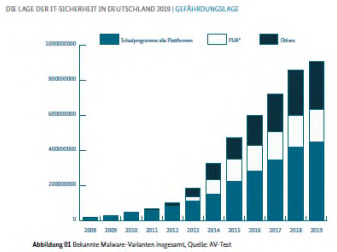
=> Sicherheitsziele der Cyber-Security sind „CIA“ (Confidentiality, Integrity, Availability); also Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Daten

=> Cyber-Bedrohungen sind Bedrohungen, die diese Sicherheitsziele gefährden können

=> Die Anforderungen auch an solche „ganz normale Cyber-Security“ steigen also schon tatsächlich leider stetig an ...

Verschiedene Arten von Cyber-Bedrohungen

Es macht Sinn etwas zu differenzieren, grobes Raster dazu z.B. ...



- **„Herkömmlicher“ Cybercrime:** Meist nichtstaatlichen Akteuren geht es mit kriminellen Mitteln schlicht um finanziellen Gewinn (lediglich „Tatmittel Internet“ oder gar „Cybercrime im engeren Sinne“ ?)

- **Cyber-Spionage:** Erlangung von „Intellectual Property“ oder sonstigen strategisch/operativ interessanten Informationen zum (wirtschaftlichen) Vorteil Akteure „gemischt“, je nach Aufgabenstellung und Zielsetzung

- **Cyber-Activism:** Idealistisch, politisch oder schlicht aus Neugier oder Geltungsbedürfnis motivierte Aktionen von i.d.R. nichtstaatlichen Akteuren
- **Cyber-Sabotage/Terrorism:** (Destruktive) Angriffe staatlicher/nichtstaatlicher Akteure

- **Cyber-War:** (Kriegerische oder kriegsähnliche) Auseinandersetzungen staatlicher Akteure mit „Cyber-Waffen“ (in der Praxis meist noch unterschwellig/verdeckt)

Verschiedene Arten von Cyber-Bedrohungen

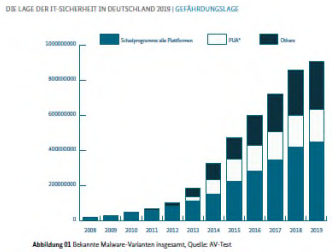


Abbildung 01 Bekannte Malware-Varianten insgesamt, Quelle: AV-Test

Auch hier macht es Sinn etwas zu differenzieren ...
Nämlich vor allem zu unterscheiden zwischen:

- **Branchenunabhängigen Cyber-Bedrohungen,**
  die branchenübergreifend jedes Unternehmen bzw. Institution betreffen können

- **Branchenspezifischen Cyber-Bedrohungen,**
  die überwiegend nur für gewisse einzelne Branchen relevant sind,
  für andere Branchen aber eine eher untergeordnete Bedeutung haben

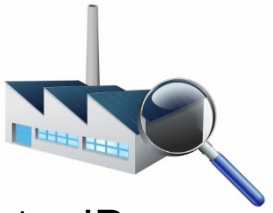
- **Unternehmensindividuellen Cyber-Bedrohungen,**
  die ganz spezifisch für nur gewisse einzelne Unternehmen zutreffen
  oder ganz unternehmensspezifische Charakteristika aufweisen,
  für andere Unternehmen aber relativ irrelevant sein können

Beispiele branchenspezifischer Cyber-Bedrohungen

Banken und Zahlungsverkehr

- Schwerpunkt „herkömmlicher“ Cybercrime
- Online-Banking: „Phishing“ und „Banken-Trojaner“
  (in der Praxis überwiegend als Angriffe gegen Kunden bzw. Kundensysteme)
- Kreditkarten „card not present“: wie oben plus ggf. „Data Leakages“ bei Betreibern

=> Banken sind indirekt über ihre Kundenbeziehungen auch mit vielen anderen Spielarten des Cybercrime befasst, da dieser i.d.R. Zahlungen auslöst.



Industrie und produzierendes Gewerbe

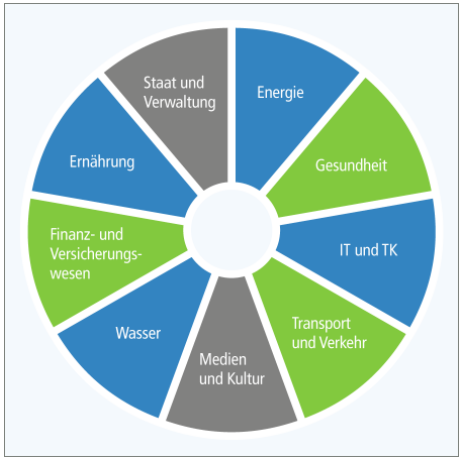
- Schwerpunkt „Cyber-Spionage“ gegen Intellectual Property
- Faktisch muss man davon ausgehen, dass jedes Unternehmen mit relevanter IP Ziel und Gegenstand von solchen Angriffsbemühungen ist !

=> Im worst case bleiben solche Angriffe monatelang (oder gar völlig) unentdeckt

Beispiele branchenspezifischer Cyber-Bedrohungen

„Kritische Infrastrukturen“

Im Sinne der EU-Richtlinie 2008/114/EG ist eine „**kritische Infrastruktur**“ eine Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung ist und deren Störung oder Zerstörung erhebliche Auswirkungen hätte, da ihre Funktionen nicht aufrechterhalten werden könnten



- Hauptmotivation der staatlichen Initiativen primär „Verfügbarkeit“
- Dort betrachtete Cyber-Bedrohungen bzw. Angriffsszenarien daher auch eher aus dem Umfeld Cyber-Sabotage/Terrorism/War
- Hier können sich nun diverse (aber längst nicht alle) Branchen wiederfinden, bzgl. Einzelunternehmen ist aber meist gewisse Systemrelevanz vorausgesetzt

=> Wer dazu gehört, hat schon durch IT-Sicherheitsgesetz und Co. gewisse „Mindest-Hausaufgaben“ zu machen (siehe z.B. §8 IT-Sicherheitsgesetz) (die ihn für seine ganz individuellen Bedrohungen aber u.U. kaum voranbringen)

Beispiele branchenspezifischer Cyber-Bedrohungen

Weitere Beispiele für sehr branchenspezifische Cyber-Bedrohungen

- **Telekommunikationsanbieter:** z.B. Angriffe gegen TK-Anlagen, Missbrauch von „Mehrwertdiensten“, „Gebühren-Karusselle“, Roaming-Protokolle (SS7), ...
- **Internet-Service-Provider:** z.B. Ressourcenverbrauch durch SPAM/Bot-Netze, „schwarze Schafe“ im eigenen Netzwerk, ...
- **Verkehr (Bahn, Airlines):** z.B. Missbrauch Buchungssysteme für Cashout, ...
- **Logistik B2C:** z.B. Warenlieferungsbetrug, Stichwort u.a. „Packstation“, ...
- **Logistik B2B:** z.B. Missbrauch Tracking-Systeme LKWs, ...
- **E-Commerce/Online-Shops:** z.B. Missbrauch Warenbestellungen, ...
- **File Sharing Dienste**: z.B. Diebstahl von Bitcoin-Wallets, ...
- **Online-Wettbüros/Gaming:** z.B. DDOS-Angriffe, u.a. kurz vor Großereignissen, ...
- usw. usw. usw. (das können Sie ggf. besser beurteilen und einschätzen)

Branchenspezifische Cyber-Bedrohungen

Was also nun als Hinweis für die einzelne Branche oder gar einzelnes Unternehmen/Institution bzgl. solch individueller Cyber-Bedrohungen?

- Eine genauere Kenntnis Branchen- oder gar Unternehmensspezifischer Cyber-Bedrohungen erfordert genaues Branchen oder gar Unternehmens-Knowhow
- Neben allgemeiner Kenntnis von ggf. relevanten Cyber-Bedrohungen ...
- ... wäre dazu also vor allem Ihr ganz eigenes Branchen- oder gar Unternehmensspezifische Knowhow und Erfahrung gefragt

- Das kann Ihnen kein branchenfremder Cyber-Security-Experte ersetzen, er kann ggf. aber Methoden einbringen, die Ihnen helfen, das für sich selber zu erarbeiten
- Methoden neben diversen „Self Assessment Standard-Fragebögen“ dazu u.a. Workshops im Sinne „Identify your Crown Jewels“
- Ferner Aufsetzung gutes Reporting über Cyber-Incident- und Fraud-Management

Branchenunabhängige Cyber-Bedrohungen

Neben solchen allgemeinen Anregungen zur Beschäftigung mit der eigenen, ggf. ganz branchenspezifischen oder gar unternehmensindividuellen „Cyber-Bedrohungslage“ ...

... zurück zu den aktuell relevantesten branchenübergreifenden Cyber-Bedrohungen gegen wirklich alle Unternehmen/Institutionen:

„CEO-Fraud“ und Co

- Seit etwa 2014, Tendenz in „Westkontinentaleuropa“ eher leicht abklingend, aber nach wie vor auch hier noch „virulent“
- Prominente Fälle aus dem deutschen Sprachraum z.B. FACC (Dez.2015, 50 Mio EUR), Leoni (Aug.2016, 40 Mio EUR)

Ransomware gezielt gegen Unternehmen und Institutionen

- „Historisch“ prominente Fälle u.a. Krankenhaus Neuss (Feb.2016), Deutsche Bahn (Mai.2017), Maersk (Jan.2018)
- „Echt gezielt“ gegen Unternehmen/Institutionen seit 2018, Tendenz stark zunehmend
- Für aktuelle Beispiele einfach eine News-Suche nach „Ransomware“ (liefert tagesweise Resultate von Kammergericht Berlin bis Fa. Pilz …)

Branchenunabhängige Cyber-Bedrohungen
„CEO-Fraud“ und Co.

„CEO-Fraud“, auch bekannt als „Fake President“

- Täter geben sich gegenüber (gezielt ausgesuchten) Mitarbeitern eines Unternehmens als vermeintlicher „CEO/CFO“, „President“ o.ä. aus
- Tatmittel dazu meist E-Mail mit mehr oder weniger gut gemachten Absender-Adressen (von „CFO@googlemail.com“ bis zu „CFO@xy-firma.com“) bis zu ggf. sogar übernommenen echten Firmenkunden Mail-Accounts
- Stories variierend (oft „Firmenübernahmen“, aber auch „Strafzahlungen“ etc.)
- Grundprinzip aber immer: Zwingend hochgeheim, es darf mit absolut niemand darüber gesprochen werden !!!
- Gerne wird im Verlauf dritte Partei (z.B. entsprechende „Rechtsanwälte“, Wirtschaftsberatungen o.ä.) eingeführt, die das weitere Procedere und Abwicklung übernehmen sollen
- Am Ende sind typischerweise 5-6 stellige Zahlungsanweisungen fällig
- Bei offensichtlicher Leichtgläubigkeit (d.h. „Erfolg“ bei erster Zahlung) wird ggf. versucht bis zur „Schmerzgrenze“ nachzulegen

Branchenunabhängige Cyber-Bedrohungen
„CEO-Fraud“ und Co. (verwandte Modi Operandi)

Gefälschte Rechnungen / Invoice Fraud

- Täter platzieren komplett gefälschte Rechnungen, oder versuchen Rechnungen bekannter Zahlungsempfänger mit gefälschten Bankverbindungen einzuschleusen

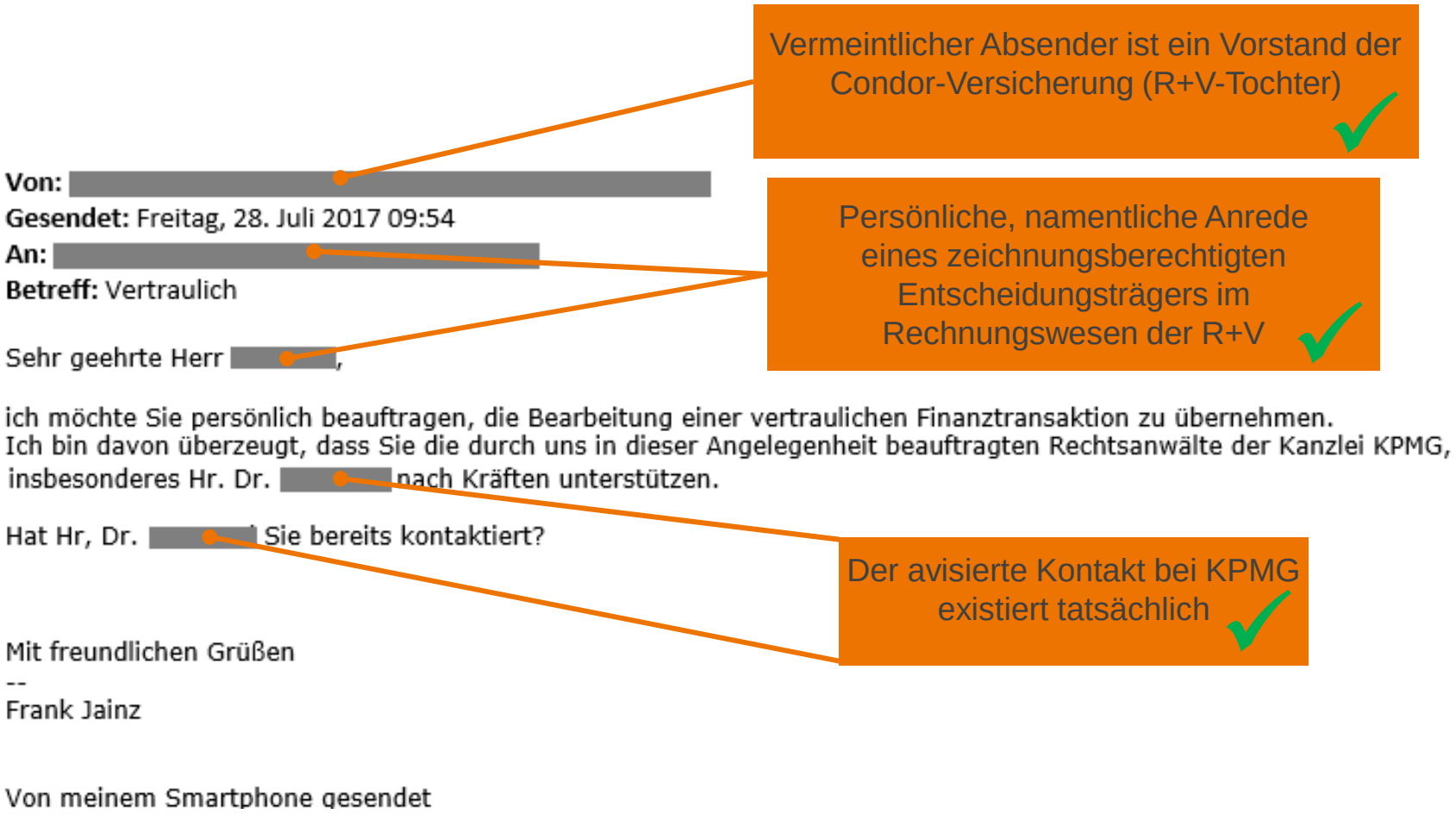
Mandatsbetrug / Mandate Fraud

- Täter geben sich gegenüber der Firma als vermeintlicher Lieferant aus und teilen mit, dass sich die Bankverbindung geändert habe
- Folgt die Buchhaltung dieser Anweisung ohne Rückfragen/Kontrollen, erfolgen zukünftige Rechnungsbegleichungen dann auf die „neue Bankverbindung“
- Nach einiger Zeit (das kann sich hinziehen …) meldet sich der echte Lieferant, dass er schon länger keine Zahlungseingänge mehr zu verzeichnen hatte …

Business E-Mail Compromise (BEC)

- Im angelsächsischen Sprachraum oft verwendete Bezeichnung für CEO-Fraud
- Eigentlich inhaltlich dadurch völlig verkürzt dargestellt, da „fortgeschrittener“ CEO-Fraud bei weitem mehr Methoden einsetzt als nur „faked E-Mails“

Branchenunabhängige Cyber-Bedrohungen
Beispiel zu einem CEO-Fraud / Social Engineering



Branchenunabhängige Cyber-Bedrohungen
Ransomware gezielt gegen Unternehmen und Institutionen

Ransomware gezielt gegen Unternehmen und Institutionen

- „Historisch“ prominente Fälle u.a. Krankenhaus Neuss (Feb.2016), Deutsche Bahn (Mai.2017), Maersk (Jan.2018)
- Gegen Privatpersonen eigentlich „ein alter Hut“
  „Gezielt“ gegen Unternehmen/Institutionen seit etwa 2018, Tendenz stark zunehmend
- Für aktuelle Beispiele einfach eine News-Suche nach „ransomware“
  (liefert tagesweise Resultate von Kammergericht Berlin bis Pilz …)

- Eigentlich hätten wir hier genau im Detail zu erklären versucht, wie dies „funktioniert“ und was man präventiv, detektiv und reaktiv dagegen tun kann
- In Rücksichtnahme auf unseren Nachredner (mit genau diesem Thema) haben wir hier aber nun auf größere weitere Detail-Erläuterungen verzichtet
- Die Einschätzung, dass dies die derzeit mit Abstand größte „Cyber-Bedrohung“ für eigentlich alle Unternehmen/Institutionen darstellt,
  teilen wir zu 100% mit unseren heutigen Gastgeber/Veranstalter

Branchenunabhängige Cyber-Bedrohungen
Ransomware gezielt gegen Unternehmen und Institutionen

**Warum sehen wir – abgesehen von „aktuellen Tagesschwankungen“ –
Ransomware gezielt gegen Unternehmen und Institutionen
als die derzeit aktuell mit Abstand größte Cyber-Bedrohung an ?**

- Bei DDOS droht ggf. temporäre Nichtverfügbarkeit ...
  (schlimm genug, bringt die meisten Unternehmen aber nicht zur Existenzgefährdung)

- Bei CEO-Fraud drohen ggf. größere monetäre Verluste bis zu 50 Mio. EUR
  (eher noch schlimmer und kann ggf. auch mal an Existenzgefährdung heranreichen)

- **Bei gezielter Ransomware gegen Unternehmen/Institutionen droht
  im worst case aber sogar die komplette und endgültige
  Einstellung des Geschäftsbetriebs !!!**

Konkrete Handlungsempfehlungen ? – Fazit

Bei diesen beiden aktuell relevantesten branchenübergreifenden Cyber-Bedrohungen,

- „CEO-Fraud“ und Co
- Ransomware gezielt gegen Unternehmen und Institutionen

kann jeder – wenn er es nicht ohnehin schon angefangen/erledigt hat – sofort was tun !

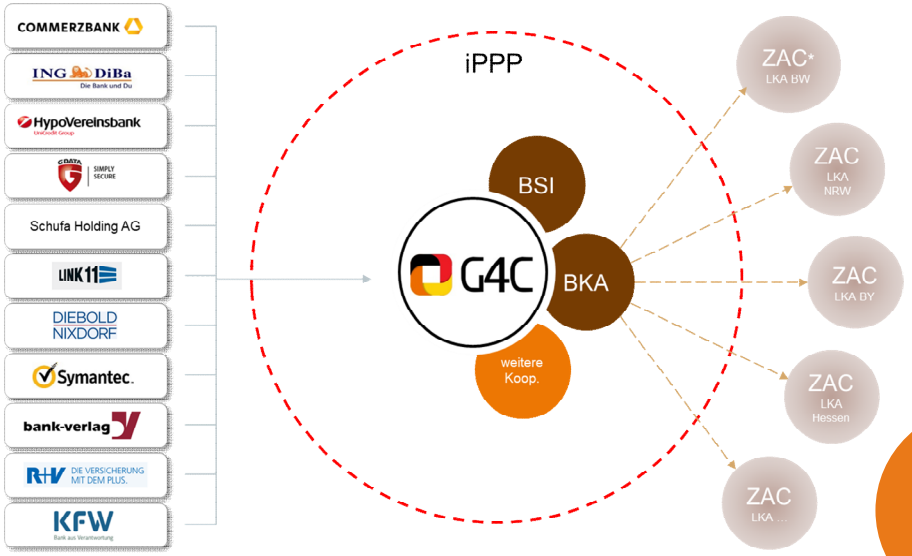
Und hier gibt es auch sehr gutes umfassendes und verständliches Material dazu, z.B.:

- Broschüre des Bankenverbandes zu „CEO-Fraud “
  (G4C-Mitgliedsbanken wesentlich daran beteiligt)
  Online zum Download unter https://bankenverband.de/publikationen/
- Broschüre des G4C zu
  „Ransomware gezielt gegen Unternehmen und Institutionen“
  (ganz aktuell und anbei auch als „Take-Away“)

Der Unterschied bei solchen „branchenübergreifend“ angelegten Broschüren ist der wirklich „branchenübergreifende Ansatz“ !
Dies kann Ihnen ggf. Mio. EUR an Kosten ersparen ...

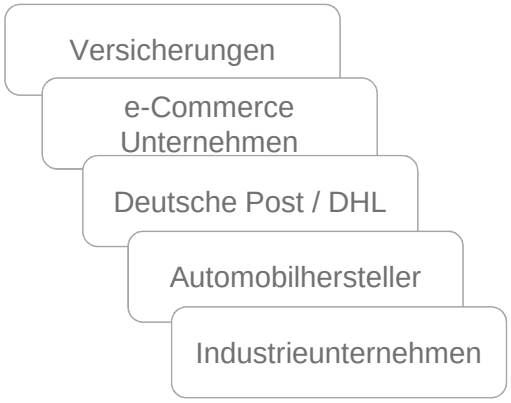
Kurzvorstellung G4C

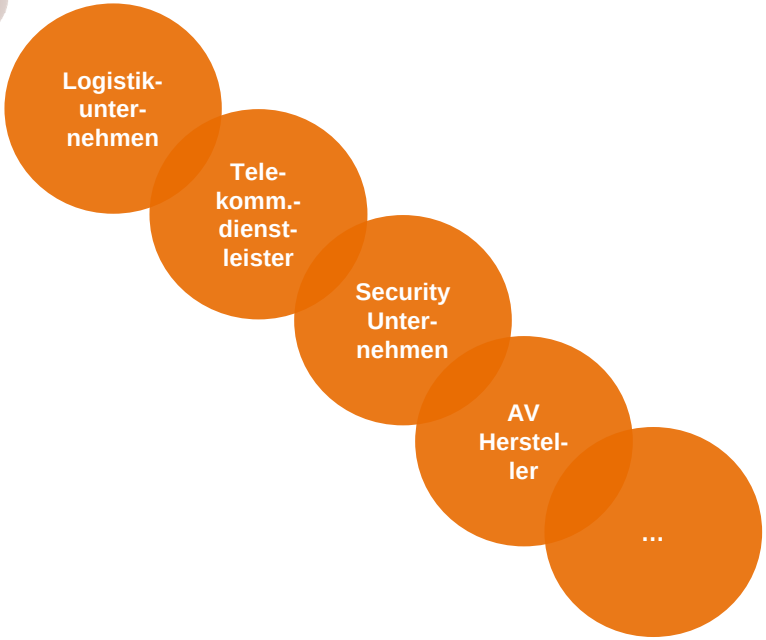
Ausbau und Zusammenarbeit auch über Branchen hinweg



Die Täter und somit die generelle Gefährdungslage im Bereich Cybercrime machen keinen grundsätzlichen Unterschied zwischen Branchen; lediglich das Motiv und das Vorgehen unterscheiden sich.

Somit ist eine branchenübergreifende und unterstützende Ausrichtung notwendig und sinnvoll !





Kurzvorstellung G4C

Alleinstellungsmerkmal und Ausrichtung - der Unterschied

Sicherheit

- Made in Germany
- eigene technische Infrastruktur
- Datensicherheit

Kooperation

- BKA (Bundeskriminalamt)
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
- Netzwerk von Experten unterschiedlicher Branchen

Zusammenarbeit

- Strategisch/operativ tätig und ggf. „Hands on“
- Workshops/Aktivitäten auf Wunsch der Mitglieder
- Gemeinnützig, nicht kommerziell

Schutz

- vertrauensvoll
- anonym(isiert)
- Informationsschutz

Kurzvorstellung G4C

Als gemeinnütziger Verein hat sich das German Competence Centre against Cybercrime (G4C) zum Ziel gesetzt, präventiv, ermittelnd und reaktiv gegen Angriffe im Cyberraum vorzugehen. G4C fungiert so als Know-how-Träger, Frühwarnsystem und Initiator eines regelmäßigen Austauschs über Bedrohungen aus dem Netz.

Operative Kooperationspartner sind das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI). Darüber hinaus besteht auch international ein Informationsaustausch mit relevanten Stellen zur Bekämpfung von Cyberangriffen

Die Arbeit des Vereins basiert auf vier Säulen: G4C baut sukzessive eine aktuelle Datenplattform neben dem direkten persönlichen vertraulichen Austausch als Frühwarnsystem aus, übernimmt Datenausleitungen für das BKA und andere Ermittlungsbehörden, und engagiert sich in der Aus- und Fortbildung sowie bei Zuverlässigkeitsüberprüfungen zur Kompetenzstärkung von Cybersicherheitsbeauftragten.

Gründer und Initialmitglieder von G4C sind Banken und Versicherungen; der Verein weitet seine Kompetenz jedoch konsequent auf weitere Branchen aus.

Kontakt

German Competence Centre against Cybercrime e. V. (G4C)
Eingetragen im Vereinsregister Wiesbaden unter der Nummer VR 6806

Postanschrift der Geschäftsstelle:
Borsigstraße 34, 65205 Wiesbaden

Telefon:
06122 178 4800

Vorstand:
Roland Wolf, Heiko Wolf, Tibor Konya