Krieg im Homeoffice?

Perspektiven zu Cyberwar und digitaler Sicherheit

Dustin Dehez
Geschäftsführer/Managing Director

28.04.2020, 17:00 – 18:30 Uhr
Konrad-Adenauer-Stiftung e.V.
Politisches Bildungsforum Baden-Württemberg
Landesbüro Stuttgart

Cyberwar im Überblick

Definitionen des Cyberkrieges

Cyberwar Definition

- Cyberwar beschreibt den Konflikt zwischen verschiedenen Akteuren im Cyberspace
- Die Nationalen Sicherheitsberater (U.S.) definieren 2010 Cyberwar als: „*Handlungen eines Nationalstaates, die darauf abzielen, in die Computer oder Netzwerke einer anderen Nation einzudringen um Schaden oder Unterbrechungen zu verursachen“*

Cyberwar Aktionen

- Störung von Infrastruktur und Dienstleistungen
- Informationen auspionieren und stehlen

Manche Experten argumentieren: Cyberwar ist weder
- *Cyber-Spionage* (Informationen stehlen, sich gegenseitig ausspionierende Staaten und Spionage des privaten Sektors)
- *Cyber-Kriminalität* (Hacken mit Fokus auf Profit; z.B. durch Lösegeld „ransomware“)
- *Informationskrieg* (Verbreitung von Desinformation, Fake News und Propaganda; z.B. "influence operations")

Motive für Cyberwar

Motivationen für Cyberwar Akteure

- Geringes Risiko für Täter aufgrund von *plausible deniability*
  - Problematik für die Opfer von Cyberwar Attacken → Wer ist Verantwortlich für den Angriff?
  - Und wer zahlt für die verursachten Kosten → notpetya und Maersk

- Geringe Kosten für Täter im Vergleich zur „klassischen“ militärischen Ausrüstung

Bekanntheit

Störung

Geld

Information

Zugang

Methoden des Cyberwar

DDoS (distributed denial of service)

- DDoS Attacken zielen darauf ab, ein Netzwerk oder einen Server mit Datenverkehr zu überlasten → z.B. geht die Website dann offline
  - 2016 wurden die Webseiten von BBC und von Donald Trump's Wahlkampf von einer großen DDoS Attacke getroffen

Malware (Malicious Software)

- Jede Software die darauf ausgelegt ist einem Computer Schaden zuzufügen
  - Einschließlich Computerviren, Würmern, Trojanischen Pferden, Ransomware
- Ein speziell entwickelter bösartiger Code um physische Systeme zu stören
  - Beispiele sind Stuxnet (2010 Zerstörung einer Zentrifugen in einer iranischen Nuklearanlage) und Crash Override (201 Ausfall des Stromnetz in der Ukraine)

Ransomware

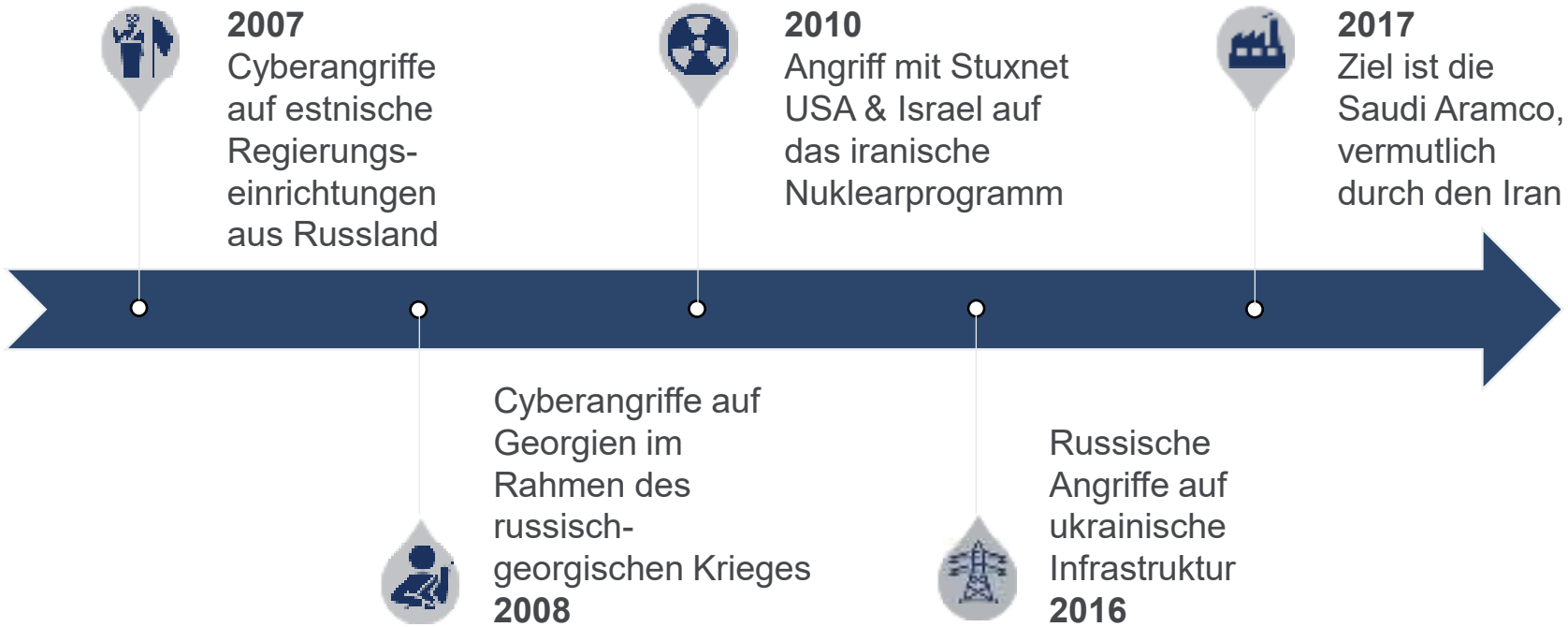
- Ransomware ist eine Art von Malware die den Zugriff auf Daten oder ein Computersystem verweigert, bis das Lösegeld bezahlt ist
  - Ein norwegischer Aluminiumhersteller wurde von der Ransomware-Attacke "LockerGoga" schwer getroffen. In der ersten Woche kam es zu einem Verlust von bis zu 35-40 Mio. US$

Disinformation campaign

- Propaganda & Fake News
- Beeinflussung der öffentlichen Meinung
  - Russlands Einmischung in die US-Wahl 2016
  - Chinas Bemühungen bei den taiwanesischen Präsidentschaftswahlen 2020

Source: https://www.upguard.com/blog/ransomware

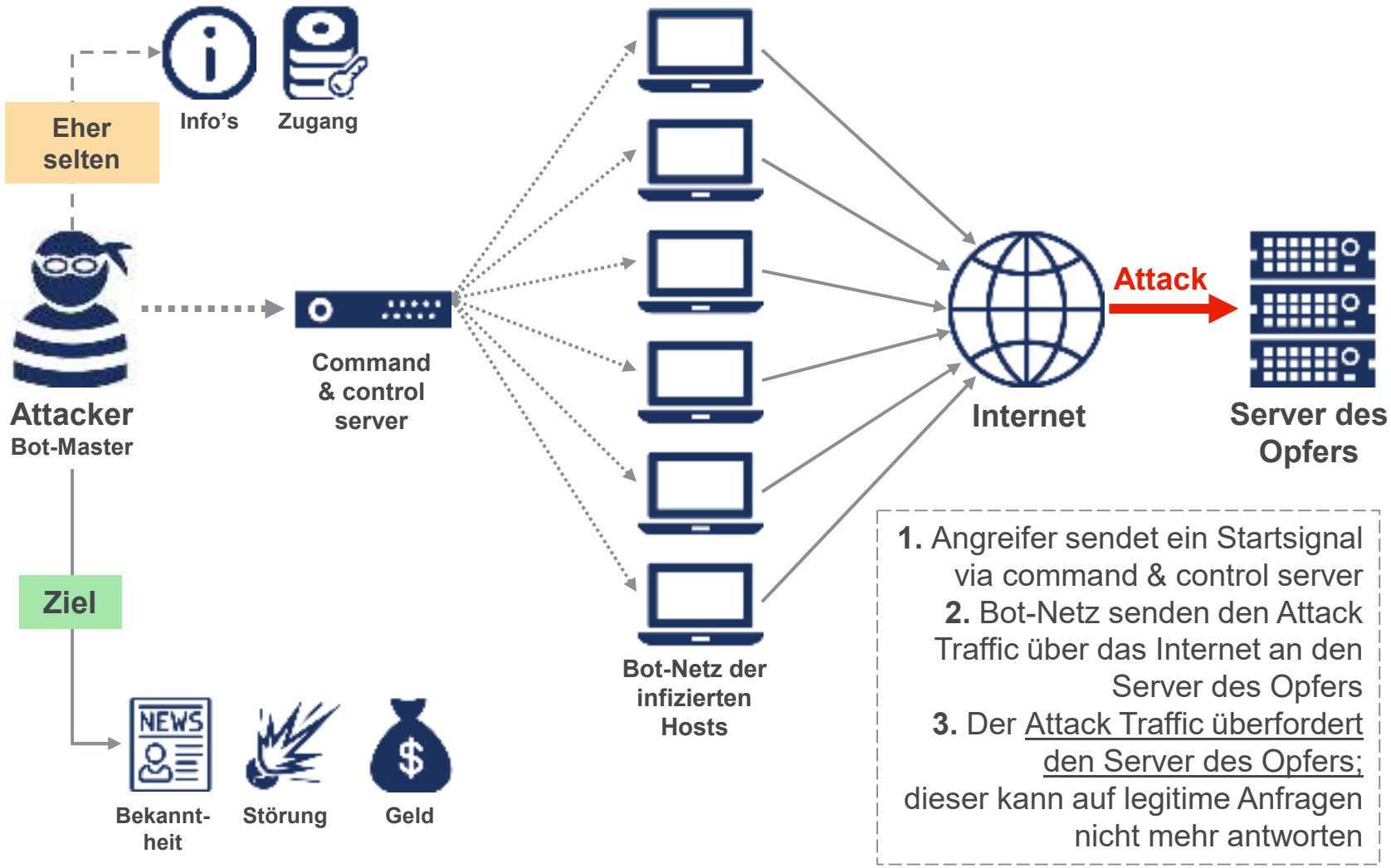
Zeitachse – Wesentliche Beispiele für Cyberangriffe



Source: https://www.ft.com/content/fcf2a06c-c8ae-11e9-af46-b09e8bfe60c0?shareType=nongift

Einführung in Distributed Denial-of-Service (DDoS) Attacks

Wie funktioniert eine DDoS Attacke – Vereinfachte Darstellung



Source: https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack-

Highlights der DDoS Attacken im Jahr 2019

Januar
Staatliche IT-Infrastrukturen von Simbabwe werden Ziel von politisch motivierten Attacken durch Anonymous

März
Energieversorger im Westen der USA wird attackiert und es kommt zur Betriebs-unterbrechung für 10h

Mai
Internetanbieter in Italien werden attackiert, dabei sollten Bitcoins erpresst werden

September
Die Website der Börse in Hong Kong ist nach einem Angriff offline, es können keine Kurse mehr angezeigt werden

Oktober
Cloud-Provider AWS wird attackiert und Infrastruktur fällt in Teilen bis zu 8h aus

Oktober
Erpressung durch Attacken auf mehrere Banken in Süd-Afrika. Dabei kommt es zum Ausfall von Online-Banking

November
Wahlkampf auf verschiedenen digitale Kanäle der britischen Labour Party wird angegriffen

Norton (U.S. Hersteller für Antivirenprogramme) beschreibt DDoS-Attacken als **eine der mächtigsten Waffen im Internet**

Source: https://www.link11.com/en/downloads/ddos-report-for-the-full-year-2019/

UN und der Cyberspace

Aus der Rede des UN Generalsekretär António Guterres über Cyberwar auf der Münchener Sicherheitskonferenz 2018

Neben der nuklearen Kriegsführung sind Cyberkriege zwischen Staaten eine globale Bedrohung

Recht und Cyberspace

- Ob und wie die Genfer Konvention & int. Völkerrecht Anwendung auf Cyberwar und Aktionen im Cyberspace finden bleibt offen
- "… die Diskussionen über den internationalen Rechtrahmen, in dem Cyberwar stattfindet, sind unerlässlich"

Verschiedene Akteure

- Die Besorgnisse gehen über Cyberwars hinaus und beziehen sich auf die permanente Verletzung der Cybersicherheit durch verschiedenen Akteure (Staaten, kriminelle Org., Terroristen etc.)
- Diese schaffen ein hohes Maß an Bedrohung auf welches es keine angemessene Antwort gibt

Fehlender Konsens

- Es gibt Schwierigkeiten, die verschiedenen Methoden der Regulierung auf nat. und int. Ebene auf den Cyberspace anzuwenden
- Darüber hinaus gibt es "... einen Mangel an Konsens in der internationalen Gemeinschaft darüber, wie das sogenannte "Internet of things" zu regulieren ist

Mehrere Interessenvertreter

- Ein Ansatz mit mehreren Beteiligten würde Regierungen, Privatsektor, Zivilgesellschaft und die akademische Welt zusammenbringen
- Dabei könnten Fortschritte erzielt und grundlegende Protokolle erstellt werden, um den Cyberspace zu einem Instrument für das Gute zu machen

Source: https://www.un.org/press/en/2018/sgsm18900.doc.htm

Cybersicherheit aus Perspektive anderer Organisationen

Summary of Tallinn Manual 2.0 (2017)
International law experts on Cyber Operations

- *Rule 1:* " The Principle of Sovereignty applies to cyberspace"

- *Rule 4:* "A State must not conduct cyber operations that violate the sovereignty of another State."
  - "For example, if an agent of one State uses a USB flash drive to introduce malware into cyber infrastructure located in another State, a violation of sovereignty has taken place."

- *Rule 14:* "A State bears international responsibility for a cyber related act that is attributable to the State and that constitutes a breach of an international legal obligation."
  - "The cyber actions of state organs, such as the CIA or NSA in the United States, are attributable to the state."

Many discussions are about **attributing cyber actions of non-state actors (proxies) to states** with whom those actors are aligned

- *Rule 17:* "In accordance with international law, cyber operations conducted by non-state actors, but carried out under the "**effective control**" of a state, are attributable to the state"
  - Cases in which States finance, organize, train, supply or select targets of a non-state group has been found not enough to reach the 'effective control' threshold
    - A state could provide cyber tools, identifying the targets, and selecting the date for the cyber operation to take place and it would still not implicate state responsibility
    - Example: Russian cyber attack on Estonia in 2007

Key question: When can states be hold accountable for cyber attacks, which are carried out by non-state groups?

Source: Jensen (2017), The Tallinn Manual 2.0: Highlights and Insights https://ssrn.com/abstract=2932110

NATO CCD COE & The Global Cybersecurity Index

Wesentliche Trends
- Mehr Staaten entwickeln Nationale Cyberstrategien
- In fast allen Staaten wird die Cybersicherheit als Teil der Nationalen Sicherheitsstrategie verstanden

NATO Strategisches Konzept
Cyberspace wird als Domäne der Kriegführung verstanden, ähnliche wie See-, Luft- und Land

Global Cybersecurity Index
- Der Index zeigt die Verpflichtung der Staaten auf die Cybersicherheit und den Reifegrad ihrer Cyberstrategien
- 5 Säulen zeigen
  - (i) legislative Maßnahmen, (ii) technische Vorkehrungen, (iii) organisatorische Maßnahmen, (iv) Capacity Building, und (v) Kooperatiom
- The index is based on a multi-stakeholder approach and initiative
  - UNDESA, UNODC, Global Cyber Alliance, Interpol, European Cybersecurity Organization, Economic Community Of West African States (…)
- The International Telecommunication Union (ITU) provides the general foundation and framework for the index

Source: https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

Cybersicherheit in Deutschland
- Blick auf die Sicherheitsorgane

Wichtige Einrichtungen der Sicherheitsbehörden

Innenministerium

- Die *Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITIS)* ist ein 2017 gegründeter Dienstleister der Sicherheitsbehörden
  - Entwickelt Tools für das Bundeskriminalamt, Verfassungsschutz und Bundespolizei

Verteidigungsministerium

- Das *Cyber Innovation Hub* dient als Schnittstelle zwischen Start-up Szene und der Bundeswehr
  - Das Ziel ist es die „digitale Innovationen innerhalb der Bundeswehr voranzutreiben“

Innenministerium und Verteidigungsministerium

- Die *Agentur für Innovation in der Cybersicherheit* wurde 2018 beschlossen und wird vorrausichtlich 2020 gegründet
  - Koordiniert Forschungsaufträge mit dem Schwerpunkt auf „Digitale Innovationen in der Außen-, Sicherheits- und Verteidigungspolitik“
  - Bundesrechnungshof bemängelt in einem Bericht die Finanzierung und Personal, darüber hinaus wird auch der Sinn des Projekts in Frage gestellt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Das *Cyberabwehrzentrum* koordiniert die operative Zusammenarbeit von Cyberschutz- und Abwehrmaßnahmen
  - Verschieden Gefährdungen: Cyberspionage, -terrorismus und -kriminalität
  - Das Ziel ist es einen schnellen Informationsaustausch/Bewertungen zu ermöglichen und daraus konkrete Handlungsempfehlungen abzuleiten

Überschätzte Cyber-Abschreckung?

Aus anderen Bereichen lernen

- Terrorismusforschung deuten darauf hin, dass Abschreckung durch Vergeltung eher gegen Staaten funktioniert, jedoch nicht gegen nicht-staatliche Akteure

Außenpolitisch ist Deutschland oftmals eher zurückhaltend

- Sicherheitsforscher bezweifeln ob die deutsche Politik dazu bereit ist, eine aktive Cyber-Abwehr zur Abschreckung einzusetzen und die Konsequenzen einer Eskalation zu ertragen
- Daher ist eine aktive Cyberabwehr nur glaubwürdig, wenn Deutschland bereit ist in die Eskalationsdynamik im Cyber-Raum einzutreten

Defensive vs. Aktive Cyberabwehr?

- Aufgrund der Defizite in den bisherigen *„deterrence by punishment“* (Aktiv) Bestrebungen Deutschlands plädieren Sicherheitsforscher für eine Verstärkung der *„deterrence by denial“* (Defensiv) Strategie

→ Wie geht aktive Verteidigung überhaupt: Sind 0-Day Kataloge in Deutschland überhaupt zulässig?

Source: https://www.swp-berlin.org/10.18449/2019A39/

Cybersicherheit in Deutschland - Blick auf den Zivilbereich

Ausschnitt wichtige Akteure im Bereich Cybersicherheit

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- 1991 wurde das BSI gegründet und gehört zum Geschäftsbereich des Innenministerium
- Die Aufgabe des BSI ist es die Sicherheit in der Informationstechnik des Bundes zu stärken
- Das BSI tritt als unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit auf
- Das BSI ist unter anderem an der Ausarbeitung von Gesetzten, Standards und Richtlinien beteiligt (siehe etwa den BSI-Grundschutz)

Allianz für Cyber-Sicherheit

- Ist eine Plattform für die Kooperation zwischen Akteuren aus Wirtschaft, Behörden und Wissenschaft.
- Die Plattform ist insbesondere auch eine Anlaufstelle für KMU
- Die Allianz für Cyber-Sicherheit wurde 2012 gegründet und über 4000 Unternehmen und Institutionen gehören der Initiative bereits an

ISACA GERMANY CHAPTER

- Berufsverbandes der IT-Revisoren, IT-Sicherheitsmanager sowie der IT-Governance-Experten
- ISACA bietet nationale und internationale Zertifizierungen im Cyberbereich an

Ausschnitt von Cybersecurity Anforderungen an den Privatsektor

KRITIS Definition

- „Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“
- Für KRITIS-Betreiber und prüfende Stellen gibt es einen Anforderungskatalog

IT-Sicherheitsgesetz 2016

- Das Gesetzt verpflichtet Organisationen zur Einhaltung eines definierten Mindestmaßes an IT-Sicherheit durch den Nachweis von TOMs
- Meldepflicht gegenüber dem BSI

BSI Standards und IT-Grundschutz

- Der IT Grundschutz ist seit über 25 Jahren die Basis(Methodik) für Informationssicherheit und gilt als Maßstab in Deutschland. Ist mit der internationalen ISO 27001 kompatibel
- Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS). Der BSI-Standard 200-2 (IT-Grundschutz-Methodik) bildet die Basis zum Aufbau eines soliden ISMS

ISO 27001

- Ist ein internationale Norm für Informationssicherheit in privaten, öffentlichen oder gemeinnützigen Organisationen. Die ISO beschreibt die Anforderungen für das Einrichten, Realisieren, Betreiben und Optimieren eines dokumentierten ISMS

Source: https://www.kritis.bund.de/SubSites/Kritis/DE/Home/home_node.html
https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html

Cyberstrategie in Deutschland

Die Strategie von 2016 enthält vier Handlungsfelder mit verschiedenen Zielen und Maßnahmen:

1. **Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung**
   - Digitale Kompetenz bei allen Anwendern fördern
   - Zertifizierung und Zulassung stärken – Einführung eines Gütesiegels für IT-Sicherheit
   - Sichere elektronische Identitäten

2. **Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft**
   - Kritische Infrastrukturen sichern
   - Unternehmen in Deutschland schützen

3. **Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur**
   - Das Nationale Cyberabwehrzentrum weiterentwickeln
   - Strafverfolgung im Cyberraum intensivieren
   - Ein Frühwarnsystem gegen Cyberangriffe aus dem Ausland

4. **Aktive Positionierung in der europäischen und int. Cybersicherheitspolitik**
   - Eine wirksame europäische Cybersicherheitspolitik aktiv gestalten
   - Die Cyberverteidigungspolitik der NATO weiterentwickeln

Source: https://www.bsi.bund.de/DE/Themen/KRITIS/Strategie/strategie_node.html
https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/cybersicherheitsstrategie-2016.html

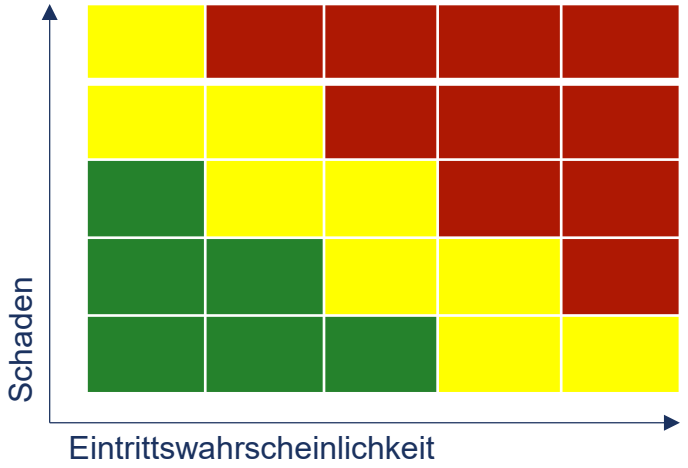
In der Praxis kritischer Infrastrukturen

Eine volle Sicherheit ist nicht herstellbar. Durchgesetzt hat sich in der Praxis ein risikobasierter Ansatz

Gemessen wir das Risiko an den Schutzzielen:
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Risiken müssen grundsätzlich „behandelt“ werden:
- Vermeiden
- Verringern
- Transferieren
- Akzeptieren

Ein Informationssicherheitsmanagement (ISMS) und dazugehörige Komponenten wie das Risikomanagement sind für die meisten Unternehmen verpflichtend.



Cyberbedrohung im Finanzsektor

Drittanbieter im Finanzbereich

Drittanbieter haben keinen Schwerpunkt auf "Insiderbedrohungen" und "Patching"

Third-Party Assessments

- Finanzinstitutionen führen <1% ihrer Beurteilung von Drittanbietern vor Ort durch

Compliance of Vendors

- 70% der Drittanbieter im Finanzsektor halten sich ungenügend an Vorschriften

Risk & Contract Management

- Finanzinstitutionen verbinden selten Risikoprogramme mit dem Vertragsmanagement

Finanzielle Risiken und Compliance-Trends bei Drittanbietern

Source: Ponemon Institute (2018) Cost of a Data Breach Study: Global Overview
https://securityintelligence.com/events/whats-the-true-cost-of-a-data-breach/

Kosten durch Daten-Vorfälle im Jahr 2019

3,86 M$ - Pro Vorfall

- Durchschnittliche Totalkosten pro Daten-Vorfall

142 % - Finanzindustrie

- Höhere Kosten, im Vergleich zu einem durchschnittliche Regulierungsverstoß

28 % - Wiederauftauchen

- Chance für eine erneutes Auftreten eines Daten-Vorfalles in den nächsten zwei Jahren

197 Tage - Versagen bei der Identifizierung

- Durchschnittliche Zeit um einen Daten-Verstoß zu identifizieren

247 % - Gesundheitsindustrie

- Höhere Kosten, im Vergleich zu einem durchschnittliche Regulierungsverstoß

→ Die durchschnittliche Kundenabwanderung nach einem Daten-Vorfall im Finanzsektor ist 6,1%

Source: Ponemon Institute (2018) Cost of a Data Breach Study: Global Overview
https://securityintelligence.com/events/whats-the-true-cost-of-a-data-breach/

Beispiel: Der Risikobegriff der EBA in Auslagerungen

EBA Guidelines on Outsourcing Arrangements – Risk

"Intergroup outsourcing is subject to the same regulatory framework as outsourcing to service providers outside the group."

- Reputationsrisiken
- Drittstaaten: stability and security situation
- Risiko durch die Verbindung mit dem Serviceprovider
- Einem Dienstleister finanziell stützen zu müssen: „Step-in risk"
- Große Zahl kritischer Funktionen im Outsourcing
- Outsourcing chains
- Risikokonzentration durch Outsourcingkonzentration bei einem oder wenigen Dienstleister(n)
- Suboutsourcing durch den Dienstleister

Das übergeordnete regulatorische Ziel ist die Erkennung von Risiken für die Finanzmarktstabilität, etwa durch Identifizierung der Risikokonzentration bei Dienstleistern

Nordish by Nature & im Herzen Frankfurts

www.secoriadvisors.com | @secoriadvisors

Secori
Security – Compliance – Risk
Ihr Partner für alle Themen rund um die Informationssicherheit
ISO 27001, DSGVO, Risikomanagement, MaRisk, BAIT, BSI-GS, KRITIS

secori advisors GmbH
Handelsregister Frankfurt am Main 101354 | Geschäftsführer: Sebastian Troch & Dustin Dehez
Neue Mainzer Str. 46-50 / Garden Tower | 60311 Frankfurt am Main
sebastian.troch@secoriadvisors.com | dustin.dehez@secoriadvisors.com