Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)120

19.01.2023

Dr. Stefanie Frey
Deutor Cyber Security Solutions GmbH
Am Turm 44
53721 Siegburg
E-Mail: stefanie.frey@deutor.de

Öffentliche Anhörung Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland

Zeit: Mittwoch, 25. Januar 2023, 14:00 - 16:00 Uhr
Ort: Sitzungssaal Marie-Elisabeth-Lüders Haus, Sitzungssaal 3.101

Sachverständigenstellungnahme von Dr. Stefanie Frey, Geschäftsführerin von Deutor Cyber Security Solutions GmbH für die Sitzung des Bundestagsausschusses für Digitales am 25.01.2023 zum Thema „Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“

Stellungnahme:

1) Im Koalitionsvertrag haben die Regierungsparteien vereinbart, dass sie „einen strukturellen Umbau der IT-Sicherheitsarchitektur“ einleiten und das „Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger“ aufbauen und es als „zentrale Stelle im Bereich IT-Sicherheit“ ausbauen wollen. Wie sollte die Cybersicherheitsarchitektur auf nationaler und europäischer Ebene ausgestaltet werden, um effektiver, wirksamer und widerspruchsfreier aufgestellt zu sein und wo bedarf es einer Neuordnung oder auch Bündelung der Kompetenzen zwischen Bund, Ländern und der Europäischen Union und bedarf es auch angesichts der aktuellen Herausforderungen einer Diskussion über innere und äußere Sicherheit und der diesbezüglichen Kompetenzen und Grenzen? Welche anderen Akteure neben dem BSI (also etwa Cyber-Abwehrzentrum, Nationaler Cyber-Sicherheitsrat, ZITiS), die in Deutschland für Cybersicherheit zuständig sind, sollten reformiert werden und wie?

Auf EU-Ebene und in den jeweiligen Mitgliedstaaten wurden in den letzten Jahren viele Bemühungen unternommen, um die Cybersicherheit zu erhöhen. Während die Richtlinie zur Netz- und Informationssicherheit (NIS1 wurde abgelöst durch NIS2) sich zum Ziel setzt, durch EU-weite Gesetzgebung ein höheres und gemeinsames Niveau der Cybersicherheit in allen Mitgliedstaaten zu erreichen, versuchen die Mitgliedstaaten durch nationale Gesetzgebung, Richtlinien, Strategien und Verträgen die nationalen und regionalen Cyber-Strukturen zu stärken. Gute Beispiel dafür in der Bundesrepublik Deutschland sind das IT-Sicherheitsgesetz (1.0 wurde abgelöst durch 2.0) und der Koalitionsvertrag. Obwohl damit Richtlinien und Gesetze zur Erhöhung und Harmonisierung der Cybersicherheitsfähigkeiten und Bekämpfung von Cyberkriminalität entwickelt wurden, hat sich die Umsetzung als schwierig erwiesen und wir sehen eine Fragmentierung des Binnenmarkts auf verschiedenen Ebenen und keine deutliche Verbesserung der Cyberlage.

Im Koalitionsvertrag steht, dass entscheidende Ziele gesetzt werden, um IT-Sicherheitslücken wirksam zu schließen, zunehmende Cyberkriminalität besser zu bekämpfen und mehr Sicherheit für Unternehmen, Behörden und Privatpersonen zu schaffen. Aktuelle Zahlen jedoch zeigen auf, das die Ziele (noch) nicht erreicht wurden.

Auf globaler Ebene wird der Schaden durch Cyber Angriffe auf mehr als USD 10,5 Trillionen bis 2025 im Vergleich zu 3 Trillionen im Jahr 2015, geschätzt; jede Minute im Jahr 2022 gingen 2.900.000 USD durch Cyberkriminalität verloren; Phishing-Angriffe machen immer noch 80 % der gemeldeten Sicherheitsvorfälle aus (trotz Training und Awareness).

Für die Bundesrepublik Deutschland sieht das Bild nicht besser aus. Der Schaden für die deutsche Wirtschaft durch Cyber-Angriffe wurde im 2020/2021 auf 223 Milliarden Euro im Vergleich zu 103 Milliarden im Jahr 2019 geschätzt; ca. 88% der deutschen Unternehmen wurden Opfer von Cyber Angriffen im Jahr 2020 im Vergleich zu 75 % im Jahr 2019; Erpressung, Systemausfälle und Betriebsstörungen haben sich mehr als vervierfacht; alle Unternehmen von kritischen Infrastrukturen, Kommunen bis zum Mittelstand sind heute das Ziel von Cyber-Angriffen.[1]

Untragbar für die Zukunft ist die Realität, dass ca. 99 Prozent der digitalen Straftaten im Dunkelfeld liegen und von den bekannten digitalen Straftaten weniger als 30 Prozent aufgeklärt werden.[2] Für uns als Krisenmanager bei Deutor Cyber Security Solutions GmbH sehen die Zahlen nicht besser aus. Die Straftaten von Cyber-Crime gegenüber unseren Kunden wurden in keinem Fall seit 2015 aufgeklärt und es gibt daher auch keine „lessons learned“ und keine Ansätze für Optimierungen und Stärkungen der Cyber-Sicherheit. Auch wenn sich die Täter oft in den Erpressungsschreiben identifizieren, wurde keine erfolgreiche Strafermittlung durchgeführt und es kam zu keinen Verurteilungen. Die Täter bewegen sich in einem rechtsfreien Raum, ohne Abschreckung durch Strafaktionen und harte Verurteilungen.

Durch die zunehmende Digitalisierung und Globalisierung sind Cyber-Angriffe meistens länder-übergreifend und involvieren verschiedene Rechtsräume, dabei findet eine Verwischung zwischen innerer und äußerer Sicherheit statt und die Zuständigkeiten sind nicht mehr klar geregelt, weil sich keiner befugt fühlt und nicht weiß, wo die Grenzen und Kompetenzen liegen. Ein gutes Beispiel dafür ist ein aktueller Fall, wobei der Cyber-Angriff im digitalen Raum stattgefunden hat (DDoS Angriff mit Erpressung) und dann in den physischen Raum übergegangen ist. Das Opfer war ein deutsches Unternehmen mit globalen Niederlassungen, wobei nach Nicht-Zahlung der Erpressungssumme Morddrohungen an die Opfer und deren Familien ausgesprochen worden sind. Obwohl der Prozess der Strafverfolgung in der Theorie gut funktioniert, greift er in der Praxis nicht, wie dieses Beispiel und viele andere aufzeigen. Cyber-Angriffe sind sehr kompliziert und werden von hochmotivierten Tätern (staatlich oder durch kriminelle Banden und Organisationen) mit klaren Zielen durchgeführt.

Im erwähnten Fall stellte sich die Frage der internationalen und nationalen Zuständigkeiten und Rechtsgrundlagen. Welche Polizei-Abteilung (Cyber-Crime, digitale Spuren, Morddezernat, etc.?) in welchem Land ist zuständig? Wie ist die länder-übergreifende Zusammenarbeit in der Praxis insbesondere mit der Staatsanwaltschaft (international) geregelt?
Die heutige Cybersicherheitsarchitektur gibt darüber keine Antwort und zeigt klar auf, dass Theorie und Praxis nicht immer im Einklang stehen. Fazit ist, dass im oben genannten Fall das Opfer keine Hilfe bekommen hat und die Täter ohne Repression und Strafaktion weiter machen.

Deutschlands staatliche Cybersicherheitsarchitektur, die von der Stiftung neue Verantwortung, aufgearbeitet wurde[3], zeigt warum die Bemühungen zur Erhöhung der Cyber-Sicherheit nicht zielführend sind und keine Verbesserung mit sich bringen. Es gibt zu viele Akteure und Agenturen sowie Kompetenzen auf allen Ebenen, die in zu vielen Beziehungen miteinander stehen. Dies führt dazu, dass nach einem Cyber-Angriff die Ansprechstellen, Kompetenzen und Fähigkeiten in dieser sehr komplizierten Cybersicherheitsarchitektur nicht mehr klar sind und somit der Melde- und Informationsprozess sowie die Ermittlungsbemühungen meistens im Sande verlaufen. Hohe finanzielle

[1] Erhebung basiert auf Bitkom 2021, Forbes, Retarus Corporate und Cybersecurity Ventures 2022
[2] https://www.bitkom.org/Bitkom/Publikationen/Zukunft-der-Polizeiarbeit
[3] https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur

Ressourcen werden in Parallelstrukturen investiert, die keinen erkennbaren Mehrwert aufweisen. Dies ist in der Strafverfolgung und Täterermittlung besonders schwierig. Die Polizei muss befähigt und befugt sein, ihre Arbeit der Strafermittlung- und Verfolgung zu tätigen. Dies inkludiert Überwachung der Täterstrukturen und deren Infrastrukturen und Befugnis der Beschlagnahmung und diese auch vom Netz nehmen zu können. Durch Beschlagnahme von Infrastrukturen werden nicht nur die Täter vorübergehend arbeitsunfähig, sie können auch die „abgezogenen" Daten nicht mehr veröffentlichen. Auch besteht ein Kompetenzwirrwarr mit zahlreichen Hotlines auf den jeweiligen Ebenen (BSI, Verbände, LfV, IHK, (Cyber-) Agenturen, etc.) die durch Unternehmen ansprechbar sind, jedoch nicht helfen können, weil ihnen die Kompetenzen und Leistungsangebote fehlen und die Schnittstelle zur Strafverfolgung nicht bedient werden.

Ein gutes Beispiel dafür ist die Situation im LKA Baden-Württemberg, in dessen Abteilung Cybercrime/Digitale Spuren 135 Mitarbeiter tätig sind. Davon sind jedoch lediglich 10 Mitarbeiter in der klassischen Cybercrime-Ermittlung, sprich Ermittlungen gegen schwere Cyber-Angriffe, wie Angriffe auf Firmennetze mit Verschlüsselung und Erpressung durch internationale Banden und organisierte Kriminalität, zuständig. Diese Cyber-Fälle binden die Ermittler oft mehrere Wochen, was eine Parallelbearbeitung der Fälle massiv erschwert.

Um eine zielführende, effektivere, wirksamere und widerspruchsfreie Cybersicherheitsarchitektur zu haben, müssen wir eine Straffung und Bündelung der Akteure und deren Kompetenzen auf allen Ebenen vornehmen. Diese Neuordnung sollte auf einem praxisnahen Ansatz, der auf echten Cyber-Angriffen und deren Auswirkungen basiert, entwickelt werden. Bei Cyber-Angriffen gehen Theorie und Praxis auseinander und nur durch ein Verständnis der Komplexität und Kettenreaktionen eines Cyber-Angriffs können wir erfolgreich die Cyber-Sicherheit erhöhen. Dabei ist es nicht zielführend mehr Akteure, Kompetenzen und Parallelstrukturen aufzubauen, sondern die bestehenden nach strukturierten und auf die Cyber-Angriffe ausgerichtete Bedürfnisse, zu stärken und zu befähigen.

Zur Neuordnung und Bündelung der Kompetenzen sind strategische Cyber-Simulationsübungen[4], die auf echten Cyberfällen beruhen, ein bewährtes Vorgehen. Die Zuständigkeiten, Rollen, Kompetenzen und Fähigkeiten, Schnittstellen und Kommunikationswege von Bund, Ländern, KRITIS sowie Unternehmen können anhand der strategischen Cyber-Simulationsübungen getestet und dabei eine Reform und Bündelung der Kompetenzen basierend auf den Herausforderungen von Cyber-Angriffen vorgenommen werden.

3) Könnten Sie bitte den Begriff der aktiven Cyberabwehr und die unterschiedlichen Stufen und Möglichkeiten der aktiven Cyberabwehr (auch vor dem Hintergrund einer allein defensiv ausgerichteten bzw. einer offensiv ausgerichteten Cyberabwehr) definieren und wo sehen Sie konkrete Defizite im geltenden Recht und in den geltenden Kompetenzen, die einer wirksamen Cyberabwehr entgegenstehen?

Wir müssen uns so aufstellen, dass wir vergleichbare Fähigkeiten zu anderen Staaten und den Cyber-Kriminellen aufbauen. Dazu gehören angemessene Verteidigungsmöglichkeiten im Cyberraum, die auch offensiv sein müssen. Ein gutes Beispiel dafür ist der Vergleich zur konventionellen Abwehr. Hier würde sich die Frage gar nicht stellen, ob wir Instrumente und Waffen zur offensiven Abwehr einsetzen sollten. Die aktuellen Waffenlieferungen an die Ukraine untermauern diesen Standpunkt. Kriege werden nur durch ein Zusammenspiel der Fähigkeiten in der Luft, am Boden, im Wasser und heute zudem im Cyber-Raum gewonnen.

Ein Take Down einer Command & Control Infrastruktur ist eine offensive Verteidigungs-Maßnahme, die zur Bekämpfung und Eindämmung einer Straftat durchgeführt wird (siehe auch Antwort zu Frage 1). Die offensive Cyber-Abwehr muss auch durch mehr Fachkompetenz in der internationalen und

[4] https://deutor.de/war-games/

nationalen Justiz und der Strafverfolgung untermauert werden, damit die Gesetze auch sinnbehaftet angewendet werden können und neue entstehen können, wo es auch zwingend notwendig ist.
Siehe auch Antworten zu Frage 5.

4) Weitere Instrumente, die der Koalitionsvertrag adressiert, sind etwa auch

- **das Recht auf Verschlüsselung (Prio 4, sollte bei Security by Design integriert sein)**
- **ein Schwachstellenmanagement (ja) und die Pflicht, Sicherheitslücken zu melden (nein, weil es keinen höheren Sicherheitsgewinn im Vergleich zum Aufwand darstellt) (Prio 3)**
- **die Stärkung der digitalen Souveränität und die Beachtung der Vertrauenswürdigkeit von Unternehmen (Prio 2, insbesondere der 2. Teil)**
- **die Vorgaben „security-by-design/default" als Standard (Prio 1)**
- **Stärkung der Produkthaftung und der IT-Sicherheitsforschung (Prio 5)**
- **das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme, etwa bei 5G oder KI. (Prio 6)**

Die Instrumente, die der Koalitionsvertrag adressiert sind, hauptsächlich technische Lösungen und auf Schwachstellenmanagement fokussiert. Cyber-Bedrohungen sind jedoch viel komplexer und können nicht nur mit technischen Lösungen und Schwachstellenmanagement durch Schließung von Sicherheitslücken angegangen werden. Der Zustand, keine Sicherheitslücken zu haben ist unerreichbar, dafür gibt es zu viele Schwachstellen/Lücken und insbesondere unbekannte Schwachstellen. Auch wenn ein Unternehmen alle Vorkehrungen trifft, eine Basishygiene zu erreichen und keine erkennbaren Lücken aufweist, kann ein Cyber-Angriff trotzdem durch eine unbekannte Lücke durchgeführt werden. Das ist das Problem von Cyber-Angriffen: Prävention allein reicht nicht. Die Täter sind hoch motiviert und haben Zeit, unsere Infrastrukturen auszuspionieren und anzugreifen, um ihre Ziele zu erreichen (jedem Cyber-Angriff geht die Cyber-Spionage voraus. Im Durchschnitt sind die Täter bis zu 6 Monaten unbemerkt in den Infrastrukturen der Opfer, bevor der Cyber-Angriff durchgeführt wird). Technische Maßnahmen können dabei nur bedingt helfen. Unser Ziel sollte sein, eine Krisen- und Reaktionsfestigkeit sowie Cyber-Resilienz zu erzielen, da wir nicht verhindern können, dass die Cyber-Angriffe durchgeführt werden. Wir können jedoch die Krise vermeiden und Maßnahmen definieren, um mit wenig Schaden durch die Lage zu kommen (Cyber-Versicherungen, die für den Schaden und das Krisenmanagement aufkommen, sind ein zentrales Element).

Der Fokus, lediglich auf IT-Maßnahmen zur Verbesserung der Cyber-Sicherheit zu setzen, ist nicht zielführend. Wir können in der Zukunft nur durch ein Zusammenspiel von präventiven (Schwachstellenmanagement und IT-Basishygiene), reaktiven (Strafverfolgung, Incident Response und Krisenmanagement) und stabilisierenden (lessons learned: Einführung von Maßnahmen, damit der letzte Angriff nicht nochmal passieren kann, Aufbau resilienter technischer und organisatorischer Infrastrukturen) Maßnahmen die Cyber-Sicherheit erhöhen, eine Cyber-Resilienz aufzubauen und eine Erhellung des Dunkelfeldes erzielen.

5) Vor dem Hintergrund des hybriden Angriffskrieges Russlands gegen die Ukraine sind erneut Forderungen nach Instrumenten der sogenannten offensiven Cyberabwehr laut geworden. Wie beurteilen Sie diese Forderungen und die Argumentation, offensive Instrumente vermeintlich unterhalb der Schwelle von Hackbacks einzusetzen, im Hinblick auf ihre Recht- und Zweckmäßigkeit?

Wir müssen uns so aufstellen, dass wir vergleichbare Fähigkeiten zu anderen Staaten und den Cyber-Kriminellen aufbauen, dazu gehören angemessene Verteidigungsmöglichkeiten im Cyberraum, die auch offensiv sein müssen (siehe Antworten zu Frage 3).

Cyber-Angriffe sind ein Mittel zum Zweck, die durch Ausnutzung von IKT durchgeführt werden, jedoch immer ein höheres Ziel haben. Daher ist es wichtig, die Ziele, die finanziell, wirtschaftlich, politisch oder militärisch ausgerichtet sind, sowie den Modus Operandi der Täter zu analysieren, um geeignete

defensive und offensive Gegenmaßnahmen zu ergreifen. Hackbacks würden nur, wenn überhaupt, Sinn ergeben, wenn wir in der Lage sind, eine klare und eindeutige Attribution (Täterermittlung) gegenüber Cyber-Angriffen zu erreichen. Unterhalb dieser Schwelle stehen uns genügend weitere Instrumente auf den verschiedenen Ebenen zur Verfügung, um eine Abwehr ohne Hackback zu erreichen. Diese sind z.B. für Cyber-Crime eine Stärkung der Täterermittlungen der Strafverfolgungsbehörden sowie Staatsanwaltschaften auf nationaler und internationaler Ebene, um eine Abschreckung zu erreichen. Bei staatlich gesteuerten Cyber-Angriffen stehen Diplomatie oder wirtschaftliche und politische Sanktionen, sowie konventionelle Abwehr-Maßnahmen zur Verfügung.

6) Was kann die Bundesrepublik Deutschland in ihrer nationalen und internationalen Cybersicherheitspolitik von anderen Ländern und internationalen best practices konkret lernen, insbesondere im Hinblick auf staatliche Stellen, Governance, verfügbare Instrumente, Fokus und Kapazitäten?

Alle demokratischen Länder kämpfen mit den gleichen Problemen, wie der Governance, unzureichende Analyse der Cyber-Bedrohungslage, zu wenig Kapazitäten und Instrumente, mangelnde best practices durch zu wenig Transparenz und länder-übergreifender Informationsaustausch (in Cyber wird oft die Geheimhaltung nach vorne geschoben).

Die Digitalisierung ist eine der größten Chancen und Herausforderung unserer Zeit. Digitalisierung wird vom Markt und von den Anwendern gefordert. Digitalisierung ohne Sicherheit führt jedoch zu mehr Unsicherheit und mehr Straftaten. Daher muss die Digitalpolitik in Deutschland neu ausgerichtet werden, damit wir gezielter die Chancen der Digitalisierung nutzen können.

Die jeweiligen Strategien müssen eng miteinander abgestimmt werden, damit die Vorteile der Digitalisierung in den jeweiligen Strategien berücksichtigt werden und ein umfassender Ansatz für die Bundesrepublik Deutschland verfolgt werden kann. Ein gutes Beispiel dafür ist die Digitalisierung von Waffensystemen, die in Zukunft für die Rüstungspolitik (siehe Waffenlieferungen an die Ukraine) Auswirkungen haben könnte. Die Herausforderungen, Chancen und deren Auswirkungen müssen in den jeweiligen Strategien berücksichtig werden.

Konkret heißt das, dass die jeweiligen Strategien nicht in Isolation entwickelt werden dürfen, sondern in enger Zusammenarbeit und unter Betrachtung eines Strategie-Gefälles. :

- Strategie zur staatlichen Sicherheitsvorsorge/ Sicherheits- und Verteidigungspolitik➔
  - Staatliche Cyber-Strategie➔
    - Staatliche Digitalisierungs-Strategie➔
      - Cyber-Strategie der Behörden und Länder➔
        - Staatliche IKT-Strategie➔
          - IT-Sicherheits-Strategien[5]

Ein zentrales Element ist jedoch nicht die Entwicklung von Strategien, sondern deren Umsetzung und Einbindung der lessons learned.

11) Wie bewerten Sie die Lage von IT-Fachkräften – insbesondere für Cybersicherheit – auf dem Arbeitsmarkt und was müssten staatliche (Sicherheits-) Behörden verbessern, um noch mehr kompetente IT-Fachkräfte zu gewinnen?

Der Fokus sollte nicht auf IT-Fachkräften, sondern auf einem umfassenden Ansatz der Cyber-Sicherheit und Cyber-Krisenmanagements aufgebaut sein. Cyber-Angriffe sind viel komplexer und beinhalten

[5] Stefanie Frey, Michael Bartsch, Cyberstrategien für Unternehmen und Behörden: Maßnahmen zur Erhöhung der Cyberresilienz, Springer Verlag, 2017

nicht nur IT-Sicherheit. IT-Sicherheit ist lediglich ein Bestandteil davon. Daher soll auch die Fachkräftegewinnung auf diesem Konzept aufgebaut sein. Bei der Bekämpfung und Behandlung von Cyber-Angriffen braucht es über die IT hinaus Rechtshilfe, strategische Analysten zur Analyse der Cyber-Bedrohungslage, Cyber-Crime Ermittler, Datenschutz, Risikomanager, etc. Dies sollte in einem Lehrgang zusammengefasst werden, der die Cyber-Sicherheit in dem umfassenden Ansatz angeht. Auch sollten die Gehälter daran angepasst werden. Insbesondere bei der Strafverfolgung braucht es in erster Linie mehr Personal und damit müssen entsprechende Qualifizierungsmöglichkeiten entstehen. Die Gehälter sind unattraktiv, was dazu führt, dass qualifiziertes Personal abgeworben wird.

13) Wie bewerten Sie die vorhandenen technischen Fähigkeiten in Deutschland für eine wirksame Cyberabwehr – auch mit aktiven Cyberabwehr-Instrumenten?

Wie die aktuellen Zahlen aufzeigen, sind die technischen und organisatorischen Fähigkeiten mangelhaft. Es fehlt an:

- Skalierung und Geschwindigkeit
- Technische Ausstattung oft mangelhaft und veraltet (insbesondere bei der Strafverfolgung. Software, Hardware und Clouds sind teuer)
- Personalmangel (schlechte Gehälter und unattraktive Arbeitsbedingungen)
- Budgetmangel (hohe Investitionen in Parallelstrukturen)
- Keine Bündelung der Akteure, Kompetenzen und Fähigkeiten (siehe Cybersicherheitsarchitektur der SNV)