Wirtschaftsrat der CDU e.V.
Luisenstr. 44, 10117 Berlin
Telefon: +49 (0) 30 / 240 87 - 0
E-Mail: digitales@wirtschaftsrat.de

Referent: Andreas Barke

Stand: 09.02.2023

Cybersicherheit und Digitale Souveränität nach der „Zeitenwende“ – Herausforderungen für die Politik

Positionspapier der Bundesfachkommission im Wirtschaftsrat der CDU e.V.

In einer Zeit, in der geopolitische und sicherheitspolitische Fragen neu bewertet werden, rückt das Thema Cybersicherheit in den Fokus. Das Ziel muss eine konsistente und ganzheitliche Strategie sein, damit die relevanten Schritte von den relevanten Instanzen korrekt umgesetzt werden. Die Bundesarbeitsgruppe Cybersicherheit des Wirtschaftsrates der CDU e. V. hat hierzu Lösungsansätze identifiziert und politische Forderungen erarbeitet:

1. Wildwuchs von Verantwortlichkeiten abbauen und Zuständigkeiten klären

Überall dort, wo digitalisiert wird, braucht es ein konsequentes Streben nach Cybersicherheit. In Deutschland führt die praktische Umsetzung jedoch zu einem **Wildwuchs an Verantwortlichkeiten**, **Mitspracherechten** und **Zuständigkeitsfragen im Rahmen des Föderalismus** (Beispiele sind umständliche Meldewege und sich überlagernde Zuständigkeiten auf Bundes- und Landesebene in Cybernotfällen). Die Anzahl der Initiativen und Strategien wächst proportional zur Anzahl der sich verantwortlich fühlenden Institutionen (siehe Cybersicherheitsarchitektur der Stiftung Neue Verantwortung). Allzu oft ergeben sich aus dem Nebeneinander sowohl von nationalen Vorgaben als auch von zunehmenden Regulierungen der Europäischen Union (EU) **Inkompatibilitäten und Inkonsistenzen zwischen nationaler und europäischer Ebene** (z.B. unklare Vorgaben zum Adressatenkreis von neuen rechtlichen Vorgaben). So kommt es bereits zwischen der Digitalstrategie der Bundesregierung, der Cybersicherheitsstrategie und Cybersicherheitsagenda des Bundesinnenministeriums sowie Nationaler Sicherheitsstrategie und dem „Aktionsplan Cybersicherheit“ des Auswärtigen Amtes zu Widersprüchen. Auf EU-Ebene kommen Vorgaben der NIS 2.0-Richtlinie, der EU-Strategie für die Cybersicherheit, dem Aktionsplan der Europäischen Kommission für eine „EU Policy on Cyber Defence“ und der EU-Cyberabwehrstrategie hinzu.

Lösungsansatz/Forderung: Anerkannt und zugestanden ist, dass es aufgrund der vielschichtigen Herausforderungen, die sich für die Sicherheit von Staaten, Wirtschaft und Gesellschaften einstellen, nicht die alleinig verantwortliche Institution geben wird. Gleichwohl werden weder die EU noch Deutschland dieses Thema angemessen behandeln können, wenn nicht klarere und einfachere Strukturen aufgestellt werden. Eine Grundvoraussetzung ist ein **übergreifender Masterplan**, der sowohl die **Verantwortlichkeiten klar zuordnet** als auch eine **konsistente Gesamtstrategie abbildet**. Statt einer Vielzahl von Lösungen von Detailproblemen braucht es dringend den Blick auf das „Große Ganze“.

Die angekündigte Nationale Sicherheitsstrategie als übergeordnete Strategie unter der Federführung des Auswärtigen Amtes in Zusammenarbeit mit den Bundesministerien des Innern (BMI) sowie der Verteidigung (BMVg) droht erkennbar auf die gleichen, oben angeführten Probleme hinauszulaufen. Zum Austarieren der Risiken für die innere und äußere sowie die wirtschaftliche und soziale Sicherheit aber eben auch der sich ergebenden Chancen sollte die **Verantwortlichkeit zentral im Bundeskanzleramt** liegen. Auf der operativen Ebene sollte das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig sein und in Cybernotfällen die Federführung übernehmen.

2. Neue Realitäten anerkennen, nationale und europäische Ebene zusammen denken

Zur neuen politischen Realität gehört, dass **Angriffsoperationen hybrid verlaufen**, als Mischform aus konventionellen und digitalen Fähigkeiten. Der Angreifer kann sich hierbei unterhalb der Schwelle eines offensichtlich kriegerischen Angriffs bewegen, die Operation verschleiern und den Angegriffenen verwirren. Exemplarisch sind hier die gezielten Angriffe Russlands auf Einrichtungen der kritischen Infrastruktur der Ukraine bereits im Vorfeld der physisch-militärischen Invasion durch die russische Armee. Parallel hinzukommen Cyber Influence Operations, also gezielte politische Kampagnen über Social Media und andere Kommunikationsplattformen zur Verbreitung von Desinformationen.

Lösungsansatz/Forderung: Auf nationaler Ebene sollten hybride Bedrohungen – konventionell gesprochen Risiken im analogen und digitalen Bereich – in den **Sicherheitsstrategien und Notfallvorbereitungen stets übergreifend betrachtet werden**. Es müssen konkrete Reaktionspläne erstellt sowie Übungen regelmäßig durchgeführt werden, um hybride Bedrohungen abzufangen. Es bedarf der engen Zusammenarbeit aller Stakeholder: BMI, BSI, weitere Behörden im Bereich Grundversorgung, Stadtwerke, Betreiber kritischer Infrastrukturen (KRITIS), Polizei, Feuerwehr, IT-Sicherheitsanbieter, etc.

Auf EU-Ebene muss die oft geäußerte Forderung, **europäisch zu denken, endlich ernst genommen werden und ihr auch Taten folgen**. Das bedeutet konsequenterweise Initiativen der EU von den Gesetzgebern und nationalen Mitgliedstaaten ergebnisoffen zu diskutieren: Angesichts der langen Verfahren zur Umsetzung von EU-Recht bedarf es ausreichender Flexibilität, um die zu beschließenden Maßnahmen anhand der sich gegebenenfalls ändernden aktuellen geopolitischen Lage umsetzen zu können. So hat die Europäische Kommission die EU-Mitgliedstaaten im Jahr 2022 gemahnt das „volle Spektrum von Fähigkeiten zur Cyberverteidigung zu leisten“. Eine zentrale Prämisse hierbei ist die Erkenntnis, dass es **keine wirksame Verteidigung gegen Cyberangriffe** geben kann, ohne Expertise darin zu besitzen, wie **Angriffe aus der Perspektive des Angreifers funktionieren**.

Zu bedenken gilt, dass der Einsatz von Cyberwaffen für die Zivilbevölkerung fatale Konsequenzen nach sich ziehen kann. Damit gewinnen Cyberangriffe und Cybersicherheit eine zunehmend völkerrechtliche Dimension, weshalb die Ächtung der ABC-Waffen durchaus um digitale Waffen ergänzt und somit auf **ABCD-Waffen** erweitert werden kann.

3. Prävention vor Reaktion, Awareness schärfen und Resilienz erhöhen

Insbesondere **kleine und mittelständische Unternehmen (KMU)** und auch öffentliche Einrichtungen in Deutschland setzen nach wie vor auf veraltete Betriebssysteme ihrer IT. Das ist insofern problematisch, weil diese bekannte Schwachstellen aufweisen, die vom Support nicht mehr geschlossen werden. Auch ältere SSL/TLS-Versionen–ein Verschlüsselungsprotokoll zur Datenübertragung–kommen nach wie vor zum Einsatz. Grund hierfür ist häufig die Vermeidung von Zusatzkosten infolge von Aktualisierungen der eingesetzten Software und der erforderlichen Umstellung der betrieblichen Prozesse. Das ist äußerst kurzfristig gedacht und ein Spiel mit dem Feuer. Der **Faktor Mensch** kann durch beabsichtigte oder unbeabsichtigte Operationen, wie z.B. Öffnen von Dateien, die mit Malware infiziert sind, ein ebenso kritisches Einfallstor darstellen. So können Betriebsausfälle zu hohen Folgekosten führen und eine **existenzielle Bedrohung** darstellen: Die durchschnittlichen Kosten für die Wiederherstellung nach einem Ransomware-Angriff im Jahr 2021 betrugen für deutsche Unternehmen ca. 1,6 Millionen Euro, die Wiederherstellung dauerte im Durchschnitt einen Monat. Angreifer müssen nur eine einzige Schwachstelle ausmachen und werden durch eine Vernachlässigung grundlegender Sicherheitsmaßnahmen geradezu eingeladen, ihr „**Geschäftsmodel Cyberangriff**“ effizient und erfolgreich umzusetzen (Cybercrime/ Ransomware-as-a-Service).

Lösungsansatz/Forderung: Der Grundbaustein für Cybersicherheit und letztlich auch der Königsweg zu einem höchstmöglichen Sicherheitsniveau im Cyberraum ist das Erreichen von **mehr Resilienz gegenüber Angriffen**. Hierzu gehören alle Akteure in Politik, Wirtschaft und Gesellschaft einbezogen. Es braucht eine Weiterentwicklung: weg von rein reaktiven Maßnahmen, hin zu **mehr Prävention**! Technische Vorkehrungen sind das Eine; der Schlüssel für Prävention ist jedoch viel grundsätzlicher und liegt in dem Gefahrenbewusstsein, der Ausbildung und der Wertschätzung von entsprechender Expertise im Umgang mit Schwachstellen. Als konkretes Positivbeispiel sind die **Vorgaben des Krankenhauszukunftsgesetzes (KHZG)** zu nennen. Es schreibt vor einen verpflichtenden Anteil von mindestens 15 Prozent von beantragten Fördermitteln eines Projekts in Maßnahmen zur Verbesserung der Cybersicherheit zu investieren. Als weitere Maßnahme in die Breite können BSI und die Industrie- und Handelskammern Präventionskampagnen anbieten, wobei insbesondere KMU für die von Cyberangriffen ausgehenden potenziell existenzgefährdenden Konsequenzen zu sensibilisieren sind (z.B. mittels anschaulicher und realitätsnaher Demonstrationen von Angriffsszenarien).

4. Security by Design und Zero Trust im Beschaffungswesen

Jede digitale Komponente in Software und Hardware ist im Cyberraum eine **potenzielle Waffe**. In der Praxis **beschafft der Staat solche Komponenten** jedoch **ohne ausreichende Sicherheitsprüfung**. Größtenteils entscheidet der Preis bzw. die Vorgabe zur Kostenminimierung. Es wird von politischer Seite zwar nach digitaler Souveränität gerufen. Gleichzeitig wird dieses Ansinnen durch den konkreten Beschaffungsvorgang konterkariert.

Lösungsansatz/Forderung: Ein wichtiger Bestandteil eines Gesamtkonzeptes im Sinne des geforderten Masterplans muss mittelfristig also das Thema **Sensibilität bei der Beschaffung** sein. Konkret sind die **Grundsätze „security by design“** und **„security by default“**, also die systematische Sicherheits- und Risikobewertung von digitalen Komponenten vor und während des Entwicklungsprozesses, ins Zentrum zu stellen, um ein Kompromittieren von IT-Lieferketten zu vermeiden. Ein weiterer zentraler Ansatz sind **Zero-Trust-Architekturen.** Dieser Ansatz geht davon aus, dass Systemkomponenten und Anwender von Grund auf zu authentifizieren und autorisieren sind, um Operationen und Datenflüsse zu legitimieren. Ein

weiterer Bestandteil ist die Abschottung von besonders schützenswerten Bereichen innerhalb einer IT-Infrastruktur mittels Netzwerksegmentierung. Solche Umstellungen sind häufig mit einem erheblichen Aufwand verbunden. Es besteht jedoch sowohl eine besonders **hohe Dringlichkeit** als auch ein **enormes Potenzial** zur **Steigerung der Sicherheit bei Betreibern von KRITIS und zentralen staatlichen Einrichtungen**. Die Konzepte „Security by design" und „Zero Trust" gehören derzeit anerkanntermaßen zu den effektivsten im Bereich der IT-Sicherheit (siehe Umstellung aller Bundesbehörden in den USA auf Prinzipien der Zero-Trust-Architektur bis Ende 2024).

5. Integrierte Konzepte und Aufbau von Ökosystemen, Kapital mobilisieren und Risiken zu Chancen machen

In Deutschland besteht ein gewaltiger **Nachholbedarf im Bereich Fachkräfte und Investitionen in Cybersicherheit.** Über die Jahre hat sich in Deutschland eine erhebliche Lücke an Expertise zu Cybersicherheit aufgebaut. Diese Lücke wird in den kommenden Jahren aufgrund von stetig steigendem Digitalisierungsgrad einerseits und demografie-bedingten Abgängen vom Arbeitsmarkt andererseits immer größer. Somit besteht in Deutschland ein immenser Bedarf, sowohl Betreibern und IT-Anwendern als auch Unternehmen in der IT-Sicherheitsbranche ausreichend Kapital bereit zu stellen.

Lösungsansatz/Forderung: Die **Wahrung der öffentlichen Sicherheit** gehört zum Kernauftrag des Staates, für die öffentliche Mittel bereitgestellt werden. Bei Cyberangriffen verschwimmen die bisherigen Grenzen zwischen öffentlicher und privater Sicherheit; die Cybersicherheit ist damit Teil des staatlichen Auftrages. Somit sollten auch öffentliche Förderungen für die Weiterentwicklung der Cybersicherheit und den Aufbau von Resilienz gegenüber Angriffen möglich sein. Insbesondere KMU benötigen kurz- und mittelfristig Investitionskapital, um Abwehrsysteme und Expertisen aufzubauen. Neben den bestehenden Haushaltsmitteln für die relevanten Behörden braucht es daher auch **steuerliche Anreize** und ggf. **konditionierte Förderprogramme für Investitionen** in Cybersicherheit, insbesondere für KMU.

Neben Investitionen geht es in der mittleren bis langen Frist auch um langfristig **intelligente, durchdachte und integrierte Konzepte**: Den hier geforderten Masterplan. Dazu gehören etwa Fragen, wie ausreichend Fachkräfte ausgebildet werden können oder wie Forschungs-ergebnisse zeitnah in kommerzielle Produkte überführt werden können. In Israel wurde aus der Erkenntnis der latenten Bedrohung nicht nur beschlossen, sich selbst um den best-möglichen Schutz zu kümmern. Vielmehr wurde auch wirtschaftspolitisch entschieden, dieses Risiko in eine Chance zu wandeln und den Anspruch zu erheben, eine führende Nation für entsprechende Lösungen in der Cybersicherheit zu werden. Ein zentraler Aspekt hierbei ist der **Aufbau von ganzheitlichen Ökosystemen** rund um das Thema Cybersicherheit, in denen der **Staat, die Bildungseinrichtungen und die Expertise von Unternehmen nahtlos miteinander verzahnt** werden. Ein wesentlicher Schlüssel für den mittelfristigen Erfolg liegt in der frühzeitigen Bildung und dem Aufbau von IT-Kompetenzen entlang der gesamten „Bildungskette".

Ein Beispiel ist der **Gav Yam Negev Advanced Technologies Park** in Be'er Scheva mit einem Joint Venture staatlicher Behörden, des israelischen Militärs, einer führenden Universität sowie führenden israelischen und internationalen Unternehmen der Cybersicherheits-branche. Erfolgsfaktor ist hierbei ein ausbalanciertes Konzept zum Aufbau von Infrastruktur, Investitionskapital und Netzwerken.

6. Cybersicherheit als Wertschöpfungsfaktor erkennen und in Politik, Wirtschaft und Gesellschaft umdenken

Produkte aus dem Bereich IT-Sicherheit werden in Deutschland häufig als **bloße Nebenprodukte oder Add-ons** von Elektrotechnik angesehen. Das Ausgabevolumen für Hardware, Software und Dienstleistungen im Bereich IT-Sicherheit in Deutschland wird für das Jahr 2022 mit rund 7,8 Milliarden Euro beziffert und stellt damit einen neuen Rekordwert auf. Für das Jahr 2025 gehen Prognosen sogar von einem Wert weit über 10 Milliarden Euro aus. Im Vergleich der Investitionen und der Wertschöpfung zum BIP mit den USA und Israel ist die deutsche IT-Sicherheitsbranche jedoch nach wie vor ein Zwerg.

Lösungsansatz/Forderung: Hier gibt es einerseits einen wirtschaftspolitischen und andererseits einen ebenso wichtigen sicherheitspolitischen Aspekt. Es braucht ein **Umdenken, welche volkwirtschaftliche Bedeutung die digitale Technologie für Deutschland einnimmt und einnehmen muss**. Das betrifft nicht nur den Bereich IT-Sicherheit sondern das gesamte Spektrum an Produkten und Dienstleistungen in einer Datenökonomie (z.B. datenbasierte Schlüsseltechnologien, wie Machine-to-Machine-Learning und Künstliche Intelligenz). Zur Sicherung und Stärkung der Wettbewerbsfähigkeit der deutschen und europäischen Digitalwirtschaft gilt es die Fähigkeiten des „German Engineering“ und der Industrie 4.0 zu mobilisieren. Eine effektive Absicherung gegen Cyberbedrohungen stellt nämlich einen **zentralen Wettbewerbsfaktor** dar und ist ein wichtiger Bestandteil **der künftigen Wertschöpfung** in Deutschland und Europa. Damit rücken also Fähigkeiten sowohl zum Programmieren als auch zum Entwickeln von Cybersicherheitslösungen (Deep Learning, Cyber Threat Intelligence) in den Fokus der Wissenschafts-, Bildungs- und Wirtschaftspolitik. Hierzu muss ein **Weiterdenken in Politik und Gesellschaft** stattfinden. Verwaltungen sollten diese Potenziale auch bei den Auftragsvergaben einbeziehen.

Um im Bereich Cybersicherheit in Deutschland und Europa voranzukommen geht es nicht um das Kopieren von Vorbildern im Detail. Die hier eingeforderten Ansätze denken die Dinge umfassend und sehen neben den bekannten Risiken zugleich auch die sich bietenden Chancen. Es müssen **heute eine Strategie und ein Masterplan entworfen** werden, um **effektive Ansätze** und **dringend gebotene Verbesserungen morgen umsetzen** zu können. Die vorgeschlagenen Lösungsansätze sind nicht kurzfristig umsetzbar, sondern erfordern ein **langfristiges Umdenken in Politik, Wirtschaft und Gesellschaft**, was einem Dauerlauf gleichkommt. Politik, Gesellschaft und Wirtschaft befinden sich zwar in einer Welt der Umbrüche. Das deutsche Wirtschafts- und Gesellschaftsmodell bietet jedoch die besten Voraussetzungen, die Zeitenwende zu gestalten: Denn **Gestaltung- und Anpassungsfähigkeit** machen den **Kern der Sozialen Marktwirtschaft** aus.