Leitlinien
der Bundesarbeitsgruppe Cybersicherheit

Wirtschaftsrat der CDU e.V.
Luisenstr. 44, 10117 Berlin
Telefon: 0 30 / 240 87 - 0
Telefax: 0 30 / 240 87 - 205
E-Mail: digitales@wirtschaftsrat.de

www.wirtschaftsrat.de

Bundesarbeitsgruppe
Cybersicherheit

Vorsitzender
Prof. Timo Kob

Stellv. Vorsitzender
Paul Kaffsack
Uwe Probst

Referent
Innovation und Digitales
Andreas G. Barke

Stand: 15.06.2022

Einführung

Mit der Digitalisierung steigt sowohl der länderübergreifende Grad der Vernetzung als auch die Schnelligkeit des wirtschaftlichen und gesellschaftlichen Austausches, während sich gleichzeitig tradierte Geschäftsmodelle anpassen müssen bzw. disruptive Entwicklungen durch neue Geschäftsmodelle antizipiert werden müssen. Dahinter stecken riesige Chancen für Wachstum und Wohlstand, gleichzeitig aber neue Risiken und Formen der Kriminalität. Digitalisierung setzt deshalb auch ein Mehr an Sicherheit voraus.

Wir sind gleichwohl davon überzeugt, dass Cybersicherheit kein Angst-Thema sein muss, sondern ein Chancen-Thema sein kann, das die Sicherheit im Cyberraum zu stärken hilft, Wachstum generiert und exportfähige Geschäftsfelder eröffnet. Dafür müssen die jeweils betroffenen Verantwortungskreise, beginnend bei der Politik und Verwaltung, über die Industrie und Hersteller bis hin zu den Anwendern und Nutzern, insgesamt zusammenwirken. Denn alle Verantwortungskreise bewegen sich in einer Gefahrengemeinschaft: Unternehmen und Staat sind gleichermaßen Angriffsziel. Deshalb ist es aus unserer Sicht geboten, gemeinsame Lösungen auf den Weg zu bringen.

Wir setzen uns für einen umfassenden Kulturwandel ein, der die IT-Sicherheit ganzheitlich in den Fokus nimmt: Erstens braucht es eine Sensibilität für Gefahren im Cyberreich, für technische Ausstattung und Notfallpläne im Ernstfall, die es in allen Verantwortungskreisen zu stärken gilt. Zweitens sind in diesem Zusammenhang alle Investitionen in IT-Sicherheit nicht als Kosten, sondern als ein essentieller Wertschöpfungsfaktor im digitalen Zeitalter zu betrachten. Drittens braucht es ein Ökosystem aus Politik, Wirtschaft und Finanzierern, bei dem es zwar einerseits um den Schutz der Wirtschaft geht, andererseits aber auch um die Stärkung der deutschen Sicherheitsbranche in Summe, um nationale Anbieter zu unterstützen und Exportchancen zu nutzen.

Während andere Länder bereits recht erfolgreich in der Digitalwirtschaft agieren, hinkt Deutschland in weiten Teilen hinterher. Mit einer wachsenden, unternehmerischen Anbieterstruktur im Bereich Cybersicherheit ist Deutschland hingegen gut aufgestellt. Wir können Deutschland zu einem Referenzmarkt für Cybersicherheit weiterentwickeln und „IT-Sicherheit made in Germany“ international positionieren. Doch dazu müssen wir die Cyberbranche in Deutschland massiv aufbauen und zu einer Exportbranche weiterentwickeln. Andere Länder gehen auch hier bereits voran und agieren mit ganz anderen Finanzierungshebeln und –modellen. Wir können es uns nicht länger leisten, dieser Entwicklung zuzuschauen, wenn wir selbst beste Voraussetzungen haben.

Damit Deutschland zum Referenzmarkt für Cybersicherheitssoftware wird, braucht es ein gesundes Maß an Verantwortung, Transparenz und Meldepflichten, gleichzeitig aber ein Verständnis dafür, dass der deutsche Mittelstand keine zusätzliche Bürokratie, eingreifende Regulierung und neue Verpflichtungen braucht.

Zusammengefasst will die Bundesarbeitsgruppe Cybersicherheit im Wirtschaftsrat einen Beitrag dazu leisten und hat sich in diesem Grundsatzpapier auf folgende Kernaspekte konzentriert:

1. **Zentralisierung der Digitalisierungspolitik in Verbindung mit dem Abbau von ebenenübergreifender Doppelregulierung und Redundanzen**
2. **Neujustierung der Forschungsförderung, die stärker innovations- und produktbezogen auf schnelle Markteinführung von anwendbaren Forschungsergebnissen abstellt.**
3. **Gezielte Anreizung von Unternehmen, eigenverantwortlich in Sicherheit zu investieren**
4. **Aufbau einer gemeinsamen Plattform für alle mitwirkenden Akteure der Branche zur kampagnenartigen Sensibilisierung von Gefahren im Cyberraum**
5. **Stärkere Einbindung der Wirtschaft in das Nationale Cybersicherheitszentrum**
6. **Entwicklung einheitlicher Standards im Rahmen des digitalen Binnenmarktes**

I. Transparenz und Kompetenz stärken

Deutschland kann sich vor dem Hintergrund der rasanten digitalen Entwicklung und der grenzüberschreitenden Vernetzung kein Kompetenzchaos von Bundesbehörden und einen Zuständigkeitsdschungel in den Bundesländern leisten. Es braucht klar zugeordnete Verantwortlichkeiten, die eine kohärente Cybersicherheitspolitik formt. Auch wenn die Cybersicherheit eine Frage der Gefahrengemeinschaft ist, besteht die Aufgabe des Staates mithin darin, Aufklärung und Sicherheit als Daueraufgabe zu begreifen. Hierin unterscheiden sich analoge und digitale Welt nicht.

Der Wirtschaftsrat empfiehlt:

- eine stärker institutionalisierte und **zentralisierte Steuerung der Digitalisierungspolitik**.
- aus Sicht der Wirtschaft, dass die Herausforderungen der Cybersicherheit – der Schutz der Bürger und der Wirtschaft, aber auch die Stärkung der nationalen Souveränität durch eine starke deutsche IT-Sicherheitswirtschaft –, **zentral im Bundesamt für Sicherheit in der Informationstechnik (BSI)** verankert werden. In Verbindung mit der zuvor empfohlenen Zentralisierung der Digitalisierungspolitik sollte aufgrund des erweiterten Aufgabenspektrums eine Herauslösung aus der Zuständigkeit des Bundesinnenministeriums geprüft werden. Auch das Cyberabwehrzentrum, in welches die Wirtschaft eingebunden werden sollte, gehörte dann an dieses Ressort angegliedert.
- **Abbau der bundes- und ländereigenen Doppelregulierung** und Redundanzen von Sicherheitsbehörden. Hierzu sollte der IT-Planungsrat stärker als Beratungsgremium in Anspruch genommen werden.
- **Stärkung der polizeilichen Strafverfolgung** im Ernstfall. Hierzu bedarf es einer entsprechenden Ausstattung der Polizeibehörden, sodass diese als Ersthelfer und Strafverfolgungsbehörde wirksam aktiv werden kann. Gleichzeitig bedarf es einer **Stärkung der nachrichtendienstlichen Partnerschaft mit der Wirtschaft**.

- **Koordinierung von Polizei- und Strafverfolgungsbehörden auf EU-Ebene** durch z.B. verbesserten Informationsaustausch und einem europaweit harmonisierten Handlungskatalog, der zur Verfolgung von Straftaten im Ernstfall taugt.
- Schneller **Aufbau der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)**. Es muss klare Regeln im Umgang mit Schwachstellen geben. So darf es zu keinem Horten von Schwachstellen führen.
- eine vom Bund initiierte **bundesweite Kampagne** zur Sensibilisierung und Prävention von Gefahrenabwehren, die einen besonderen Fokus auf die KMUs in Deutschland legt. In diesem Zusammenhang sollte eine gemeinsame Plattform für alle mitwirkenden Behörden und Initiativen, sowie allen weiteren relevanten Ansprechpartnern aufgebaut werden. Einen guten Ausgangspunkt bieten hier die kooperativen Plattformen der „Allianz für Cybersicherheit“ und „Initiative Wirtschaftsschutz“, die erweitert und finanziell besser ausgestattet werden sollen.

II. Haftung und Verantwortung zuweisen

Die Bundesregierung hat eine umfassende Cybersicherheitsstrategie bestehend aus dem IT-Sicherheitsgesetz und der Umsetzung der NIS-Richtlinie aufgesetzt. Dennoch sind noch immer Teile der Wirtschaft und Gesellschaft nicht ausreichend für das Thema IT-Sicherheit sensibilisiert; manche Schwachstellen werden nicht öffentlich. Deshalb braucht es verbindliche Regeln seitens des Gesetzgebers.

Der Wirtschaftsrat empfiehlt:

- **i**m Lichte der bisherigen Meldepflicht sollte ein rechtlicher **Haftungsanspruch für fehlerhafte Software** geprüft werden. Dieser sollte jedoch nur dann gelten, wenn bekannte Schwachstellen vom Hersteller nachweislich nicht behoben worden sind.
- **Weiterentwicklung des IT-Sicherheitsgesetzes**, um zu einer Vereinfachung der Regulierung zu kommen. Gemeinsam mit der IT-Wirtschaft sollten z.B. Leitfäden und Best-Practice-Lösungen unter Führung des BSI für KMUs als Teil des Corporate Governance-Prozesses entwickelt werden.
- Die enge Vernetzung unserer Wirtschaft führt dazu, dass Sorglosigkeit in einem Unternehmen nicht nur dieses Haus sondern auch andere Institutionen gefährdet. Es ist daher zu prüfen, wie eine **Verankerung personeller Verantwortung** für das Thema Cybersecurity im Unternehmen angereizt werden kann, die zu einer Steigerung der Sicherheit in der Breite führen, ohne bürokratische Mehraufwände zu generieren.
- **Förderung sicherer Netzwerktechnologien**. Angriffe müssen bereits durch den Einsatz sicherer Netzwerkausrüstung erschwert werden. Der Ausbau des Schutzes von IT-Infrastrukturen basierend auf den Prinzipien „Security by Design“ und „Security by Default“ ist voranzutreiben.

- **Verbindliche Regeln zum Umgang mit veralteter Software**. Eines der offensichtlichsten Einfallstore für Cyberangriffe sind Software und Betriebssysteme, die ihr Lebensende erreicht haben. Hier braucht es verbindliche Regeln, welche die Hersteller bereits zum Zeitpunkt des Markteintritts von Produkten in die Verantwortung nehmen.

III. Forschung und Investitionen fördern

Mit Blick auf den Standort Deutschland zeigt sich besonderer Handlungsbedarf immer wieder im deutschen Mittelstand und im Handwerk. Viele mittelständische Unternehmen unterschätzen die Gefahren, die in einer ungesicherten IT-Infrastruktur liegen. Deshalb müssen diese Unternehmen motiviert werden, in ihre IT-Infrastruktur und technische Sicherheit zu investieren. Ein wichtiger Hebel können überdies PPP-Modelle sein.

Der Wirtschaftsrat empfiehlt:

- ganz grundsätzlich eine Forschungsausrichtung, welche die programmatische Entwicklung von Produkten in den Blickpunkt nimmt und damit einen vor allem **an Produktlösung orientierten Ansatz** verfolgt. Weniger zielgerichtet ist es, eine Forschung alleinig auf die Grundlagenforschung auszurichten.
- Eine stärkere staatliche Verantwortung zum Aufbau breiter Kompetenzen in Forschung und Unternehmen, womit ausdrücklich nicht (nur) die Spitzenpositionen (z.B. Lehrstühle als Leuchttürme) gemeint sind.
- Etablierung eines **Anreizsystems für Investitionen** in die unternehmensbezogene IT-Sicherheitsarchitektur. Im Rahmen der **steuerlichen Forschungsförderung** sollten Investitionen in Softwarelösungen, die auf die Prävention von Cyberangriffe gerichtet sind, und immaterielle Vermögenswerte (Ausbildung, Weiterbildung, Prozessinnovationen) schützen, ebenfalls geltend gemacht werden können.
- bestehende Forschungsförderung im Cybersicherheitsbereich auf **Förderung von Start-ups**, insbesondere den Ausgründungen aus dem universitären Umfeld, umlenken. Zum einen verhilft dies der Start-up-Szene zu weiterer Marktfestigkeit, zum anderen werden gezielt technische Lösungen gefördert, die breite Anwendung im Mittelstand und zur Gefahrenabwehr im KRITIS-Sektor finden.
- eine gemeinsame Strategie von Staat und Unternehmen zur Bewältigung der Herausforderungen der Daten- und Informationssicherheit. Dazu bedarf es neben der Förderung von Venture Capital Fonds auch weiterer innovativer Modelle, die eine **schnelle Markteinführung von Forschungsergebnissen** ermöglichen und neben dem kurzfristigen betriebswirtschaftlichen Erfolg der geförderten Unternehmen und Produkte auch einen langfristigen strategischen Beitrag zur nationalen digitalen Souveränität als Ziel haben, in dem sie vor dem Ausverkauf ins Ausland geschützt werden.

- Einführung eines **Kennzeichens für IT-Sicherheit**, das jedoch nicht nur auf reine Produkteigenschaften abzielt, sondern auch prozessuale Aspekte abdeckt, vergleichbar einer ISO-Zertifizierung, wie es sie etwa beim Qualitätsmanagement gibt.
- **verstärkte Zusammenarbeit** in der Cyberabwehr zwischen staatlichen Akteuren und privatwirtschaftlichen, lizensierten Partnern, um ausreichend Ressourcen bei der Abwehr von Cybersicherheitsinitiativen, gerade auch bei KMUs, zu gewährleisten. Beispielgebend für eine sinnvolle und notwendige Einbeziehung von Wissenschaft und Forschung ist die Digitalisierungsinitiative in Bayern.
- **Stärkere Einbindung der Wirtschaft in das Nationale Cybersicherheitszentrum**. Das US-amerikanische Beispiel zeigt, dass die privatwirtschaftlichen Akteure bei der Aufklärung und Analyse dringend gebraucht werden.

IV. Fachkräftemangel durch Aus- und Weiterbildung begegnen

Die Digitalisierung bringt nicht nur für die Wirtschaft, sondern für die gesamte Gesellschaft weitreichende Veränderungen mit sich. Der Erwerb digitaler Kompetenzen in der Schule sowie in der beruflichen Aus- und Weiterbildung ist dabei ein zentraler Erfolgsfaktor. Will man eine Sensibilisierung auch für Risiken aus dem Cyberraum erreichen, braucht es folglich eine Strategie für die Aus- und Weiterbildung, welche diese aktuelle Herausforderung berücksichtigt.

Der Wirtschaftsrat empfiehlt:

- **Ausbildung von Experten, aber auch breite Kompetenzbildung fördern**. Der aktuelle Fachkräftemangel im Bereich Cybersicherheit verschärft die Lage der Unternehmen in Sicherheitsfragen zusätzlich. Wichtig ist die Ausbildung eines geeigneten Fachpersonals.
- Gemeinsame **Aus- und Weiterbildungsagenda** von Bund und Ländern, in der eine Modernisierung der ländereigenen Rahmenlehrpläne für Berufs- und weiterführende Schulen modernisiert werden. Zum Beispiel sollte die Cybersicherheit in einem Unterrichtsfach Medienkompetenz stärker Thema sein. Außerdem müssen Schüler bereits frühzeitig – am besten in der Grundschule – mit dem Programmieren in Kontakt gebracht und ihnen die notwendige Medienkompetenz vermittelt werden. Zudem ist eine Einführung der **Anpassung der Lehreraus- und -weiterbildung** angezeigt.
- Gezielter **Aufbau von IT-Kompetenzen**, z.B. über entsprechende universitäre Lehrstühle und universitäre Studiengänge. Darüber hinaus gilt es, eine Stärkung der relevanten Fachrichtungen der dualen Ausbildung vorzunehmen.
- **Schaffung entsprechender Berufspositionen mit cybersicherheitsrelevanter Ausrichtung** in Unternehmen, um Fachpersonal in den Unternehmen zu etablieren

V. Europäische und internationale Cybersicherheitspolitik forcieren

Cyberangriffe und Wirtschaftsspionage aus dem digitalen Raum machen nicht an Grenzen Halt. Für die Politik bedeutet das ein Mehr an europäischer und internationaler Zusammenarbeit. Es braucht über ein gemeinsames Verständnis und eine gemeinsame Cyberabwehr insbesondere auch einheitliche Standards für den Markteintritt von Produkten und deren Verfallsdatum.

Der Wirtschaftsrat empfiehlt:

- **Cybersicherheit zum Bestandteil der Außenpolitik machen**. Die Bundesregierung muss eine kohärente, abgestimmte Cyberaußenpolitik etablieren mit dem Ziel der Schaffung eines verbindlichen Abkommens für verantwortliches Handeln im Cyberraum.
- Im Sinne der Vertrauenswürdigkeit braucht es einen **Schnittstellendialog**, in dem geprüft werden muss, wie ausländische Unternehmen angekoppelt und Vertrauen in der gesamten Wertschöpfungskette gestärkt werden können.
- **Schaffung eines europäischen digitalen Binnenmarkts**, der einheitliche Mindeststandards für die IT-Sicherheit in Unternehmen befördert.
- **Europaweit einheitliche Standards bei der öffentlichen Beschaffung**, um einseitige Abschottungen des Marktes durch jeweils einzelstaatliche Standards zu verhindern
- **Verstetigung der deutschen Beteiligung in der European Cybersecurity Organization (ECSO)**, insbesondere um Kohärenz von Erfahrungswissen und geplanter Legislativakte der Europäischen Kommission herzustellen.
- **Anpassung der derzeitigen Exportkontrolle**, die eine einseitige Benachteiligung europäischer Cybersicherheits-Unternehmen bedeutet. Hierzu sollten Produkt- und Länderlisten für kritische Güter und Länder für eine Stärkung der Transparenz im Rahmen der Dual-Use-Reform eingeführt werden.
- Stärkung der internationalen Wettbewerbsfähigkeit vorantreiben, indem sämtliche Abkommen für weltoffene Märkte eintreten
- **Weiterentwicklung internationaler Rechtshilfeabkommen**. Die zukünftige internationale Kooperation zwischen Sicherheitsbehörden und IT-Wirtschaft muss auf Grundlage von modernisierten, transparenten und vereinheitlichten Rechtsvorschriften erfolgen. Dafür sollte sich die Bundesrepublik auf europäischer Ebene gezielt einsetzen.