WIRTSCHAFTSRAT Deutschland

Empfehlungen für die neue Bundesregierung

Cybersecurity als strategische Schlüsselaufgabe der Digitalpolitik

Wirtschaftsrat der CDU e.V.

Die Stimme der Sozialen Marktwirtschaft

Cybersecurity als strategische Schlüsselaufgabe der Digitalpolitik

Die Diskussion um die digitale Zukunft Deutschlands muss Cybersicherheit als ein zentrales Kernelement der Digitalpolitik behandeln. Angesichts der rasanten digitalen Transformation, der zunehmenden Bedrohungen durch Cyberangriffe und der steigenden Anforderungen an digitale Souveränität sind klare und langfristige Strategien notwendig.

Es ist daher entscheidend, dass die folgenden Themen in den Sondierungsgesprächen und Koalitionsverhandlungen auf den Tisch kommen und später im Koalitionsvertrag verankert werden.

1. Klärung der Governance der Digitalpolitik mit Cybersicherheit als Kernelement

Die Governance der Digitalpolitik, insbesondere in Bezug auf Cybersicherheit, muss klar strukturiert und entschieden werden. Eine zentrale Frage dabei ist die Notwendigkeit eines Digitalministeriums, das als Steuerungseinheit für alle digitalen Belange fungiert. Dies würde sicherstellen, dass Cybersicherheit nicht nur als technisches Thema, sondern als **strategische Herausforderung** behandelt wird. Ein Digitalministerium ist aber nur sinnvoll, wenn dieses nicht nur ein „Weiter so unter anderem Namen“ darstellt, sondern wirkliche Entscheidungsbefugnisse über Ressortgrenzen hinaus bekommt.

Ein zentrales Steuerungsgremium sollte die Verantwortung für die Koordination übernehmen und die Umsetzung der Digitalstrategie sowie der Cybersicherheitsmaßnahmen vorantreiben. Ein **dediziertes Cybersecurity-Budget und klare Abgrenzungen** der Zuständigkeiten zum BSI sind dabei essenziell, um die Abwehr von Cyberbedrohungen gezielt und effizient zu gestalten.

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** sollte gestärkt und mit einem entsprechenden Budget ausgestattet werden, gerade auch für die Umsetzung von NIS2 inklusive in den staatlichen Institutionen.

Das BSI muss als **zentrale Instanz** für Cybersicherheit in Deutschland zu fungieren.

Die Bereitstellung ausreichender Mittel für das BSI und der Ausschluss des Bereichs Cyber von Kürzungen sind von zentraler Bedeutung, um eine starke Cyberabwehr zu gewährleisten.

Zentrale Aufgaben wie Forschung und Entwicklungsaufträge für Cybersicherheitslösungen sollten gezielt an die Privatwirtschaft vergeben werden – orientiert **an Vorbildern wie Israel**.

Empfehlung:

- **Schaffung eines Digitalministeriums**, das als Steuerungseinheit für alle digitalen Belange fungiert, um Cybersicherheit nicht nur als technisches Thema, sondern als strategische Herausforderung zu behandeln.

- **Bildung eines zentralen Steuerungsgremiums** zur Koordination und Umsetzung der Digitalstrategie sowie der Cybersicherheitsmaßnahmen.
- **Bereitstellung eines dedizierten Cybersecurity-Budgets** und klare Zuständigkeitsabgrenzungen zum BSI, um gezielte Abwehr von Cyberbedrohungen zu gewährleisten.
- **Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI)** und Ausstattung mit ausreichenden Mitteln zur Umsetzung von NIS2.

2. Re-Industrialisierung, Sicherheit und Aufbau eines GovTech-Ökosystems

Cybersicherheit bildet die Grundlage für eine erfolgreiche Re-Industrialisierung Deutschlands.

Besonders im Bereich der Schlüsseltechnologien wie Halbleiter-Produktion, **Industrie 4.0, KI und Cloud-Infrastrukturen** muss die Sicherheit digitaler Prozesse gewährleistet sein. Hierfür ist es wichtig, dass Deutschland eine führende Rolle in der Entwicklung eines europäischen GovTech-Ökosystems einnimmt. Dieses Ökosystem sollte den Weg für Innovationen in Zukunftstechnologien ebnen, die Resilienz erhöhen und die **Wettbewerbsfähigkeit** Europas auf internationaler Ebene stärken.

Empfehlung:

- **Deutschland sollte eine führende Rolle** in der Entwicklung eines europäischen GovTech-Ökosystems einnehmen, das Innovationen in Zukunftstechnologien wie Halbleiterproduktion, Industrie 4.0, KI und Cloud-Infrastrukturen vorantreibt.
- **Sicherstellung der Cybersicherheit** digitaler Prozesse als Grundlage für eine erfolgreiche Re-Industrialisierung und Stärkung der Wettbewerbsfähigkeit Europas auf internationaler Ebene.

3. Gezielte Investitionen in Schlüsseltechnologien mit Fokus auf Cybersicherheit

Investitionen in Schlüsseltechnologien wie KI, Quantencomputing und Cloud-Infrastrukturen müssen mit einem klaren Fokus auf Cybersicherheit erfolgen. Investitionen in Deutschland und der EU sind entscheidend, um der wachsenden Dominanz globaler Hyperscaler etc. entgegenzuwirken und gleichzeitig wirtschaftliches Potenzial in der Cybersicherheitsbranche zu schaffen.

Die Hightech-Strategie des Bundes sollte sich verstärkt auf Cybersicherheit konzentrieren, um die digitale Souveränität Deutschlands langfristig zu sichern, die Resilienz zu steigern aber auch um Cybersecurity als positiven Wirtschaftsfaktor zu nutzen.

Empfehlung:

- **Investitionen in Schlüsseltechnologien** wie KI, Quantencomputing und Cloud-Infrastrukturen sollten mit einem klaren Fokus auf Cybersicherheit erfolgen.

- **Förderung der Investitionen in Deutschland und der EU**, um der wachsenden Dominanz globaler Hyperscaler entgegenzuwirken und gleichzeitig die Cybersicherheitsbranche zu stärken.
- **Integration von Cybersicherheit in die Hightech-Strategie** des Bundes zur Sicherung der digitalen Souveränität und Steigerung der Resilienz.

4. Digitalisierung und Resilienz der öffentlichen Verwaltung

Ein zentraler Bestandteil der Digitalpolitik muss der Schutz und die Weiterentwicklung der öffentlichen Verwaltung sein. Hierzu gehört die Förderung von Resilienz auf allen staatlichen Ebenen, einschließlich der Kommunen. Das föderale System darf nicht zu einem Hindernis für eine einheitliche Cyberabwehr werden. Es muss gewährleistet sein, dass alle staatlichen Ebenen und auch private Unternehmen wie Telekommunikationsanbieter und Anbieter und Hersteller von Cybersicherheitslösungen und -dienstleistungen in das nationale Lagebild integriert werden.

Wichtig ist zudem die Verringerung des Wildwuchses individueller Architekturen und Systeme, insbesondere auf kommunaler Ebene. Dies kann durch die Einführung von Musterarchitekturen, die den Kommunen angeboten werden, erreicht werden. Eine enge Zusammenarbeit mit dem BSI ist hierbei unerlässlich, um eine bessere Unterstützung bei Vorfällen zu gewährleisten.

Empfehlung:

- **Der Schutz und die Weiterentwicklung der öffentlichen Verwaltung** müssen zentrale Bestandteile der Digitalpolitik sein.
- **Einführung von Musterarchitekturen** zur Verringerung von Fragmentierung und Wildwuchs individueller IT-Systeme, insbesondere auf kommunaler Ebene.
- **Enge Zusammenarbeit** mit dem BSI, um bei Cybervorfällen bessere Unterstützung zu gewährleisten und die Resilienz auf allen staatlichen Ebenen zu fördern.

5. Förderung von Forschung, Entwicklung und Innovation in Cybersicherheit

Zukunftsfähige Cybersicherheitslösungen entstehen aus gezielten Investitionen in Forschung und Entwicklung. Daher müssen sowohl wissenschaftliche Institute als auch Unternehmen stärker in Forschungsprojekte eingebunden werden, die innovative Sicherheitslösungen entwickeln. Auch der Aufbau eines fundierten Innovations-Ökosystems, das insbesondere digitale Start-ups unterstützt, ist von zentraler Bedeutung, um die Cybersicherheitsindustrie in Deutschland zu stärken und die digitale Souveränität zu sichern.

Die enge Verzahnung von Forschung, Wirtschaft und Start-up-Szene fördert die Entwicklung und Marktreife von innovativen Lösungen. Eine gezielte Förderung von F&E-Projekten sollte daher im Koalitionsvertrag verankert werden.

Deutschland ist gut in der Grundlagenforschung, aber leider auch gut in der Fernhaltung dieser Ergebnisse von der Markteinführung. Dies muss enden, im Gegenteil: die praktische Umsetzung sollte ein Erfolgsindikator werden, anstelle ängstlicher Barrieren wegen Sorgen um Beihilfe-Verstöße.

Empfehlung:

- **Stärkere Einbindung von Unternehmen** in Forschungsprojekte wissenschaftlicher Institute zur Entwicklung innovativer Cybersicherheitslösungen.
- **Aufbau eines Innovations-Ökosystems**, das insbesondere digitale Start-ups unterstützt und die Cybersicherheitsindustrie in Deutschland stärkt.
- **Förderung von F&E-Projekten und praktischen Umsetzungen**, die die Markteinführung von innovativen Lösungen vorantreiben.

6. Förderung der digitalen Souveränität und Reduzierung globaler Abhängigkeiten

Die digitale Souveränität ist ein Schlüsselfaktor für die Zukunftsfähigkeit der deutschen Wirtschaft. Die Abhängigkeit von ausländischen Anbietern, insbesondere aus den USA, muss reduziert werden, um den Wirtschaftsstandort Deutschland und der EU zu stärken. Die Schaffung nationaler und europäischer IT-Sicherheitslösungen und die Sicherstellung einer unabhängigen digitalen Infrastruktur sind daher von großer Bedeutung.
Hierzu gehört auch die verstärkte Förderung der Beschaffung deutscher und europäischer Produkte für die öffentliche Verwaltung. Digitale Souveränität muss bei Beschaffungen für die Verwaltungen von Bund, Ländern und Kommunen ein wichtiges Vergabekriterium werden, wobei dies natürlich nicht mit dem Preis niedrigerer Qualität erkauft werden darf. Gleichzeitig kann der Bund so das nationale Ökosystem für IT-Sicherheitslösungen stärken und den Aufbau deutscher und europäischer Unternehmen indirekt unterstützen.

Der Bund muss hierbei als Vorbild agieren und durch gezielte Ausschreibungen den Aufbau eines robusten, nationalen IT-Sicherheitsmarktes unterstützen.
Zur digitalen Souveränität gehört auch, dass wir importierte Produkte technologisch jederzeit überprüfen und gegebenenfalls in ihren Funktionen, auch was den Abfluss von Daten betrifft, beschränken können.

Empfehlung:

- **Reduzierung der Abhängigkeit von ausländischen Anbietern**, insbesondere aus den USA, durch die Schaffung nationaler und europäischer IT-Sicherheitslösungen.
- **Förderung der Beschaffung** deutscher und europäischer IT-Sicherheitsprodukte für die öffentliche Verwaltung.
- **Der Bund soll als Vorbild agieren**, um den Aufbau eines robusten, nationalen IT-Sicherheitsmarktes zu unterstützen.

7. Umsetzung von NIS2 und KRITIS-Dach-Gesetz

Die Umsetzung des NIS2 und des KRITIS-Dach-Gesetzes muss zügig und integriert erfolgen, um klare und einheitliche Sicherheitsstandards für kritische Infrastrukturen und volkswirtschaftlich bedeutsame Unternehmen zu etablieren. Dies erfordert eine klare Rolle des BSI als zentrale Stelle für die nationale Cybersicherheit. Eine Reform des Nationalen Cyberabwehrzentrums und des Nationalen Cybersicherheitsrats sind hierfür unerlässlich, um auf Bedrohungen schnell und effektiv reagieren zu können.

Empfehlung:

- **Zügige und integrierte Umsetzung von NIS2 und des KRITIS-Dach-Gesetzes**, um klare und einheitliche Sicherheitsstandards für kritische Infrastrukturen zu etablieren.
- **Reform** des Nationalen Cyberabwehrzentrums und des Nationalen Cybersicherheitsrats, um eine schnelle und effektive Reaktion auf Bedrohungen zu gewährleisten.

8. Stärkung der deutschen Cybersicherheitswirtschaft und Bekämpfung des Fachkräftemangels

Um die digitale Souveränität zu sichern, muss die deutsche Cybersicherheitsindustrie nachhaltig gestärkt werden.
Anstatt einer direkten Wirtschaftsförderung sollte Forschung und Entwicklung gestärkt werden, ein Ansatz wäre etwa ein „Trust4Trust“-Fonds (privates Kapital und fachliche Begleitung durch das BSI) für praxisnahe Forschung und Entwicklung im Bereich Cybersecurity.
Wichtig sind aber auch Änderungen an den Ausschreibungsregeln, die bisher teilweise durch ihre Kriterienwahl die Nutzung von nicht-europäischen Produkten befördern und den Marktzugang für deutsche Unternehmen (z.B. durch Größenkriterien) verhindern. Die Stärkung der digitalen Souveränität muss hier als Kriterium mit einfließen, wobei technische Qualität natürlich weiterhin der Hauptfaktor bleiben muss.

Darüber hinaus müssen Maßnahmen ergriffen werden, um den Fachkräftemangel in der IT- und Cybersicherheitsbranche zu bekämpfen.
Die ausschließliche Fokussierung auf akademische Berufswege muss enden. Wir brauchen dringend die Nutzung des dualen Ausbildungsweges – der in so vielen Bereichen der deutschen Industrie ein Erfolgsmodell ist – auch für die Cybersecurity.
Die Schaffung von Ausbildungsberufen, Weiterbildungs- und Umschulungsinitiativen, die auch die Steigerung des Anteils von Frauen in MINT-Berufen fördern, ist ein wichtiger Bestandteil dieser Strategie, ebenso muss das Thema Cybersecurity in die schulische Ausbildung integriert werden.

Empfehlung:

- **Stärkung** der deutschen Cybersicherheitsindustrie durch gezielte Forschung und Entwicklung, beispielsweise durch einen „Trust4Trust“-Fonds für praxisnahe Forschung.

- **Förderung von Ausbildungs- und Weiterbildungsinitiativen**, einschließlich der Integration von Cybersecurity in die schulische Ausbildung.
- **Bekämpfung des Fachkräftemangels durch verstärkte Nutzung** des dualen Ausbildungssystems und Förderung von Frauen in MINT-Berufen.

9. Vision für eine sichere und souveräne digitale Zukunft

Eine langfristige Vision für Deutschlands digitale Souveränität könnte darin bestehen, dass bis 2040 die Schäden durch Cyberangriffe in Deutschland auf unter 50 Milliarden Euro (auf Basis der bekannten jährlichen Bitkom-Studie) sinken, während die deutsche Cybersicherheitsindustrie 40 Prozent des nationalen Marktes und 10 Prozent des weltweiten Marktes abdeckt.
Diese Vision muss von der gesamten Gesellschaft getragen und durch konkrete Maßnahmen wie gezielte Investitionen, Ausbildung und Innovation unterstützt werden. Ein weiteres Beharren und Verharren im Ressortdenken und föderalen Strukturen können wir uns nicht erlauben.

Empfehlung:

- Bis 2040 sollte **das Ziel** sein, die Schäden durch Cyberangriffe in Deutschland auf unter 50 Milliarden Euro zu senken und die deutsche Cybersicherheitsindustrie 40 % des nationalen Marktes und 10 % des weltweiten Marktes abzudecken.
- Diese Vision sollte durch **konkrete Maßnahmen** wie Investitionen, Ausbildung und Innovation unterstützt und von der gesamten Gesellschaft getragen werden.

10. Cyber-Proofing: Integration von Cyber-Sicherheitsbewertungen in Regulierungsvorhaben

Es wäre sinnvoll Rechtsvorschriften „cybersicher“ zu machen, indem strikte Folgenabschätzungen durchgeführt werden. Cybersicherheits-Folgenabschätzungen würden sicherstellen, dass die Gesetzgebung der (Cyber-)Sicherheit in Europa Vorrang einräumt und diese nicht untergräbt. Dies ist besonders wichtig in einer Zeit, in der sich die Technologie schnell weiterentwickelt, komplex ist und alle Bereiche des täglichen Lebens berührt.

Verfahren zur Überprüfung der Cybersicherheit sollen sicherstellen, dass die gesamte Cyberregulierung im Auge behalten wird, um unnötige Überschneidungen zwischen Rechtsvorschriften, widersprüchliche Anforderungen oder Anforderungen, die anderweitig bestehende Schutzmaßnahmen untergraben, zu vermeiden.

Empfehlung:

- **Rechtsvorschriften** sollten „cybersicher“ gemacht werden durch strikte Folgenabschätzungen, die sicherstellen, dass Gesetzgebung die Cybersicherheit nicht untergräbt.

- **Standardisierte** Cybersicherheits-Folgenabschätzungen sollten durchgeführt werden, um unnötige Überschneidungen zwischen Rechtsvorschriften zu vermeiden.

11. Cyberversicherung und Prävention

Cyberversicherung ist ein maßgeblicher Faktor, um die finanzielle Resilienz der Wirtschaft zu stärken. **Versicherungsschutz muss aber mit Cyberprävention Hand in Hand gehen** und es müssen gemeinsam Lösungen erarbeitet werden, um die Cyber-Resilienz in der Breite zu erhöhen. Die Cyber-Resilienz der Wirtschaft muss in der Breite gestärkt werden. Dabei dürfen nicht nur große Unternehmen und die kritische Infrastruktur adressiert werden. Zwei Drittel der deutschen Unternehmen erfüllen **nicht die Grundvoraussetzungen für Cyberversicherungsschutz**. Damit haben wir als Wirtschaftsstand Deutschland ein Problem insgesamt – mangelnde Cybersicherheit ist ein Standort- und Wettbewerbsnachteil.

Empfehlung:

- **Cyberversicherung** muss eng mit Präventionsmaßnahmen verbunden werden, um die Cyber-Resilienz der Wirtschaft zu erhöhen.
- **Fokus auf die gesamte Wirtschaft**, nicht nur auf große Unternehmen und kritische Infrastrukturen, um den Cyberversicherungsmarkt zu stärken und den Wettbewerbsnachteil Deutschlands zu verringern.

Fazit

Cybersicherheit muss als strategische Schlüsselaufgabe der Digitalpolitik verankert werden. Gezielte Investitionen in Forschung, Entwicklung, Ausbildung und die Stärkung der Cybersicherheitsarchitektur ermöglichen es Deutschland, eine führende Rolle in der digitalen Zukunft einzunehmen. Der Fokus muss auf der Stärkung der digitalen Souveränität, der Schaffung eines resilienten IT-Sicherheitsmarktes und der Bekämpfung des Fachkräftemangels liegen. Nur so kann Deutschland in einer zunehmend unsicheren und geopolitisch turbulenten Welt seine digitale Zukunft nachhaltig und sicher gestalten.