Wahlprüfsteine des Wirtschaftsrates aus dem Bereich Cybersicherheit zu den Wahlen des 21. Deutschen Bundestags

Zusammenfassung:
Deutschland steht vor enormen Herausforderungen im Bereich der Cybersicherheit. Die digitale Transformation und die Lehren der „Zeitenwende“ erfordern ein tiefgreifendes Umdenken in der staatlichen Cybersicherheitsarchitektur und der Zusammenarbeit zwischen Staat, Wirtschaft und Gesellschaft. Die hier vorgestellten Empfehlungen zeigen Wege auf, wie Deutschland eine führende Rolle in der Cybersicherheit einnehmen kann – und das effizient und zukunftsgerichtet.

1. Staatliche Cybersicherheitsarchitektur grundlegend neu denken

Die aktuelle Diskussion über eine mögliche Zentralstellenfunktion des Bundesamtes für Sicherheit in der Informationstechnik (BSI), einschließlich einer notwendigen Grundgesetzänderung, sowie Klagen über die Probleme des Föderalismus verdecken die wahren Ursachen: Die Digitalisierung durchdringt alle Lebensbereiche und erfordert ein fundamentales Umdenken in der staatlichen Cybersicherheitsarchitektur.

Empfehlungen:

- Entwicklung einer neuen, zentralen Cybersicherheitsarchitektur, die Bund und Länder umfasst und auf Effizienz und Wirksamkeit fokussiert ist.
- Erhalt funktionierender Strukturen, jedoch Integration in einen schlankeren, modernen Rahmen, um nicht nur schneller zu agieren, sondern auch um in Zeiten knapper Kassen Haushaltsmittel effektiver zu nutzen.
- Hierzu gehört auch die Diskussion nach Kompetenzbündelung in einem echten Digitalministerium

2. Bedingte Verteidigungsfähigkeit 2.0

Die Reaktionsfähigkeit des Staates auf großflächige Cyberangriffe ist unzureichend. Bei der Terrorismusbekämpfung gab es eine Bündelung von Verantwortlichkeiten und die Schaffung klarer Strukturen nach den Anschlägen vom 11. September 2001

Empfehlungen:

- Dringende Einführung klarer Regelungen und eine Verantwortungsbündelung für den Ernstfall eines großangelegten Cyberangriffs, einschließlich hybrider Bedrohungen.

- Vermeidung rechtlicher Unsicherheiten durch klare und verbindliche Regelungen zwischen Bund, Ländern, Kommunen und relevanten Akteuren wie BKA und Bundeswehr.

3. Kritische Infrastrukturen umfassen auch Staat und Verwaltung

Die Entscheidung, Länder und Kommunen von der Regulierung durch NIS2 auszuklammern, ist ein falsches Signal. Die kommunalen Verwaltungen sind eine kritische Infrastruktur, die besonders schlecht geschützt ist.

Empfehlungen:

- Schaffung eines klaren Zeitplans und Vorgehensmodells für ein verbindliches Sicherheitsniveau für Bund, Länder und Kommunen, um eine sichere digitale Infrastruktur zu gewährleisten.
- Entwicklung eines Plans, wie durch die Harmonisierung der IT-Architekturen von Bund und Ländern bis hinunter zu den Kommunen ein einheitlicher Schutz gewährleistet werden kann.

4. Bessere Transparenz und Kooperation zwischen Staat und Wirtschaft

Ein effektiver Informationsaustausch zwischen Staat und Wirtschaft, insbesondere den Kritischen Infrastrukturen, bleibt unzureichend. Der geplante Ausbau eines Information-Sharing-Portals durch das BSI ist ein richtiger Schritt, aber alleine nicht ausreichend.

Empfehlungen:

- Optimierung des Informationsaustauschs durch eine zentrale Plattform, die alle relevanten Akteure bündelt und effiziente Erkenntnisgewinne ermöglicht.
- Personelle und organisatorische Aufstockung des BSI, um eine zielgerichtete Implementierung von Informationsaustausch-Portalen zu gewährleisten.

5. Von Strategien zur Umsetzung

Zu viele Einzelstrategien und Arbeitskreise verhindern ein kohärentes Vorgehen in der Cybersicherheit. Viele Strategiepapiere dienen mehr der Simulation von Fortschritt, als dass sie konkrete Ergebnisse hervorbringen.

Empfehlungen:

- Zusammenführung bestehender Teilstrategien und eine ganzheitliche Betrachtung der Cybersicherheit im Gesamtkontext (z.B. Nationale Sicherheitsstrategie, Nationale Cybersicherheitsstrategie, Eckpunkte Wirtschaftsschutz, Digitalstrategie,...)

Wahlprüfsteine des Wirtschaftsrates aus dem Bereich Cybersicherheit zu den Wahlen des 21. Deutschen Bundestags

- Entwicklung konkreter Maßnahmen, die direkt aus diesen Strategien abgeleitet und umgesetzt werden, bevor neue Strategiepapiere verfasst werden.

6. Den Fachkräftemangel 2025 und 2045 gleichzeitig angehen

Der Fachkräftemangel ist eine der größten Herausforderungen im Bereich der Cybersicherheit. Sowohl kurz- als auch langfristige Maßnahmen sind notwendig, um diese Lücke zu schließen.

Empfehlungen:

- Einführung praxisorientierter Ausbildungsberufe wie „Fachinformatiker Cybersecurity“ und Intensivierung von Weiterbildungs- und Umschulungsprogrammen.
- Integration der Themen Digitalisierung und Cybersicherheit in die Lehrpläne von Grundschulen.
- Aufbau von interaktiven Online-Angeboten („Classroom as a Service“), um den Mangel an Lehrkräften zu kompensieren.

7. Steigerung der Resilienz der Bevölkerung

Die gesellschaftliche Widerstandsfähigkeit gegen Cybergefahren ist unzureichend ausgeprägt. Ähnlich wie bei früheren Aufklärungskampagnen in den Bereichen Verkehrssicherheit und AIDS-Bekämpfung, muss auch hier die Bevölkerung besser sensibilisiert werden.

Empfehlungen:

- Staatliche Awareness-Kampagnen zur Cybersecurity, unter Einbeziehung von Wirtschaft und Gesellschaft.
- Nutzung innovativer Methoden zur Kostensenkung und zur Förderung von Bewusstseinsbildung in der Bevölkerung.

8. Cybersecurity als Chance für Industriepolitik

Deutschland hat das Potenzial, ein führender Standort für Cybersicherheitslösungen zu werden, verpasst jedoch oft die Gelegenheit, die vorhandene Innovationskraft und Gründungsbereitschaft zu nutzen.

Empfehlungen:

- Einführung einer aktiven Industriepolitik zur Förderung von Cybersecurity-Lösungen „Made in Germany“, um die Forderung nach Digitaler Souveränität mit Inhalt zu füllen.
- Unterstützung von Startups durch intelligente Mittel-Allokation und Modernisierung der staatlichen Beschaffungsvorgaben, um die Marktreife schneller zu erreichen und eine Marktdurchdringung zu fördern.