Cyber-Sicherheit und Cyber-Resilienz als Grundpfeiler der Digitalisierung konsequent stärken

BACDJ – Fachkommission Daten & Digitalisierung

Digitalisierung und IT-Netze sind längst zu den Lebensadern unserer Gesellschaft geworden. Mehr Digitalisierung und die Nutzung von Daten, die aus Vernetzung entstehen, sind nötig, um viele Herausforderungen zu lösen, vor denen die Menschheit steht. Die Bekämpfung der Folgen des Klimawandels, eine Gesellschaft, die Partizipation und Teilhabe noch einfacher ermöglicht und alle mitnimmt, sowie vor allem Produktivitätsgewinne, Innovation und wirtschaftliche Prosperität gehören dazu.

Mehr Digitalisierung und Vernetzung bedeutet mehr Angriffsflächen für Cyber-Attacken und potenziell höhere Schäden bei erfolgreichen Cyber-Angriffen. Organisierte Cyber-Kriminalität, staatlich gesteuerte oder geduldete Hacker-Gruppen sowie Hacktivisten nutzen das Internet und die Vernetzung der Welt, um ihre kriminellen, staatlichen oder ideologischen Ziele durchzusetzen. Instabile politische Situationen begünstigen und verstärken dies.

Der BSI-Lagebericht zur Lage der IT-Sicherheit in Deutschland zeigt einen signifikanten Anstieg von Cyber-Angriffen. Angesichts dessen ist der Bundesarbeitskreis Christlich-Demokratischer Juristen (BACDJ) überzeugt, dass innere und äußere Sicherheit zusammengedacht werden müssen. Dieses Papier soll die Diskussion befördern.

1. Bildungs- und Bewusstseinswandel für mehr Cyber-Sicherheit

Während Cyber-Attacken immer neue Hochstände erreichen, bleiben viele Stellen in der IT-Sicherheit unbesetzt. Die Einführung von neuen und zusätzlichen Hochschulstudiengängen reicht nicht aus.

Der Mensch ist der wichtigste Faktor für erfolgreiche Digitalisierung und gleichzeitig das größte Einfallstor für Cyber-Angriffe. Daher müssen Menschen überall in ihrer Lebens- und Arbeitsbezügen Freude daran finden, die digitale Transformation voranzutreiben. Dies ist nur nachhaltig, wenn alle Beteiligten für Cyber-Sicherheit hinreichend sensibilisiert sind.

Es bedarf einer Stärkung der digitalen Querschnittskompetenz in der ganzen Breite der Gesellschaft, um die digitale Teilhabe und das notwendige Verständnis für die Bedrohungen im digitalen Raum zu schärfen. Die Förderung digitaler Allgemeinbildung sowie digitaler Problemlösungsfähigkeiten muss im gesamten Bildungssystem von Anfang an und ein Leben lang gezielt gefördert werden.

Dazu schlagen wir vor:

- Digitale Bildung in allen Bereichen des Bildungssystems sowie in der Aus- und Weiterbildung von Lehrenden zum Standard zu machen.
- Die Einführung verbindlichen Informatikunterrichts beschleunigen.
- Die von der IT-Wirtschaft zur Verfügung gestellten Lernangebote zur Stärkung digitaler Kompetenzen intensiver nutzen, um aktuelle IT-Entwicklungen in Aus- und Weiterbildung besser einbinden zu können.
- Das Cyber-Sicherheitsbewusstsein in der Breite durch Bündelung vorhandener staatlicher und privater Initiativen sowie durch zusätzliche Kampagnen zu verbessern.

2. Stärkung der Cyber-Resilienz

Digitalisierung ist ein fortlaufender Prozess. Jede technische Innovation verändert das digitale Spielfeld. Das Sicherheitskonzept der alten digitalen Welt war stark auf den Standort als Indikator für Vertrauen ausgerichtet. Ein Ansatz, der allein auf Orte ausgerichtet ist, genügt in der heutigen Welt nicht.

Zur Abwehr von Cyber-Attacken bedarf es eines angemessenen Bewusstseins für aktuelle Bedrohungen und notwendige Verteidigungsmaßnahmen. Deutschland ist insgesamt nicht gut vorbereitet.

Der BACDJ ist der Überzeugung, dass es bei der Herstellung von Cyber-Resilienz nicht darum geht, hundertprozentige Sicherheit zu erreichen. Vielmehr muss es um eine dem jeweiligen Risiko angemessene Sicherheit gehen. Ein Denken in Kategorien der Resilienz soll dabei ermöglichen, Gefahren zu erkennen und Risiken einzuschätzen, um sie zur Grundlage einer individuellen und dynamischen Cyber-Sicherheitsstrategie zu machen.

Dazu schlagen wir vor:

- Ausgewählte technische und organisatorische Maßnahmen zur Herstellung von Cyber-Sicherheit und zur Verbesserung der Reaktionsgeschwindigkeit sowie -fähigkeit bei Sicherheitsvorfällen treffen.
- Cyber-Sicherheitsübungen regelmäßig konsequent abhalten, um Gefahrenlagen zu simulieren und sowohl technisch als auch rechtlich gut darauf vorbereitet zu sein.
- Individuell erprobte, belastbare Maßnahmen für ein praktikables und sinnvolles Business Kontinuitätsmanagement (BKM) ergreifen.
- Förderung von Maßnahmen zur Sicherung digitaler Identitäten, zur Vorbeugung ihres Missbrauchs und eine konsequente Umsetzung des Zero-Trust-Ansatzes.

3. Umgang mit Schwachstellen modernisieren

Cyber-Sicherheit, die Sicherheit kritischer Infrastrukturen und das Vertrauen in Digitalisierung lässt sich nur durch einen verantwortungsbewussten Umgang mit Schwachstellen erzielen. Es muss rechtlich zulässig sein, Computersysteme auf Sicherheitslücken methodisch testen zu können. Erkannte Schwachstellen müssen transparent gemanagt werden. Staatliche Institutionen dürfen davon nicht ausgenommen sein.

Dazu schlagen wir vor:

- Anpassung des § 202c StGB zur Beseitigung des Risikos einer Kriminalisierung des Umgangs mit Schadsoftware und der Suche nach Schwachstellen.
- Aufbau eines transparenten, europäischen Managements von Schwachstellen.
- Stärkung eines unabhängigen und personell wie finanziell gut ausgestatteten Bundesamtes für Sicherheit in der Informationstechnologie (BSI).
- Einführung einer konsequenten Unterrichtungspflicht betroffener Hersteller zur Bereitstellung von Patches und Updates, um Schwachstellen zu schließen.

4. Datenschutz und Datensicherheit neu denken

Das vielfach genutzte Narrativ der Konkurrenz zwischen Datenschutz und Datensicherheit führt in die Irre und beeinträchtigt Deutschlands Cyber-Resilienz. Es muss daher vom Kopf auf die Füße gestellt werden: Datenschutz und Datensicherheit sind untrennbar und bedingen sich wechselseitig.

Zur Förderung der Rechtssicherheit und für eine datenschutzkonforme Digitalisierung bedarf es einer konsequent einheitlichen Auslegung und Anwendung des geltenden Datenschutzrechts durch die Aufsichtsbehörden in Deutschland.

Für eine sichere Digitalisierung sind hergebrachte Sicherheitskonzepte zu überdenken. Deutschland muss weg von seinem Fokus auf Komponenten hin zu einer Prozessorientierung in der Cyber-Sicherheit.

Dazu schlagen wir vor:

- Bei datenschutzrechtlichen Bewertungen Datensicherheit stärkeres Gewicht beimessen, damit Datenschutz Datensicherheit nicht verhindert.
- Open-Source-Lösungen bei Datensicherheit nicht privilegieren. Open-Source-Lösungen müssen bei datenschutzrechtlichen Bewertungen im Rahmen der Beschaffung daraufhin geprüft werden, ob Mindestanforderungen an IT-Sicherheit erfüllt sind.
- Den BSI IT-Grundschutz an die neuen Bedrohungslagen dahingehend anpassen, dass der Fokus weniger auf Komponenten und mehr auf einer Sicherheitsprozessorientierung liegt.
- Die Auslegung der Datenschutz-Grundverordnung (DSGVO) in Deutschland stärker vereinheitlichen, um Standortnachteile für die Wirtschaft abzubauen und die Rechtssicherheit bei der Umsetzung der Digitalisierung zu erhöhen.