Cybersicherheit

Wo wir stehen & was wir wollen

Diebstahl, Industriespionage oder Sabotage verursachten im vergangenen Jahr Schäden von 266,6 Milliarden Euro.[1] Insbesondere KMU sind nur bedingt auf Cyberangriffe vorbereitet und der Fachkräftemangel setzt ihnen zu. Auch Verwaltung und Politik stehen im Zentrum von Attacken, die neben finanziellen Absichten auch auf die Schädigung unserer Demokratie abzielen.

Ziel für die nächste Legislaturperiode sollte sein, Cybersicherheit in der Breite zu stärken. Klar ist: Der richtige Umgang hier schützt nicht nur die deutsche Bevölkerung und Wirtschaft, er stärkt gerade auch die digitale Souveränität Deutschlands. Dafür braucht es erstens einen Fokus auf die praxisnahe Umsetzung der jüngst eingeführten europäischen Gesetzgebung, wie NIS2, CRA und CER. Dies ist notwendig, um ein einheitliches Sicherheitsniveau zu schaffen, gleichzeitig darf die Wirtschaft nicht durch weitere Regulierung eingeschränkt werden. Zweitens benötigt es eine gute Zusammenarbeit mit der Wirtschaft und Wissenschaft. Nur so kann eine Datengrundlage für den sinnvollen Einsatz von innovativen Technologien für mehr Cybersicherheit generiert werden. Drittens ist wichtig, dass die Verwaltung angemessene Sicherheitsstandards einhält, nur dann kann der Staat Vorbild sein. Am Ende der Legislaturperiode sollte Cybersicherheit wirksam in der Breite umgesetzt sein sowie als Innovationsförderer im Sinne einer digitalen Souveränität für selbstbestimmtes Handeln im digitalen Raum betrachtet werden.

10,5
Mrd. Euro

werden deutsche Unternehmen voraussichtlich 2024 in IT-Sicherheit investieren, das ist eine Steigerung 13,1% im Vergleich zum Vorjahr.[1]

Handlungsempfehlungen für die neue Legislaturperiode

- **Praxisnahe und harmonisierte Cybersicherheitsgesetze**: Statt auf Meldepflichten sollten Unternehmen sich auf die tatsächliche Stärkung ihrer Cybersicherheit konzentrieren können. Damit das geht, müssen die neuen Cybersicherheitsgesetze unbürokratisch, europaweit einheitlich und praxisnah umgesetzt werden. NIS2 und das KRITIS-Dachgesetz sollten harmonisiert umgesetzt werden, um Rechtssicherheit zu schaffen und divergierende Verpflichtungen zu vermeiden. Beim CRA ist die Erarbeitung von harmonisierten Normen entscheidend. Das Computerstrafrechts muss im Sinne von Sicherheitsforschenden modernisiert werden. Zusätzlich gilt es, Unternehmen bei der Wahrung ihrer Sicherheit zu unterstützen: Der Staat sollte daher Möglichkeiten zur Sicherheitsüberprüfung von Beschäftigten mit kritischen Tätigkeiten schaffen.

1 ↗Bitkom Studie »Wirtschafsschutz«, 2024

- **Öffentliche Verwaltung absichern**: Die nächste Bundesregierung muss die Cybersicherheit der Verwaltung gezielt stärken, um Vorbild zu sein. Für den Bund bedeutet dies, die gleichen Sicherheitsstandards im NIS2UmsuCG zu setzen, die für Unternehmen gelten – und auch bei den Bundesländern für die Erhöhung der Standards zu werben. Idealerweise zeigt der Staat auch, was noch möglich ist: Daher sollten die sicherheitskritischen Infrastrukturen des Bundes ein Schutzniveau erhalten, das über das NIS2 hinausgeht. Grundsätzlich müssen Innovation, Sicherheit und Praxisorientierung im Sinne von Security by Design gemeinsam gedacht werden; z. B. bei der Etablierung von agilen Verschlüsselungstechnologien oder beim Einsatz von Confidential Computing im Cloud-Computing. Bei Zielkonflikten sollten Entscheidungen stets zugunsten der Cybersicherheit, aber im Einklang mit hohem Innovationsgrad, getroffen werden. Grundstein für diese Arbeiten sollte eine Zentralisierung behördlicher Zuständigkeiten sein. Wir empfehlen daher den Ausbau des BSI zur Zentralstelle für die Bund-Länder-Koordination und eine weitere Stärkung der Cyberagentur.

- **Investitionen in Cybersicherheit stärken**: Zu oft scheuen Unternehmen und gerade KMU vor hohen Investitionen in ihre Cybersicherheit zurück – nur um im Schadensfall vor deutlich höheren Kosten zu stehen. Um dieses Problem zu beseitigen, fordern wir die Schaffung finanzieller Anreize für den Einsatz von Cybersicherheitslösungen bei End Usern. Dazu gehören insb. steuerliche Abschreibungen für neu beschaffte Produkte, Dienstleistungen, Schulungen sowie ein dezidiertes Digitalbudget zur Förderung der Cybersicherheit. Insbesondere KMU in kritischen Sektoren sollten von diesen Maßnahmen profitieren. Förderprogramme müssen daher bürokratie- und aufwandsarm gestaltet werden. Zudem müssen Startups im Bereich Cybersicherheit mit Steuererleichterungen, Mietzuschüsse und Zugang zu Technologien gefördert werden.

- **Menschen mitdenken**: Menschen müssen wissen, wie sie sicher im digitalen Raum handeln können. Die Grundlage hierfür legt eine gute digitale Bildungspolitik[2] ab der Grundschule. Neben der Förderung von Medienkompetenz und Wissen zur Digitalisierung gilt es auch das lebenslange Lernen zu stärken: Bildungsgutscheine für Azubis können helfen, genauso wie Kompetenzförderung im Vorfallmanagement oder Wissenschaftskooperationen für berufsbegleitende universitäre Weiterbildungsmodelle. Technische Maßnahmen, wie z. B. Content Credentials gegen Desinformation, können ebenfalls unterstützen. Wichtig ist außerdem: Cybersicherheit ist neben der Bildung auch eine Fachkräftefrage. Einem möglichst einfachen Zuzug von Fachkräften und der Stärkung von Frauen in der IT kommt daher hohe Bedeutung zu.[3]

- **Cybersicherheitstechnologien priorisieren und fördern**: Cybersicherheit ist nicht zuletzt ein technologischer Wettlauf. Um ein hohes Cybersicherheitsniveau auf breiter Front zu gewährleisten, braucht es daher die stetige Erforschung neuer Cybersicherheitstechnologien und die exakte Messung ihres Einsatzes. Neue Technologien wie Quantencomputer erfordern zudem ein Umdenken, wenn Sicherheitspläne erarbeitet werden. Statt zu kürzen und an der Sicherheit zu sparen, braucht es daher eine Investitionsoffensive bei der Cybersicherheitsforschung durch die Bundesregierung. In diesem Rahmen sollte sie sich etwa stärker an der Co-Finanzierung europäischer Förderprogramme wie dem Digital Europe Programme beteiligen.

90 %

der deutschen Unternehmen gehen davon aus, dass die Anzahl der Cyberattacken auf ihr Unternehmen in den nächsten 12 Monaten zunehmen wird.[4]

76 %

der deutschen Unternehmen sagen, dass die öffentliche Verwaltung viel schlechter auf Cyberangriffe vorbereitet ist als die deutsche Wirtschaft.[4]

2 Siehe in diesem Zusammenhang auch das ↗Kapitel »Digitale Bildung«
3 Mehr hierzu in unseren Kapiteln ↗»Fachkräfte« & ↗»Frauen für die Digitalisierung«
4 ↗Bitkom Studie »Wirtschafsschutz«, 2024