EXPERTENKOMMISSION
FORSCHUNG
UND INNOVATION

EFI

Presseinformation

Cyber-Angst lähmt Innovation

Gefahr durch Cyberangriffe wächst – Cyberbedrohung schwächt Innovationsaktivität von Unternehmen – Sehr hoher Bedarf an Cybersicherheitsfachleuten zurzeit nicht zu decken – Deutschland bei Innovationen in Cybersicherheit deutlich hinter internationalen Wettbewerbern

Berlin, 19. Februar 2020 – Das aktuelle Jahresgutachten der Expertenkommission Forschung und Innovation (EFI), das heute der Bundeskanzlerin in Berlin übergeben wurde, widmet sich dem Thema Cybersicherheit und den Auswirkungen von Cyberrisiken auf Innovationsaktivitäten. „Die fortschreitende Digitalisierung und digitale Vernetzung bieten neue Angriffspunkte auf innovative Unternehmen. Die Mehrheit der innovativen deutschen Unternehmen in der Informationswirtschaft und im verarbeitenden Gewerbe sieht deshalb einen hohen Schutzbedarf ihrer IT für Innovationstätigkeiten. Außerdem geht über die Hälfte dieser innovativen Unternehmen davon aus, dass die Gefahr durch Cyberangriffe auf ihr Unternehmen in den kommenden Jahren weiter zunehmen wird“, so der Vorsitzende der EFI, Prof. Uwe Cantner von der Universität Jena.

Die Innovationsaktivitäten der Unternehmen seien von dieser Gefahr direkt betroffen (siehe Kasten) und es ergäben sich aus Cyberangriffen mittelbar negative Auswirkungen auf das wirtschaftliche Wachstum Deutschlands. „Das gilt insbesondere auch für den Wachstumsbeitrag digitaler Zukunftstechnologien wie der künstlichen Intelligenz oder des Internets der Dinge, denn der Erfolg dieser Technologien hängt nicht zuletzt von ihrer Sicherheit ab“, wie Prof. Irene Bertschek vom ZEW Mannheim und Mitglied der EFI erklärt.

Befragung zu Cybersicherheit und Innovationen:

Die Expertenkommission ließ untersuchen, ob sich die Bedrohung durch Cyberangriffe auf die Innovationsaktivitäten der Unternehmen auswirkt: Eine im Auftrag der EFI durchgeführte repräsentative Umfrage bei Unternehmen in der Informationswirtschaft und im verarbeitenden Gewerbe im dritten Quartal 2019 zeigt zwar, dass 64 Prozent der Unternehmen keine Beeinflussung ihrer Innovationsprojekte durch die Gefahr eines Cyberangriffs sehen. Bei immerhin rund 30 Prozent der Unternehmen verzögern sich jedoch existierende Innovationsprojekte wegen der Gefahr eines Cyberangriffs. Bei rund 17 Prozent der Unternehmen werden geplante Innovationsprojekte durch die Gefahr eines Cyberangriffs erst gar nicht begonnen. Rund 12,5 Prozent der Unternehmen planen aus diesem Grund sogar keine neuen Innovationsprojekte.

Die Cybersicherheit ist wiederum selbst Gegenstand von Innovationen und trägt mit ihren Produkten und Dienstleistungen zu wirtschaftlichem Wachstum und Wohlstand in Deutschland bei. Demnach belief sich die Bruttowertschöpfung der deutschen IT-Sicherheitswirtschaft im Jahr 2017 auf 15,5 Milliarden Euro und machte damit 14,3 Prozent an der gesamten IT-Branche aus (108,6 Milliarden Euro). Von 2010 bis 2017 wuchs die Bruttowertschöpfung in der IT-Sicherheitswirtschaft nominal um durchschnittlich 5,6 Prozent pro Jahr, stärker als die IT-Branche insgesamt oder die Gesamtwirtschaft.

Trotzdem liegt Deutschland bei Patentanmeldungen im Bereich der Cybersicherheit mit einem Anteil von 6,2 Prozent deutlich hinter den USA (33,5 Prozent), Japan (13,7 Prozent) und China (11,6 Prozent) zurück. „Unter den 150 innovativsten Cybersicherheits-Unternehmen der Welt sind 112 aus den USA, 18 aus Israel und leider nur eines aus Deutschland“, wie Prof. Bertschek feststellt.

„Einer Steigerung der Cybersicherheit – und damit einer Steigerung der Innovationsaktivitäten deutscher Unternehmen – stehen allerdings eine Reihe von Hemmnissen entgegen“, so Prof. Christoph Böhringer von der Universität Oldenburg und Mitglied der EFI. Individuelle Akteure investieren zu wenig in Cybersicherheit, weil sie die positiven Auswirkungen ihres Schutzes für andere nicht berücksichtigen. Nutzerinnen und Nutzer von IT-Produkten wie Hard- oder Software haben nur begrenzt Einsicht in das Sicherheitsniveau, das von Anbietern bereitgestellt wird. Unternehmen fällt es oftmals schwer, das Risiko eines Cyberangriffs zu quantifizieren und daraus folgende potenzielle Schäden abzuschätzen. Ein starkes Hemmnis für mehr Cybersicherheit ist zurzeit der Mangel an Cybersicherheitskompetenz: „Aktuell sind Unternehmen sowie der Staat bestrebt, Cybersicherheitsfachleute einzustellen. Allerdings“, mahnt Prof. Bertschek „bleiben entsprechende Stellen für einen langen Zeitraum unbesetzt, weil genau diese Fachleute fehlen“, was insbesondere kleineren Unternehmen zu schaffen macht.

Ausgehend von ihrer Analyse empfiehlt die Expertenkommission der Bundesregierung ein Bündel von Maßnahmen:

Bedarf an Fachkräften und Kompetenzen decken

- Die Vermittlung von Cybersicherheitskenntnissen in der beruflichen Aus- und Weiterbildung sowie an Hochschulen – mit der Schaffung von Studiengängen zur Ausbildung von Cyber-Expertinnen und -Experten – ist weiter voranzutreiben.

Sicherheit digitaler Infrastrukturen gewährleisten

- Die Zulassung von Komponenten digitaler Infrastrukturen sollte auf Basis von Kriterien erfolgen, die im gesamten europäischen Binnenmarkt gelten. Diese Kriterien sollten technische und nicht-technische Aspekte berücksichtigen und für Anbieter aus EU- und Nicht-EU-Ländern gleichermaßen gelten.

- Die Bundesregierung sollte multilaterale Initiativen wie die Datencloud GAIA-X forcieren, um so Impulse für sichere digitale Infrastrukturen auf nationaler und EU-Ebene zu geben.

Neue Cyberagentur zügig starten

- Die von der Bundesregierung geschaffene Agentur für Innovation in der Cybersicherheit sollte 2020 den Geschäftsbetrieb zügig aufnehmen.

Informationslage zu Cyberbedrohungen verbessern

- Es ist wichtig – insbesondere für kleine und mittlere Unternehmen (KMU) – Informations- und Beratungsangebote zur Verfügung zu stellen. Bestehende Programme zur Förderung von Cybersicherheit in KMU sollten auf ihre Wirksamkeit überprüft und an die sich ständig verändernde Bedrohungslage angepasst werden.
- Initiativen zur Entwicklung von Mindeststandards und Zertifizierungen bei der Cybersicherheit – insbesondere auf europäischer Ebene – sollten unterstützt werden. Es ist zu prüfen, ob die bestehenden Meldepflichten zu Cyberangriffen ausgeweitet werden sollen.

Für Presseanfragen:

Dr. Helge Dauchert (Leiter der EFI-Geschäftsstelle)

E-Mail: helge.dauchert@e-fi.de +++ Tel: 030 / 322 982 562 +++ www.e-fi.de