Bitkom e.V. |

BDI, Bitkom und DIHK zur Fortführung der Nationalen Cyber-Sicherheitsstrategie: Cyber-Sicherheitskompetenzen in Staat und Unternehmen deutlich stärken

- **Umfrage zur Cyber-Sicherheitsstrategie offenbart Umsetzungsmängel**

Berlin, 22. September 2020 - Eine wirkungsvolle Nationale Cyber-Sicherheitsstrategie ist für die deutsche Wirtschaft von enormer Bedeutung – insbesondere vor dem Hintergrund der verstärkten Nutzung digitaler Technologien im Zuge der Corona-Pandemie. Das betonen die Verbände BDI, Bitkom und DIHK anlässlich der heutigen Sitzung des Cyber-Sicherheitsrats. Daher unterstützen BDI, Bitkom und DIHK ausdrücklich die Fortschreibung der Cyber-Sicherheitsstrategie der Bundesregierung.

Allerdings sehen Unternehmen in Deutschland die aktuell geltenden strategischen Ziele und Maßnahmen zur Verbesserung der Cyber-Sicherheit nicht als erfüllt an. Das ist das Ergebnis einer Umfrage der drei Verbände zur Weiterentwicklung der Cyber-Sicherheitsstrategie, die die Verbände dem Nationalen Cyber-Sicherheitsrat vorgestellt haben.

Nach Ansicht der Mehrheit der befragten 181 Unternehmen hat die Bundesregierung die bisherige Nationale Cyber-Sicherheitsstrategie nicht hinreichend umgesetzt. Es mangele noch immer an dem angestrebten vertrauensvollen Informationsaustausch zwischen Staat und Wirtschaft. Mehr als jedem zweiten Unternehmen fehlt zudem eine ausreichende Unterstützung durch die Wirtschaftspolitik. Auch den Schutz von Unternehmen vor Cyber-Kriminalität bewertet nur knapp die Hälfte der Unternehmen als zufriedenstellend.

Die Fortführung der Nationalen Cyber-Sicherheitsstrategie muss nach Ansicht der befragten Unternehmen folgende fünf Top-Prioritäten enthalten:

1. Digitale Souveränität – die Wahrung eigener Gestaltungs- und Innovationsspielräume im internationalen Zusammenhang – stärken.
2. Alle Unternehmen – vor allem kleine und mittelständische – dabei unterstützen, ihre Cyber-Sicherheit zu stärken.
3. Sicherheitsbehörden mit Cyber-Kompetenzen ausstatten.
4. Überschaubare Cyber-Sicherheitsarchitektur mit klaren Zuständigkeiten der Sicherheitsbehörden schaffen.
5. IT-Sicherheit als Teil des lebenslangen Lernens etablieren.

Iris Plöger, Mitglied der Hauptgeschäftsführung des BDI: „Deutsche Unternehmen erleiden jedes Jahr Milliardenschäden durch digitale Industriespionage. Die Bundesregierung muss in ihrer Cyber-Sicherheitsstrategie den Schwerpunkt auf europäische Lösungen im Kampf gegen Cyberkriminelle legen. Cyberkriminalität macht keinen Halt an nationalen Grenzen. Die Strafverfolgungsbehörden der EU-Mitgliedstaaten müssen Hand in Hand arbeiten. Nur wenn Europa das Know-how der deutschen Wirtschaft auch digital schützt, wahrt es seine digitale Souveränität langfristig.“

Unternehmen, Behörden und Staat trügen gemeinsam Verantwortung, um Cyber-Angriffe wirksam zu unterbinden, betont **Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung**:

„Die Anzahl und auch die Qualität von Cyber-Attacken nehmen mit jedem Jahr zu. Umso mehr gilt es, Politik, Wirtschaft und Gesellschaft besser vor digitalen Angriffen zu schützen. Die Cyber-Sicherheitsstrategie der Bundesregierung schafft die Voraussetzung dafür. Entscheidend ist aber, dass die Strategie künftig mit konkreten Maßnahmen umgesetzt wird. Erstes Ziel muss sein, mehr IT-Sicherheitsfachkräfte in der Breite aus- und fortzubilden. Zweitens müssen Sicherheitsbehörden besser ausgestattet werden – mit Ressourcen statt mit immer neuen Befugnissen. Drittens sollte der

Austausch zwischen Behörden und Wirtschaft noch enger werden, wenn es um drohende Gefahren aus der Cyber-Welt geht.“

Ilja Nothnagel, Mitglied der Hauptgeschäftsführung des Deutschen Industrie- und Handelskammertags e.V. (DIHK e.V.), fordert ein besonderes Augenmerk auf die praktische Umsetzbarkeit der Cyber-Sicherheitsstrategie – vor allem für kleine und mittelständische Unternehmen: „Deutsche Unternehmen brauchen ein konkretes, umsetzbares Gesamtkonzept zur Daten- und Informationssicherheit. Dabei müssen insbesondere auch die kleinen und mittleren Unternehmen im Blick gehalten werden. Zum einen benötigen die Unternehmen zielgerichtete Unterstützungsangebote, zum anderen sind sie auf sichere Vorprodukte angewiesen, z. B. verschlüsselte Ende-zu-Ende-Kommunikation bei Maschinendaten. Im Schadensfall benötigen die Unternehmen die Unterstützung durch die Sicherheitsbehörden. Der Erfolg der Cyber-Sicherheitsstrategie muss anhand eines konkreten Umsetzungsplans messbar gemacht werden.“

Zur Umsetzung der fünf Prioritäten sind aus Sicht der drei Verbände eine bessere Kooperation der Akteure, aber auch praktische Hilfen für Unternehmen erforderlich. Konkret können vor allem folgende Maßnahmen helfen:

1. Einführung einer zentralen Telefonnummer für Hilfe bei Cyber-Angriffen und Angebot konkreter Handreichungen für Unternehmen in Fällen von Cyber-Kriminalität.
2. Intensivierung der Kooperation von Staat und Wirtschaft in den bestehenden Cyber-Sicherheitsinitiativen.
3. Verbesserung der grenzüberschreitenden Verfolgung und Bekämpfung von organisierter Cyber-Kriminalität.

Die vollständige Umfrage finden Sie im Anhang und unter diesem Link:

https://www.dihk.de/de/aktuelles-und-presse/presseinformationen/cyber-sicherheitskompetenzen-in-staat-und-unternehmen-deutlich-staerken--30466

Kontakt

Andreas Streim
Pressesprecher
Telefon: +49 30 27576-112
E-Mail: a.streim@bitkom.org
Download Pressefoto

Felix Kuhlenkamp
Leiter Sicherheit
Download Pressefoto
Nachricht senden

Link zur Presseinformation auf der Webseite:
https://www.bitkom.org/Presse/Presseinformation/BDI-Bitkom-und-DIHK-zur-Fortfuehrung-der-Nationalen-Cyber-Sicherheitsstrategie