Bitkom e.V. | Presseinformation zur Pressekonferenz

Mehrheit der Deutschen hat Angst vor Cyberangriffen – und einem Cyberkrieg

- **7 von 10 sehen große Gefahr durch Cybercrime für Deutschland, 6 von 10 fürchten einen Cyberkrieg**
- **Als größte Cyberbedrohung gelten Russland und China – aber ein Drittel sieht auch die USA als Gefahr**
- **Bitkom legt Cyber-Bilanz der Nationalen Sicherheitsstrategie anlässlich der Munich Cyber Security Conference vor**

Berlin, 13. Februar 2025 – In Deutschland greift die Angst vor Cyberangriffen und sogar einem Cyberkrieg um sich. Zugleich gelten Behörden und Verwaltung als schlecht vorbereitet auf diese Bedrohungen. 70 Prozent der Menschen in Deutschland schätzen die Gefahr durch Cybercrime insgesamt als hoch ein und ebenso viele halten Deutschland für schlecht vorbereitet. 61 Prozent haben Angst vor einem Cyberkrieg und für rund zwei Drittel (64 Prozent) ist Deutschland dafür nicht gut gewappnet. Das sind Ergebnisse einer Studie im Auftrag des Digitalverbands Bitkom, für die 1.115 Personen ab 16 Jahren in Deutschland telefonisch befragt wurden. Zugleich sind von 30 Cybersicherheitsvorhaben in der Nationalen Sicherheitsstrategie bislang gerade einmal 2 umgesetzt worden, wie aus einer Bitkom-Analyse hervorgeht, die heute ebenfalls anlässlich der Munich Cyber Security Conference (MCSC) vorgestellt wurde. Die MCSC findet am 13. und 14. Februar im Vorfeld der Münchener Sicherheitskonferenz statt. „Deutschland wird täglich digital angegriffen. Die Grenzen zwischen Cybercrime und hybrider Kriegsführung, zwischen privaten und staatlichen Akteuren sind inzwischen fließend“, sagt Bitkom-Präsident Dr. Ralf Wintergerst. „Die Bedrohungslage wird sich verschärfen, wir müssen deshalb unsere nationale Sicherheit sowohl klassisch als auch im digitalen Raum stärken – in Behörden und der Verwaltung, aber auch in kritischer Infrastruktur und in den Unternehmen.“

Cybercrime: Sorge vor ausländischen Geheimdiensten und organisierter Kriminalität

Während die Bedrohung für sich selbst und die eigene Familie nur von 37 Prozent der Menschen in Deutschland als sehr hoch (11 Prozent) oder eher hoch (26 Prozent) eingeschätzt wird, gilt die Bedrohungslage für Deutschland allgemein 70 Prozent als sehr hoch (33 Prozent) oder eher hoch (37 Prozent). Gefahren für die Cybersicherheit gehen dabei vor allem von ausländischen Geheimdiensten (78 Prozent) sowie der Organisierten Kriminalität (67 Prozent) aus, gefolgt von politischen oder religiösen Extremisten (59 Prozent) sowie einzeln handelnden Kriminellen (41 Prozent) und Einzelpersonen ohne kriminelle oder politische Absichten (32 Prozent) – so die Meinung der Deutschen.

Aus Sicht der Bevölkerung kommt die größte Cyberbedrohung aus Russland (98 Prozent) sowie China (84 Prozent). Dahinter folgt mit deutlichem Abstand Nordkorea (44 Prozent). Ein Drittel (32 Prozent) sieht die USA als große Bedrohung für die Cybersicherheit in Deutschland an – noch vor dem Iran (29 Prozent), Belarus (17 Prozent) sowie osteuropäischen Staaten außerhalb der EU (14 Prozent). „Die USA waren und sind für Deutschland und Europa ein wichtiger Partner. Die Einschätzung der Menschen zeigt aber, dass die Grenzen zwischen Freund und Feind nicht mehr so klar sind, wie noch vor 10 oder 20 Jahren“, sagt Wintergerst. „Wichtig ist, dass wir das Ziel echter digitaler Souveränität in Deutschland und Europa mit Nachdruck und Erfolg verfolgen.“

Nur ein Viertel glaubt, dass Behörden gut vorbereitet sind

Im Angesicht der wachsenden Bedrohungen gilt Deutschland als schlecht vorbereitet auf Cyberangriffe. Nur 23 Prozent meinen, dass die öffentliche Verwaltung und Institutionen wie Polizei oder Bundeswehr sehr gut oder eher gut vorbereitet sind. Umgekehrt sehen sie 29 Prozent als eher

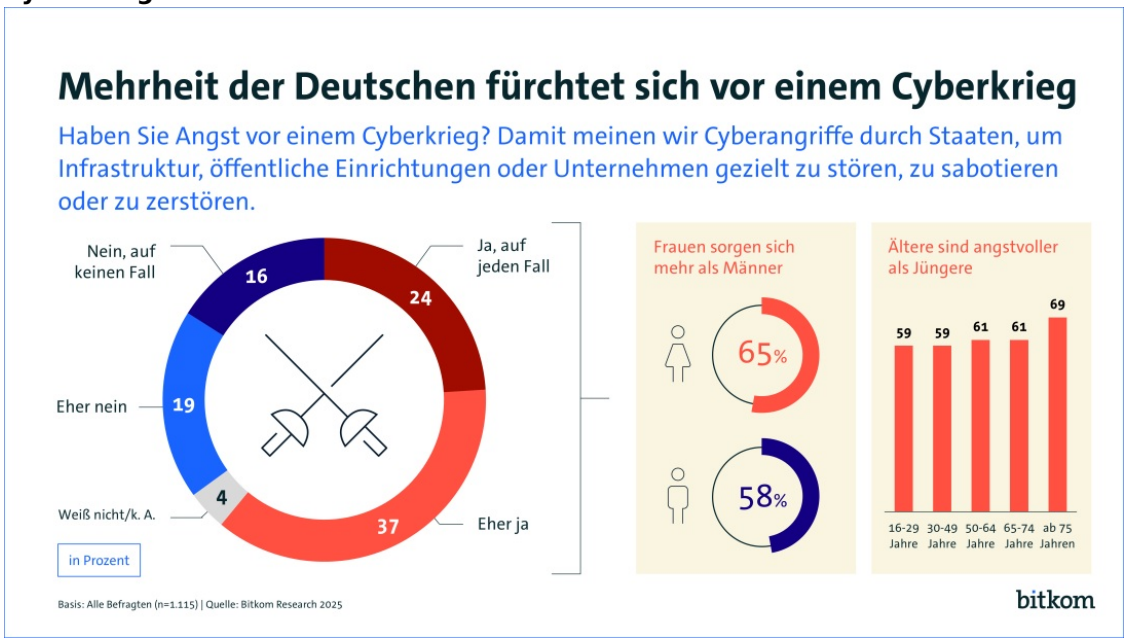
nicht gut und 41 Prozent sogar als gar nicht gut vorbereitet. Zugleich geht es nach Ansicht der Bevölkerung um mehr als nur die Anfälligkeit für Datendiebstahl oder Erpressung mit Ransomware. 71 Prozent sagen, dass Kriege in Zukunft überwiegend auch mit digitalen Mitteln geführt werden. 63 Prozent denken, dass Cyberangriffe auf kritische Infrastrukturen für Deutschland eine größere Bedrohung darstellen als konventionelle militärische Angriffe. Zwei Drittel (66 Prozent) sind entsprechend der Meinung, dass Cyberangriffe genauso behandelt werden müssten wie militärische Angriffe. Wintergerst: „Wer im Cyberraum angreifbar ist, wird sich auch in der physischen Welt nicht erfolgreich verteidigen können. Landesverteidigung bedeutet heute nicht mehr nur Investitionen in Panzer und Flugabwehr, sondern den gezielten Einsatz digitaler Technologien und digitalen Know-hows."

Zwei Drittel sind von Anschlägen auf Untersee-Kabel beunruhigt

Ein aktuelles Beispiel für beunruhigende Angriffe auf kritische digitale Infrastrukturen sind mehrere Anschläge auf Untersee-Kabel, die zentral für die Internetversorgung sind. Fast zwei Drittel (63 Prozent) der Deutschen macht es Angst, dass der internationale Datenverkehr so leicht zu sabotieren ist. 80 Prozent sind daher dafür, mehr Kabel zu verlegen, um unabhängiger von einzelnen Unterbrechungen zu werden. Spezielle Einheiten zur schnellstmöglichen Behebung der Schäden (77 Prozent) und zur Ermittlung der Täter (68 Prozent) werden ebenfalls von einer deutlichen Mehrheit gefordert. 7 von 10 (69 Prozent) sagen, Anschläge auf Untersee-Kabel sollten wie militärische Angriffe bewertet werden. Und 6 von 10 (60 Prozent) plädieren für einen besseren Schutz der Kabel, etwa durch eine lückenlose Satellitenüberwachung. „Die vermutliche Sabotage von Untersee-Kabeln zeigt auch die physische Bedrohung unserer kritischen Infrastruktur durch nicht staatliche und nicht militärische Akteure", so Wintergerst.

63 Prozent der Deutschen erwarten, dass sich private Akteure durch Cyberangriffe verstärkt in Krisen einmischen werden. Und ebenfalls 63 Prozent befürchten, dass uns auch befreundete Staaten mit digitalen Mitteln Schaden zufügen werden, um die eigene Wirtschaft zu stärken.

Cyberkrieg: Deutschland soll sich besser vorbereiten



Weit verbreitet ist die Angst vor einem Cyberkrieg. 61 Prozent haben aktuell Angst vor einem solchen Szenario. Jüngere (59 Prozent bei den 16- bis 29-Jährigen sowie den 30- bis 49-Jährigen) sind dabei etwas weniger besorgt als die Älteren (69 Prozent bei den ab-75-Jährigen), Frauen haben mit 65 Prozent etwas mehr Sorge als Männer (58 Prozent). Vor allem jenen Staaten, die als Cyberbedrohung gelten, werden gute technische Fähigkeiten für eine solche Auseinandersetzung zugesprochen. Ganz oben stehen Russland (76 Prozent), die USA (75 Prozent) und China (74 Prozent). Nordkorea ist für 52 Prozent gut gerüstet, der Iran für 46 Prozent. Deutschland nennen 61 Prozent, Israel 52 Prozent, Frankreich 46 Prozent, am Ende liegen Großbritannien (42 Prozent) und die Ukraine (41 Prozent). „Europa muss eigene Fähigkeiten für den Fall eines Cyberkriegs aufbauen", so Wintergerst.

Denn obwohl Deutschland nach Meinung einer deutlichen Mehrheit über die technischen Fähigkeiten für einen Cyberkrieg verfügt, gilt die Bundesrepublik im Cyberraum aktuell in der Praxis nur als bedingt abwehrbereit. Zwei Drittel (64 Prozent) halten Deutschland für sehr schlecht (26 Prozent) oder eher schlecht (38 Prozent) vorbereitet, nur 24 Prozent für gut und gerade einmal 4 Prozent für sehr gut. Gefragt nach nötigen Maßnahmen fordern 75 Prozent die Gründung eines digitalen Katastrophenschutzes, 73 Prozent Investitionen in die Cybersicherheit kritischer Infrastrukturen und 71 Prozent die Schaffung eigener Fähigkeiten für Cyberangriffe. Dahinter folgen Cyber-Bündnisse mit anderen Staaten wie eine Cyber-Nato (68 Prozent), Investitionen in Cyber-Abwehreinheiten (64 Prozent), Notfallschulungen für die Bevölkerung (56 Prozent) sowie Wirtschaftssanktionen zur Abschreckung (43 Prozent). Nur 2 Prozent meinen, Deutschland solle sich nicht zusätzlich auf einen Cyberkrieg vorbereiten.

Umsetzung der Nationalen Sicherheitsstrategie stockt

Allerdings stockt die Umsetzung von Cybersicherheitsvorhaben, die sich die Bundesregierung in der Nationalen Sicherheitsstrategie vorgenommen hat. Dort sind 30 Einzelmaßnahmen angekündigt. Nach einer Bitkom-Auswertung sind allerdings gerade einmal 2 dieser 30 Maßnahmen abgeschlossen, 19 sind in der Umsetzung und 9 wurden nicht einmal begonnen. Wintergerst: „Ambitionierte Strategien und Agenden nützen nichts, wenn es beim beschriebenen Papier bleibt. Die nächste Bundesregierung muss die nötigen Maßnahmen ohne weitere Verzögerung umsetzen.“

Umgesetzt sind Prüfmöglichkeiten für systemkritische Komponenten in Kommunikationsnetzen, auch die Cyberagentur hat wie geplant ihre Arbeit aufgenommen und vergibt gezielt Forschungsaufträge. Zumindest in Umsetzung sind Maßnahmen zur Digitalisierung und Einführung digitaler Technologien, allerdings wurden die Mittel zuletzt gekürzt. Der geplante Ausbau des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu einer Zentralstelle der Cybersicherheit fand keine parlamentarische Mehrheit und wurde auf die nächste Legislatur verschoben. Auch die angekündigte verstärkte Zusammenarbeit mit der Wirtschaft ist nicht in Fahrt gekommen und leidet an Unterfinanzierung. Völlig verfehlt wurden die Ziele, Investitionen für die Cybersicherheit kritischer Infrastruktur zu erhöhen oder belastbare Abstimmungs- und Entscheidungsprozesse für den Cyber-Krisenfall zu etablieren. Auch die versprochene neue Cybersicherheitsstrategie wurde nicht vorgelegt. „Die Erhöhung der Cybersicherheit muss eine zentrale Aufgabe der Sicherheits- und Verteidigungspolitik der künftigen Bundesregierung sein. Wir brauchen nicht nur ambitionierte Ziele, wir brauchen vor allem Fortschritt in der Umsetzung“, sagt Wintergerst.

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

Hinweis zur Methodik

Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.115 Personen ab 16 Jahren in Deutschland telefonisch befragt. Die Befragung fand im Zeitraum von KW 49 2024 bis KW 2 2025 statt. Die Umfrage ist repräsentativ.

Direktlink: ***https://www.bitkom.org/Presse/Presseinformation/Mehrheit-Angst-Cyberangriffen-Cyberkrieg***