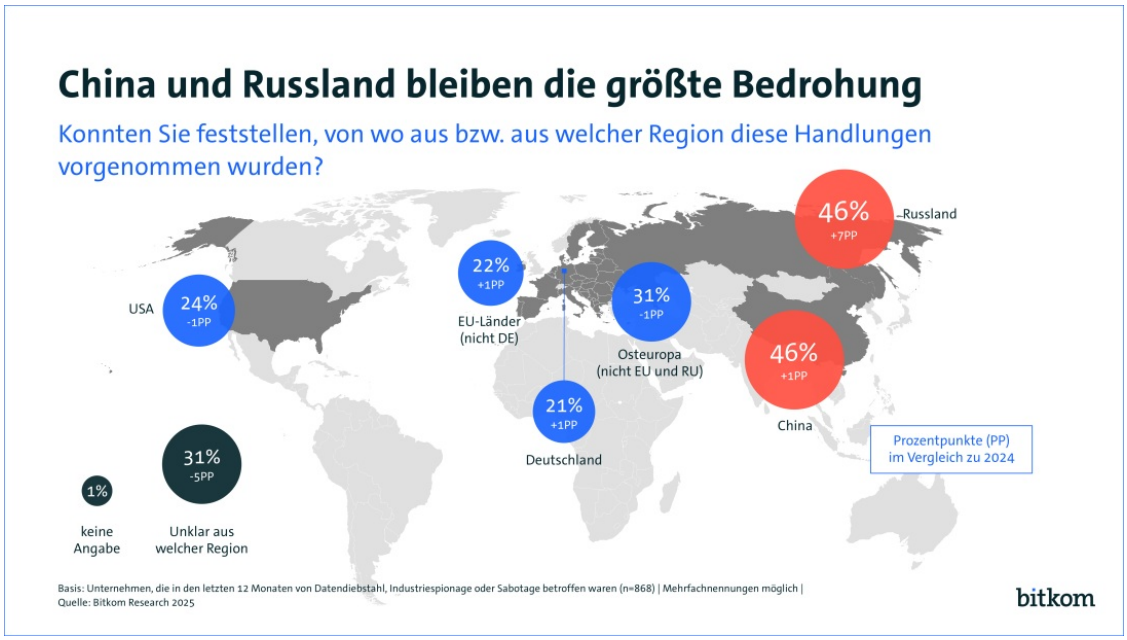
Bitkom e.V. | Presseinformation zur Pressekonferenz

Russland und China nehmen deutsche Wirtschaft ins Visier

- **Schaden durch Datendiebstahl, Industriespionage und Sabotage steigt auf 289 Milliarden Euro**
- **Die Spur führt öfter nach Osten – und zu ausländischen Geheimdiensten**
- **Cyberattacken: Knapp drei von vier Unternehmen registrieren Zunahme von Angriffen**
- **Jedes dritte Unternehmen hat nach Ransomware-Attacken Lösegeld gezahlt**

Berlin, 18. September 2025 – Angriffe auf die deutsche Wirtschaft haben in den vergangenen zwölf Monaten weiter zugenommen – und immer öfter führt die Spur nach Russland und China. Knapp 9 von 10 Unternehmen (87 Prozent) berichten von Diebstahl von Daten und IT-Geräten, digitaler und analoger Industriespionage oder Sabotage, vor einem Jahr lag der Anteil noch bei 81 Prozent. Wie bereits im Vorjahr vermuten weitere 10 Prozent Angriffe. Der Schaden durch diese analogen und digitalen Angriffe ist im Vergleich zum Vorjahr um rund 8 Prozent auf 289,2 Milliarden Euro gestiegen. Darin enthalten sind direkte Kosten etwa für Betriebsausfälle, Ersatzmaßnahmen, Erpressungen oder Rechtsstreitigkeiten, aber auch Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen oder durch Plagiate. Das sind Ergebnisse einer Studie im Auftrag des Digitalverbands Bitkom, für die mehr als 1.000 Unternehmen quer durch alle Branchen repräsentativ befragt wurden.



Erneut zugenommen haben Taten, die nach Russland und China zurückverfolgt werden konnten. Von den betroffenen Unternehmen haben 46 Prozent mindestens einen Angriff aus Russland (2024: 39 Prozent) festgestellt, ebenso viele aus China (2024: 45 Prozent). Mit deutlichem Abstand folgen Attacken aus Osteuropa außerhalb der EU (31 Prozent, 2024: 32 Prozent), aus den USA (24 Prozent, 2024: 25 Prozent), aus EU-Ländern (22 Prozent, 2024: 21 Prozent) sowie Deutschland (21 Prozent, 2024: 20 Prozent). Rund jedes dritte Unternehmen (31 Prozent, 2024: 36 Prozent) konnte die Angriffe keinem Herkunftsland zuordnen. Dabei nehmen ausländische Geheimdienste die deutsche Wirtschaft verstärkt ins Visier. 28 Prozent der betroffenen Unternehmen konnten mindestens einen Angriff einem ausländischen Nachrichtendienst zuordnen, vor einem Jahr waren es erst 20 Prozent, 2023 sogar nur 7 Prozent. Am häufigsten kamen die Täter jedoch aus der organisierten Kriminalität (68 Prozent, 2024: 70 Prozent). Wintergerst: „Der Anteil jener Unternehmen, die Täter oder Herkunftsland mit Hilfe von Informationen von Behörden ermitteln konnten, ist deutlich gestiegen.

Die Zusammenarbeit zwischen Unternehmen und Behörden funktioniert immer besser.“ 35 Prozent der angegriffenen Unternehmen, die Täter ermittelt haben, konnten die Behörden bei der Spurensuche helfen, 2024 waren es erst 24 Prozent. Damit ist dieser Austausch mit staatlichen Stellen inzwischen wirksamer als interne (32 Prozent) oder externe (20 Prozent) Untersuchungen.

„Ein umfassender Schutz muss essenzieller Bestandteil der Digitalisierung von Unternehmen sein. Die Frage ist nicht, ob Unternehmen angegriffen werden, sondern wann – und ob sie diese Angriffe erfolgreich abwehren können“, sagt **Bitkom-Präsident Dr. Ralf Wintergerst**. „Unsere Verteidigungsfähigkeit muss zudem in den Fokus der Politik rücken – auch im Cyberraum. Hybride Kriegsführung durch fremde Staaten ist keine theoretische Gefahr, sie findet heute jeden Tag hundertfach in Deutschland statt.“

Der **Vizepräsident des Bundesamts für Verfassungsschutz, Sinan Selen**, sagt bei der Vorstellung der Studie: „Die Bitkom-Studie zeigt erneut, dass die Schwerpunktsetzung des BfV als Abwehrdienst in Bezug auf die Detektion und Verhinderung von Übergriffen verschiedener staatlicher und staatsnaher Akteure richtig und notwendig ist. Wir werden diese Priorisierung weiter fortsetzen und unsere Aufgabenwahrnehmung ausbauen. Zahlen und Trends der aktuellen Studie decken sich mit unseren Erkenntnissen. Deutschland ist seit Jahren, mit steigender Intensität, im Zielspektrum russischer Akteure. Diese hybriden Aktivitäten erfordern eine Doppelbotschaft: Deutschland steht im Fokus von Cyberangriffen staatlicher und nichtstaatlicher Akteure und wir stärken unsere Abwehrbereitschaft und Handlungsfähigkeit kontinuierlich und konsequent.

Inzwischen erhalten mehr als 35 Prozent der Unternehmen Hinweise auf die jeweiligen Angreifer durch Behörden – das ist Ergebnis einer verstärkten Zusammenarbeit der Sicherheitsbehörden mit den Unternehmen verschiedener Branchen. Neben der zunehmenden Bedrohung der Wirtschaft durch Cyberangriffe sehen wir aber auch Angriffe auf Politik, Verwaltung, Wissenschaft und die Zivilgesellschaft. Die Grenzen zwischen Cyberspionage und Cybercrime verschwimmen zunehmend, ein Trend, der sich verstetigt. Wir sehen, dass staatliche Akteure kriminelle Aktivitäten privater Gruppierungen dulden oder aktiv einsetzen. Deshalb kommt es entscheidend darauf an, dass wir als Cyber- und Spionageabwehr die enge und gute Zusammenarbeit der nationalen und internationalen Sicherheitsbehörden weiter ausbauen, gleichzeitig aber auch die deutschen Wirtschaftsunternehmen enger und intensiver einbinden. Wirtschaftsschutz ist eine eindeutige Priorität des BfV.

Unsere zentrale Aufgabe als Abwehrdienst ist es, illegitime Operationen frühzeitig zu detektieren, Schadensausmaß und Hintergründe einzuordnen und im Verbund der Sicherheitsbehörden Angriffe effektiv zu unterbinden. Das BfV baut angesichts der verstetigten Bedrohungslage seine Rolle als Abwehrdienst in personeller und technischer und operativer Hinsicht umfassend aus. Dies gilt insbesondere im Bereich der Fähigkeiten im digitalen Raum, die derzeit eine Neuaufstellung erfahren.“

Knapp drei Viertel der Unternehmen sehen eine große Bedrohung

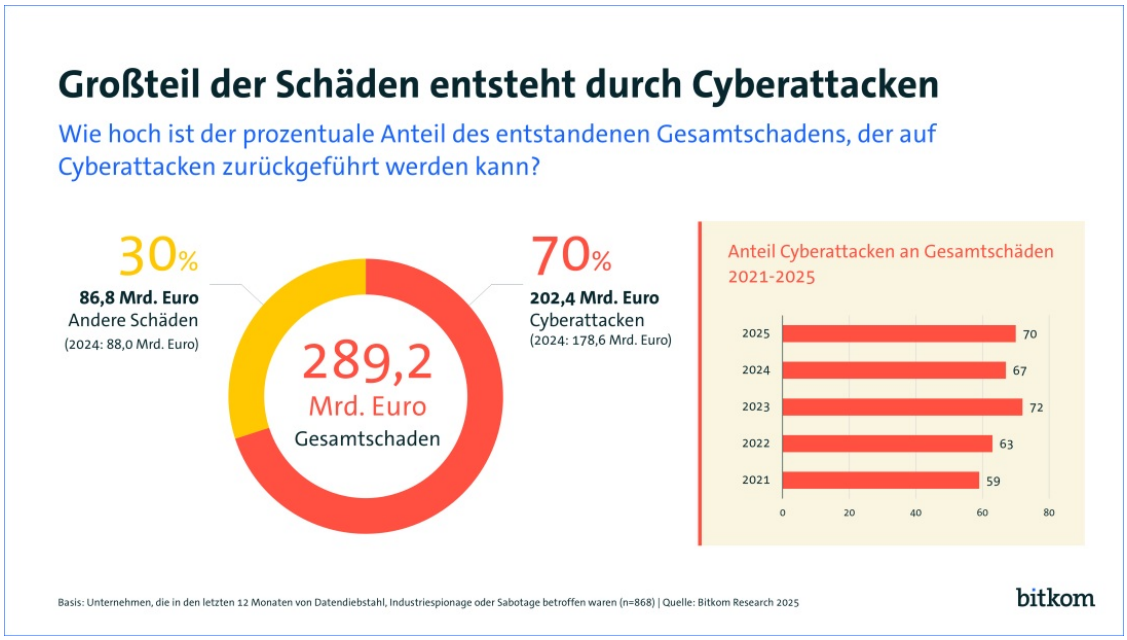
89 Prozent der Unternehmen sehen sich durch Diebstahl, Sabotage und Industriespionage bedroht: 72 Prozent sprechen von einer großen Bedrohung, weitere 17 Prozent von einer eher geringen Bedrohung. Nur 10 Prozent fühlen sich sehr gering oder gar nicht bedroht. Dabei wird die deutsche Wirtschaft weiterhin auch in klassisch analoger Form angegriffen. So wurden 54 Prozent der Unternehmen Opfer von Diebstahl von IT- oder Telekommunikationsgeräten oder vermuten das, bei 41 Prozent wurden sicher oder vermutlich physische Dokumente entwendet wie Akten oder Muster und Bauteile. Bei 32 Prozent wurden Besprechungen vor Ort abgehört oder sie vermuten dies, bei 22 Prozent kam es gesichert oder vermutet zu physischer Sabotage von Produktionssystemen oder Betriebsabläufen. „Digitaler und physischer Schutz müssen zusammengedacht und implementiert werden“, so Wintergerst.

Die meisten Angriffe auf Unternehmen erfolgen aber inzwischen digital. 73 Prozent aller deutschen Unternehmen waren von digitaler Sabotage betroffen oder vermutlich betroffen. Bei 62 Prozent wurde digitale Kommunikation wie E-Mails oder Videokonferenzen sicher oder vermutlich ausgespäht. Zwei Drittel (66 Prozent) wurden Geschäftsdaten gestohlen oder sie vermuten das. Den davon betroffenen Unternehmen entwendeten die Täter vor allem Kommunikationsdaten (69 Prozent), Kundendaten (57 Prozent) sowie Finanzdaten (39 Prozent). Geistiges Eigentum wie Patente oder Informationen aus Forschung und Entwicklung flossen bei 29 Prozent der betroffenen Unternehmen ab, gefolgt von Zugangsdaten und Passwörtern (27 Prozent) sowie Daten von

Beschäftigten (24 Prozent).

Cyberangriffe nehmen zu, der Anteil am Gesamtschaden steigt auf 70 Prozent

Fast drei Viertel der Unternehmen (73 Prozent) haben in den vergangenen zwölf Monaten eine Zunahme von Cyberangriffen registriert, ein weiteres Viertel (26 Prozent) sieht die Anzahl der Cyberattacken unverändert. Und dieser Trend dürfte sich fortsetzen: Rund ein Drittel (35 Prozent) geht davon aus, dass Cyberangriffe in den kommenden zwölf Monaten stark zunehmen werden. 47 Prozent rechnen damit, dass sie eher zunehmen und 18 Prozent gehen von einem gleichbleibenden Niveau aus. Kein Unternehmen glaubt an einen Rückgang von Cyberattacken.



Und während nur jedes zweite Unternehmen (50 Prozent) glaubt, auf Cyberangriffe sehr gut vorbereitet zu sein, fühlen sich 59 Prozent durch Cyberangriffe in ihrer geschäftlichen Existenz bedroht. Das sind zwar etwas weniger als 2024 mit 65 Prozent, aber deutlich mehr als in den Vorjahren mit 52 Prozent 2023, 45 Prozent 2022 und sogar nur 9 Prozent 2021. „Ein erfolgreicher Cyberangriff kann für Unternehmen das wirtschaftliche Aus bedeuten. Eine umfassende Cybersicherheit muss deshalb integraler Teil jeder Digitalstrategie sein“, sagt Wintergerst. „Es geht darum, Angriffe abzuwehren, aber auch im Fall einer erfolgreichen Attacke den Schaden möglichst klein zu halten und rasch wieder arbeitsfähig werden zu können.“

Schaden durch Cyberangriffe steigt erstmals über 200 Milliarden Euro

Der Anteil, den Cyberattacken am Gesamtschaden der deutschen Wirtschaft durch Datendiebstahl, Sabotage und Industriespionage haben, ist von 67 Prozent auf 70 Prozent gestiegen. Das entspricht einer Summe von 202,4 Milliarden Euro nach 178,6 Milliarden Euro im Vorjahr. Betroffen sind Unternehmen vor allem von Ransomware-Attacken, wobei Daten verschlüsselt und nur gegen Lösegeldzahlung wieder freigegeben werden. 34 Prozent der Unternehmen waren davon betroffen, das sind fast dreimal so viele wie noch 2022 mit 12 Prozent. Etwa jedes siebte betroffene Unternehmen (15 Prozent) hat bei Ransomware-Angriffen bereits Lösegeld bezahlt, weitere 15 Prozent wollten oder konnten dazu keine Angabe machen. 19 Prozent der Unternehmen, die auf die Forderung der Ransomware-Erpresser eingegangen sind, haben zwischen 10.000 und 100.000 Euro bezahlt, 34 Prozent zwischen 100.000 und 500.000 Euro und 12 Prozent zwischen 500.000 Euro und 1 Million Euro. 4 Prozent haben sogar mehr als 1 Million Euro gezahlt. 31 Prozent wollten oder konnten zu den Summen keine Angabe machen. „Wer bei Ransomware Lösegeld bezahlt, finanziert Cyberkriminelle und legt den Grundstein für den nächsten erfolgreichen Angriff – häufig sogar erneut auf das eigene Unternehmen“, so Wintergerst.

Ein Viertel (25 Prozent) hat Schaden durch Distributed Denial of Service (DDoS)-Angriffe erlitten, bei denen zum Beispiel Webserver von Unternehmen lahmgelegt werden. 24 Prozent wurden mit anderer Schadsoftware infiziert, 22 Prozent waren von Phishing-Angriffen und 21 Prozent von Angriffen auf Passwörter betroffen.

Bislang noch sehr selten entsteht Schaden durch neuere Angriffsmethoden wie Deepfakes (4 Prozent) und Robo Calls (3 Prozent), bei denen KI genutzt wird, um Opfern eine falsche Identität des Angreifers vorzugaukeln. Allerdings berichten 23 Prozent der Unternehmen von Angriffen durch Robo Calls und 11 Prozent von Deepfake-Attacken, bei denen kein Schaden entstanden ist. Zwei Drittel (66 Prozent) aller Unternehmen haben den Eindruck, dass bei Angriffen verstärkt Künstliche Intelligenz eingesetzt wird. „Wer Verantwortung für die IT-Sicherheit von Unternehmen trägt, muss sich mit KI auseinandersetzen. Künstliche Intelligenz erlaubt völlig neue Angriffsmethoden, etwa mit Deepfakes, verbessert aber auch klassische Angriffe, zum Beispiel durch viel glaubwürdigere Phishing-Mails“, so Wintergerst. „Wichtig ist, die Beschäftigten hierfür zu schulen und zu sensibilisieren.“

Unternehmen investieren verstärkt in Cybersicherheit

Weiter leicht gestiegen ist der Anteil der IT-Sicherheit am IT-Budget der Unternehmen – von 17 Prozent auf nun 18 Prozent. 2022 waren es gerade einmal 9 Prozent. 4 von 10 Unternehmen (41 Prozent) investieren dabei sogar 20 Prozent oder mehr ihres IT-Budgets in IT-Sicherheit, weitere 43 Prozent zwischen 10 und 20 Prozent. Nur bei 8 Prozent beträgt der Anteil zwischen 5 und 10 Prozent, bei gerade einmal 2 Prozent weniger als 5 Prozent. „Die Investitionen in IT-Sicherheit befinden sich auf dem richtigen Weg. Allerdings wendet mehr als die Hälfte der Unternehmen immer noch weniger als die von BSI und Bitkom empfohlenen 20 Prozent ihres IT-Budgets für Sicherheit auf. Bei den Sicherheitsbudgets müssen wir angesichts der Bedrohungslage noch eine Schippe drauflegen“, sagt Wintergerst.

Dabei rücken Aspekte digitaler Souveränität verstärkt in den Fokus. Zwei Drittel (67 Prozent) halten ihr Unternehmen für zu abhängig von Sicherheitslösungen aus den USA. Drei Viertel (74 Prozent) wollen, dass die Politik deutsche Anbieter von Cybersicherheitslösungen stärker unterstützt. „Cybersicherheit gehört mit ins Zentrum der Politik für ein digital souveränes Deutschland“, so 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 1.002 Unternehmen ab 10 Beschäftigten und einem Jahresumsatz von mindestens 1 Mio. Euro in Deutschland telefonisch befragt. Die Befragung fand im Zeitraum von KW 16 bis KW 24 2025 statt. Die Umfrage ist repräsentativ.

Direktlink: ***https://www.bitkom.org/Presse/Presseinformation/Russland-China-deutsche-Wirtschaft-Visier***