Bitkom e.V. | Presseinformation zur Pressekonferenz

Angriffe auf die deutsche Wirtschaft: Spur führt immer öfter zu ausländischen Geheimdiensten

- **Mehr als jedes dritte betroffene Unternehmen kann Angriff einem ausländischen Nachrichtendienst zuordnen, 2023 waren es erst 7 Prozent**
- **Mehr als 211 Milliarden Euro Schaden durch Datendiebstahl, Industriespionage und Sabotage**
- **Drei Viertel der Schäden entfallen auf Cyberattacken – dort spielt KI eine zunehmende Rolle**

Berlin, 26. August 2026 – Ausländische Geheimdienste nehmen deutsche Unternehmen immer stärker ins Visier. 37 Prozent der von Datendiebstahl, Industriespionage oder Sabotage betroffenen Unternehmen konnten in den vergangenen zwölf Monaten mindestens einen Angriff einem fremden Nachrichtendienst zuordnen, vor einem Jahr waren es noch 28 Prozent und 2023 sogar erst 7 Prozent. Insgesamt waren zuletzt 96 Prozent aller Unternehmen von Datendiebstahl, Industriespionage oder Sabotage betroffen oder vermuten es. Im Vorjahr lag der Wert mit 97 Prozent auf demselben hohen Niveau. Allerdings können immer weniger Unternehmen sicher sagen, ob ein solcher Angriff tatsächlich stattgefunden hat. Nur noch 67 Prozent der Unternehmen konnten einen erfolgreichen Angriff mit Sicherheit feststellen, vor einem Jahr waren es hingegen 87 Prozent. Gleichzeitig ist der Anteil derer, die einen Angriff vermuten, aber nicht sicher belegen können, von 10 auf 29 Prozent gestiegen. Die Schäden durch Datendiebstahl, Industriespionage oder Sabotage gingen auf 211 bis 270,8 Milliarden Euro zurück. Die Schadenssumme umfasst direkte Kosten etwa für Betriebsausfälle, Ermittlungen und Ersatzmaßnahmen, Rechtsstreitigkeiten und Erpressung ebenso wie Umsatzeinbußen durch Plagiate und den Verlust von Wettbewerbsvorteilen. Mehr als die Hälfte der sicher betroffenen Unternehmen (52 Prozent, 2025: 46 Prozent) konnten mindestens einen Angriff nach China zurückverfolgen, dahinter folgt Russland mit 49 Prozent (2025: 46 Prozent). Erst mit deutlichem Abstand folgen Osteuropa ohne die EU (34 Prozent), die USA (27 Prozent), EU-Länder (26 Prozent, ohne Deutschland) und Deutschland (12 Prozent). Neu als relevanter Player der Wirtschaftskriminalität ist der Iran. Rund jedes zehnte Unternehmen (9 Prozent) konnte Angriffe in den Iran zurückverfolgen, im Vorjahr waren es lediglich 4 Prozent. Das sind Ergebnisse einer repräsentativen Befragung von 1.003 Unternehmen ab 10 Beschäftigten in Deutschland im Auftrag des Digitalverbands Bitkom.

„Das Dunkelfeld bei Datendiebstahl, Industriespionage und Sabotage wird größer. Fast alle Unternehmen sind von Angriffen nachweislich betroffen oder vermuten es, dabei sind ausländische Nachrichtendienste deutlich häufiger die Täter. Nachrichtendienste arbeiten professioneller und verdeckter und stellen die angegriffenen Unternehmen vor neue Herausforderungen. Zugleich erhalten auch weniger professionelle Angreifer durch KI ganz neue Möglichkeiten“, sagt Bitkom-Präsident Dr. Ralf Wintergerst. „Entscheidend ist, Angriffe frühzeitig zu erkennen und abzuwehren, Beweise zu sichern und Erkenntnisse schnell mit den Sicherheitsbehörden zu teilen. Nur so lassen sich Spionage und Sabotage wirksamer begrenzen.“

Der Präsident des Bundesamts für Verfassungsschutz, Sinan Selen, sagt bei der Vorstellung der Studie: „Die Ergebnisse der Bitkom-Studie fügen sich nahtlos in das Bild der aktuell hohen Bedrohungslage ein. Sie zeigen dieses Jahr erneut, dass der Wirtschaftsstandort Deutschland im Zielspektrum von Cyberoperationen staatlicher sowie nicht-staatlicher Akteure steht. Ausländische Nachrichtendienste haben ihre hybriden Aktivitäten intensiviert und sind zunehmend für die Angriffe auf die deutsche Wirtschaft verantwortlich. Sowohl der anhaltende Angriffskrieg Russlands, als auch die voranschreitende, verschleierte Nutzung von KI bei Cyberangriffen stellen die Unternehmen vor große Herausforderungen. Dabei werden häufig ganze Branchen ins Visier genommen, sensible Daten gestohlen und Abläufe des alltäglichen Lebens gestört. Nicht zuletzt stellt die Sicherheits- und Verteidigungswirtschaft eine besonders attraktive Zielfläche ausländischer Dienste dar. Als Abwehrdienst legen wir unseren Fokus auf die Detektion, Disruption und Prävention von Angriffen auf unsere Wirtschaft.“

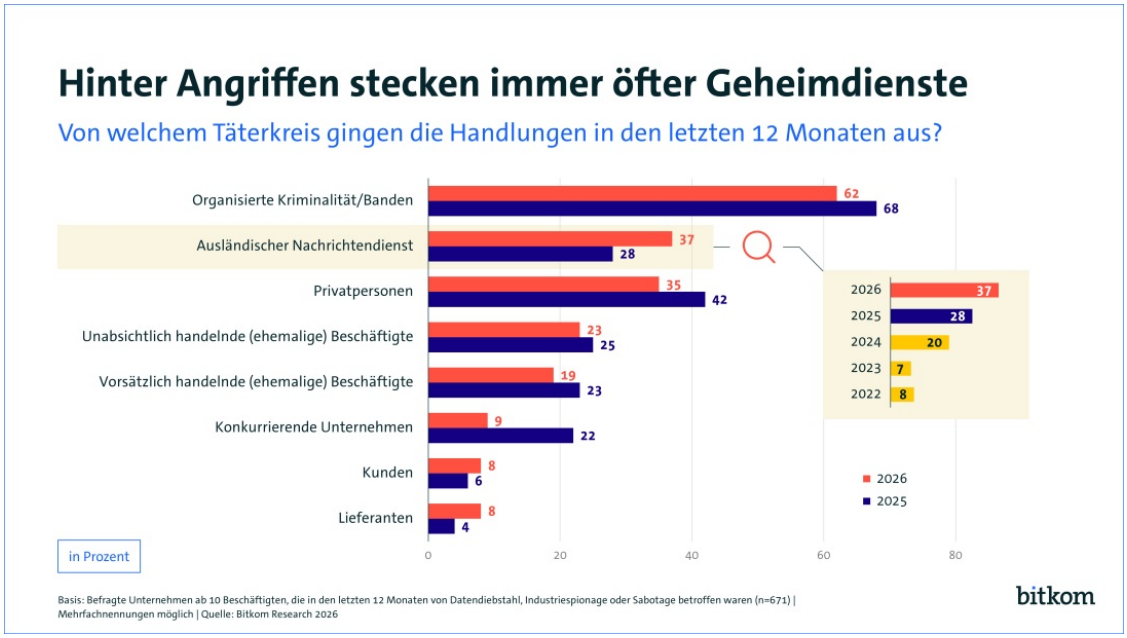
Die große Mehrheit der Unternehmen fühlt sich bedroht

Die große Mehrheit der Unternehmen sieht sich durch analoge und digitale Angriffe bedroht. 28 Prozent sehen eine sehr große Bedrohung, 45 Prozent eine eher große Bedrohung. Jeweils 13 Prozent sehen hingegen lediglich eine eher geringe bzw. eine sehr geringe oder gar keine Bedrohung.

In den vergangenen zwölf Monaten wurden viele Unternehmen sowohl klassisch als auch auf digitalem Weg angegriffen. 60 Prozent waren vom Diebstahl von IT- oder Telekommunikationsgeräten betroffen oder vermuten dies, 37 Prozent vom Diebstahl physischer Dokumente, Muster oder Bauteile, 33 Prozent vom Abhören von Besprechungen vor Ort und 23 Prozent von physischer Sabotage von Produktionssystemen oder Betriebsabläufen. Dabei sind digitale Angriffe weit verbreitet. 57 Prozent der Unternehmen waren sicher oder vermutlich von digitaler Sabotage betroffen, 54 Prozent vom Ausspähen ihrer Kommunikation, 45 Prozent vom digitalen Diebstahl von Geschäftsdaten.

Ein Angriff bleibt zudem häufig nicht auf ein Unternehmen beschränkt. Jedes fünfte Unternehmen (21 Prozent), das von Datendiebstahl, Industriespionage oder Sabotage betroffen war, gibt an, dass der Vorfall Auswirkungen auf andere Unternehmen hatte, etwa in Form von Produktionsausfällen bei Geschäftspartnern oder Reputationsschäden bei Auftraggebern. „Wer die eigenen Schutzmaßnahmen vernachlässigt, gefährdet andere. Wer sein Unternehmen schützen will, muss physische und digitale Sicherheit gemeinsam angehen und sollte auch seine Partner in die Pflicht nehmen“, sagt Wintergerst.

Organisierte Kriminalität bleibt die größte Bedrohung



Die wichtigste Tätergruppe bleibt die Organisierte Kriminalität. 62 Prozent der Unternehmen, die Opfer von Datendiebstahl, Industriespionage oder Sabotage wurden, konnten mindestens einen Angriff dorthin zurückverfolgen. Verglichen mit den 68 Prozent im Vorjahr ist das ein leichter Rückgang. Erstmals folgen direkt dahinter ausländische Nachrichtendienste mit 37 Prozent, ein deutlicher Anstieg zum Vorjahr mit 28 Prozent. „Die Grenzen zwischen Organisierter Kriminalität und den Geheimdiensten sind in vielen Ländern fließend. Nachrichtendienste bedienen sich krimineller Strukturen, umgekehrt wird Kriminellen freie Hand gelassen, solange sie ihre Ziele den politischen Vorgaben entsprechend wählen“, sagt Wintergerst. Als Tätergruppe ebenfalls relevant sind Privatpersonen mit 35 Prozent (2025: 42 Prozent) sowie unabsichtlich (23 Prozent, 2025: 25 Prozent) und vorsätzlich (19 Prozent, 2025: 23 Prozent) handelnde aktuelle oder ehemalige Beschäftigte des angegriffenen Unternehmens. Nur noch 9 Prozent der Unternehmen (2025: 22 Prozent) wurden von Wettbewerbern angegriffen, am Ende rangieren mit je 8 Prozent Kunden (2025: 6 Prozent) und Lieferanten (2025: 4 Prozent).

Engere Zusammenarbeit mit Behörden

Bei der Aufklärung hilft immer öfter der Staat: Jedes zweite Unternehmen (50 Prozent), das Täter oder Herkunft ermitteln konnte, erhielt dafür Hinweise von Behörden. Im vergangenen Jahr waren es erst 35 Prozent, vor zwei Jahren sogar nur 24 Prozent. „Der Austausch zwischen Wirtschaft und staatlichen Stellen funktioniert heute besser als noch vor einigen Jahren. Jetzt müssen wir auf ein gemeinsames Lagebild hinarbeiten, von dem beide Seiten profitieren würden“, sagt Wintergerst. Neben Behörden liefern den Unternehmen interne (37 Prozent) und externe (21 Prozent) Untersuchungen wichtige Informationen. Ebenso spielen spezifische Muster der Angriffstechnik eine Rolle (20 Prozent) sowie der Austausch mit anderen Unternehmen (16 Prozent), die Überwachung von Foren im Darknet (10 Prozent), Auffälligkeiten bei Personen oder Geschäftsabläufen (6 Prozent) sowie Hinweise oder Geständnisse von Beteiligten (6 Prozent). Wichtigste technische Erkenntnisquelle bleibt die Analyse von Log-Dateien (68 Prozent).

Cyberangriffe verursachen drei Viertel der Schäden

Auf Cyberattacken entfallen inzwischen 76 Prozent der Gesamtschäden. Vor einem Jahr lag der Anteil bei 70 Prozent, vor fünf Jahren sogar erst bei 59 Prozent. Die Schäden durch Cyberattacken summieren sich damit auf einen Betrag von 160,4 bis 205,8 Milliarden Euro. Im Vorjahr waren es 202,4 Milliarden Euro. Fast zwei Drittel (63 Prozent) aller Unternehmen haben in den vergangenen zwölf Monaten eine Zunahme von Cyberangriffen registriert. Und mit 69 Prozent gehen noch etwas mehr davon aus, dass Cyberangriffe in den kommenden zwölf Monaten zunehmen, kein einziges der befragten Unternehmen rechnet mit einem Rückgang. Auffällig ist: Obwohl sich nur noch 43 Prozent für sehr gut auf Cyberangriffe vorbereitet sehen (2025: 50 Prozent), fällt der Anteil der Unternehmen, die ihre geschäftliche Existenz durch eine erfolgreiche Cyberattacke bedroht sehen, von 59 auf 45 Prozent. „In den Unternehmen zeigt sich eine etwas trügerische Sicherheit, die möglicherweise auf einen Gewöhnungseffekt schließen lässt. Ein erfolgreicher Cyberangriff kann für

Unternehmen nach wie vor das wirtschaftliche Aus bedeuten“, sagt Wintergerst. „Cybersicherheit muss integraler Teil jeder Digitalstrategie sein. Es geht darum, Angriffe abzuwehren und im Ernstfall schnell wieder arbeitsfähig zu werden.“

Künstliche Intelligenz verschiebt die Angriffsmuster im Cyberraum

Bei Cyberangriffen richtet Ransomware weiterhin am häufigsten einen Schaden an. Bei 25 Prozent aller Unternehmen haben Angreifer Daten verschlüsselt und wollten sie nur gegen Lösegeld freigeben. Auch hier zeigt sich verglichen mit dem Vorjahr mit 34 Prozent ein deutlicher Rückgang. „Viele Unternehmen haben sich auf Ransomware-Angriffe vorbereitet und können so Schäden verhindern oder minimieren. Unser Ziel muss sein, aus diesem bislang einmaligen Rückgang eine echte Trendwende zu machen“, so Wintergerst. Neben Ransomware sind auch Angriffe auf Passwörter (18 Prozent), Phishing (16 Prozent), DDoS-Attacken, um Netzwerke lahmzulegen (15 Prozent) sowie Infizierung mit sonstiger Schadsoftware und Spoofing (je 11 Prozent) weit verbreitet.

Zugleich verschieben sich die Muster. Während klassische Angriffsarten seltener Schaden anrichten, nehmen KI-gestützte Methoden auf niedrigem Niveau sichtbar zu. Schäden durch automatisierte Robo Calls sprangen von 3 auf 14 Prozent, Deepfakes von 4 auf 8 Prozent. Und so gehen 8 von 10 Unternehmen (82 Prozent) davon aus, dass Angreifer verstärkt Künstliche Intelligenz einsetzen. Allerdings sind sich nur 31 Prozent dessen sicher, 51 Prozent vermuten den KI-Einsatz lediglich. Die Unternehmen machen das fest an der automatisierten Anpassung von Angriffsversuchen (53 Prozent), an hoher Qualität von gefälschten Audio- und Videoaufnahmen (48 Prozent), der hohen Qualität von Textnachrichten und Mails (38 Prozent), der sehr hohen Frequenz von Angriffen (34 Prozent) und stark personalisierten Inhalten (28 Prozent). 17 Prozent haben entsprechende Hinweise zudem aus der forensischen Analyse. „Künstliche Intelligenz verändert das Angriffsgeschehen grundlegend. Leistungsfähige Modelle können Schadcode generieren und werden künftig auch für autonome Angriffsarten verwendet werden. Deepfakes oder täuschend echte Anrufe und Mails mit sehr persönlichem Bezug machen Betrug einfacher und Angriffe schwerer erkennbar. Künstliche Intelligenz kann aber auch eingesetzt werden, um Angriffe schneller aufzudecken und zu verhindern – diese Chance müssen Unternehmen nutzen“, so Wintergerst.

Womit Unternehmen es Angreifern leicht machen

Insgesamt haben 6 von 10 Unternehmen (58 Prozent) in den vergangenen zwölf Monaten einen Schaden durch Cyberangriffe erlitten. Als wichtigsten Grund dafür, dass ein Angriff auch zu einem Schaden führte, nennen 59 Prozent der geschädigten Unternehmen die unzureichende Erkennung von Sicherheitsvorfällen. Es folgen Fehlkonfigurationen von IT-Systemen (57 Prozent) und ein unzureichendes Identitäts- und Zugriffsmanagement (55 Prozent), erst danach folgen technische Schwachstellen (50 Prozent), veraltete Hard- oder Software (43 Prozent) sowie eine Kompromittierung über externe Dienstleister oder Zulieferer (8 Prozent). Nur 18 Prozent führen die erfolgreichen Cyberangriffe auf ein unzureichendes Sicherheitsbewusstsein der Beschäftigten zurück. „Die häufigsten Schadensursachen sind keine besonders ausgefeilten oder exotische Angriffe, sondern blinde Flecken im eigenen System. Wer Vorfälle nicht zuverlässig erkennt, kann auch nicht rechtzeitig handeln und wird am Ende womöglich nicht einmal sicher sagen können, was überhaupt passiert ist“, sagt Wintergerst. „Wer in Angriffserkennung, saubere Konfigurationen und ein striktes Identitätsmanagement investiert, schließt die wichtigsten Lücken, die Angreifer heute nutzen.“

Investitionen in Cybersicherheit stagnieren

Der Anteil der IT-Sicherheit am gesamten IT-Budget stagniert wie im Vorjahr bei 18 Prozent. BSI und Bitkom empfehlen, 20 Prozent des IT-Budgets für Sicherheit aufzuwenden. Immerhin 45 Prozent der Unternehmen investieren aber 20 Prozent oder mehr ihres IT-Budgets in Sicherheit, im Vorjahr waren es 41 Prozent. 40 Prozent geben zwischen 10 und unter 20 Prozent, 6 Prozent zwischen 5 und unter 10 Prozent und 4 Prozent weniger als 5 Prozent ihres IT-Budgets für IT-Sicherheit aus. „IT-Sicherheit betrifft jedes Unternehmen, ausreichende Investitionen sind unerlässlich. Unternehmen dürfen es nicht darauf ankommen lassen, dass ihnen nichts passieren wird.“, so Wintergerst.

Auch bei der Cybersicherheit beschäftigten sich die Unternehmen mit Fragen der Digitalen Souveränität. 59 Prozent halten ihr Unternehmen für abhängig von Sicherheitslösungen aus den

USA, 70 Prozent finden, Behörden und Unternehmen in Deutschland sollten auf deutsche und europäische Sicherheitslösungen setzen. „Zur Souveränität gehört, die zentralen Fragen der Sicherheit in die eigene Hand nehmen zu können – das gilt insbesondere auch im Cyberraum“, so Wintergerst. Die Bundesregierung müsse bei ihren Programmen für ein digital souveränes Deutschland einen Schwerpunkt im Bereich der Cybersicherheit setzen.

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 1.003 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 23 2026 statt. Die Umfrage ist repräsentativ. Aufgrund der deutlich gewachsenen Unsicherheit in den Unternehmen weist Bitkom in diesem Jahr erstmals einen Schadenskorridor aus, dessen unteres Ende bei 211 und dessen oberes Ende bei 270,8 Milliarden Euro liegt. Grundlage ist wie in den Vorjahren eine Hochrechnung. Sie basiert am unteren Ende auf den Schäden, die jene Unternehmen beziffern, die im Untersuchungszeitraum einen Angriff sicher nachweisen können. Im Szenario zur Berechnung des oberen Endes des Korridors wird der über den Fünfjahres-Durchschnitt überschießende Teil der 2026 vermutlich betroffenen Unternehmen in die Hochrechnung einbezogen. Im Schnitt der Jahre 2021-2025 lag der Anteil der vermutlich betroffenen Unternehmen bei 10 Prozent, 2026 bei 29 Prozent.

Direktlink: ***https://www.bitkom.org/Presse/Presseinformation/Angriffe-auf-deutsche-Wirtschaft-Spur-auslaendische-Geheimdienste***