Bitkom e.V. | Presseinformation zur Pressekonferenz

Ohne Internet steht nach einem Tag alles still

- **Im Schnitt können Unternehmen ihr Geschäft nur 20 Stunden aufrechterhalten**
- **8 von 10 Unternehmen erwarten ernsthafte Krise in Deutschland als Folge hybrider Angriffe**
- **Lediglich 12 Prozent der Unternehmen halten sich für gut vorbereitet – viele planen aber höhere Investitionen**

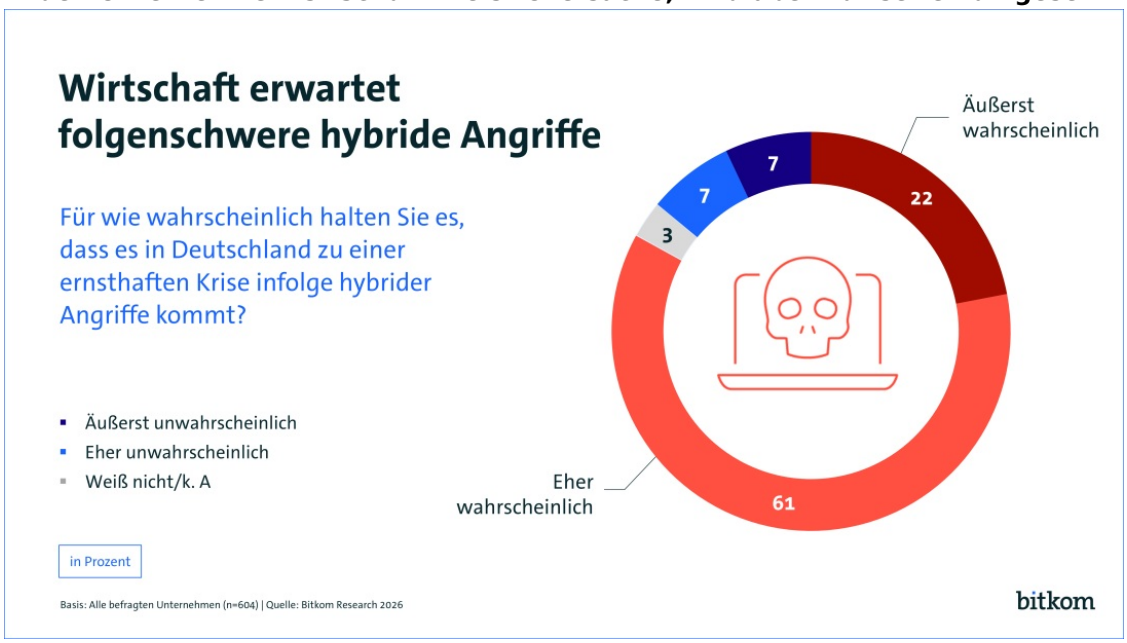
Berlin, 11. Februar 2026 - Stromausfall durch zerstörte Leitungen, gezielte Sabotage von Internetkabeln in der Ostsee oder mit Ransomware lahmgelegte Fabriken: Deutschland ist Ziel von digitalen und klassischen Angriffen, zugleich ist die deutsche Wirtschaft schlecht auf solche hybriden Bedrohungen vorbereitet. Bei einem Internetausfall könnten Unternehmen im Schnitt ihren Geschäftsbetrieb nur 20 Stunden aufrechterhalten, jedes fünfte (21 Prozent) müsste sogar sofort die Arbeit einstellen. Umgekehrt sind nur 8 Prozent sicher, länger als 48 Stunden weiterarbeiten zu können. Zugleich rechnen drei Viertel der Unternehmen (74 Prozent) wegen der zunehmenden Spannungen zwischen Russland und der NATO mit einer erhöhten Gefahr hybrider Angriffe, 8 von 10 (83 Prozent) erwarten eine ernsthafte Krise in Deutschland in Folge von hybriden Angriffen. Und 53 Prozent gehen sogar von einer militärischen Konfrontation zwischen Russland und der NATO in den kommenden fünf Jahren aus. Das sind Ergebnisse einer Befragung von 604 Unternehmen ab 10 Beschäftigten in Deutschland im Auftrag des Digitalverbands Bitkom, die heute im Vorfeld der Münchener Sicherheitskonferenz und der Munich Cyber Security Conference vorgestellt wurde. „Anfang Januar mussten nach einem Anschlag mehr als 100.000 Menschen in Berlin bei Minustemperaturen tagelang ohne Strom auskommen, mehr als 2.000 Unternehmen waren betroffen. Hybride Angriffe auf Deutschland, die sich in einer Grauzone zwischen Krieg und Frieden abspielen, sind kein potenzielles Risiko, sie sind Realität. Deshalb müssen wir die Resilienz von Wirtschaft, Staat und Gesellschaft massiv hochfahren“, sagt Bitkom-Präsident Dr. Ralf Wintergerst. Aktuell sagen drei Viertel (73 Prozent) der Unternehmen, Deutschland sei im internationalen Vergleich unzureichend auf hybride Angriffe vorbereitet.

Energieversorgung, Finanzwesen und Kommunikation im Fokus

Als besonders gefährdet gelten nach Ansicht der Unternehmen die Energieversorgung (90 Prozent) sowie Banken und Versicherungen (89 Prozent). 77 Prozent sagen, die Wasser- und

Abwasserversorgung sei stark gefährdet, 67 Prozent die Lebensmittelversorgung, 65 Prozent das Gesundheitswesen mit Krankenhäusern und Ärzten und 64 Prozent Telekommunikation und IT. Rund die Hälfte nennen Transport und Verkehr (54 Prozent) sowie die öffentliche Verwaltung (50 Prozent). Schlusslichter sind die Abfallentsorgung (28 Prozent) sowie Medien und Kultur (21 Prozent). Große Auswirkungen auf das eigene Unternehmen hätten demnach erfolgreiche Attacken auf die Energieversorgung (97 Prozent), Banken und Versicherungen (88 Prozent) sowie Telekommunikation und IT (85 Prozent). Dahinter folgen Wasserversorgung (69 Prozent) sowie Transport und Verkehr (67 Prozent). „Neben der Energieversorgung sind das Finanzwesen und die Kommunikation die neuralgischen Punkte der deutschen Wirtschaft“, so Wintergerst. „Zum notwendigen Schutz gehört zuallererst, es potenziellen Angreifern nicht unnötig leicht zu machen. Wir sollten darauf verzichten, Datenleitungen im Gigabit-Grundbuch öffentlich zugänglich zu verzeichnen, denn das bedeutet ein zusätzliches Risiko für Sabotageakte. Wir brauchen im Bereich kritischer Infrastrukturen Datensparsamkeit und ein strenges Sicherheits- und Zugangskonzept.“

In den Unternehmen ist Schutz meist Chefsache, wird aber nur selten umgesetzt



Die Wirtschaft ist nicht nur indirekt von hybriden Angriffen betroffen, Unternehmen werden auch ganz unmittelbar Opfer von Cyberangriffen und Sabotage. Eine deutliche Mehrheit von 59 Prozent hält es für wahrscheinlich, selbst Ziel hybrider Angriffe zu werden, bei 61 Prozent ist der Schutz vor diesen Attacken Chefsache. Zugleich hält sich kein Unternehmen für sehr gut darauf vorbereitet, nur 12 Prozent für eher gut. 38 Prozent geben an, eher schlecht vorbereitet zu sein, weitere 40 Prozent sind gar nicht vorbereitet: 35 Prozent planen aber, Vorkehrungen zu treffen, 5 Prozent haben das nicht vor. 10 Prozent können oder wollen keine Angaben zum Stand der Vorbereitungen auf hybride Angriffe machen. „Wir müssen die Lücke zwischen Gefahrenbewusstsein und Schutzniveau schnellstmöglich schließen“, so Wintergerst.

Die Unternehmen haben zwar eine Vielzahl von konkreten Vorkehrungen zum Umgang mit erfolgreichen hybriden Angriffen getroffen, es fehlt aber ein flächendeckender und umfassender Schutz. 58 Prozent verfügen für solche Fälle über alternative Kommunikationsmittel, 27 Prozent planen das. 57 Prozent verfügen über Backups ihrer Daten und haben auch erfolgreiche Restore-Tests durchgeführt, 15 Prozent haben das vor. In 51 Prozent gibt es Ausweicharbeitsplätze bzw. Homeoffice-Regelungen für den Fall, dass im Unternehmen nicht gearbeitet werden kann (Planung: 25 Prozent). Rund ein Viertel (28 Prozent) hat für den Krisenfall durch zusätzliche Lagerhaltung vorgesorgt, 17 Prozent planen dies. Und 16 Prozent haben Vereinbarungen mit alternativen Lieferanten (Planung: 32 Prozent), falls die bestehenden Lieferketten ausfallen. 28 Prozent setzen auf Sicherheitsüberprüfungen in sensiblen Bereichen, 17 Prozent denken darüber nach. Ebenfalls 28 Prozent haben ein Krisen- oder Notfallmanagement, 25 Prozent wollen eines einführen. Über eine Notstromversorgung verfügen 20 Prozent, 30 Prozent wollen sie einrichten. Und nur jedes zehnte Unternehmen (10 Prozent) führt regelmäßige Krisenübungen durch, 26 Prozent haben sich das vorgenommen. „Wir müssen bei den konkreten Vorsorgemaßnahmen für den Fall einer Krise besser werden. Einen Notfallplan braucht jedes Unternehmen, er entscheidet über die Handlungsfähigkeit in den wichtigen ersten Stunden”, sagt Wintergerst. „Die Unternehmen brauchen konkrete

Handreichungen und Unterstützung, wie sie vorsorgen müssen und vorsorgen können.“

Bei einer Krisenlage müssen Unternehmen auf Beschäftigte verzichten

Im Fall einer militärischen Auseinandersetzung stehen Unternehmen auch vor einer ungewohnten Herausforderung: Viele Beschäftigte, die beim Zivilschutz oder bei der Bundeswehr tätig sind, könnten im Job fehlen. Nur 30 Prozent der Unternehmen haben einen guten Überblick, wie viele Mitarbeiterinnen und Mitarbeiter den Zivilschutz unterstützen, etwa bei Feuerwehren oder Technischem Hilfswerk. Und gerade einmal 20 Prozent wissen, wie viele bei der Bundeswehr tätig würden. Selbst von denen, die einen guten Überblick haben, kann jedes fünfte (21 Prozent) keine genaue Zahl benennen, im Schnitt gehen die Unternehmen, die eine Schätzung abgeben können, von 9 Prozent ihrer Belegschaft aus, die ausfallen würde.

Viele Unternehmen wollen den Schutz hochfahren. 4 von 10 Unternehmen planen höhere Investitionen (37 Prozent), dabei wollen 9 Prozent in diesem Jahr deutlich mehr Geld ausgeben, 28 Prozent eher mehr. 44 Prozent planen unveränderte Investitionen in die Vorbereitung auf hybride Angriffe und deren Folgen. Kein Unternehmen will die Ausgaben senken, 5 Prozent treffen gar keine Vorsorge.

Behörden informieren noch nicht gut, dabei vertraut die große Mehrheit auf den Staat

Ein Problem für die Unternehmen sind fehlende Informationen über mögliche hybride Angriffe. Nur rund jedes fünfte Unternehmen (22 Prozent) fühlt sich aktuell ausreichend durch Sicherheitsbehörden informiert. Zugleich erwarten 80 Prozent im Fall eines hybriden Angriffs die verlässlichsten Informationen von staatlichen Stellen wie dem BSI oder dem Katastrophenschutz. „Einheitliche und klare Informationen des Staates sind von herausragender Bedeutung“, so Wintergerst. 73 Prozent vertrauen dabei auf den öffentlich-rechtlichen Rundfunk, 67 Prozent auf private Medien, 63 Prozent auf internationale Organisationen wie NATO oder EU und 60 Prozent auf Branchenverbände. 48 Prozent erwarten die verlässlichsten Informationen von privaten Sicherheitsdienstleistern, 44 Prozent über soziale Netzwerke und 11 Prozent aus eigenen Analysen oder dem eigenen Security Operation Center.

Insgesamt sehen nur 39 Prozent der befragten Unternehmen die Wirtschaft allgemein als sehr gut oder eher gut vorbereitet, bei Krankenhäusern und Ärzten sind es 38 Prozent. Dahinter rangieren die öffentliche Verwaltung (32 Prozent) und die Bevölkerung (29 Prozent). An der Spitze stehen die Bundeswehr (52 Prozent) und die Polizei (60 Prozent).

Von der Politik erwarten die Unternehmen mehr Information, Prävention aber auch konkrete Aktion. So wünschen sich 71 Prozent eine staatliche Informationskampagne zum Verhalten bei hybriden Angriffen, 62 Prozent wollen, dass hybride Angreifer öffentlich benannt werden, und 50 Prozent plädieren für ein Lagebild zu hybriden Angriffen. Um die Prävention zu stärken, unterstützen 79 Prozent verpflichtende Sicherheitsstandards mit praxisnahen Leitlinien, zugleich erwarten 68 Prozent aber auch Förderprogramme für Sicherheitsmaßnahmen. 54 Prozent sprechen sich für eine massive Förderung der deutschen Sicherheitsindustrie aus und 49 Prozent für regelmäßige bundesweite Übungen mit Bevölkerung und Unternehmen. 6 von 10 Unternehmen (60 Prozent) halten Cyberangriffe der Bundeswehr gegen feindliche Hackergruppen für sinnvoll, 58 Prozent die Ausweitung der Überwachungsbefugnisse von Sicherheitsbehörden im digitalen Raum und 49 Prozent sagen, massive Cyberangriffe auf einen NATO-Staat sollten wie ein militärischer Angriff betrachtet werden. „Wir müssen die Resilienz von Verwaltung, Wirtschaft, Bevölkerung und Infrastruktur zu einem Top-Thema machen“, sagt Wintergerst. „Damit das schnellstmöglich gelingt, sollten wir uns an den Staaten orientieren, die dabei schon weiter sind als wir, etwa in Skandinavien.“

Alle Ergebnisse der Befragung gibt es auch online im Bitkom-Dataverse unter:
www.bitkom.org/Bitkom-Dataverse/HybrideAngriffeUnternehmen

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

Nemo Buschmann
Referent Öffentliche Sicherheit & Verteidigung
Nachricht senden

Hinweis zur Methodik

Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 604 Unternehmen ab 10 Beschäftigten und einem Jahresumsatz von 1 Mio. Euro oder mehr telefonisch befragt. Die Befragung fand im Zeitraum von KW 47 2025 bis KW 3 2026 statt. Die Umfrage ist repräsentativ.

Link zur Presseinformation auf der Webseite:
https://www.bitkom.org/Presse/Presseinformation/Ohne-Internet-steht-nach-einem-Tag-alles-still