Bitkom e.V. | Presseinformation

Angriffe auf die deutsche Wirtschaft nehmen zu

- **8 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen**
- **Rekordschaden von rund 267 Milliarden Euro**
- **China wird immer mehr zum Standort Nr. 1 für Angreifer**
- **Cyberangriffe: Zwei Drittel der Unternehmen fühlen sich in ihrer Existenz bedroht**

Berlin, 28. August 2024 - Deutsche Unternehmen rücken verstärkt in den Fokus von Angreifern aus dem In- und Ausland. In den vergangenen zwölf Monaten waren 81 Prozent aller Unternehmen vom Diebstahl von Daten und IT-Geräten sowie von digitaler und analoger Industriespionage oder Sabotage betroffen. Weitere 10 Prozent vermuten dies. 2023 lagen die Anteile noch bei 72 und 8 Prozent. Zugleich ist der Schaden, der durch diese analogen und digitalen Angriffe entstand, von 205,9 Milliarden Euro um etwa 29 Prozent auf nun 266,6 Milliarden Euro gestiegen. Damit wird auch der bisherige Rekordwert von 223,5 Milliarden Euro aus dem Jahr 2021 übertroffen. Das sind Ergebnisse einer Studie im Auftrag des Digitalverbands Bitkom, für die mehr als 1.000 Unternehmen quer durch alle Branchen repräsentativ befragt wurden. Dabei konnten 70 Prozent der Unternehmen, die Opfer wurden, Angriffe der organisierten Kriminalität zuordnen. Vor einem Jahr waren es erst 61 Prozent. Ausländische Geheimdienste wurden mit 20 Prozent deutlich häufiger als Täter genannt (2023: 7 Prozent). Zur wichtigsten Ausgangsbasis für Angriffe auf die deutsche Wirtschaft hat sich China entwickelt. 45 Prozent der betroffenen Unternehmen konnten mindestens einen Angriff in das Land zurückverfolgen (2023: 42 Prozent). Auf Platz zwei liegt Russland mit 39 Prozent (2023: 46 Prozent). Zugenommen haben zugleich Angriffe aus osteuropäischen Staaten außerhalb der EU und Russland mit 32 Prozent (2023: 25 Prozent). Rückläufig sind demgegenüber Angriffe aus Deutschland (20 Prozent, 2023: 29 Prozent).

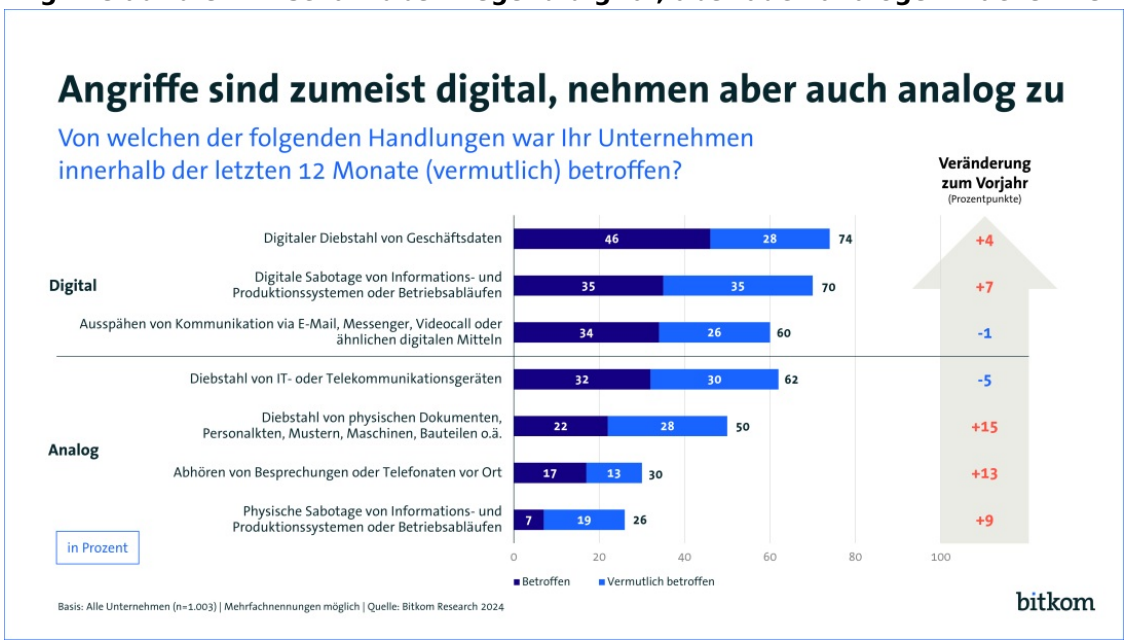
„Die Bedrohungslage für die deutsche Wirtschaft verschärft sich. Die Unternehmen müssen ihre Schutzmaßnahmen weiter hochfahren. Das gilt für digitale ebenso wie klassische Angriffe, wie etwa das Abhören von Besprechungen oder den Diebstahl von physischen Dokumenten“, sagt **Bitkom-Präsident Dr. Ralf Wintergerst**. Eine besondere Gefahr für die Wirtschaft bilden allerdings Cyberangriffe. So sehen sich inzwischen zwei Drittel (65 Prozent) der Unternehmen durch Cyberattacken in ihrer Existenz bedroht, vor einem Jahr waren es noch 52 Prozent, 2021 sogar erst 9 Prozent. Zugleich glaubt nur die Hälfte (53 Prozent), dass ihr Unternehmen sehr gut auf Cyberangriffe vorbereitet ist. „In einer digitalen, vernetzten Welt kommt der IT-Sicherheit eine

besondere Bedeutung zu. IT-Sicherheit muss überall Aufgabe der Unternehmensführung sein. Zugleich müssen wir den Austausch zwischen Wirtschaft und staatlichen Behörden noch stärker ausbauen, um Schutzmaßnahmen und Strafverfolgung zu koordinieren.“

Der Vizepräsident des Bundesamts für Verfassungsschutz, Sinan Selen sagte bei der Vorstellung der Studie: „Die Studienergebnisse korrespondieren mit unserer Lagebewertung. Internationale Konflikte und systemische Rivalitäten prägen die Sicherheitslage im Cyberraum wie im geopolitischen Raum. Ein Vormarsch in Richtung Blockbildung spiegelt sich in politischer und operativer Haltung wider. Wirtschaftlichen und wissenschaftlichen Austausch müssen wir in dieser Gesamtlage ganzheitlich betrachten. Die Angriffsvektoren auf die deutsche Wirtschaft haben sich verschoben. Die Verzahnung von Cyberspionage und Cybercrime hat weiter zugenommen. Und wir sehen auch eine noch engere Verbindung zwischen digitalen und analogen Angriffen. Die Angreifer verfolgen das Ziel durch passgenaues Social Engineering die Tür für klassische Spionageaktivitäten zu öffnen. Gleichzeitig nimmt die Bedrohung durch digitale und physische Sabotage weiter zu. Sorge bereitet uns der starke Anstieg analoger Angriffe, darunter Sabotage von Betriebsabläufen und Anlagen.

Da unsere Gegner ganzheitlich operieren, müssen auch Wirtschaftsunternehmen und Sicherheitsbehörden ganzheitlich agieren. Wir dürfen digitale und physische Sicherheit nicht isoliert betrachten. Bei einem ganzheitlichen Ansatz muss auch die Sicherheit von Lieferketten mit bedacht werden. Cyberakteure haben die gesamte supply-chain im Blick, während Unternehmen diese häufig vernachlässigen. Hier sehen wir erheblichen Nachbesserungsbedarf. Awareness und Readiness steigen, wir sind jedoch noch nicht am Ziel. Wir müssen Naivität abbauen und durch Aufmerksamkeit ersetzen. Uns muss klar sein: Wir sind nur dann machtlos, wenn wir nicht kooperieren und keine gemeinsamen Lösungen finden. Wir sind resilient, wenn wir von Angriffen auf Unternehmen schnell erfahren – nur dann können wir handeln und beraten.“

Angriffe auf die Wirtschaft überwiegend digital, aber auch analoge Attacken nehmen zu



Nachdem sich bereits im vergangenen Jahr ein deutlicher Trend hin zu digitalen Angriffen auf die deutsche Wirtschaft gezeigt hatte, nehmen digitale Attacken 2024 nochmals zu. Zugleich steigen aber auch klassische analoge Angriffe. So waren 74 Prozent der Unternehmen von digitalem Ausspähen von Geschäftsdaten betroffen oder vermutlich betroffen, ein Plus von 4 Prozentpunkten im Vergleich zum Vorjahr. Dabei berichten die von Datendiebstahl betroffenen Unternehmen deutlich häufiger, dass Kundendaten (62 Prozent, plus 6 Prozentpunkte), Zugangsdaten oder Passwörter (35 Prozent, plus 12 Prozentpunkte) sowie geistiges Eigentum wie Patente und Informationen aus Forschung und Entwicklung (26 Prozent, plus 9 Prozentpunkte) entwendet wurden. Am häufigsten sind weiterhin auch allgemeine Kommunikationsdaten wie E-Mails betroffen (63 Prozent, plus 1 Prozentpunkt). Seltener geht es um Finanzdaten (19 Prozent, minus 1 Prozentpunkt) sowie Daten von Mitarbeiterinnen und Mitarbeitern (16 Prozent, minus 17 Prozentpunkte). 70 Prozent der Unternehmen berichten von digitaler Sabotage von Systemen oder Betriebsabläufen (plus 7 Prozentpunkte), 60 Prozent vom Ausspähen digitaler Kommunikation, etwa E-Mails, Messenger oder

Videocalls (minus 1 Prozentpunkt).

Deutlich zugenommen haben die meisten klassisch analogen Angriffe. So war zwar der Diebstahl von IT- und Telekommunikationsgeräten, von dem 62 Prozent betroffen oder vermutlich betroffen waren, mit minus 5 Prozentpunkten leicht rückläufig. Allerdings gibt es ein Plus von 15 Prozentpunkten auf 50 Prozent beim Diebstahl von physischen Dokumenten, Mustern oder etwa Bauteilen und ein Plus von 13 Prozentpunkten auf 30 Prozent beim Abhören von Telefonaten oder Besprechungen vor Ort. Ebenfalls zugenommen - um 9 Prozentpunkte auf 26 Prozent - hat die physische Sabotage von Systemen oder Abläufen. „Wenn ein Videocall praktisch unangreifbar verschlüsselt ist, kann die Wanze im Hotelzimmer das Mittel der Wahl sein“, so Wintergerst. „Unternehmen müssen digitale und analoge Sicherheit zusammendenken und implementieren, das gilt zum Beispiel auch bei der Absicherung von IT-Systemen vor physischer Sabotage.“

Viele Unternehmen vernachlässigen die Lieferkette

Ein mögliches Einfallstor für Angreifer sind auch die immer komplexeren Lieferketten. 13 Prozent aller Unternehmen wissen, dass Zulieferer in den vergangenen zwölf Monaten Opfer von Datendiebstahl, Industriespionage oder Sabotage geworden sind, bei weiteren 13 Prozent gab es einen Verdacht und 21 Prozent können dazu nichts sagen. In 44 Prozent der Unternehmen, bei denen Zulieferer betroffen oder vermutlich betroffen waren, hatten die durchgeführten oder vermuteten Attacken auf Zulieferer Auswirkungen auf das eigene Unternehmen, etwa Produktionsausfälle, Lieferengpässe oder auch Reputationsschäden. Bei 40 Prozent gab es keine Folgen, 16 Prozent wissen es nicht oder machen keine Angaben. Zugleich sagen aber nur 37 Prozent der Unternehmen, die mit Zulieferern arbeiten, dass sie einen Notfallplan haben, wie sie auf Sicherheitsvorfälle in der Lieferkette reagieren. 33 Prozent stehen in engem Austausch mit Zulieferern, um das Risiko von Angriffen in der Lieferkette zu minimieren. Und 19 Prozent führen sogar regelmäßig Sicherheitsbewertungen bei Zulieferern durch, um das Risiko von Angriffen zu minimieren. 37 Prozent räumen ein, dass es im eigenen Unternehmen am Bewusstsein für die Risiken von Angriffen auf die Lieferkette fehlt, 13 Prozent machen sich Sorgen, dass die Zulieferer nicht dieselben Sicherheitsstandards einhalten wie das eigene Unternehmen und so zum Einfallstor für Angreifer werden könnten. „Sicherheitsmaßnahmen und insbesondere Maßnahmen zur IT-Sicherheit sind immer nur so gut wie für das schwächste Glied in der Kette. Unternehmen sollten deshalb unbedingt ihre gesamte Lieferkette in den Blick nehmen“, sagt Bitkom-Präsident Wintergerst.

Cyberattacken nehmen zu – und machen Großteil des Schadens aus

Die Mehrheit (80 Prozent) der Unternehmen hat in den vergangenen zwölf Monaten eine Zunahme von Cyberattacken verzeichnet, gerade einmal bei 2 Prozent sind es weniger geworden. Und für die kommenden zwölf Monate erwarten sogar 90 Prozent mehr Cyberattacken, die übrigen 10 Prozent gehen von einem unveränderten Niveau aus. Aktuell sind Cyberattacken für zwei Drittel (67 Prozent) des gesamten Schadens verantwortlich, der der deutschen Wirtschaft durch Datendiebstahl, Sabotage und Industriespionage entsteht: 178,6 Milliarden Euro betrug der Schaden durch Cybercrime. Das sind rund 30 Milliarden Euro mehr als im Vorjahr (2023: 148,2 Milliarden Euro).

Am häufigsten berichten Unternehmen von Schäden durch Ransomware (31 Prozent, plus 8 Prozentpunkte), dahinter folgen Phishing-Attacken (26 Prozent, minus 5 Prozentpunkte), Angriffe auf Passwörter (24 Prozent, minus 5 Prozentpunkte) und Infizierung mit Schadsoftware (21 Prozent, minus 7 Prozent). Ebenfalls häufig Schäden verursachen sogenannte Distributed Denial of Service-Angriffe, durch die zum Beispiel Webserver lahmgelegt werden (18 Prozent, plus 6 Prozentpunkte). „Wird mein Unternehmen Opfer von Cybercrime? – Das ist keine Frage des Ob, es geht lediglich um das Wann und Wie. Wichtig ist ein guter Schutz, und dazu gehören auch Maßnahmen, um Schäden möglichst gering zu halten, wie regelmäßige Backups“, so Wintergerst.

Eher selten sind noch Schäden durch neue Angriffsmethoden wie Deep Fakes und Robo Calls (je 3 Prozent), die vor allem durch die Verbreitung von Künstlicher Intelligenz einfacher werden. Dabei sehen die Unternehmen in der KI sowohl Risiken als auch Chancen für die IT-Sicherheit. So sagen 83 Prozent, dass KI die Bedrohungslage für die Wirtschaft verschärft und 70 Prozent meinen, dass KI Cyberangriffe erleichtert. Aber 61 Prozent sagen auch, dass der Einsatz von KI die IT-Sicherheit deutlich verbessern kann.

Ausgaben für IT-Sicherheit legen deutlich zu

Drei Viertel (75 Prozent) der Unternehmen beklagen, dass die Sicherheitsbehörden machtlos gegen Cyberangriffe aus dem Ausland sind. Zugleich sehen 69 Prozent, dass sich in Folge der zahlreichen Kriege und Konflikte die Bedrohung des eigenen Unternehmens durch Cyberangriffe verschärft hat.

In Reaktion auf die zunehmend als unsicher wahrgenommene Weltlage reagieren die Unternehmen mit steigenden Ausgaben für die IT-Sicherheit. 54 Prozent haben Maßnahmen getroffen, um sich vor physischen Angriffen auf die IT-Infrastruktur zu schützen. Und 62 Prozent haben ihre IT-Sicherheitsmaßnahmen verschärft. Der durchschnittliche Anteil der Ausgaben für IT-Sicherheit am gesamten IT-Budget der Unternehmen ist in diesem Jahr auf 17 Prozent gestiegen. 2023 waren es noch 14 Prozent, 2022 sogar nur 9 Prozent. Inzwischen wenden 4 von 10 Unternehmen (39 Prozent) 20 Prozent oder mehr ihres IT-Budgets für IT-Sicherheit auf, dies entspricht einer Forderung von Bitkom und dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Weitere 38 Prozent geben 10 bis unter 20 Prozent aus, 9 Prozent nur 5 bis unter 10 Prozent und 5 Prozent sogar weniger als 5 Prozent. „Bei den durchschnittlichen Ausgaben für IT-Sicherheit nähern wir uns dem Zielwert an. Wichtig ist, dass die Investitionen in die IT-Sicherheit dauerhaft auf hohem Niveau gehalten werden. Cyberkriminelle sind Moving Targets und da heißt es: dranbleiben!“, so Wintergerst.

IT-Sicherheit als Frage der digitalen Souveränität

In der Wirtschaft wird IT-Sicherheit zunehmend auch als Frage der digitalen Souveränität betrachtet. So bemängeln 54 Prozent, dass die Politik in Deutschland die IT-Sicherheit im internationalen Vergleich vernachlässige, 76 Prozent beklagen, dass die öffentliche Verwaltung viel schlechter gegen Cyberangriffe gesichert sei als die deutsche Wirtschaft. Und 72 Prozent wünschen sich, dass deutsche IT-Sicherheitsunternehmen gezielt von der Politik gefördert werden. 71 Prozent achten beim Einkauf von IT-Sicherheitslösungen besonders auf das Herkunftsland des Anbieters. „IT-Sicherheit ist kein Zustand, IT-Sicherheit ist ein Prozess und ihn müssen wir aktiv betreiben. Der Schutz gegen Cyberangriffe gehört mit ins Zentrum einer Strategie für ein sicheres und digital souveränes Deutschland“, so Wintergerst.

Kontakt

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

Felix Kuhlenkamp
Bereichsleiter Sicherheitspolitik
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 24 2024 statt. Die Umfrage ist repräsentativ.

Link zur Presseinformation auf der Webseite:
https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024