Bitkom e.V. | Presseinformation

203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen

- **9 von 10 Unternehmen werden Opfer von Datendiebstahl, Spionage oder Sabotage**
- **Rolle der organisierten Kriminalität bei den Attacken nimmt stetig zu**
- **Starker Anstieg von Angriffen aus Russland und China**

Berlin, 31. August 2022 - Der deutschen Wirtschaft entsteht ein jährlicher Schaden von rund 203 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage. Damit liegt der Schaden etwas niedriger als im Rekordjahr 2021 mit 223 Milliarden Euro. In den Jahren 2018/2019 waren es erst 103 Milliarden Euro. Das sind Ergebnisse einer Studie im Auftrag des Digitalverbands Bitkom, für die mehr als 1.000 Unternehmen quer durch alle Branchen repräsentativ befragt wurden. Praktisch jedes Unternehmen in Deutschland wird Opfer: 84 Prozent der Unternehmen waren im vergangenen Jahr betroffen, weitere 9 Prozent gehen davon aus. Dabei sind die Angriffe aus Russland und China zuletzt sprunghaft angestiegen. 43 Prozent der betroffenen Unternehmen haben mindestens eine Attacke aus China identifiziert (2021: 30 Prozent). 36 Prozent haben Urheber in Russland ausgemacht (2021: 23 Prozent). Zugleich gehen die Angreifer immer professioneller vor. Erstmals liegen das organisierte Verbrechen und Banden an der Spitze der Rangliste der Täterkreise. Bei 51 Prozent der betroffenen Unternehmen kamen Attacken aus diesem Umfeld. Vor einem Jahr lag ihr Anteil gerade einmal bei 29 Prozent, vor drei Jahren bei 21 Prozent.

„Spätestens mit dem russischen Angriffskrieg gegen die Ukraine und einer hybriden Kriegsführung auch im digitalen Raum ist die Bedrohung durch Cyberattacken für die Wirtschaft in den Fokus von Unternehmen und Politik gerückt. Die Bedrohungslage ist aber auch unabhängig davon hoch“, sagte Bitkom-Präsident Achim Berg. „Die Angreifer werden immer professioneller und sind häufiger im organisierten Verbrechen zu finden, wobei die Abgrenzung zwischen kriminellen Banden und staatlich gesteuerten Gruppen zunehmend schwerfällt. Allerdings zeigen die Ergebnisse in diesem Jahr auch, dass Unternehmen mit geeigneten Maßnahmen und Vorsorge dafür sorgen können, dass Angriffe abgewehrt werden oder zumindest der Schaden begrenzt wird.“

Verfassungsschutz-Vizepräsident Sinan Selen sagte bei der Vorstellung der Studie: „Die Bewertungen in der Studie spiegeln sich auch in der Lageeinschätzung der Cyberabwehr des BfV wider. Die Grenzen zwischen Cyberspionage und Cybercrime verschwimmen zunehmend. Wir müssen uns nicht nur auf ein ‚Outsourcing‘ von Spionage einstellen, sondern auch darauf, dass

Staaten Cybercrime als Deckmantel für eigene Operationen nutzen. Wir stellen eine Vermischung analoger und digitaler Angriffsvektoren fest. Zudem wechseln staatliche Akteure ihr Zielspektrum flexibel, je nach politischer Agenda, von Wirtschaft zu Politik und umgekehrt. Als Nachrichtendienst kann das BfV diesen Herausforderungen begegnen, da wir wertvolle Erkenntnisse aus operativen Maßnahmen und aus dem Austausch mit internationalen Partnern kombinieren können."

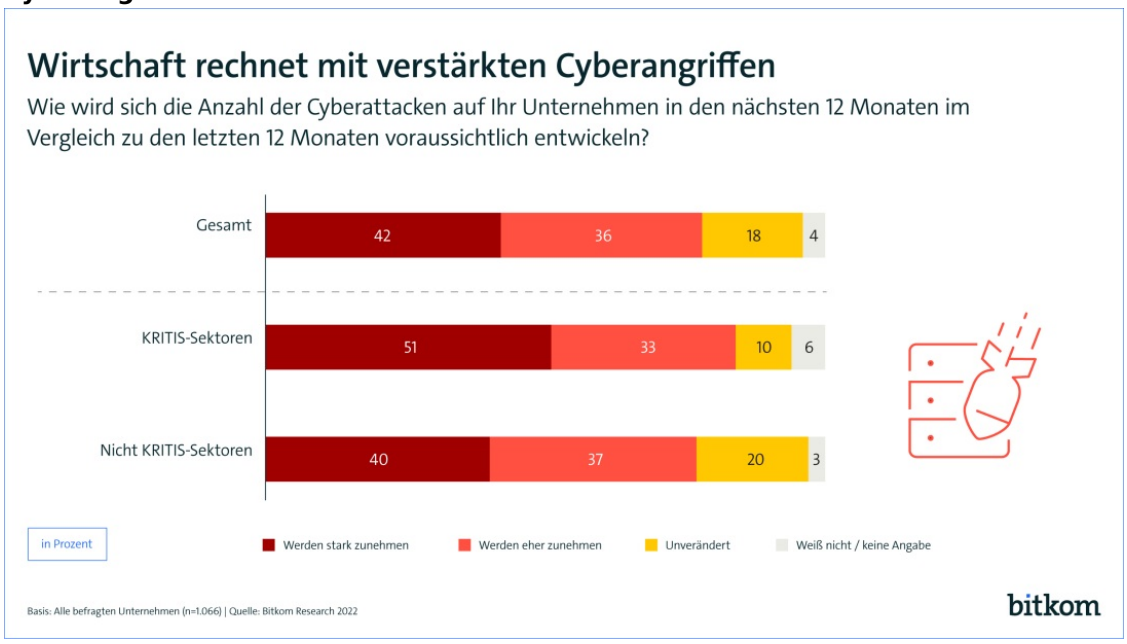
Digitale Angriffe nehmen zu, analoge gehen leicht zurück

Angriffe auf die Wirtschaft haben sich im vergangenen Jahr weiter in den digitalen Raum verlagert. So geben zwei Drittel der Unternehmen (69 Prozent) an, dass sie in den vergangenen zwölf Monaten von Diebstählen von IT- und Telekommunikationsgeräten betroffen oder vermutlich betroffen waren, ein Anstieg um 7 Prozentpunkte zum Vorjahr. 63 Prozent berichten vom Diebstahl sensibler Daten (plus 3 Prozentpunkte), bei 57 Prozent wurde digitale Kommunikation ausgespäht (plus 5 Prozentpunkte) und 55 Prozent sind von der digitalen Sabotage von Systemen oder Betriebsabläufen betroffen oder vermuten dies (plus 3 Prozentpunkte). Leicht rückläufig sind dagegen der analoge Diebstahl von physischen Dokumenten, Unterlagen oder Mustern (42 Prozent, minus 8 Prozentpunkte), das Abhören von Besprechungen oder Telefonaten (28 Prozent, minus 9 Prozentpunkte) sowie die analoge Sabotage (22 Prozent, minus 3 Prozentpunkte). „Unternehmen in Deutschland haben seit Beginn der Corona-Pandemie die Digitalisierung vorangetrieben. Damit verlagern sich auch die Angriffe zunehmend in den digitalen Raum", so Berg.

Datendiebstahl: Täter haben es auf die Daten Dritter abgesehen

Beim Diebstahl digitaler Daten haben es die Angreifer verstärkt auf Daten Dritter abgesehen. So geben 68 Prozent der von diesem Delikt betroffenen Unternehmen an, dass Kommunikationsdaten wie E-Mails entwendet wurden (2021: 63 Prozent). Bei fast jedem Zweiten (45 Prozent) waren Kundendaten im Visier – nach nur 31 Prozent vor einem Jahr. Berg: „Die Täter scheinen genau zu wissen, an welcher Stelle sie am härtesten zuschlagen können. Wenn Daten Dritter entwendet werden, droht den Unternehmen zusätzlicher Schaden. Der reicht von Reputationsverlust bis hin zu möglichen Bußgeldern der Aufsichtsbehörden." In jedem dritten betroffenen Unternehmen wurden unkritische Business-Informationen (38 Prozent) oder Cloud-Zugangsdaten (32 Prozent) gestohlen. Jedes vierte Unternehmen meldet den Verlust kritischer Business-Informationen wie Marktanalysen (28 Prozent) sowie Daten von Mitarbeiterinnen und Mitarbeitern (25 Prozent). In rund jedem fünften betroffenen Unternehmen (18 Prozent) hatten es die Täter auf geistiges Eigentum wie Patente abgesehen, in 14 Prozent flossen Finanzdaten ab.

Cyberangriffe: 45 Prozent fürchten um Existenz



Insbesondere digitale Angriffe beunruhigen die Wirtschaft. 39 Prozent haben in den vergangenen zwölf Monaten erlebt, dass Cyberattacken auf ihr Unternehmen stark zugenommen haben, 45 Prozent meinen, sie haben eher zugenommen. Vor allem Betreiber kritischer Infrastrukturen erleben einen Anstieg der Angriffe: Hier sagen 49 Prozent, die Attacken haben stark zugenommen, und 38

Prozent, sie haben eher zugenommen. Die Sorgen vor den Folgen einer Cyberattacke wachsen: 45 Prozent der Unternehmen meinen, dass Cyberattacken ihre geschäftliche Existenz bedrohen können – vor einem Jahr lag der Anteil bei gerade einmal 9 Prozent.

Bei den Cyberangriffen wurden vor allem Attacken auf Passwörter, Phishing und die Infizierung mit Schadsoftware bzw. Malware für die Unternehmen teuer – in jeweils jedem vierten Unternehmen (25 Prozent) ist ein entsprechender Schaden entstehen. Dahinter folgen DDoS-Attacken, um IT-Systeme lahmzulegen (21 Prozent). Ransomware-Attacken haben in 12 Prozent der Unternehmen Schäden verursacht, das ist nach dem Rekordjahr 2021 mit 18 Prozent ein deutlicher Rückgang. „Bei Ransomware gilt: Durch technische Vorkehrungen und Schulung der Beschäftigten lassen sich Angriffe abwehren. Und wer aktuelle Backups zur Verfügung hat und einen Notfallplan aufstellt, der kann den Schaden einer erfolgreichen Attacke zumindest deutlich reduzieren“, so Berg. „Auf keinen Fall sollte ein Lösegeld gezahlt werden. Häufig erhalten die Opfer ihre Daten selbst dann nicht in einem brauchbaren Zustand zurück – und zugleich werden die Täter zu weiteren Angriffen motiviert, und die können auch auf dasselbe Unternehmen erneut treffen.“

Einen Anstieg gab es beim sogenannten Social Engineering. Fast jedes zweite Unternehmen (48 Prozent) berichtet von entsprechenden Versuchen. Dabei wird vor allem und deutlich häufiger als in der Vergangenheit versucht, über das Telefon (38 Prozent, 2021: 27 Prozent) und über E-Mail (34 Prozent, 2021: 24 Prozent) an sensible Informationen zu gelangen. Sie können dann für Cyberattacken verwendet werden. Berg: „Eine regelmäßige Schulung von Mitarbeiterinnen und Mitarbeitern zu Sicherheitsfragen, damit sie sich auch bei Social-Engineering-Versuchen richtig verhalten, sollte in jedem Unternehmen selbstverständlich sein.“

Weitere Zunahme von Cyberattacken erwartet – vor allem auf kritische Infrastruktur

Die Unternehmen erwarten in den kommenden zwölf Monaten eine weitere Zunahme von Cyberangriffen. 42 Prozent der Unternehmen rechnen mit einem starken Anstieg, 36 Prozent mit einem eher starken. Die Betreiber kritischer Infrastruktur stellen sich sogar auf noch heftigere Attacken ein: Hier rechnen 51 Prozent mit einem starken, 33 Prozent mit einem eher starken Anstieg. Die Wirtschaft fürchtet dabei vor allem Ransomware-Angriffe, die 92 Prozent als sehr oder eher bedrohlich einschätzen. Dahinter folgen Zero-Day-Exploits (91 Prozent) und Spyware-Attacken (85 Prozent). 72 Prozent sehen mögliche Angriffe mit Quantencomputern als künftige Bedrohung. Aber auch Entwicklungen auf dem Arbeitsmarkt beunruhigen die Unternehmen: 72 Prozent sehen den Mangel an IT-Sicherheitsexperten als Bedrohung, 58 Prozent die zunehmende Fluktuation von Beschäftigten.

Der Anteil der Ausgaben für IT-Sicherheit am IT-Budget der Unternehmen ist verglichen mit dem Vorjahr leicht gestiegen. 9 Prozent geben die Unternehmen im Schnitt aus, vor einem Jahr waren es 7 Prozent. „Bei den Ausgaben für IT-Sicherheit müssen die Unternehmen dringend zulegen. Die Erkenntnis, welche dramatischen Folgen ein erfolgreicher Angriff haben kann, ist längst da – den notwendigen Schutz davor gibt es aber nicht zum Nulltarif. Hier müssen Vorstände und Geschäftsleitungen umgehend aktiv werden“, sagte Berg.

Von der Politik wünschen sich 98 Prozent mehr Einsatz für eine verstärkte EU-weite Zusammenarbeit bei Cybersicherheit. 97 Prozent fordern, dass die Politik stärker gegen Cyberattacken aus dem Ausland vorgehen soll. Und drei Viertel (77 Prozent) meinen, die Politik solle die Ermittlungsbefugnisse erweitern, damit Cyberangriffe aufgeklärt werden können. Zugleich beklagen 77 Prozent, dass der bürokratische Aufwand bei der Meldung von Vorfällen zu hoch ist.

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 Digitalverband Bitkom durchgeführt hat. Dabei wurden 1.066 Unternehmen ab 10 Beschäftigten und einem Jahresumsatz von mindestens 1 Mio. Euro in Deutschland telefonisch befragt. Die Umfrage ist repräsentativ für die Gesamtwirtschaft.

Link zur Presseinformation auf der Webseite:
https://www.bitkom.org/Presse/Presseinformation/203-Milliarden-Euro-Schaden-pro-Jahr-durch-Angriffe-auf-deutsche-Unternehmen