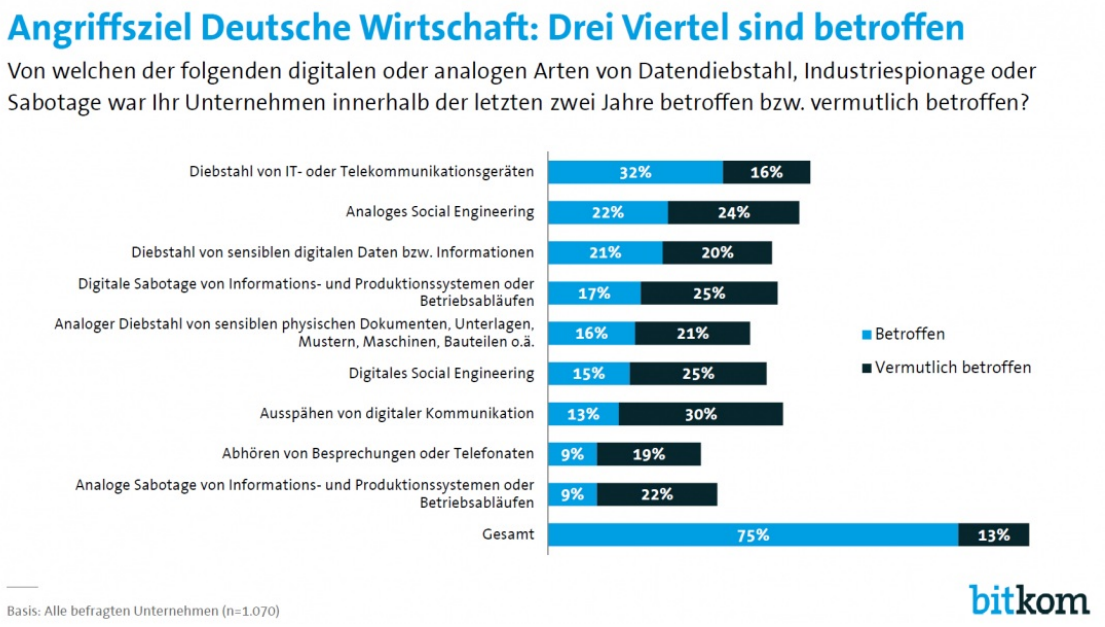
Bitkom e.V. |

Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr

- **3 von 4 Unternehmen wurden Opfer von Sabotage, Datendiebstahl oder Spionage**
- **Die Spur zeigt oft nach Osten**



Berlin, 06. November 2019 - Kriminelle Attacken auf Unternehmen verursachen in Deutschland Rekordschäden. Durch Sabotage, Datendiebstahl oder Spionage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 102,9 Milliarden Euro – analoge und digitale Angriffe zusammengenommen. Der Schaden ist damit fast doppelt so hoch wie noch vor zwei Jahren (2016/2017: 55 Milliarden Euro p.a.). Drei Viertel der Unternehmen (75 Prozent) waren in den vergangen beiden Jahren von Angriffen betroffen, weitere 13 Prozent vermuten dies. In den Jahren 2016/2017 wurde nur jedes zweite Unternehmen (53 Prozent) Opfer. Das ist das Ergebnis einer Studie des Digitalverbands Bitkom, für die mehr als 1.000 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Branchen repräsentativ befragt wurden. „Umfang und Qualität der Angriffe auf Unternehmen haben dramatisch zugenommen“, sagt Bitkom-Präsident Achim Berg. „Die Freizeithacker von früher haben sich zu gut ausgerüsteten und technologisch oft sehr versierten Cyberbanden weiterentwickelt – zuweilen mit Staatsressourcen im Rücken.“ Digitale Angriffe haben in den vergangenen beiden Jahren bei 70 Prozent der Unternehmen einen Schaden versursacht, im Jahr 2017 waren es erst 43 Prozent.

Diebstahl und Social Engineering häufige Delikte

Demnach berichtet jedes fünfte Unternehmen (21 Prozent), dass sensible digitale Daten abgeflossen sind, bei 17 Prozent wurden Informations- und Produktionssysteme oder Betriebsabläufe digital sabotiert. Bei jedem achten Unternehmen (13 Prozent) ist die digitale Kommunikation ausgespäht worden. Es wird aber nach wie vor noch oft analog angegriffen. Bei einem Drittel der Unternehmen (32 Prozent) wurden IT- oder Telekommunikationsgeräte entwendet, sensible physische Dokumente, Maschinen oder Bauteile wurden bei jedem Sechsten gestohlen. Weiter auf dem Vormarsch ist das sogenannte Social Engineering. Dabei werden Mitarbeiter manipuliert, um an sensible Informationen zu kommen, mit denen dann in einem weiteren Schritt zum Beispiel Schadsoftware auf die Firmenrechner gebracht werden kann. Mehr als jedes fünfte Unternehmen (22 Prozent) war davon analog betroffen, 15 Prozent digital.

Hierzu Michael Niemeier, Vizepräsident des Bundesamtes für Verfassungsschutz (BfV): „Spionage und Sabotage gefährden den Wirtschaftsstandort Deutschland. Die Aufklärung solcher Verdachtsfälle ist eine der Kernkompetenzen des Verfassungsschutzes."

Daten aller Art im Visier: Finanz-, Mitarbeiter- und Kundendaten

Angreifer haben bei ihren Attacken unterschiedlich sensible Daten erbeutet. Bei fast der Hälfte (46 Prozent) der betroffenen Unternehmen wurden Kommunikationsdaten wie Emails gestohlen. Bei jedem vierten Unternehmen sind durch digitale Angriffe jeweils Finanzdaten (26 Prozent), Mitarbeiterdaten (25 Prozent) und Kundendaten (23 Prozent) abgeflossen. Kritische Geschäftsinformationen wie Marktanalysen oder Preisgestaltung sind bei jedem achten Unternehmen (12 Prozent) in kriminelle Hände gefallen. „Im globalen Wettbewerb kann jede Information über die Konkurrenz zum Vorteil werden – dafür greifen immer mehr Unternehmen zu kriminellen Mitteln“, sagt Berg.

Ehemalige Mitarbeiter als Gefahrenquelle

Wer sind die Täter? Vor allem ehemalige Mitarbeiter verursachen Schäden. Ein Drittel der Betroffenen (33 Prozent) sagt, dass sie von früheren Mitarbeitern vorsätzlich geschädigt wurden. Ein knappes Viertel (23 Prozent) sieht vormals Beschäftigte in der Verantwortung, ohne ihnen ein absichtliches Fehlverhalten zu unterstellen. Vier von zehn Betroffenen (38 Prozent) führen Angriffe auf Einzeltäter bzw. sogenannte Hobby-Hacker zurück. Bei einem Fünftel geht die Spur jeweils zur organisierten Kriminalität (21 Prozent) oder zu konkurrierenden Unternehmen (20 Prozent). Bei 12 Prozent stammen Attacken von ausländischen Nachrichtendiensten.

Auch wenn die regionale Herkunft nicht immer eindeutig ist, verorten fast drei von zehn Betroffenen (28 Prozent) den Ursprung der Angriffe in Osteuropa (ohne Russland). Bei ähnlich vielen (27 Prozent) stammen die Attacken aus China, 19 Prozent sehen Russland als Ursprung, dicht gefolgt von den USA (17 Prozent). Für vier von zehn Betroffenen (39 Prozent) gingen kriminelle Handlungen aus Deutschland aus, für ein Viertel (24 Prozent) war die Herkunft unklar.

Interne Sicherheitsmaßnahmen sind entscheidend

Häufig sind es aber auch Mitarbeiter, die auf der anderen Seite dafür sorgen, dass kriminelle Handlungen aufgedeckt werden. Sechs von zehn betroffenen Unternehmen (62 Prozent) sind so erstmals auf Angriffe aufmerksam geworden. Mehr als die Hälfte (54 Prozent) erhielt Hinweise auf Angriffe durch eigene Sicherheitssysteme, bei fast drei von zehn (28 Prozent) war es hingegen reiner Zufall. „Gut geschulte Mitarbeiter sind der effektivste Schutz. So lässt sich unbeabsichtigten Schäden vorbeugen, Angriffe von außen werden besser abgewehrt und sind sie doch erfolgreich, lässt sich schnell gegensteuern“, so Berg.

Wirtschaft fordert mehr Zusammenarbeit

Nur bei 13 Prozent der Unternehmen gingen erste Hinweise auf Delikte durch externe Strafverfolgungs- oder Aufsichtsbehörden ein. Auch deshalb fordern praktisch alle Unternehmen eine engere Zusammenarbeit mit Staat und Behörden. So sind 96 Prozent der Meinung, dass der Informationsaustausch zu IT-Sicherheitsthemen zwischen Staat und Wirtschaft verbessert werden sollte. Ebenso viele sagen: Die zuständigen Behörden sollten die Wirtschaft bei Fragen zur IT-Sicherheit besser unterstützen. Und 91 Prozent finden, dass der Informationsaustausch zwischen staatlichen Stellen verbessert werden sollte.

Für die Zukunft prognostiziert eine breite Mehrheit der Unternehmen eine weitere Verschärfung der Sicherheitslage. 82 Prozent gehen davon aus, dass die Zahl der Cyberattacken auf ihr Unternehmen in den nächsten zwei Jahren zunehmen wird. Berg: „Staat und Behörden können Unternehmen noch besser bei der Gefahrenabwehr unterstützen, etwa durch ein umfassendes Lagebild und einen besseren Informationsaustausch. Das von der Bundesregierung geplante Cyber-Abwehrzentrum plus sollte möglichst schnell aufgebaut werden, um das vorhandene Wissen bestmöglich zu teilen und anzuwenden.“

„Der Bitkom ist für das BfV ein wichtiger Partner im Wirtschaftsschutz. Das BfV hat daher bereits im Jahr 2016 mit dem Bitkom ein 'gemeinsames Handeln für digitale Sorgfalt und zum Schutz von Know-

how in Deutschland' vereinbart. Daraus haben sich eine fruchtbare Kooperation und vielfältige Aktivitäten ergeben“, so BfV-Vizepräsident Niemeier.

Wie sich Unternehmen vor Angriffen schützen können, hat Bitkom unter folgendem Link zusammengetragen: https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Oeffentliche-Sicherheit-Wirtschaftsschutz/Goldene-Regeln-fuer-den-Wirtschaftsschutz.html

Hinweis zur Methodik: Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.070 Unternehmen mit 10 oder mehr Mitarbeitern befragt. Die Interviews wurden mit Führungskräften durchgeführt, die in ihrem Unternehmen für das Thema Wirtschaftsschutz verantwortlich sind. Dazu zählen Geschäftsführer sowie Führungskräfte aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement und Finanzen. Die Umfrage ist repräsentativ für die Gesamtwirtschaft.

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
