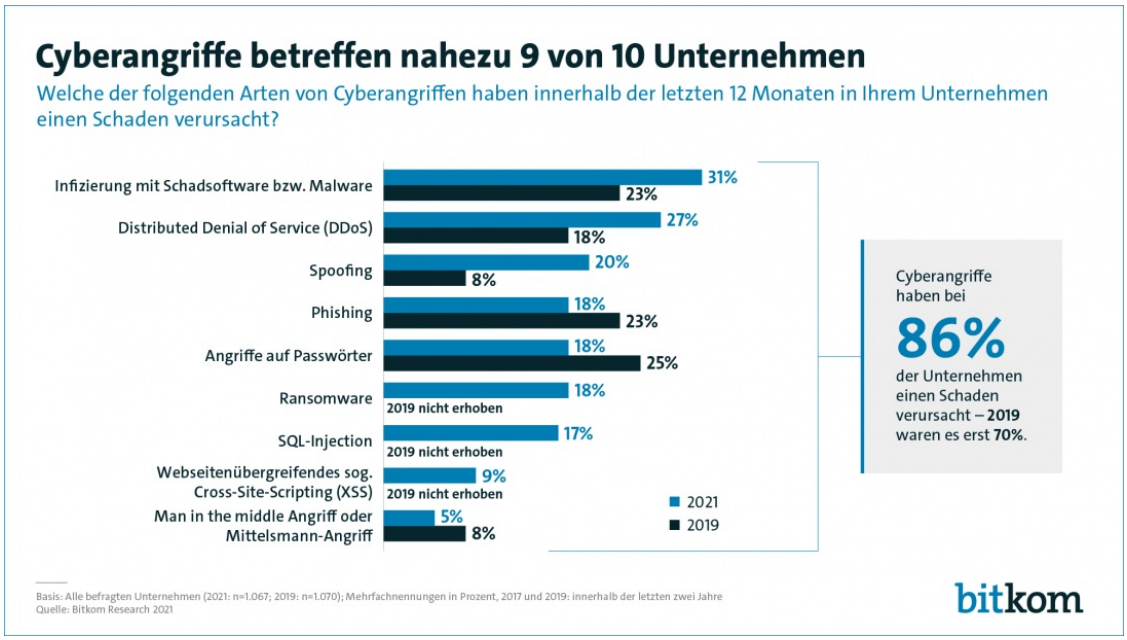
Bitkom e.V. |

Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr

- **Diebstahl, Spionage, Sabotage: Neun von zehn Unternehmen wurden Opfer**
- **Erpressung, Systemausfälle und Betriebsstörungen mehr als vervierfacht**
- **Bereits jedes zehnte Unternehmen sieht seine geschäftliche Existenz bedroht**



Berlin, 05. August 2021 - Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro. Damit haben kriminelle Attacken erneut für Rekordschäden gesorgt: Die Schadenssumme ist mehr als doppelt so hoch wie in den Jahren 2018/2019, als sie noch 103 Milliarden Euro p.a. betrug. Neun von zehn Unternehmen (88 Prozent) waren 2020/2021 von Angriffen betroffen. In den Jahren 2018/2019 wurden drei Viertel (75 Prozent) Opfer. Das sind Ergebnisse einer repräsentativen Studie des Digitalverbands Bitkom, für die mehr als 1.000 Unternehmen quer durch alle Branchen befragt wurden.

Haupttreiber des enormen Anstiegs sind Erpressungsvorfälle, verbunden mit dem Ausfall von Informations- und Produktionssystemen sowie der Störung von Betriebsabläufen. Sie sind meist unmittelbare Folge von Ransomware-Angriffen. Durch sie werden Computer und andere Systeme blockiert, anschließend werden die Betreiber erpresst. Die so verursachten Schäden haben sich im Vergleich zu den Vorjahren 2018/2019 mehr als vervierfacht (+358 Prozent). Aktuell sieht jedes zehnte Unternehmen (9 Prozent) seine geschäftliche Existenz durch Cyberattacken bedroht.

„Die Wucht, mit der Ransomware-Angriffe unsere Wirtschaft erschüttern, ist besorgniserregend und trifft Unternehmen aller Branchen und Größen“, kommentiert Bitkom-Präsident Achim Berg die aktuelle Entwicklung. Systeme würden verschlüsselt und der Geschäftsbetrieb lahmgelegt. Gestohlene Kunden- und Unternehmensdaten erzeugten nicht nur Reputationsschäden, sondern führten auch zum Verlust von Wettbewerbsfähigkeit, mahnte Berg: „Der Diebstahl von geistigem Eigentum kann für die innovationsgetriebene deutsche Wirtschaft schwerwiegende Konsequenzen haben.“

Verfassungsschutz-Vizepräsident Sinan Selen, der die Ergebnisse gemeinsam mit Berg vorstellte, erklärte: „Die aktuelle Bitkom-Studie macht deutlich, wie wichtig eine resiliente Wirtschaft für den Standort Deutschland ist. Die Corona-Pandemie hat die Notwendigkeit drastisch verstärkt. Nur durch eine intensive Zusammenarbeit zwischen Wirtschaft und Behörden können wir den Bedrohungen

durch Sabotage und Spionage effektiv entgegentreten.“

Social Engineering Startpunkt vieler Angriffe, Homeoffice zusätzliches Einfallstor

Ein Großteil der Angriffe beginnt mit Social Engineering, der Manipulation von Beschäftigten. Die Kriminellen nutzen den „Faktor Mensch“ als vermeintlich schwächstes Glied der Sicherheitskette aus, um etwa sensible Daten wie Passwörter zu erhalten. Bei 41 Prozent der befragten Unternehmen gab es zuletzt solche Versuche – 27 Prozent der Befragten gaben an, unter anderem per Telefon kontaktiert worden zu sein, 24 Prozent per E-Mail. Das dürfte vor allem auch auf die veränderten Arbeitsbedingungen im Zuge der Corona-Pandemie zurückzuführen sein.

59 Prozent der befragten Unternehmen, bei denen Homeoffice grundsätzlich möglich ist (817 Unternehmen), gaben an, seit Beginn der Pandemie habe es IT-Sicherheitsvorfälle gegeben, die auf die Heimarbeit zurückzuführen seien. In 24 Prozent dieser Unternehmen sei das sogar häufig geschehen. Sofern ein Angriff mit dem Homeoffice in Verbindung stand, ist daraus in der Hälfte der Fälle (52 Prozent) auch ein Schaden entstanden. Berg: „Mitarbeiterinnen und Mitarbeiter einfach zum Arbeiten nach Hause zu schicken, genügt nicht. Ihre Geräte müssen gesichert, die Kommunikationskanäle zum Unternehmen geschützt und die Belegschaft für Gefahren sensibilisiert werden. Wer das nicht tut, verhält sich fahrlässig.“

Als Reaktion auf die verschärfte Bedrohungslage haben die Unternehmen ihre Investitionen in IT-Sicherheit aufgestockt: 24 Prozent haben sie deutlich erhöht, 39 Prozent etwas. In 33 Prozent der Unternehmen sind die Ausgaben unverändert geblieben. Gemessen am gesamten IT-Budget sind die Aufwendungen für ein Mehr an Sicherheit aber weiter gering. Durchschnittlich 7 Prozent ihrer IT-Mittel setzen die Unternehmen für IT-Sicherheit ein.

Malware, DDoS-Angriffe und Spoofing auf dem Vormarsch

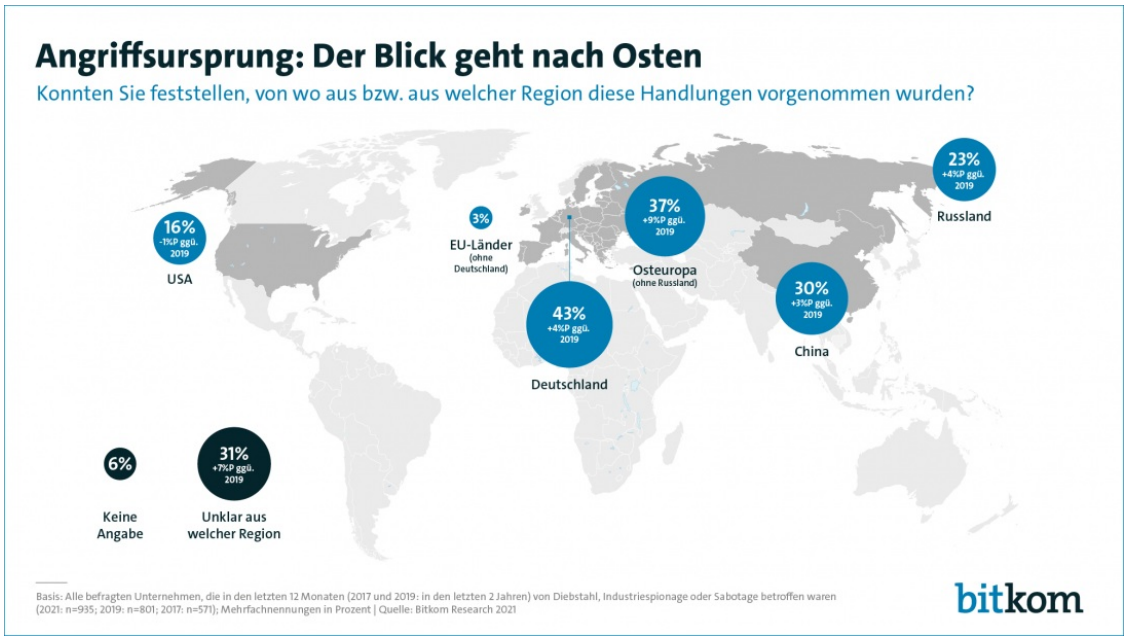
Die Infizierung mit Schadsoftware setzt die deutsche Wirtschaft besonders unter Druck: Schadsoftware hat 2020/2021 in 31 Prozent der befragten Unternehmen Schäden verursacht. Sogenannte DDoS-Attacken, bei denen Angreifer bestimmte Ressourcen gezielt überlasten und zum Beispiel Server mit massenhaften Anfragen in die Knie zwingen, betrafen 27 Prozent. Spoofing, das Vortäuschen einer falschen Identität, und Phishing, das Abfangen persönlicher Daten, haben in 20 bzw. 18 Prozent der Unternehmen Schäden verursacht. Besonders stark stieg die Zahl der Spoofing-Versuche. Sie wuchs im Vergleich zu den Jahren 2018/2019 um 12 Prozentpunkte. Das Angriffsgeschehen mit DDoS-Attacken stieg um 9 Prozentpunkte.

Kommunikationsdaten und geistiges Eigentum im Fokus der Angreifer

Dabei haben es Datendiebe mehr denn je auf Kommunikationsdaten und geistiges Eigentum abgesehen. In 63 Prozent der Unternehmen, in denen zuletzt sensible digitale Daten gestohlen wurden, handelte es sich um Kommunikationsdaten. Geistiges Eigentum wie Patente oder Forschungsinformationen wurden bei 18 Prozent gestohlen – ein Plus von 11 Prozentpunkten gegenüber den Jahren 2018/2019. Darüber hinaus wurden unkritische Geschäftsdaten (44 Prozent), Kundendaten (31 Prozent), Finanzdaten (29 Prozent) und kritische Geschäftsinformationen wie Marktanalysen (19 Prozent) erbeutet. In 19 Prozent der Fälle wurden Zugangsdaten zu Cloud-Diensten entwendet.

Organisierte Kriminalität wächst weiter

Ein Blick auf die Beteiligten, von denen die schädigenden Handlungen ausgehen (Mehrfachnennungen möglich) zeigt: In 61 Prozent der von Diebstahl, Spionage und Sabotage betroffenen Unternehmen wurden Schäden durch Mitarbeiterinnen und Mitarbeiter verursacht, teils auch nachdem sie bereits aus dem betroffenen Unternehmen ausgeschieden waren. 42 Prozent der betroffenen Unternehmen berichten von Mitarbeiterinnen und Mitarbeitern, die unabsichtlich gehandelt haben. 28 Prozent der Unternehmen gehen dagegen davon aus, dass Schäden vorsätzlich herbeigeführt wurden. Eine unzureichend geschulte oder unaufmerksame Belegschaft und Innentäter bleiben damit ein zentrales Problem für die deutsche Wirtschaft. Viele Angriffe kommen aber von außen, beispielsweise von Privatpersonen bzw. Hobby-Hackern (40 Prozent). Der stärkste Zuwachs im Vergleich zu den Vorjahren ist allerdings der organisierten Kriminalität zuzurechnen: In den Jahren 2016/2017 führten 7 Prozent der betroffenen Unternehmen Attacken auf organisierte Kriminalität zurück, 2018/2019 bereits 21 Prozent. 2020/2021 ist der Wert nun auf 29 Prozent gestiegen.



Die meisten Angriffe kommen aus Deutschland: 43 Prozent der geschädigten Unternehmen vermuten die Täterinnen und Täter im Inland. 37 Prozent geben an, die Handlungen wurden aus Osteuropa (ohne Russland) vorgenommen (2018/2019: 28 Prozent). China (30 Prozent) und Russland (23 Prozent) wurden ebenfalls häufig als Ursprungsregionen identifiziert; seltener die USA (16 Prozent). Indes konnten 31 Prozent der Unternehmen keine Angaben machen, woher sie angegriffen wurden. Dieser Wert stieg im Vergleich zu den Jahren 2018/2019 um 7 Prozentpunkte – ein Indiz für erfolgreichere Verschleierungstaktiken der Angreifer.

Keine Entspannung in Sicht: Kritische Infrastruktur besonders bedroht

In den kommenden Monaten wird die Bedrohungslage durch Cyberattacken sogar noch ernster, so die in der deutschen Wirtschaft dominierende Meinung: 83 Prozent der Unternehmen befürchten, die Zahl der Angriffe werde bis Ende dieses Jahres zunehmen, 45 Prozent rechnen dabei sogar mit einer starken Zunahme. Besonders bedroht sehen sich Betreiber kritischer Infrastrukturen (52 Prozent erwarten starke Zunahme von Angriffen auf ihr Unternehmen) und mittlere Unternehmen mit 100 bis 499 Mitarbeiterinnen und Mitarbeitern (50 Prozent erwarten starke Zunahme).

Die größte Gefahr messen Unternehmen dabei Angriffen mit Ransomware zu. 96 Prozent halten solche Attacken für bedrohlich. Die Ausnutzung neuer Sicherheitslücken (Zero-Day-Schwachstellen) fürchten 95 Prozent der Unternehmen. Auch Spyware-Angriffe (83 Prozent), Angriffe mit Quantencomputern (79 Prozent) sowie eingebaute Hintertüren, sogenannte „Backdoors“ (78 Prozent) werden von der Wirtschaft als bedrohlich erachtet.

Um künftig besser vor Diebstahl, Spionage und Sabotage geschützt zu sein, erwartet die deutsche Wirtschaft wirksame politische Antworten: Jeweils 99 Prozent der Unternehmen fordern ein stärkeres Vorgehen gegen Cyberattacken aus dem Ausland, eine verstärkte EU-weite Zusammenarbeit bei Cybersicherheit und einen besseren Austausch zu IT-Sicherheit zwischen Staat und Wirtschaft. 94 Prozent wünschen sich ein Förderprogramm für mehr IT-Sicherheit im Homeoffice. Einen stärkeren Einsatz der Politik, um Unternehmen vor Cyberangriffen zu schützen, erhoffen sich 85 Prozent der Unternehmen.

Bitkom-Präsident Berg appellierte bereits jetzt an die kommende Bundesregierung: „Der Schutz der deutschen Wirtschaft entscheidet wesentlich über den Erfolg und die Strahlkraft des Wirtschaftsstandorts Deutschland. Neben dem offenen und ehrlichen Dialog mit der Wirtschaft braucht es in der kommenden Legislaturperiode mehr Tatkraft auf allen Ebenen“, so Berg. Die Stärkung des Wirtschaftsschutzes und der Aufbau notwendiger Cyber-Resilienz könnten nur gelingen, „wenn die nächste Bundesregierung den Schulterschluss mit der Wirtschaft sucht.“

Dazu hat der Bitkom konkrete Handlungsempfehlungen für die nächste Legislaturperiode erarbeitet und diese heute erstmalig veröffentlicht. Die notwendigen Maßnahmen reichen von der Vereinfachung staatlicher Zuständigkeitsstrukturen über die Bereitstellung von Echtzeitinformationen zur Cyber-Bedrohungslage bis hin zu einem notwendigen Paradigmenwechsel im Bildungsbereich.

Die Handlungsempfehlungen stehen zum kostenlosen Download bereit unter:
https://www.bitkom.org/Bitkom/Publikationen/Forderungspapier-Cybersicherheit-zur-Bundestagswahl

Hinweis zur Methodik: Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt hat. Dabei wurden 1.067 Unternehmen mit 10 oder mehr Mitarbeiterinnen und Mitarbeitern befragt. Die Interviews wurden mit Führungskräften durchgeführt, die in ihrem Unternehmen für das Thema Wirtschaftsschutz verantwortlich sind. Dazu zählen Geschäftsführerinnen und Geschäftsführer sowie Führungskräfte aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder 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

Link zur Presseinformation auf der Webseite:
https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr