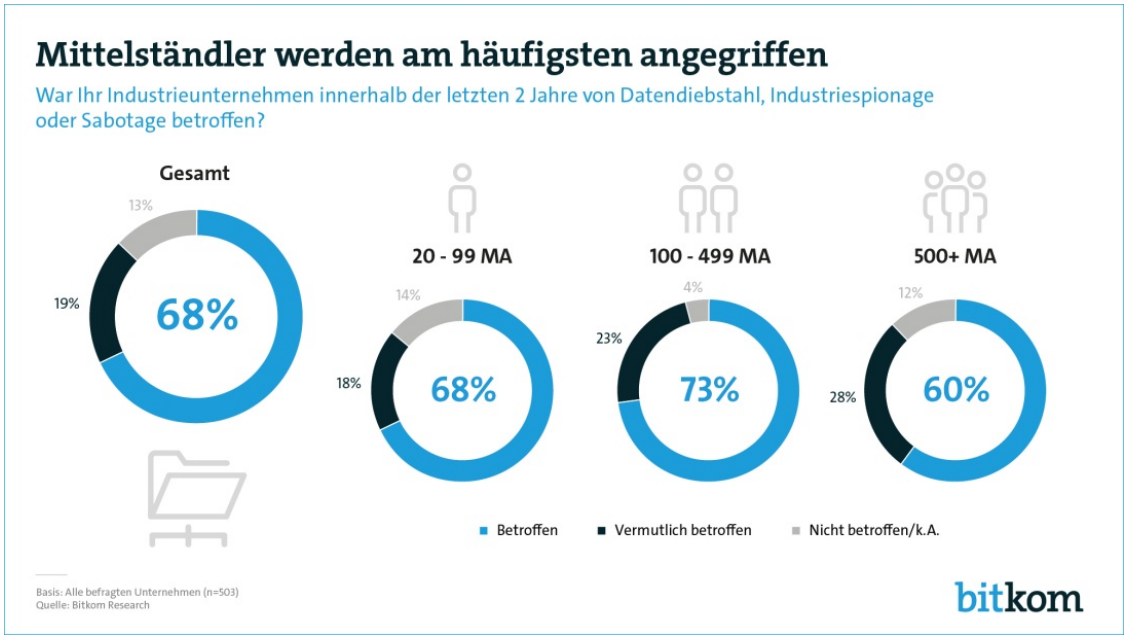
Bitkom e.V. |

Attacken auf deutsche Industrie verursachten 43 Milliarden Euro Schaden

- 7 von 10 Industrieunternehmen wurden Opfer von Sabotage, Datendiebstahl oder Spionage in den vergangenen zwei Jahren



Berlin, 13. September 2018 - Kriminelle Attacken treffen Industrieunternehmen besonders hart: Durch Sabotage, Datendiebstahl oder Spionage ist der deutschen Industrie in den vergangenen beiden Jahren ein Gesamtschaden von insgesamt 43,4 Milliarden Euro entstanden. Sieben von zehn Industrieunternehmen (68 Prozent) sind in diesem Zeitraum Opfer entsprechender Angriffe geworden, jedes fünfte Unternehmen (19 Prozent) vermutet dies. Das ist das Ergebnis einer Studie des Digitalverbands Bitkom, für die 503 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Industriebranchen repräsentativ befragt wurden. „Mit ihren Weltmarktführern ist die deutsche Industrie besonders interessant für Kriminelle“, sagte Bitkom-Präsident Achim Berg bei der Vorstellung der Studie in Berlin. „Wer nicht in IT-Sicherheit investiert, handelt fahrlässig und gefährdet sein Unternehmen.“ So wurden in den vergangenen zwei Jahren bei einem Drittel der Unternehmen (32 Prozent) IT- oder Telekommunikationsgeräte gestohlen, bei fast einem Viertel (23 Prozent) sind sensible digitale Daten abgeflossen. „Illegaler Wissens- und Technologietransfer, Social Engineering und auch Wirtschaftssabotage sind keine seltenen Einzelfälle, sondern ein Massenphänomen“, betonte Thomas Haldenwang, Vizepräsident des Bundesamtes für Verfassungsschutz (BfV).

Nicht nur Diebstahl macht der Industrie zu schaffen. Jedes fünfte Industrieunternehmen (19 Prozent) berichtet von digitaler Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen. Weitere 28 Prozent vermuten, dass es solch einen Vorfall bei ihnen gab. Bei 11 Prozent wurde die digitale Kommunikation ausgespäht, beispielweise E-Mails oder Messenger-Dienste. Insgesamt haben digitale IT-Angriffe bei fast der Hälfte der Befragten (47 Prozent) einen Schaden verursacht. Klassische analoge Attacken sind für die Industrie auch ein Thema, fallen aber vergleichsweise weniger ins Gewicht. 21 Prozent der Befragten haben einen Diebstahl von sensiblen physischen Dokumenten, Unterlagen, Mustern oder Maschinen festgestellt, bei 10 Prozent kam es in den vergangenen zwei Jahren zur analogen Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen, z.B. durch die Manipulation von Geräten vor Ort in Unternehmen. Dazu BfV-Vizepräsident Haldenwang: „Neben der klassischen Wirtschaftsspionage beschäftigen uns vermehrt Attacken, bei denen davon ausgegangen werden muss, dass Schadsoftware mit dem Ziel in IT-

Systeme eingebracht wird, Sabotage-Akte vorzubereiten“.

Kritische Unternehmensdaten im Visier von Angreifern

Angreifer haben im Rahmen ihrer Attacken unterschiedlich sensible Daten erbeutet. Bei fast der Hälfte (48 Prozent) der betroffenen Industrieunternehmen wurden Kommunikationsdaten wie Emails gestohlen. Bei jedem fünften Unternehmen sind durch digitale Angriffe jeweils Kundendaten (21 Prozent) und Finanzdaten (20 Prozent) abgeflossen. Patente und Ergebnisse aus Forschung und Entwicklung sind bei jedem zehnten Unternehmen (10 Prozent) in kriminelle Hände gefallen. „Viele Unternehmen nehmen das Thema Sicherheit noch zu sehr auf die leichte Schulter, auch weil ihnen das entsprechende Know-how fehlt“, so Berg. „Erster und wichtigster Schritt ist, IT-Sicherheit im Unternehmen zur Chefsache zu machen.“

Dabei stammen die Täter häufig aus den eigenen Reihen. Bei fast zwei Drittel der Betroffenen (63 Prozent) gingen Delikte von ehemaligen oder derzeitigen Mitarbeitern aus. Die Hälfte der geschädigten Unternehmen (48 Prozent) hat Kunden, Lieferanten, externe Dienstleister oder Wettbewerber als Täter identifiziert. Bei drei von zehn (29 Prozent) waren es Privatpersonen oder Hobbyhacker, 17 Prozent der Betroffenen berichten von organisierter Kriminalität, jedes neunte betroffene Unternehmen (11 Prozent) gibt ausländische Nachrichtendienste als Täter an.

Aufmerksame Mitarbeiter als effektivster Schutz

Mitarbeiter sind es, die auf der anderen Seite aber auch dafür sorgen, dass kriminelle Handlungen aufgedeckt werden. Sechs von zehn betroffenen Industrieunternehmen (61 Prozent) sind so erstmalig auf Angriffe aufmerksam geworden. 40 Prozent der Betroffenen erhielten Hinweise auf Angriffe durch eigene Sicherheitssysteme, bei fast einem Viertel (23 Prozent) war es hingegen reiner Zufall. Nur bei 3 Prozent der Unternehmen gingen erste Hinweise auf Delikte durch externe Strafverfolgungs- oder Aufsichtsbehörden ein. „Der effektivste Schutz vor Spionage, Diebstahl oder Sabotage sind motivierte, gut geschulte und aufmerksame Mitarbeiter“, sagte Berg.

Künftige Bedrohungen sehen Unternehmen vor allem durch digitale Angriffe. Nahezu alle Befragten (97 Prozent) nennen sogenannte Zero-Day-Exploits als größte Gefahr. Dabei nutzen Angreifer Sicherheitslücken in Software aus, die bis dahin unbekannt waren. 93 Prozent fürchten die Infizierung mit Schadsoftware, zwei Drittel (68 Prozent) geben den Mangel an qualifizierten IT-Sicherheitskräften als Bedrohung an. Die zunehmende Fluktuation von Mitarbeitern ist für 58 Prozent der Unternehmen ein Risiko. Dass Kriminelle die Rechenleistungen von Internetnutzern anzapfen, etwa zum unbemerkten Schürfen von Kryptowährungen, nehmen hingegen nur 29 Prozent der Unternehmen als echte Gefahr wahr.

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

Direktlink: ***https://www.bitkom.org/Presse/Presseinformation/Attacken-auf-deutsche-Industrie-verursachten-43-Milliarden-Euro-Schaden.html***