

Cyberangriffe aus China: Deutsche Unternehmen in alarmierender Gefahr

Eine Bitkom-Studie enthüllt, dass Cyberangriffe auf die deutsche Wirtschaft zunehmend aus China gesteuert werden.

Die Bedrohung durch Cyberangriffe hat sich für viele deutsche Unternehmen in den letzten Jahren erheblich verschärft. Eine aktuelle Umfrage des Digitalverbands Bitkom, die über 1.000 Unternehmen befragte, zeigt ein besorgniserregendes Bild: Ein Großteil der Angriffe auf die deutsche Wirtschaft kommt nachweislich aus China. Bis zu 45 Prozent der Unternehmen, die betroffen sind, können die Angriffe direkt auf die Volksrepublik zurückverfolgen.

Die Studie, die vor kurzem in Berlin veröffentlicht wurde, verdeutlicht, dass China 2023 zur primären Quelle für Cyberangriffe auf die deutsche Wirtschaft geworden ist. Diese Entwicklung ist alarmierend, da viele Unternehmen nun mit enormen finanziellen Schäden rechnen müssen. Die prognostizierten Verluste belaufen sich auf mehr als 250 Milliarden Euro. Besonders auffällig ist der Anstieg der Bedrohung durch organisierte Kriminalität, die von den befragten Firmen in 70 Prozent der Fälle als verantwortliche Täter vermutet wird.

Die Täter und ihre Motivationen

Die Umfrage brachte weitere interessante Erkenntnisse über die Ursprünge der Cyberangriffe. 39 Prozent der Firmen glaubten, dass ihre Angreifer aus Russland stammten, während 20 Prozent

von einem deutschen Standort aus attackiert wurden. Ein Viertel der Unternehmen vermutet, dass die Angreifer aus den USA kamen. Darüber hinaus waren auch Hacker aus Osteuropa und der Europäischen Union in einem signifikanten Teil der Angriffe involviert.

Ein alarmierender Trend zeigt sich auch in der Anzahl der Angriffe und deren Häufigkeit: 81 Prozent der befragten Unternehmen berichteten, dass sie in den letzten zwölf Monaten Ziel von Datendiebstahl, Industriespionage und Sabotageangriffen geworden waren. Diese Angriffe waren nicht nur digital, sondern umfassten auch physische Bedrohungen wie das Abhören von Besprechungen.

Ein wesentlicher Teil der Angriffe wurde zudem als persönliche Racheakte von ehemaligen und aktiven Mitarbeitern eingestuft. Diese Erkenntnis unterstreicht die Notwendigkeit für Unternehmen, nicht nur technische Schutzmaßnahmen zu ergreifen, sondern auch eine Kultur des Vertrauens und der Sicherheit innerhalb der Belegschaft zu fördern.

Wichtige Schutzmaßnahmen für die Unternehmen

Angesichts der dramatisch steigenden Bedrohung sehen sich zwei Drittel der Unternehmen (65 Prozent) in ihrer Existenz gefährdet, eine signifikante Steigerung im Vergleich zu den Vorjahren. Bitkom-Präsident Ralf Wintergerst betont die Dringlichkeit, die Sicherheitsvorkehrungen zu stärken. „Die Unternehmen müssen ihre Schutzmaßnahmen weiter hochfahren“, sagte er, und verwies auf die Notwendigkeit, sich sowohl gegen digitale als auch gegen traditionelle Angriffe abzusichern.

In dieser kritischen Zeit müssen Unternehmen innovative Strategien entwickeln, um sich besser zu verteidigen. Dies könnte die Implementierung neuer Technologien, umfassende Schulungen für die Mitarbeiter oder auch die Zusammenarbeit

mit externen Sicherheitsexperten umfassen. Die aktuelle Lage erfordert schnelles Handeln, um die Integrität und den Fortbestand der Unternehmen in einem zunehmend feindlichen digitalen Umfeld zu gewährleisten.

dpa/con

Details

Besuchen Sie uns auf: [n-ag.de](https://www.n-ag.de)