NACHRICHTEN AG

28. August 2024

Cyberangriffe aus China: Bedrohung für die deutsche Wirtschaft wächst

Immer häufiger kommen Cyberangriffe aus China auf deutsche Firmen, wie eine aktuelle Bitkom-Studie zeigt. 65% der Unternehmen fühlen sich bedroht.

Die zunehmende Bedrohung durch Cyberangriffe auf Unternehmen in Deutschland ist alarmierend. Laut einer Studie des Digitalverbands Bitkom, die kürzlich in Berlin vorgestellt wurde, hat sich China im vergangenen Jahr zur Hauptquelle für diese Angriffe entwickelt. Von über 1.000 befragten Unternehmen gaben 45 Prozent an, die Angriffe auf ihre Systeme zurückverfolgen zu können. Im Gegensatz zu den Vorjahren zeigen die Zahlen, dass auch andere Länder wie Russland und die USA immer wieder im Verdacht stehen, Cyberattacken durchzuführen.

Besonders besorgniserregend ist die Tatsache, dass 36 Prozent der angegriffenen Firmen nicht eindeutig bestimmen konnten, woher die Angriffe kamen. Dazu kommt, dass 20 Prozent der Opfer vermuten, dass die Angreifer ihren Sitz innerhalb Deutschlands hatten, während 25 Prozent aus den USA als mögliche Quelle für Angriffe sahen. Auch die Aktivitäten von Hackern aus Osteuropa sind nicht zu unterschätzen, die laut den Befragten für etwa 32 Prozent der Vorfälle verantwortlich gemacht werden. Der Mangel an klaren Informationen über die Herkunft der Angreifer macht es schwierig, gezielte Abwehrmaßnahmen zu ergreifen.

Ursprung und Motivation der Angriffe

Die Täter hinter diesen Angriffen sind vielfältig und werden häufig der organisierten Kriminalität zugeordnet. Über 70 Prozent der betroffenen Firmen sehen hier die Hauptursache. In der Befragung gaben 20 Prozent der Unternehmen an, auch ausländische Geheimdienste könnten hinter den Attacken stecken, was einen signifikanten Anstieg im Vergleich zu den 7 Prozent des Vorjahres darstellt. Zudem vermuten 27 Prozent der Angriffe, dass ehemalige oder aktuelle Mitarbeiter motiviert waren, hier Rache zu üben.

Die enormen finanziellen Auswirkungen dieser Cyberangriffe sind nicht zu unterschätzen. Bitkom schätzt den insgesamt entstandenen Schaden auf rund 267 Milliarden Euro, was eine Steigerung von 29 Prozent im Vergleich zum Vorjahr darstellt. Dies bedeutet, dass die Bedrohung durch Industriespionage, sowohl digital als auch analog, für viele Unternehmen tatsächlich existenziell sein könnte.

Die Herausforderung für Unternehmen

Bitkom-Präsident Ralf Wintergerst betont die Dringlichkeit, mit der Unternehmen ihre Sicherheitsmaßnahmen steigern müssten. „Die Bedrohungslage für die deutsche Wirtschaft verschärft sich“, sagt er und fordert verstärkte Anstrengungen sowohl gegen digitale Bedrohungen als auch gegen klassische Methoden wie das Abhören von Meetings oder den Diebstahl von physischen Dokumenten. Diese Sichtweise ist nicht nur eine reaktive Haltung, sondern eine proaktive Notwendigkeit in einer zunehmend digitalisierten Welt.

Die Umfrage verdeutlicht auch einen besorgniserregenden Trend: Zwei Drittel der Unternehmen, das sind 65 Prozent, fühlen sich durch Cyberangriffe in ihrer Existenz bedroht. Damit hat sich die Angst vor Cyberangriffen innerhalb eines Jahres deutlich erhöht; ein Jahr zuvor waren es noch 52 Prozent, und im Jahr 2021 waren es gerade einmal 9 Prozent. Diese Entwicklungen zeigen, dass die digitale Landschaft für Unternehmen zunehmend riskanter geworden ist.

Angesichts dieser alarmierenden Situation ist es von größter Bedeutung, dass Unternehmen nicht nur auf aktuelle Bedrohungen reagieren, sondern auch langfristige Strategien zur Risikominderung entwickeln. Klare Kenntnisse über potenzielle Angreifer und deren Methoden müssen genauso entwickelt werden wie effektive Sicherheitsprotokolle und Schulungen für Mitarbeiter. Während die Zahlen steigend sind und die Gefahren immer klarer werden, steht die deutsche Wirtschaft vor der Herausforderung, kreative und wirkungsvolle Lösungen zur Abwehr von Angriffen zu finden.

Wachsamkeit und Innovation als Schlüssel

Für Unternehmen bedeutet dies letztlich, dass sie auf Wachsamerkeit und Innovation setzen müssen, um den sich ständig verändernden Bedrohungen aus der digitalen Welt zu begegnen. Die Implementierung neuer Technologien und eine kontinuierliche Schulung der Mitarbeiter im Umgang mit Cyberbedrohungen sind essenziell, um nicht nur die Sicherheit der Firmendaten zu garantieren, sondern auch das Vertrauen der Kunden langfristig zu sichern. In einer Zeit, in der Cyberangriffe immer ausgefeilter und häufiger werden, ist es entscheidend, die eigene Sicherheitsarchitektur regelmäßig zu überprüfen und anzupassen.

Die zunehmenden Cyberangriffe auf die deutsche Wirtschaft sind nicht nur alarmierend, sondern auch ein Symptom für ein größeres Problem im globalen digitalen Raum. Die Komplexität und die zunehmende Professionalität der Angreifer stellen sowohl Unternehmen als auch Regierungen vor große Herausforderungen. Angesichts der steigenden Anzahl an Angriffen ist es entscheidend, dass Unternehmen effektive Strategien entwickeln, um ihre Daten und Systeme zu schützen. Unternehmen investieren zunehmend in Cybersecurity-Maßnahmen, jedoch ist die Umsetzung oft noch nicht ausreichend, um die Bedrohungen abzuwenden.

Die Politik muss ebenfalls aktiver werden, um

Rahmenbedingungen zu schaffen, die den Schutz von Unternehmen verbessern. Dazu gehört unter anderem die Einführung verbindlicher Sicherheitsstandards sowie die Förderung von Kooperationen zwischen öffentlichen und privaten Einrichtungen, um schnell auf Vorfälle reagieren zu können. Der Austausch von Informationen über Bedrohungen und Sicherheitsvorfälle kann, wenn er richtig gestaltet ist, einen enormen Mehrwert bieten.

Zusammenspiel von Technologie und Bedrohungen

Ein wesentlicher Faktor, der zu der Zunahme von Cyberangriffen beiträgt, ist die rasante Entwicklung von Technologien, die sowohl von Unternehmen als auch von Angreifern genutzt werden. Viele Unternehmen haben in den letzten Jahren verstärkt auf Cloud-Dienste und IoT (Internet of Things) gesetzt, was die Angriffsflächen erheblich erweitert hat. Mit der Digitalisierung von Geschäftsprozessen ist die Herausforderung, das richtige Gleichgewicht zwischen Innovation und Sicherheit zu finden, größer denn je.

Zudem nutzen Angreifer immer ausgeklügeltere Methoden, um in Systeme einzudringen. Techniken wie Phishing, Ransomware und DDoS-Angriffe kommen immer häufiger zum Einsatz. Laut dem Bericht von Statista zu Cybercrime in Deutschland hat sich die Zahl der Cyberkriminalitätsfälle im Jahr 2022 auf über 100.000 erhöht, was einem Anstieg von 40 Prozent im Vergleich zum Vorjahr entspricht. Unternehmen sind gut beraten, ihre Mitarbeiter regelmäßig zu schulen und über potenzielle Bedrohungen aufzuklären, um die menschliche Fehleranfälligkeit zu reduzieren.

Rechtliche und wirtschaftliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen für den Schutz von

Unternehmen gegen Cyberangriffe sind in Deutschland und der EU strenger geworden. Die Datenschutz-Grundverordnung (DSGVO) verpflichtet Unternehmen zur Einhaltung sehr spezifischer Regelungen, die auch den Schutz personenbezogener Daten betreffen. Bei einem Datenverlust können schwerwiegende rechtliche Konsequenzen drohen, die zusätzlich zu den finanziellen Schäden durch den Angriff selbst kommen.

Die Investitionen in Cybersecurity sind nicht nur eine Reaktion auf unmittelbare Bedrohungen, sondern auch eine strategische Notwendigkeit für Unternehmen, die langfristig im digitalen Zeitalter erfolgreich sein wollen. Laut einer Prognose des Marktforschungsunternehmens Gartner wird erwartet, dass die globalen Ausgaben für IT-Sicherheit bis 2025 auf über 170 Milliarden Euro anwachsen werden. Dies zeigt, dass Unternehmen die Risiken ernst nehmen und bereit sind, Investitionen zu tätigen, um ihre Cyberabwehr zu stärken.

Details