NACHRICHTEN AG

28. August 2024

Cyberangriffe aus China: Eine wachsende Bedrohung für die deutsche Wirtschaft

China wird zur größten Bedrohung für die deutsche Wirtschaft: 81% der Firmen erlebten Cyberangriffe. Studie zeigt alarmierende Trends.

Im Jahr 2023 hat China eine beunruhigende Rolle als Hauptursprung von Cyberangriffen auf die deutsche Wirtschaft eingenommen. Diese Erkenntnisse stammen aus einer aktuellen Studie des Digitalverbands Bitkom, die eine umfassende Befragung von über 1.000 Unternehmen in verschiedenen Branchen in Berlin durchgeführt hat. Die Daten zeigen, dass 45 Prozent der befragten Firmen angaben, die Angriffe auf ihre Systeme in China zurückverfolgen zu können. Im Vergleich dazu lag dieser Anteil im Vorjahr bei 42 Prozent.

Diese Entwicklung ist alarmierend, da sie die globalen Tendenzen im Bereich der Cyberkriminalität widerspiegelt. Neben dem näher rückenden Einfluss aus China, gaben 39 Prozent der betroffenen Unternehmen an, dass Russland der Ursprung ihrer Angriffe gewesen sei. Im Jahr zuvor war dieser Anteil noch höher, nämlich bei 46 Prozent. Der Bericht zeigt zudem, dass ein Drittel der gefragten Firmen (36 Prozent) keine klaren Informationen über die Angreifer hatte und dass 20 Prozent der Angriffe möglicherweise sogar von Deutschland aus initiiert wurden.

Die Täter im Visier

Die Ergebnisse decken auch auf, wer die Hauptverdächtigen

hinter diesen Cyberattacken sind. Die Unternehmen vermuten, dass sich hinter 70 Prozent der Angriffe organisierte Kriminalität verbirgt. Dies ist ein deutliches Warnsignal, da kriminelle Vereinigungen immer raffinierter und gezielter vorgehen. Daneben wurden ausländische Nachrichtendienste in 20 Prozent der Fälle als mögliche Täter identifiziert – ein Anstieg von nur 7 Prozent im Vorjahr. Zudem wird angenommen, dass 27 Prozent der Cyberangriffe als Racheakte von ehemaligen oder aktuellen Mitarbeitern motiviert waren.

Die Studie verdeutlicht auch das enorme Ausmaß der Bedrohungen, die die Firmen in Deutschland ausgesetzt sind. Eine erschreckende Zahl von 81 Prozent der Unternehmen berichtete, dass sie in den letzten zwölf Monaten Opfer von Diebstahl, Industriespionage und Sabotage geworden sind. Darüber hinaus vermuten weitere 10 Prozent, solche Vorfälle in ihrem Betrieb erlebt zu haben. Der geschätzte finanzielle Schaden durch diese Angriffe beläuft sich auf ca. 267 Milliarden Euro, was einen Anstieg von 29 Prozent im Vergleich zum Vorjahr darstellt.

Existenzielle Bedrohung für Firmen

Bitkom-Präsident Ralf Wintergerst äußerte sich besorgt über die sich verschärfende Bedrohungslage für die deutsche Wirtschaft. Er betont die Notwendigkeit, dass Unternehmen ihre Schutzmaßnahmen – sowohl im digitalen als auch im physischen Bereich – verstärken müssen. Diese Aufforderung zum Handeln wird dringlicher, je mehr sich die Auswirkungen von Cyberangriffen zeigen. Laut der Studie fühlen sich mittlerweile zwei Drittel der Unternehmen (65 Prozent) in ihrer Existenz durch Cyberangriffe ernsthaft bedroht, was einen dramatischen Anstieg im Vergleich zu 52 Prozent im Vorjahr darstellt.

Diese Situation ist nicht einfach eine Geschäftsweltgedöns; es ist ein ernstes Problem, das Auswirkungen auf die wirtschaftliche Stabilität in Deutschland haben kann. Die Unternehmen sind gefordert, proaktive Maßnahmen zur Sicherung ihrer Daten und

Systeme zu ergreifen, um so den steigenden Risiken begegnen zu können. In diesem Kontext können umfassende Schulungen der Mitarbeiter und Investitionen in modernste Sicherheitstechnologien von entscheidender Bedeutung sein, um den Gefahren aus dem Cyberraum zu trotzen.

Wachsende Cyberbedrohungen aus dem Osten

Die Entwicklungen sind ein klares Signal, dass die Cyberkriminalität ein immer größer werdendes Risiko darstellt, besonders in Bezug auf geostrategische Spannungen. Mit dem zunehmenden Einfluss Chinas auf die internationale Bühne wird auch die Bereitschaft zu Cyberangriffen wahrscheinlicher. Unternehmen müssen nun ihre Strategien überdenken und Sicherheitsarchitekturen entwickeln, die so resistent wie möglich gegen Bedrohungen aus dem Ausland sind.

Das wachsende Problem der Cyberangriffe auf deutsche Unternehmen hat auch internationale Implikationen. Der Anstieg von Cyberoperationen, die auf strategische Sektoren abzielen, führt zu einer verstärkten Zusammenarbeit zwischen verschiedenen Ländern im Bereich der Cyberabwehr. Dies geschieht vor dem Hintergrund, dass viele Staaten erkennen, wie wichtig die Sicherheit ihrer digitalen Infrastruktur ist. In diesem Kontext hat die EU Initiativen zur Verbesserung der Cyber-Sicherheitsstandards angestoßen und einen gemeinsamen Rahmen für die Cybersicherheit in den Mitgliedsstaaten gefordert. Dies zeigt, wie interdependent die Sicherheitsarchitekturen von Staaten in einer zunehmend vernetzten Welt geworden sind.

Über Ländergrenzen hinweg wird es für Unternehmen immer wichtiger, sicherzustellen, dass ihre Systeme robust genug sind, um gegen Bedrohungen gewappnet zu sein, die von verschiedenen Akteuren ausgehen. Die verstärkten Richtlinien und Standards der EU, wie etwa die EU-Cybersecurity-Strategie, zielen darauf ab, die Reaktionsfähigkeit der Mitgliedstaaten zu

erhöhen und eine gemeinsame Front gegen Cyberkriminalität zu bilden. Diese Maßnahmen sind besonders relevant für die deutschen Unternehmen, die einen hohen Anteil an kritischer Infrastruktur besitzen und Exportwirtschaften sind.

Auswirkungen auf die Unternehmen

Die wachsende Bedrohung durch Cyberangriffe hat nicht nur finanzielle Auswirkungen, sondern beeinflusst auch die strategische Ausrichtung von Unternehmen. Viele Firmen investieren zunehmend in Cybersecurity-Lösungen und schulen ihre Mitarbeiter, um Sicherheitsbewusstsein zu fördern. Laut einer Umfrage von Bitkom haben 70 Prozent der Unternehmen Sicherheitsmaßnahmen verstärkt oder neue Technologien implementiert, um sich besser zu schützen.

Zudem hat der Anstieg der Cyberangriffe zu einer verstärkten Diskussion über Haftung und Regulierung geführt. Unternehmen sehen sich zunehmend in der Verantwortung, sicherzustellen, dass ihre Systeme gegen Angriffe geschützt sind und dass sie auf solche Vorfälle vorbereitet sind. Dies hat auch rechtliche Konsequenzen, da Verletzungen von Datensicherheitsrichtlinien zu hohen Strafen führen können, wie sie seit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) in der EU verhängt werden.

Ein Blick auf die Statistiken

Die Ergebnisse der Umfrage von Bitkom offenbaren alarmierende Trends. Unternehmen berichteten 2023 von einem Anstieg der Angriffe, was die Notwendigkeit unterstreicht, robuste Sicherheitsstrategien zu entwickeln. 54 Prozent der Befragten gaben an, in den letzten Jahren mindestens einen Cyberangriff erlitten zu haben. Die häufigsten Angriffsarten umfassten Phishing (62 Prozent), Schadsoftware (45 Prozent) und DDoS-Angriffe (34 Prozent). Diese Statistiken verdeutlichen nicht nur die Häufigkeit der Angriffe, sondern auch die Vielseitigkeit der Methoden, die von Angreifern verwendet

werden.

Zusätzlich schätzen Experten, dass sich die finanziellen Auswirkungen von Cyberangriffen auf die deutsche Wirtschaft über die übernommenen Kosten für Software, Schulungen und notwendige Sicherheitsmaßnahmen hinaus erstrecken. Die Gesamtschätzung der wirtschaftlichen Verluste beläuft sich auf mehr als 300 Milliarden Euro im Jahr, was die Dringlichkeit der Problematik verdeutlicht.

Die kontinuierliche Lagebeurteilung und Anpassung der Sicherheitsstrategien ist unerlässlich, da Cyberbedrohungen ständig im Wandel sind. Daher ist die Implementierung einer ganzheitlichen Cybersecurity-Strategie nicht nur wünschenswert, sondern notwendig, um die Integrität der Unternehmen zu wahren und deren langfristige Wettbewerbsfähigkeit zu sichern.

Details