Allianz

Allianz Suisse

26.10.2022 – 07:00 Uhr

AGCS-Report: Ransomware bleibt Top-Cyber-Risiko für Unternehmen, aber neue Bedrohungen nehmen zu

Wallisellen (ots) -

- Cyber-Bericht der Allianz Global Corporate & Specialty: Wachsende Kosten von Ransomware-Angriffen belasten Unternehmen jeder Grösse
- Auch Komplexität und Häufigkeit von Angriffen auf geschäftliche E-Mails nehmen zu
- Aktuelle Risikotrends: erhöhtes Risiko staatlich gesponserter Angriffe, die sich entwickelnde Haftpflichtlandschaft für Dritte, der Mangel an Cybersicherheitsexperten und die Cyber-Governance unter zunehmender ESG-Prüfung
- Bessere Erkenntnisse über Cyberrisiken tragen zur Schaffung eines nachhaltigen Cyberversicherungsmarktes bei

Ransomware-Attacken stellen nach wie vor das grösste Cyber-Risiko für Unternehmen weltweit dar, während die Zahl der Vorfälle steigt, bei denen Geschäfts-E-Mails kompromittiert werden. Dies wird in der "Deep Fake"-Ära weiter zunehmen. Gleichzeitig geben der Krieg in der Ukraine und die allgemeinen geopolitischen Spannungen Anlass zu großer Sorge, da die Feindseligkeiten auf den Cyberspace übergreifen und gezielte Angriffe auf Unternehmen, Infrastruktur oder Lieferketten verursachen könnten, so ein neuer Bericht von Allianz Global Corporate & Specialty (AGCS).

Die Häufigkeit von Ransomware-Angriffen bleibt weltweit hoch, ebenso wie die damit verbundenen Schadenkosten. Im Jahr 2021 gab es einen Rekord von 623 Millionen Angriffen, doppelt so viele wie im Jahr 2020. Obwohl die Häufigkeit in der ersten Jahreshälfte 2022 weltweit um 23% zurückgegangen ist, übersteigt die Gesamtzahl der Ransomware-Angriffe im bisherigen Jahresverlauf immer noch die der Jahre 2017, 2018 und 2019, während die Angriffe in Europa in diesem Zeitraum stark angestiegen sind. Es wird prognostiziert, dass Ransomware bis 2023 weltweit Schäden in Höhe von 30 Mrd. US-Dollar verursachen wird. Aus Sicht der AGCS machte der Wert der Ransomware-Schäden, an denen das Unternehmen zusammen mit anderen Versicherern beteiligt war, in den Jahren 2020 und 2021 weit über 50 % aller Kosten für Cyber-Schäden aus.

Doppelte und dreifache Erpressung die Norm

"Die Kosten für Ransomware-Angriffe sind gestiegen, da die Kriminellen grössere Unternehmen, kritische Infrastrukturen und Lieferketten ins Visier genommen haben. Die Kriminellen haben ihre Taktik verfeinert, um mehr Geld zu erpressen", erklärt Scott Sayce, Global Head of Cyber bei AGCS und Group Head des Cyber Centre of Competence. "Doppel- und Dreifach-Erpressungsangriffe sind jetzt die Norm - neben der Verschlüsselung von Systemen werden zunehmend sensible Daten gestohlen und als Druckmittel für Erpressungsforderungen an Geschäftspartner, Lieferanten oder Kunden verwendet." Die Schwere der Ransomware-Angriffe wird wahrscheinlich eine Hauptbedrohung für Unternehmen bleiben, angeheizt durch die zunehmende Raffinesse der Banden und die steigende Inflation, die sich in den erhöhten Kosten für IT- und Cybersicherheitsspezialisten niederschlägt.

Kleinere und mittelgrosse Unternehmen, denen es oft an Kontrollen und Ressourcen für Investitionen in die Cybersicherheit mangelt, geraten zunehmend ins Visier von Banden, während grössere Unternehmen mehr in die Sicherheit investieren. Die Banden setzen auch eine breite Palette von Belästigungstechniken ein, stimmen ihre Lösegeldforderungen auf bestimmte Unternehmen ab und setzen erfahrene Verhandlungsführer ein, um den Gewinn zu maximieren.

"Wir sehen zwar gute Fortschritte, aber unsere Erfahrung zeigt auch, dass viele Unternehmen ihre Cyber-Kontrollen noch verstärken müssen, insbesondere in Bezug auf IT-Sicherheitsschulungen, eine bessere Netzwerksegmentierung für kritische Umgebungen sowie Reaktionspläne für Cyber-Vorfälle und Sicherheitsmanagement. Als Cyber-Versicherer sind wir bereit, über den reinen Risikotransfer hinauszugehen und unseren Kunden zu helfen, sich an eine sich verändernde Risikolandschaft anzupassen und ihr Schutzniveau zu erhöhen."

Raffinierte Betrügereien

BEC-Angriffe (Business Email Compromise) nehmen weiter zu. Begünstigt wird dies durch die zunehmende Digitalisierung und Verfügbarkeit von Daten, die Verlagerung von Arbeitsplätzen ins Home-Office und zunehmend durch "Deep Fake"-Technologie und virtuelle Konferenzen. Nach Angaben des FBI belaufen sich BEC-Betrügereien von 2016 bis 2021 weltweit auf insgesamt 43 Milliarden US-Dollar, wobei die Zahl der Betrügereien allein zwischen Juli 2019 und Dezember 2021 um 65 % angestiegen ist. Die Angriffe werden immer raffinierter und gezielter, da die Kriminellen nun virtuelle Meeting-Plattformen nutzen, um Mitarbeiter zur Überweisung von Geldern oder zur Weitergabe sensibler Informationen zu bewegen.

Die Bedrohung durch einen Cyberkrieg

Der Krieg in der Ukraine und die allgemeinen geopolitischen Spannungen sind ein wichtiger Faktor, der die Cyber-Bedrohungslandschaft verändert, da sie das Risiko von Spionage, Sabotage und zerstörerischen Cyber-Angriffen gegen Unternehmen mit Verbindungen zu Russland und der Ukraine sowie zu Verbündeten und Unternehmen in Nachbarländern erhöhen.

Staatlich geförderte Cyberangriffe könnten sich gegen kritische Infrastrukturen, Lieferketten oder Unternehmen richten. "Bislang hat der Krieg zwischen Russland und der Ukraine noch nicht zu einem nennenswerten Anstieg der Ansprüche aus Cyberversicherungen geführt, aber er deutet auf ein potenziell erhöhtes Risiko durch Nationalstaaten hin", erklärt Sayce. Obwohl Kriegshandlungen in der Regel von traditionellen Versicherungsprodukten ausgeschlossen sind, hat das Risiko eines hybriden Cyberkriegs die Bemühungen auf dem Versicherungsmarkt beschleunigt, das Thema Krieg und staatlich geförderte Cyberangriffe in den Formulierungen zu berücksichtigen und den Kunden Klarheit über den Versicherungsschutz zu verschaffen.

Pressekontakt:

Heidi Polke-Markmann
Tel.: +49 89 3800 14303, heidi.polke@allianz.com
Daniel Aschoff
Tel.: +49 89 3800 18900, daniel.aschoff@allianz.com
Bernd de Wall
Tel.: +41 358 84 14, bernd.dewall@allianz.ch