FEHLER. „Eines der häufigsten Missverständnisse in der Cybersecurity-Domäne ist es, in teure Sicherheitslösungen zu investieren und zu glauben, dass man damit sicher ist", sagt Florian Skopik.

FOTO: AIT

Quantencomputer sind potenzielle Gamechanger

Florian Skopik vom Austrian Institute of Technology warnt: Die Gefahr von Cyberangriffen wird unterschätzt, die Attacken werden ausgeklügelter.

Interview: Raja Korinek

Die Zahl der Cyberangriffe häufen sich weltweit. Einen hundertprozentigen Schutz gibt es dabei nicht, konstatiert Florian Skopik, Leiter des Cyber Security Research Program bei der österreichischen Forschungs- und Technologieeinrichtung Austrian Institute of Technology (AIT). Im Interview mit dem *Börsianer* hebt Skopik wesentliche Entwicklungen hervor.

Herr Skopik, was sind die häufigsten Formen von Cyberangriffen? – *Florian Skopik:* Sie sind vor allem im Bereich des Social Engineerings zu finden, zielen also auf Schwächen der Mitarbeiter ab. Dabei hat sich die Ausprägung, wie diese Angriffe durchgeführt werden, geändert. Dies waren bis vor wenigen Jahren eher stümperhaft formulierte E-Mails. Heute können dies zum Beispiel perfekt gefälschte Telefonanrufe – etwa Deepfakes mit sehr gut gefälschten Bildern, Videos – und gezielt auf den jeweiligen Mitarbeiter zugeschnittene Betrugsversuche sein.

Deepfakes werden freilich anhand Künstlicher Intelligenz (KI) erstellt. Welche Veränderungen sehen Sie aufgrund KI noch? – KI senkt die Einstiegshürde in die Cyberkriminalität stark. Auch unerfahrene Akteure können nun komplexe Attacken automatisiert durchführen. Die dabei verwendeten Tools passen sich aufgrund der KI an ihre Ziele an. Mit einem erhöhten Angriffsaufkommen ist also zu rechnen. Gleichzeitig kann KI aber für einen effektiven Schutz vor solchen komplexen Attacken genutzt werden. Dazu gehören beispielsweise KI-basierte Tools, die automatisiert Anomalien in großen Netzwerken erkennen können, was für Menschen manuell nicht mehr überschaubar ist. Solche Werkzeuge werden am AIT im Rahmen großer Forschungsprojekte für unterschiedliche Zielgruppen wie Betreiber kritischer Infrastrukturen, Behörden, aber auch Unternehmen entwickelt.

Software und andere IT-Dienstleistungen werden zunehmend als externen Service zugekauft und nicht mehr am eigenen Server installiert. Wie verändert dies die Bedrohungslage? – Die Wandlung der IT, vieles „as a Service" zuzukaufen, hat die Problematik von Angriffen auf die Lieferkette nochmals verstärkt. Früher musste etwa ein Angreifer, dessen Ziel es ist, Unternehmen zu erpressen, dutzende Organisationen angreifen, um bei zumindest einer erfolgreich zu sein. Heute reicht ein erfolgreicher Angriff auf einen Dienstleister, der hunderte Kunden serviciert.

Wie verändert Quantencomputing die Welt der Cybersicherheit? – Quantencomputer sind tatsächlich ein potenzieller Gamechanger. Der Grund liegt in ihrer Fähigkeit, Rechenprobleme zu lösen, die für klassische Computer praktisch nicht zu knacken sind. Fast alle gängigen asymmetrischen Verschlüsselungsverfahren, die etwa zum Aufbau verschlüsselter Verbindungen im Internet verwendet werden, basieren darauf, dass bestimmte mathematische Aufgaben extrem lange dauern. Ein ausreichend leistungsfähiger Quantencomputer kann diese Hürde mit speziellen Algorithmen überwinden. So lassen sich Sicherheitscodes, für die heutige Supercomputer aktuell Milliarden Jahre bräuchten, in Stunden oder Minuten knacken.

Gibt es Lösungsansätze? – Die Forschung arbeitet weltweit an der sogenannten Post-Quantum-Kryptografie. Das sind neue Verschlüsselungsmethoden, die auch mit Quantencomputern praktisch nicht angreifbar sind. Organisationen wie das US-amerikanische NIST oder auch die EU treiben gerade Standards für solche Verfahren voran.

Können sich kleinere Unternehmen oder auch einzelne Personen den aktuellsten Cyberschutz noch leisten? – Eines der häufigsten Missverständnisse in der Cybersecurity-Domäne ist es, in teure Sicherheitslösungen zu investieren und zu glauben, dass man damit sicher ist, anstatt in Prozesse zu investieren. Cybersecurity ist nicht allein die Aufgabe einiger weniger, die sich um die Sicherheit des Netzwerks oder der Server kümmern. Die meisten Angriffe beginnen nicht mit dem Ausnutzen einer technischen Schwachstelle, sondern mit einer betrügerischen Masche gegenüber unbedarften Mitarbeitern.

% Meine Rendite

In einer zunehmend digitalisierten Welt spielt auch Cybersicherheit eine große Rolle. Die Angriffe nehmen zu, Lösungsansätze werden laufend weiterentwickelt. Quantencomputer könnten das Spiel um die Sicherheit neu definieren. Es braucht braucht neue Verschlüsselungsmethoden. —