Neue Qualität der Cyber-Angriffe

KPMG und das Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrums Sicheres Österreich (KSÖ) präsentierten mit der Studie „Cybersecurity in Österreich“ einen Überblick, Trends und Herausforderungen zum Thema Cyber-Kriminalität und -Sicherheit.

Akteure der internationalen Kriminalität sowie Vertreter autokratischer Regime richten mit ihren Angriffen Schäden in Millionenhöhe an. Die Pressekonferenz „Cybersecurity in Österreich 2025“, wurde am 13. Mai 2005 von *KPMG Austria (https://kpmg.at)* in Kooperation mit dem „Sicherheitsforum Digitale Wirtschaft“ des *Kompetenzzentrums Sicheres Österreich (KSÖ)* organisiert. Dieser Analyse lag eine Befragung von Repräsentanten 1.391 österreichischer Unternehmen zugrunde. Experten wie Oliver Schmerold, ehemaliger Direktor des *ÖAMTC* und KSÖ-Vorstandsmitglied, Andreas Tomek, *KPMG*-Partner im Bereich der Cybersecurity, sowie der Autor der Studie, Robert Lamprecht, der als *KPMG*-Partner auf dem Gebiet der Informations- und Datensicherheit tätig ist, erklärten die aktuelle Studie.

„Für die weltweite Vernetzung der Wirtschaft und anderer Bereiche sowie für die Bereitstellung und den Austausch von Daten und Anwendungen bieten digitale Dienstleister Cloud-Services an. Die künstliche Intelligenz ermöglicht Kriminellen mit wenig Aufwand großflächige Angriffe auf die IT-Infrastruktur“, erklärte Schmerold. Die wichtigste Frage in diesem Zusammenhang ist: Wie sicher ist Österreich und seine Wirtschaft?

Die Kooperation gewerblicher Akteure mitstaatlichen Institutionen eröffnet eine Vielfalt an Möglichkeiten, das Land gegen Cyber-Angriffe sicherer zu machen. „Gerade dieses Thema hat im KSÖ gegenwärtig eine besondere Bedeutung“, sagte Schmerold. Die Sensibilisierung gegenüber dieser immer stärker auftretenden Gefahr gehört zu den Aufgaben fachlich versierter Institutionen. „Sehr wichtig ist die Erfassung der tatsächlichen und der regulativen Sicherheit. Gegenwärtig geschieht auf diesem Gebiet hinsichtlich neuer Gesetze einiges in der EU“, berichtet Tomek.

Cyber-Security-Studie. Für die Studie wurden Vertreterinnen und Vertreter österreichischer Unternehmen befragt.

Die Zahl der Angriffe durch staatlich unterstütze Akteure hat sich im Vorjahresvergleich mehr als verdoppelt. Jeder 7. Cyber-Angriff in Österreich ist erfolgreich

Foto: Stock.Adobe.com

Ergänzt wurde die Studie mit elf Interviews, in denen Fachleute aus Unternehmen und der öffentlichen Sicherheit Stellung beziehen. Die Studie gibt u. a. Einblicke in das aktuelle Lagebild, den Einsatz künstlicher Intelligenz, Angriffe auf die kritische Infrastruktur, Lieferkettensicherheit sowie die zukünftigen Cybersecurity-Entwicklungen.

An erster Stelle liegen der Einsatz von Schadsoftware gemeinsam mit Phishing-Angriffen sowie „Spear Phishing“, bei denen Daten bestimmter Personen oder Institutionen gestohlen werden. „Im Schnitt dauert es 72 Minuten vom Klick auf eine Phishing-E-Mail bis zum erfolgreichen Angriff“, berichtete Lamprecht.

Weitere Methoden sind Scam-Anrufe, bei denen sich Kriminelle als Firmen- oder Behördenvertreter ausgeben und mit dem erschlichenen Vertrauen sensible Informationen ihrer Opfer abfragen oder „Business-E-Mail-Compromises“ (BECs), bei denen sich die Täter als leitende Mitarbeiter eines Unternehmens ausgeben, um Geld oder Betriebsdaten zu erlangen.

Leicht rückläufig ist die Zahl der „Denial-of-Service“-Angriffe, bei denen Täter Netzwerke einer Firma blockieren. Dies kann durch Datenüberlastung geschehen oder indem technische Schwachstellen des Systems genützt werden. So werden Webseiten, Online-Dienste sowie Netzwerke unzugänglich. Die Folgen können Arbeits- und Produktionsunterbrechungen sein, die zu finanziellen Schäden führen. Derartige Attacken schädigen auch den Ruf des angegriffenen Betriebes. Die beschriebenen Angriffe erfolgen zu 48 Prozent von Mitgliedern organisierter Kriminalität. Immer stärker treten auch staatlich unterstützte Täter und Tätergruppen auf und liegen mit 28 Prozent auf dem zweiten Platz. „Damit ist klar, dass geopolitische Konflikte im Cyber-Raum angekommen sind“, sagt Lamprecht. Die Attacken werden hochprofessionell durchgeführt und fokussieren sich in ihrer Häufigkeit auf die kritische Infrastruktur mit dem Ziel maximalen Schaden anzurichten.

41 Prozent der Angriffe kommen aus dem asiatischen Raum. „Die Angriffe aus Asien haben sich gegenwärtig dramatisch erhöht“, erklärte Lamprecht. „Weitere 29 Prozent der Angriffe kommen aus europäischen Ländern. Allerdings muss man bei der Datenerfassung vorsichtig sein, denn Cyber-Kriminelle verlegen ihre Taten durch Verschleierungstaktiken öfter in andere Weltgegenden. „Fast die Hälfte der von uns befragten Unternehmensmitarbeiter weiß nicht, woher die Angriffe auf ihr Unternehmen kommen.“

Beim Abhören der Kommunikation, dem Datendiebstahl sowie der Anwendung von Ransomeware (Lösegelderpressung durch den Einsatz von Schadsoftware) werden seit dem Vorjahr leichte Zunahmen verzeichnet. Rückläufig sind Angriffe gegen Cloud-Services.

Gegenmaßnahmen. Vor allem große Unternehmen investieren mehr finanzielle Mittel in die Cyber-Sicherheit. Kleine und mittelständische Unternehmen müssten allerdings mehr in ihre IT-Sicherheit investieren. Sie sind vor allem von Ransomeware verstärkt betroffen. Jedes vierte Unternehmen offenbart ein unzureichendes Patch-Management und jedes fünfte eine unzureichende Sicherheit der Anmeldedaten. Wichtig für die Erstellung von zeitgemäßen Sicherheitsmaßnahmen ist eine genaue Schadensanalyse. An erster Stelle steht die Beeinträchtigung der Betriebsabläufe und der Wertschöpfungskette.

„Anhand der Studie sehen wir, dass Firmen rund zwei Wochen benötigen, um nach einem Cyber-Sicherheitsvorfall die Wiederherstellungsmaßnahmen in Gang zu setzen“, stellte Lamprecht

Präsentation der Cybersecurity-Studie 2025: Oliver Schmerold (KSÖ), Michael Höllerer (KSÖ), Robert Lamprecht (KPMG), Andreas Tomek (KPMG)

klar. Auch die Sabotage, die bislang weniger Beachtung fand, hat stark zugenommen. Viele Betriebe sind diesbezüglich nicht in der Lage den Schaden zu quantifizieren, um auf dieser Grundlage Vorsorgemaßnahmen zu treffen. Ransomeware und Datendiebstahl kommen in Österreich seltener vor. Im Mittelfeld der statistischen Erfassung liegen der Passwortdiebstahl sowie „Denial-of-Service“-Attacken.

Im oberen Spitzenfeld finden sich „Spoofing“-Angriffe (Der Täter nutzt eine gefälschte Identität einer anderen Person oder Organisation), „Social-Engineering“ (menschliche Eigenschaften wie Hilfsbereitschaft oder Respekt werden bei den Opfern ausgenützt, um an wertvolle Daten zu gelangen) aber auch sogenannte „Innentäter“, also Mitarbeiterinnen und Mitarbeiter, die aus Frust- und Rachegefühlen das Unternehmen schädigen.

„Technik allein reicht nicht, um den Herausforderungen zu begegnen. Es braucht Menschen, die Verantwortung übernehmen, Risiken verstehen und aktiv an Lösungen mitwirken. Behörden, Wirtschaft und Wissenschaft müssen an einem Strang ziehen und gemeinsam eine Sicherheitskultur gestalten, die auf Kooperation, Transparenz und gemeinsames Handeln baut“, sagte Michael Höllerer, Präsident des KSÖ.

Michael Ellenbogen

FOTOS: EVA KELETY, KPMG AUSTRIA, ÖAMTC/WIRLPHOTO