Fachkräftemangel: Fast drei Viertel der befragten Unternehmen haben gemäß der Cyber-Security-Studie Schwierigkeiten beim Rekrutieren von IT- und Security-Experten.

Trends und Herausforderungen

Laut der Cyber-Security-Studie von KPMG und KSÖ sind die größten Herausforderungen für Unternehmen der Fachkräftemangel, Ransomware-Attacken und staatliche Angreifer.

In der siebenten Cyber-Security-Studie des Wirtschafts- und Beratungsunternehmens *KPMG Austria* mit dem *Kompetenzzentrum Sicheres Österreich (KSÖ)* wird deutlich, dass es den Unternehmen und Behörden besonders an Fachkräften für Cyber-Sicherheit mangelt. Die Cyber-Sicherheit sei ein Bereich im ständigen Wandel, sagte *KPMG*-Direktor Robert Lamprecht, bei der Präsentation der Studie am 3. Mai 2022 in Wien. „Die durch die weltweite Covid-Pandemie beschleunigte Digitalisierung hat gerade in Zusammenhang mit Cyber-Kriminalität für eine neue Dynamik gesorgt“, ergänzte Erwin Hameseder, Präsident des *Kompetenzzentrums Sicheres Österreich*.

Anstieg bei der Internetkriminalität. Im Sicherheitsbericht 2020 des Bundesministeriums für Inneres ist erkennbar, dass die Internetkriminalität in den zehn Jahren zwischen 2010 und 2020 kontinuierlich zunahm. Allein im Jahr 2020 stieg die Zahl der Internetdelikte von 28.439 auf 35.915. Das ist ein Plus von 26,3 Prozent. Die Aufklärungsquote blieb mit 33 Prozent nahezu gleich, heißt es im Sicherheitsbericht. Die Verlagerung der Kriminalität in den Cyber-Raum verlange vom Bundesministerium für Inneres Anpassungen und Vorbereitungen, wie Innenminister Gerhard Karner erklärte: „So wird etwa das C4, das Cyber-Crime-Competence-Center im Bundeskriminalamt, sowohl strukturell als auch technisch angepasst und personell verstärkt.“ Staaten als Angreifer werden ebenfalls immer mehr zum Problem: „Die digitale Kriegsführung hat deutlich zugenommen“, sagte der Innenminister. „Vor allem die Ukraine und Russland sind seit dem Beginn des Krieges verschiedenen Gruppen ausgesetzt – auch Firmen, die in den jeweiligen Staaten aktiv sind, wurden bereits Opfer von Attacken.“

Ransomware-Angriffe. „Ein Anstieg der Zahl an Cyber-Angriffen und immer neuen Angriffsvektoren stellen uns vor neue Herausforderungen, die nicht isoliert von einer Stelle alleine – weder vom Staat noch von der Wirtschaft – gelöst werden können“, sagte Hameseder. Allein im vergangenen Jahr erhöhten sich die Anzahl der Ransomware-Angriffe laut *World Economic Forum* weltweit um 435 Prozent. Ransomware-Angriffe sind Angriffe durch die Unternehmensdaten verschlüsselt werden und die Angreifer Lösegeld (engl.: Ransom) für die Entschlüsselung verlangen. Nicht immer sei klar, ob die Kriminellen trotz Zahlung des Lösegelds auch wirklich die Schlüssel zur Entschlüsselung preisgeben würden. In jedem Fall habe man ein großes Daten- und Sicherheitsproblem.

In der Cyber-Security-Studie 2022 gaben 14 Prozent der österreichischen Unternehmen an, von Ransomware-An-

FOTO: PIXEL-SHOT.COM (LEONID YASTREMSKIY)/ADOBE.STOCK.COM

Präsentation der Cyber-Security-Studie: Engelbert Theuermann, Victoria Überreich, Andreas Tomek, Erwin Hameseder, Katharina Raabe-Stuppnig, Iva Herceg, Michael Schirmbrand, Robert Lamprecht, Alexander Janda.

griffen betroffen gewesen zu sein. Stefan Fink, *KPMG*-Chief-Economist, erläuterte in einem Interview in der Studie, dass sich die Cyber-Security-Konzepte der Zukunft auf das Thema der Cyber-Resilienz konzentrieren müssen, jedoch vielerorts die notwendigen Fachkräfte fehlen würden.

Cybersecurity sei kein IT-Thema, heißt es in der Studie. Vielmehr sei der Mensch „Dreh- und Angelpunkt in allen Cybersicherheitsbelangen". Er sei „die beste und stärkste Firewall, die wir haben", andererseits aber auch die größte Schwachstelle. Der weitaus größte Teil der Cyber-Sicherheitsprobleme gehe auf menschliches Versagen zurück, schreibt *KPMG*. Und je perfider die Angriffsmethoden, desto entscheidender sei der Mensch. Verschärft werde die Situation dadurch, dass hybride Arbeitswelten anfälliger für Angriffe sind.

Studienergebnisse. Besonders überraschend war, dass jeder dritte Unternehmensvertreter angab, in Zukunft eine Verschlechterung der Cybersecurity zu erwarten und somit eher pessimistisch in die Zukunft blickt. Abgesehen von Ransomware-Angriffen, macht die Studie auf das Problem von Phishing-Angriffen aufmerksam. Bei einem Phishing-Angriffv versuchen Kriminelle durch Täuschung – meist ein echt aussehendes E-Mail eines Bank-Instituts oder einer anderen Einrichtung – die Opfer zur Herausgabe ihrer persönlichen Daten und Passwörter zu bewegen. Die Cyber-Security-Studie 2022 ergab, dass von den 550 betroffenen österreichischen Unternehmen 51 Prozent der festgestellten Angriffe Phishing-Angriffe waren. Insgesamt waren 67 Prozent der Unternehmen, Opfer eines Cyber-Angriffs. Bei 20 Prozent der Opfer entstand ein finanzieller Schaden.

Meldestelle. Innenminister Karner ist überzeugt, dass Präventionsarbeit ein wichtiger Ansatz ist, auch um die Sensibilisierung weiter zu erhöhen und die Scheu vor der Anzeige dieser Straftaten zu reduzieren. Sollte der Verdacht auf Internetkriminalität bestehen, so können Betroffene sich bei der Meldestelle für Internetkriminalität im Bundeskriminalamt melden *(https://bundeskriminalamt.at/306/start.aspx)*. Geschädigte können die Straftat bei jeder Polizeidienststelle zur Anzeige bringen.

Fachkräftemangel. Fast drei Viertel der Unternehmen gaben an, Schwierigkeiten beim Rekrutieren von IT- und Security-Experten zu haben. Etwa die Hälfte der Unternehmen benötigt für die Suche von qualifiziertem Personal vier bis sechs Monate. So überrascht es nicht, dass sich viele Unternehmen ihre Security-Experten untereinander abwerben. Rund 40 Prozent der Befragten werben aktiv Sicherheitsexperten von anderen Unternehmen ab.

Dem Fachkräftemangel in der Cyber-Security-Branche wirken Events entgegen wie die *Austria Cyber-Security-Challenge (ACSC)*, die dieses Jahr zum elften Mal ausgetragen wird *(https://verbotengut.at)*. Die *ACSC* ist Österreichs erste IT-Security-Talentsuche zur Rekrutierung von qualifizierten Menschen im Bereich der Cybersecurity. Die *ACSC* findet in Zusammenarbeit mit dem Bundesministerium für Inneres und dem Bundesministerium für Landesverteidigung statt und wird vom Bundeskanzleramt unterstützt.

Die Studie kann unter *https://home.kpmg/at/de/home/insights/2022/05/cyber-security-oesterreich-2022.html* angefordert werden. *Michael Tögel*

FOTO: KPMG AUSTRIA/ANNA RAUCHENBERGER