Gefahr für Unternehmen

Laut der Cyber-Security-Studie 2022 von KPMG und KSÖ finden täglich Cyber-Attacken auf heimische Unternehmen statt. Jeder zehnte Angriff 2022 war erfolgreich.

Das Jahr 2023 wird in punkto Cybersecurity eine außergewöhnliche Rolle einnehmen und deutliche Spuren hinterlassen“, kündigte IT-Advisory-Direktor Robert Lamprecht vom Wirtschaftsprüfungs- und Beratungsunternehmen *KPMG* zu Beginn der Studienpräsentation „Cybersecurity in Österreich“ an, die am 3. Mai 2023 gemeinsam mit dem *Kompetenzzentrum Sicheres Österreich (KSÖ)* präsentiert wurde. Zu Recht, angesichts der zentralen Studienergebnisse: Cyber-Attacken auf heimische Unternehmen finden mittlerweile täglich statt. Gegenüber dem Vorjahr haben sie um 201 Prozent zugenommen. Darüber hinaus gaben alle 903 befragten Unternehmen an, im Jahr 2022 zumindest mit einer Phishing-Attacke konfrontiert gewesen zu sein. Insgesamt jede zehnte Cyber-Attacke war erfolgreich.

Präsentation der Cybersecurity-Studie: Andreas Tomek (Partner KPMG), Christoph Neumayer (Generalsekretär IV), Michael Höllerer (Generaldirektor RLB Niederösterreich-Wien/KSÖ-Präsident), Lisa Katharina Promok (Universität Salzburg), Victoria Überreich-Gollhofer (digireich), Robert Lamprecht (KPMG), Bernd Pichlmayer (Bundeskanzleramt), Gerhard Christiner (APG)

Existenzbedrohung. „Die damit verbundenen Schäden sind enorm, beinahe jedes siebte Unternehmen musste aufgrund eines Ransomware-Angriffs Betriebsunterbrechungen von mehr als vier Wochen in Kauf nehmen. Ein Drittel der Unternehmen immerhin rund eine Woche. Das kann eine klare Existenzbedrohung darstellen“, sagte *KPMG*-Partner Andreas Tomek. Während Cyber-Angriffe für Kriminelle nach wie vor ein lukratives Geschäftsmodell und meist nur mit geringen Kosten verbunden seien, sind Cyber-Vorfälle für die betroffenen Unternehmen wesentlich kostenintensiver. Bei jedem zehnten Unternehmen beläuft sich der finanzielle Schaden mittlerweile auf über eine Million Euro.

Neben dem Reputationsverlust „sind es vor allem der betriebliche Stillstand und die Kosten für die Aufarbeitung der Attacke, die den finanziellen Schaden in die Höhe treiben“, konstatieren die Studienautoren. Auch Angriffe auf die kritische Infrastruktur werden laufend zielgerichteter und komplexer. Krankenhäuser, Windparks zur Stromerzeugung, Supermärkte und Handelsketten, aber auch IT-Dienstleister seien immer häufiger von Ransomware-Attacken betroffen. „Multiple Krisen – von geopolitischen Konflikten über die Teuerung bis hin zur Inflation – öffnen Cyber-Kriminellen Tür und Tor in die Systeme von Unternehmen“, analysierte Lamprecht. Während die österreichischen Firmen in den letzten Jahren viel in den Bereich technische Infrastruktur investiert haben, gebe es „auf personeller Seite“ nach wie vor Defizite. „Heimische Firmen haben im Technologie-Bereich aufgerüstet, aber organisatorisch-personell noch nicht alle Hausaufgaben erledigt“, befand Lamprecht. Ein Befund, der sich empirisch belegen lässt: Immer öfter werden laut *KPMG*-Studie Mitarbeiterinnen und Mitarbeiter von Firmen gezielt manipuliert, um Gelder zu erpressen oder zu Last-Minute-Überweisungen zu drängen.

„Der Mensch ist zwar Eintrittspunkt für viele Cyber-Angriffe, gleichzeitig aber auch einer der wirksamsten Sicherheitsfaktoren, wenn es um die Prävention und das Erkennen geht“, betonte der Präsident des *Kompetenzzentrum Sicheres Österreich (KSÖ)*, Michael Höllerer. Es brauche eine gelebte Cybersecurity-Kultur in den Unternehmen. Cybersecurity sei längst kein Wettbewerbsvorteil oder notwendige Pflichterfüllung mehr, sondern „überlebensnotwendig für Unternehmen“.

Europäische Lösung. „Um der Gefahr von Cyber-Angriffen nachhaltig entgegenwirken zu können, braucht es eine stärkere Zusammenarbeit zwischen den Unternehmen und öffentlichen Stellen – auch über die Landesgrenzen hinweg“, so die Macher der Studie.

74 Prozent der Befragten gaben demnach an, dass eine verstärkte EU-weite Zusammenarbeit im Kampf gegen die Cyber-Kriminalität „essenziell“ sei. „Wir müssen und werden uns mit der Frage der digitalen Souveränität in Europa auseinandersetzen. Die Chancen für österreichische bzw. europäische Lösungen sind gerade beim Thema Cyber-Sicherheit sehr groß. Die Anstrengung, gemeinsam tragfähige Wege und Lösungen zu finden, wird sich lohnen“, ist sich Höllerer sicher.

Die gute Nachricht: Die Sensibilisierung durch die Vielzahl der Angriffe in den vergangenen Jahren habe dazu geführt, dass Unternehmen sich besser vorbereiten. Die technische Infrastruktur und Schutzmaßnahmen seien sukzessive ausgebaut worden. *Jürgen Belko*

Die Studie kann angefordert werden unter *https://info.kpmg.at/cyber-security-2023*

FOTO: WWW.ANNARAUCHENBERGER.COM / ANNA RAUCHENBERGER