

bar machen“, sagt Gottfried Tonweber, Leiter Cybersecurity und Data Privacy bei EY Österreich, und warnt: „Dabei unterschätzen sie die Kreativität und Professionalität der Angreifer, denn die Arten der Angriffe werden immer unauffälliger. Angesichts der komplexen digitalen Umgebungen – sei es durch Ausweitung von Homeoffice, Mobile Devices oder Cloud Computing – werden auch die Angriffsflächen immer größer und die Sicherung der eigenen Systeme immer schwieriger. Dadurch können Hacker unbemerkt in die unternehmens-eigene Infrastruktur eindringen und großen Schaden anrichten.“

#### Was passiert, wenn's passiert

Bei einem Angriff auf die IT-Systeme eines Unternehmens oder dem Verdacht auf Manipulation gilt es, schnell und richtig zu handeln – insbesondere Verantwortliche für die Informationssicherheit sollten auf den Ernstfall vorbereitet sein.

57% der Führungskräfte geben in der Studie an, dass sie einen

#### Cyberexpertin

„Der Mensch ist weiterhin die größte Schwachstelle im Bereich der IT-Sicherheit“, meint Senior Manager Cybersecurity & Data Privacy bei EY Österreich, Birgit Eschinger.

Krisenplan zur Reaktion auf Cyberangriffe in ihrem Unternehmen haben, knapp zwei Drittel (63%) üben die Abläufe jährlich oder mehr als einmal im Jahr. Jedes dritte Unternehmen (33%) hat nach eigener Aussage keinen Krisenplan, zehn Prozent sind gerade in der Ausarbeitung. Knapp die Hälfte der österreichischen Unternehmen (45%) lässt ihre IT-Systeme jährlich oder halbjährlich von externen Stellen auf Schwachstellen im Hinblick auf Datendiebstahl prüfen. Um im Falle, dass es trotz aller getroffenen Sicherheitsmaßnahmen zu einem Cyberangriff kommt, vor schwerwiegenden Folgen geschützt zu sein, haben 47% der Unternehmen derzeit eine Versicherung gegen Cyberrisiken.

#### Personellen Ressourcen

Knapp ein Drittel der Unternehmen über 100 Beschäftigten (31%) beschäftigt eine eigene IT-Security-Abteilung mit mehr als zwei Vollzeit-Mitarbeitern, in kleineren Unternehmen unter 100 Mitarbeitenden stehen nur jedem zehnten umfassende Personalressourcen zur Verfügung. KMU bis 49 Beschäftigte bilden hier das Schlusslicht: 34% geben an, dass es keine Personalressourcen für Cybersecurity in ihrem Unternehmen gibt.

Auch wenn in vielen Betrieben IT-Sicherheit zur Chefsache erklärt wurde, es ist eine Vogel-Strauß-Politik: „Obwohl auch kleine KMU erwiesenermaßen ein interessantes Angriffsziel sind, werden viele grundlegende Schutzmaßnahmen nicht in ausreichendem Maße umgesetzt. Viele Unternehmen blenden diese reale Gefahr aus dem digitalen Raum weiterhin aus oder scheinen zu träge oder von der Problematik überfordert zu sein, um entsprechende Maßnahmen zu ergreifen und das Risiko zu adressieren“, so Tonweber.

Das Homeoffice kann für viele Unternehmen zum Risikofaktor



#### Cyberleiter

Für Gottfried Tonweber, Leiter Cybersecurity und Data Privacy bei EY Österreich, braucht es neben medialer Beachtung des Themas weitere Anstrengungen, um die Umsetzung von Cybersecurity-Maßnahmen zu erhöhen.

werden, Remote-Verbindungen zu einem attraktiven Einfallstor für Cyberkriminelle: In den meisten Fällen musste neue Software installiert werden, und private Laptops sind oft nicht mit derselben Software, etwa einer vernünftigen Firewall, geschützt wie Firmen-PCs.

#### Werkzeug Sensibilisierung

Viele heimische Unternehmen haben dieses gesteigerte Risiko erkannt und in den letzten Monaten ihre Cybersecurity-Maßnahmen verschärft. 56% setzen auf die Sensibilisierung der Mitarbeiter, 54% auf die Modernisierung der IT-Infrastruktur und 46% auf die Verschärfung der Sicherheitsrichtlinien.

Dazu rät Birgit Eschinger, Senior Manager Cybersecurity & Data Privacy bei EY Österreich: „Der Mensch ist weiterhin die größte Schwachstelle im Bereich der IT-Sicherheit. Sei es aus Gutgläubigkeit, Unwissenheit oder auch böser Absicht heraus – vertrauliche Unternehmensdaten geraten schnell in die falschen Hände, oder das Netzwerk ist infiziert. Schulungen und Trainings, um Awareness bei Mitarbeitenden zu schaffen und das nötige Know-how zu vermitteln, sollten daher hohe Priorität haben, um allfällige Angriffe abzuwehren.“ (hk)

202

#### EY-Studie

Für „Cyberangriffe und Datendiebstahl: virtuelle Gefahr – reale Schäden“ wurden 202 Führungskräfte aus IT-Sicherheit und Datenschutz von österreichischen Unternehmen ab 20 Mitarbeitern befragt.

