INFORMATIONSSICHERHEIT – Fast im Wochentakt beherrschen Cyberangriffe die Schlagzeilen. Dass diese Angriffe immer häufiger KMU betreffen, hat einen einfachen Grund: Es fehlt die Sensibilisierung – und damit die Informationssicherheit.

Auch KMU haben viel zu verlieren

KMU sind ein dankbares Cyberangriffsziel. Mit anderen Worten: KMU machen es Cyberkriminellen oft viel zu einfach, in ihre Systeme einzudringen und Schaden anzurichten, weil entsprechende Sicherheitsmassnahmen entweder ganz fehlen, veraltet sind oder nur halbherzig umgesetzt werden.

Während grosse Firmen grosse Anstrengungen unternehmen, um ihre Daten und Informationen bestmöglich zu sichern und zu schützen – und ein Angriff deshalb viel mehr Know-how und Mühe erfordert – ist die Bedeutung der Informationssicherheit vielen KMU zwar bekannt, sie scheuen aber oftmals Aufwand und Ressourcen.

Beliebtes Angriffsziel: KMU werden immer häufiger von Cyberkriminellen ins Visier genommen. Bild: Fotolia

Keine Ausreden

Die ganze Sicherheitsthematik ist für ein KMU eh zu kompliziert, zu teuer, zu arbeitsintensiv, und letztlich wird schon nichts passieren. Nur: Denken KMU auch so, wenn es um das eigene Hab und Gut geht? Oder lassen sie Fenster und Türen weit offen, weil schon nichts passieren wird und die Schlüsselsuche zu mühsam ist?

Daten und Informationen sind wertvoll und wichtig und verdienen wirkungsvollen Schutz. Nicht nur, weil gestohlene oder verlorene Daten weit mehr Arbeit (und Geld!) bedeuten als angemessene, aber konsequente Informationssicherheit. Auch weil solche Vorfälle die Reputation einer Firma arg beschädigen oder gar deren Existenz gefährden können.

Vertrauenspunkte sammeln

Wer auf Informationssicherheit Wert legt, schafft Vertrauen – im Unternehmen und bei Kunden. Informationssicherheit sorgt für mehr Sicherheit, aber auch für mehr Transparenz, und gerade mit dem Thema Datenschutz können KMU Vertrauenspunkte sammeln (Stichwort Datenschutzgesetz oder DSGVO).

Über die Notwendigkeit von Informationssicherheit ist sich im Übrigen auch das Parlament einig – trotz Nichteintreten auf das Informationssicherheitsgesetz im März dieses Jahres. Strittig war einzig die Art der Ausgestaltung des Gesetzes.

Konsequent sein

Der Weg zu wirkungsvoller Informationssicherheit ist bei Weitem nicht so steinig wie befürchtet. Genau wie bei der klassischen Einbruchprävention reichen einige Massnahmen, um Daten und Informationen zu schützen (*vgl. Kasten*). Vor allem aber muss Informationssicherheit gelebt und Teil der Unternehmenskultur werden – egal wie klein das Unternehmen ist.

Die grösste Sicherheitsschwachstelle ist und bleibt der Mensch. Gerade deshalb ist es unabdingbar, dass alle Mitarbeitenden für Sicherheitsthemen und -risiken sensibilisiert und bezüglich Informationssicherheit geschult werden. Besser heute als morgen.

Reto C. Zbinden,
Experte für Informationssicherheit

NÜTZLICHE INFOS

Die Hochschule Luzern hat die Informationssicherheit in KMU untersucht und verrät auf **blog.hslu.ch/informatik/8-nuetzliche-tipps-fuer-die-informationssicherheit-im-kmu/**, welche Massnahmen sofort mehr Sicherheit bringen.

Ebenfalls empfehlenswert: Aus der KMU-Schriftenreihe «Aus der Praxis – für die Praxis»: Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU) der Arbeitsgruppe KMU + Informationssicherheit des Vereins InfoSurance. Download auf **www.kmu.admin.ch** unter der Rubrik «Praktisches Wissen», «KMU betreiben» und «Infrastruktur und IT».

CYBERRISIKEN – Cyberattacken gehören zum Alltag. Eine Fachgruppe hat einen Schnelltest entwickelt.

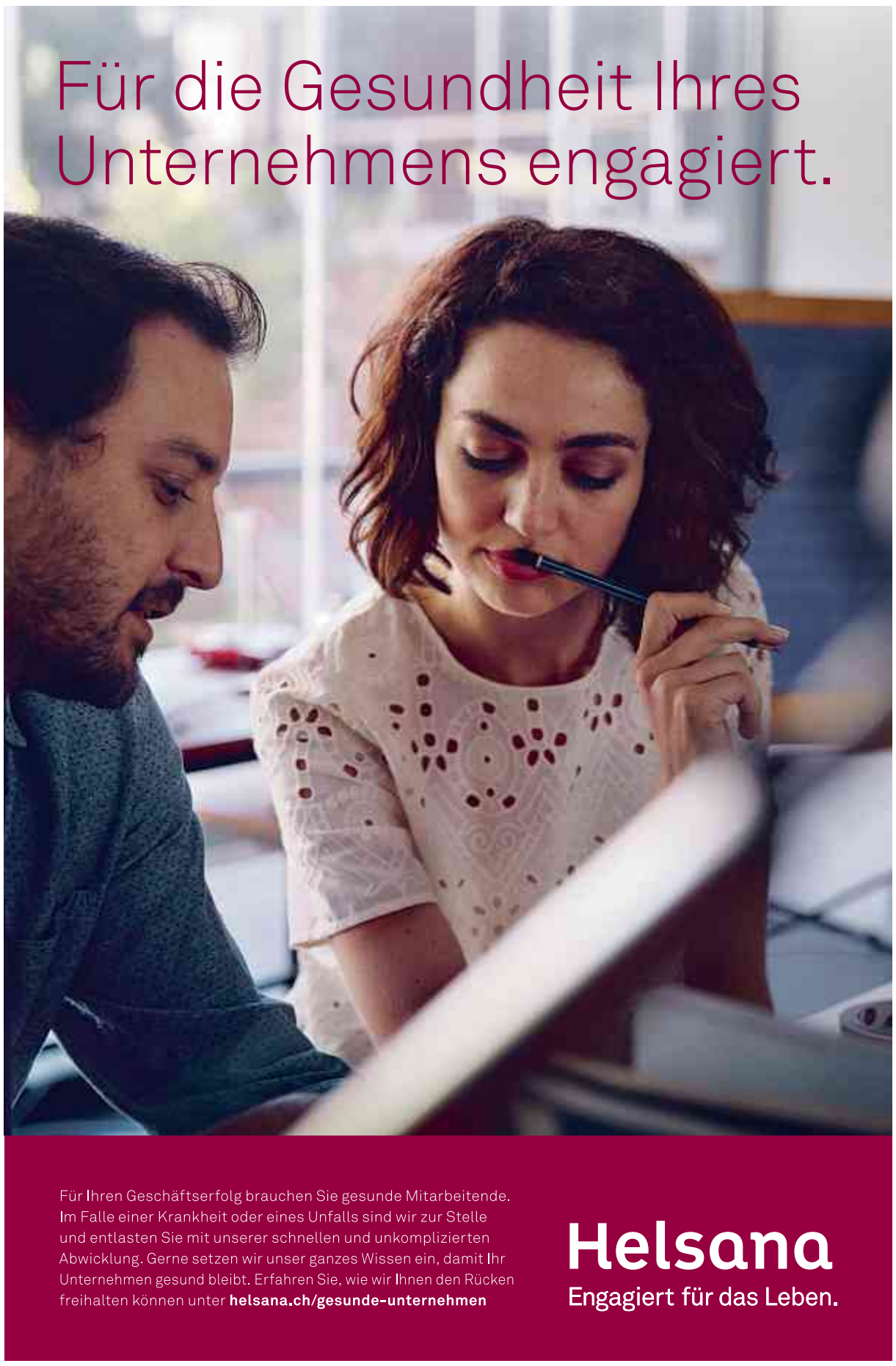
Cybertest für KMU

Mehr als 98 Prozent der Schweizer Unternehmen sind KMU. Sie bilden das Rückgrat der Schweizer Wirtschaft. Um langfristig erfolgreich zu sein, müssen KMU mittels digitaler Technologien Lieferanten, Mitarbeitende und Kunden in ihre Prozesse einbeziehen. Dies bedingt eine zunehmende Vernetzung von Unternehmensinfrastrukturen und -daten mit dem Internet. Dadurch erhöhen sich die Risiken aus dem Cyberspace drastisch.

Hacker richten ihre Cyberattacken vermehrt auf sogenannte «low hanging fruits» – nicht ausreichend geschützte KMU. Die im Dezember 2017 publizierte Studie «Cyberrisiken in Schweizer KMU» spricht eine deutliche Sprache: Rund ein Drittel der KMU war bereits von Viren oder Trojanern betroffen. Datenverlust und Erpressungen übers Netz kamen bei vier Prozent der befragten Unternehmen schon vor. Viele Firmen beschäftigen sich mit dem Thema erst dann gebührend, wenn bereits Schaden entstanden ist: «Wir spüren bei KMU immer wieder grosse Unsicherheit betreffend Cybersecurity. Viele wissen nicht, wie sie das Thema anpacken sollen. Der Schnelltest ist ein guter Einstieg, um sich damit auseinanderzusetzen und allfälligen Handlungsbedarf zu identifizieren», so **Nicole Barandun,** Präsidentin des Gewerbeverbandes der Stadt Zürich GVZ.

Schnelltest mit 12 Themenbereichen

Ziel der Initiative ist es, ein Instrument zur Selbstbeurteilung, insbesondere auch für kleinere Unternehmen, zur Verfügung zu stellen. Nicht eine umfassende und komplette Analyse steht im Vordergrund: Gerade auch KMU mit wenig ausgeprägten Kenntnissen bezüglich Informatik und IT-Sicherheit können sich unkompliziert und schnell ins Bild setzen, ob ihre technischen, organisatorischen und mitarbeiterbezogenen Massnahmen zum Schutz vor Cyberrisiken ausreichend sind. Ein kurz und einfach gehaltenes Begleitdokument gibt bei Unsicherheiten weiterführende Hinweise zu jedem Themenbereich. «Der Schutz vor Cyberrisiken ist eine gemeinsame Verantwortung von Wirtschaft, Gesellschaft und Staat. Somit leisten wir einen wichtigen Beitrag zur Umsetzung der neuen Cyberstrategie und stellen den KMU ein Werkzeug zur Verfügung, welche ihnen hilft, ihr eigenes Cyberrisiko besser einzuschätzen», so **Pascal Lamia,** Leiter der Melde- und Analysestelle Informationssicherung (MELANI).

www.cybersecurity-check.ch

ANZEIGE