

Digitalisierung

Finanzen

Internationalisierung

Arbeit

Cybersicherheit: Warum die IT Chefsache werden muss

Hilfestellungen für KMU

20. März 2019

Cybersicherheit: Warum die IT Chefsache werden muss

Hilfestellungen für KMU

Adress- und Kontaktdaten, Konto- und Gesprächsauszüge, private Urlaubs- und Familienfotos – für jedermann im Internet einsehbar. Ein Albtraum für viele Menschen. Zum Vorjahresende bittere Realität für mehrere hundert Politiker und Personen des öffentlichen Lebens, die ihre sensiblen Daten ungefiltert im Netz wiederfanden. Als „schwerwiegenden Angriff“ wertete Justizministerin Katarina Barley etwa diesen konkreten Fall.

Diesem Negativbeispiel auch positive Seiten abzugewinnen, ist kaum möglich. Wenn überhaupt, dann ist es die Aufmerksamkeit, die das Thema Cybersicherheit durch die Attacke erfahren hat. Für die betroffenen Personen ist das natürlich ein sehr schwacher Trost, aber das Thema digitale Sicherheit wurde lange vernachlässigt – besonders auch mit Hinblick auf kleine und mittlere Unternehmen (KMU). Gerade kleine Unternehmen sind dabei zunehmend ein Ziel von Cyberangriffen, denn oft sind sie vergleichsweise schlecht geschützt.

Je kleiner das Unternehmen, desto größer die Gefahr?

Inwiefern KMU aus dem deutschen Mittelstand von digitaler Wirtschaftsspionage und Datendiebstahl betroffen sind, ist weitestgehend unbekannt. Verlässliches Zahlenwerk existiert kaum, eine hohe Dunkelziffer ist wahrscheinlich: Der Digitalverband Bitkom hat für eine [Studie](#) aus dem vergangenen Jahr (2018) 503 Industrieunternehmen mit mindestens 10 Mitarbeitern zum Thema Wirtschaftsschutz befragt: 68 Prozent der befragten Unternehmen mit 10 bis 99 Mitarbeiter sind bereits Opfer von digitaler Spionage, Sabotage und Datendiebstahl gewesen. 46 Prozent der Unternehmen in dieser Größenordnung hat in der Vergangenheit bereits wirtschaftliche Schäden durch digitale Angriffe erfahren.

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat 2018 das Meinungsforschungsinstitut Forsa beauftragt, 300 KMU zu den Cyberrisiken im Mittelstand zu [befragen](#). Demnach haben 30 Prozent der KMU bereits Schäden durch Cyberangriffe erlitten. Ein weiteres Ergebnis: je kleiner das Unternehmen, desto häufiger sind Attacken erfolgreich – denn gerade die Kleinen schätzen das Risiko, selbst ein Opfer digitaler Angriffe zu werden, am geringsten ein. Dabei spielen Kategorien wie Umsatz- oder Mitarbeiterzahlen bei massenhaften und ungezielten Cyberattacken überhaupt keine Rolle für die Angreifer. Das größte Einfallstor für Cyberangriffe ist übrigens laut der GDV-Studie der E-Mail-Posteingang.

Die Bunderegierung hat das Problem erkannt, lösen müssen es KMU aber selbst.

Viele Sicherheitsrisiken für KMU sind mit relativ einfachen Mitteln zu beseitigen: Mitarbeiterschulungen und verbindliche Regeln für den korrekten Umgang mit E-Mails sind beispielsweise probate und kostengünstige Schutzmaßnahmen. Wichtig ist es deshalb, ein

grundsätzliches Problembewusstsein innerbetrieblich zu etablieren und klare Zuständigkeiten für die IT-Sicherheit zu formulieren.

Ein solches Problembewusstsein für Cybersicherheit hat auch (endlich) die Bundesregierung: im Koalitionsvertrag wurde unter anderem ein [Bündnis für Cybersicherheit](#) mit der Wirtschaft angekündigt, welches im vergangenen Herbst etabliert worden ist. Zudem soll laut der Regierungskoalition das Bundesamt für Sicherheit in der Informationstechnik (BSI) als „nationale Cybersicherheitsbehörde“ in der laufenden Legislaturperiode ausgebaut und als unabhängige und neutrale Beratungsstelle – gerade auch für KMU – für Fragen der IT-Sicherheit gestärkt werden.

Doch auch verbesserte Beratungsstrukturen helfen nicht viel, wenn das Angebot nicht in Anspruch genommen wird. Unternehmer müssen sich deshalb proaktiv dem Thema widmen und Cybersicherheit ganz sprichwörtlich zur Chefsache erklären.

Weiterführende Links und Hilfestellungen zum Thema Cybersicherheit für KMU

- ❖ Das [Bundesamt für Sicherheit in der Informationstechnik](#) (BSI) stellt eine Vielzahl von Empfehlungen zur präventiven Absicherung vor und effektiven Reaktion auf Cyber-Angriffe für KMU zur [Verfügung](#).
- ❖ Mit der Initiative „[IT-Sicherheit in der Wirtschaft](#)“ unterstützt das Bundesministerium für Wirtschaft und Energie Unternehmen darin, ihre IT-Sicherheit zu verbessern. Insbesondere KMU sollen für das Thema sensibilisiert werden. Eine Reihe an hilfreichen Ratgebern wie der [IT-Sicherheitsnavigator](#) oder ein [Webseiten-Sicherheitscheck für KMU](#) stehen kostenfrei zur Verfügung.
- ❖ Das [Hasso-Plattner-Institut](#) (HPI) bietet eine Reihe an Services, Tools sowie interaktive Online-Kurse. Mit dem [Identity Leak Checker](#) zum Beispiel können Sie mithilfe Ihrer E-Mailadresse prüfen, ob Ihre persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. [openHPI](#) ist die Internet-Bildungsplattform des Hasso-Plattner-Instituts mit interaktiven Online-Kursen zu verschiedenen IT-Themen.
- ❖ Das [Fraunhofer-Institut für Sichere Informationstechnologie](#) (Fraunhofer SIT) bietet umfassende Informationen und Hilfestellungen zum IT-Grundschutz. So etwa der kostenlose [Online-Kurs IT-Grundschutz](#), der sich besonders an Anwender aus KMU richtet.