DEUTSCHER MITTELSTANDS-BUND

Digitalisierung	Arbeit & Bildung	Energiewende	Finanzen

Deutscher Mittelstands-Bund (DMB) | Simon Nentwich

Cybersecurity: Warum die IT Chefsache werden muss

Je kleiner das Unternehmen, desto größer die Gefahr?

04. April 2021

Kontakt zur Redaktion:
Deutscher Mittelstands-Bund (DMB) e.V.
Grafenberger Allee 125
40237 Düsseldorf

www.mittelstandsbund.de
Tel. +49 (0) 211 / 2005 25-0
Fax +49 (0) 211 / 2005 25-99
Mail: info@mittelstandsbund.de

Herausgeber (V.i.S.d.P.):
Marc S. Tenbieg
Geschäftsführender Vorstand
meinung@mittelstandsbund.de

Cybersecurity: Warum die IT Chefsache werden muss

Softwareunternehmen, Versicherer und Wirtschaftsprüfungsgesellschaften haben jüngst einen starken Anstieg von Cyberangriffen in Deutschland beobachtet. Nicht nur die Häufigkeit, sondern auch die Art der Attacke verändert sich: während früher Schadsoftware insbesondere über Emails eingeschleust wurde, haben sich die Werkzeuge der Cyber-Kriminellen inzwischen stark diversifiziert. Die Angriffe werden gezielter und individualisierter durchgeführt. Gefahren und Risiken werden häufig verdrängt.

Die hannoverische Madsack Mediengruppe ist ein jüngeres Beispiel eines Angriffs. Die Verlagsangebote waren über mehrere Tage nur eingeschränkt verfügbar. Das gleiche Schicksal ereilte die Funke-Mediengruppe im Dezember 2020. Cyberkriminalität ist jedoch ein branchenübergreifendes Problem. Jede Unternehmensgröße, jede Unternehmensform kann betroffen sein. Dazu gehören auch kleine und mittlere Unternehmen, die häufig vergleichsweise schlecht geschützt und damit gefährdet sind. Das Thema der digitalen Sicherheit wurde im Mittelstand lange vernachlässigt. Doch die Sicherheitsarchitektur des Unternehmens sollte höchste Priorität haben – und somit zur Chefsache werden.

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 (2020) 1.070 Unternehmen mit mindestens 10 Mitarbeiter*innen zum Thema Wirtschaftsschutz befragt: 75 Prozent der befragten Unternehmen sind bereits Opfer von digitaler Spionage, Sabotage und Datendiebstahl gewesen. Weitere 13 Prozent der Unternehmen gaben an, vermutlich betroffen gewesen zu sein. Bei den kleineren Unternehmen mit einer Mitarbeiterzahl zwischen 10 und 99 beläuft sich der Anteil sogar auf 79 Prozent. Weitere 9 Prozent vermuteten digitale Angriffe.

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat 2020 das Meinungsforschungsinstitut Forsa beauftragt, 300 KMU zu den Cyberrisiken im Mittelstand zu befragen. Demnach schätzen 69 Prozent der befragten Unternehmen Cyber-Kriminalität als eine Gefahr für den Mittelstand ein. Aber nur 28 Prozent sehen ein Risiko für das eigene Unternehmen. Das geringe Risikobewusstsein manifestiert sich darin, dass Cybersecurity für viele Befragte keine Priorität hat. Dabei gaben 26 Prozent der befragten Mittelständler an, bereits Opfer einer Cyberattacke gewesen zu sein. Die Hälfte der befragten Unternehmen brauchte bis zu drei Tage, um die erlittenen Schäden wieder zu beheben. Bei 22 Prozent dauerte es sogar länger. 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 nach wie vor 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 kündigte sie den Ausbau des Bundesamts für Sicherheit in der Informationstechnik (BSI) als „nationale Cybersicherheitsbehörde“ an. Das BSI sollte als unabhängige und neutrale Beratungsstelle – gerade auch für KMU – für Fragen der IT-Sicherheit gestärkt werden. Mit dem Entwurf des IT-Sicherheitsgesetzes 2.0 wird der Auftrag des BSI in diesem Jahr erweitert. Auch die Cyber-Sicherheitsstrategie wird derzeit fortgeschrieben. Im Herbst 2020 traf sich der Nationale Cyber-Sicherheitsrat zur Evaluierung der bisherigen Ergebnisse. Die aktualisierte Fassung soll bis Mitte 2021 vom Kabinett beschlossen werden. Aus dieser Strategie ist auch der Nationale Pakt Cybersicherheit hervorgegangen, dessen Ziel es ist, alle wichtigen gesellschaftlichen Gruppen in gemeinsamer Verantwortung für digitale Sicherheit einzubinden. In einem ersten Kompendium von November 2020 wurde die Cybersicherheitslandschaft in Deutschland skizziert. Das im Koalitionsvertrag angekündigte Bündnis für Cybersicherheit mit der Wirtschaft wurde im Herbst 2018 etabliert. Seitdem gibt es jedoch keine nennenswerten Aktivitäten oder Ergebnisse. Für KMU wurden die Beratungsangebote ausgebaut. So bietet das BSI ein „Erste-Hilfe-Paket“ für Unternehmen an, die von einem IT-Sicherheitsvorfall betroffen sind.

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