Cyberangriff im KMU: Warum der Verwaltungsrat nicht auf die IT zeigen kann

Ein einziger unbedachter Klick der Belegschaft kann den Verwaltungsrat in juristische Bedrängnis bringen. Cybersicherheit ist schon lange kein reines IT-Problem mehr, sondern eine unübertragbare rechtliche Pflicht der Unternehmensführung. Die Rechtskolumne.

ANDRÉ BRUNSCHWEILER

Jüngste Phishing-Wellen im Namen bekannter Schweizer Softwareanbieter zeigen, wie denkbar einfach ein Cyberangriff erfolgen kann: Ein Mitarbeiter erhält eine E-Mail, die scheinbar vom vertrauten IT-Dienstleister stammt. Aus Sicherheitsgründen müsse das Passwort sofort erneuert werden, andernfalls werde das Konto gesperrt. Der enthaltene Link führt auf eine täuschend echt aussehende Anmeldeseite. Nach der Eingabe der Zugangsdaten verschaffen sich die Angreifer Zugang zum Unternehmenskonto, ändern Zahlungsinformationen und greifen auf geschäftsrelevante Daten zu.

Diese Vorfälle illustrieren zweierlei: Erstens betreffen Cyberrisiken längst nicht mehr nur Grossunternehmen. Zweitens muss das eigene Unternehmen nicht einmal direkt gehackt werden, um betroffen zu sein. Externe IT-Provider, Cloud-Lösungen, Buchhaltungssoftware, Payroll-Anbieter oder andere Dienstleister können ebenfalls zum Einfallstor werden. Eine Auslagerung kann effizient und sinnvoll sein. Rechtlich bedeutet sie aber keine Entlastung. Für die Geschäftsleitung und den Verwaltungsrat können sich daraus Haftungsrisiken ergeben.

Cybersicherheit als Pflicht

Für die meisten KMU gibt es in der Schweiz kein allgemeines, umfassendes Cybersecurity-Gesetz. Die Pflichten ergeben sich vielmehr aus verschiedenen Rechtsquellen, insbesondere aus dem Gesellschaftsrecht, Datenschutzrecht, Vertragsrecht und je nach Branche auch aus Spezialregulierungen.

Für den Verwaltungsrat stehen die allgemeinen aktienrechtlichen Pflichten im Vordergrund: Die Oberleitung der Gesellschaft, die Festlegung der Organisation und die Oberaufsicht über die Geschäftsführung gehören zu seinen unübertragbaren Aufgaben (Artikel 716a OR). Zudem müssen Verwaltungsräte ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren (Artikel 717 OR). Dazu gehört heute auch der Umgang mit wesentlichen Cyberrisiken.

Der Verwaltungsrat muss keine Firewall konfigurieren. Er muss auch keine Serverprotokolle lesen. Aber er ist verantwortlich dafür, dass die wichtigsten Risiken erkannt sind, die Zuständigkeiten geklärt sind, Schutzmassnahmen bestehen und das Vorgehen im Ernstfall definiert ist. Cybersicherheit ist technisch in der Umsetzung, aber organisatorisch ein Führungsthema. Eine Vernachlässigung des Themas kann haftungsrechtliche Folgen für Verwaltungsräte haben. Ein Cyberangriff allein begründet zwar noch keine Haftung. Kritisch wird es aber, wenn der Verwaltungsrat erkennbare Risiken ignoriert, keine Verantwortlichkeiten festlegt oder elementare Schutzmassnahmen nicht verlangt.

Kommt es bei einem Cybervorfall zu einem Abfluss von Personendaten, wird aus dem IT-Problem rasch auch ein Datenschutzthema. Das Datenschutzgesetz verlangt, dass Verantwortliche und Auftragsbearbeiter durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten (Artikel 8 DSG). Dazu gehören je nach Situation etwa Zugriffsbeschränkungen, Verschlüsselungen, Protokollierung, Backups und klare Berechtigungskonzepte.

Wer im Chefsessel sitzt, trägt am Ende die Verantwortung. •••••QUELLE/XYZ•••••

Bei mangelnder Vorbereitung drohen Verwaltungsrat und Geschäftsleitung Haftungsrisiken.

Konkrete Massnahmen

Cyberrisiken sollten im Verwaltungsrat regelmässig behandelt und die notwendigen Sicherheitsmassnahmen beschlossen werden. Welche Themen dabei zu behandeln und welche Vorkehrungen zu treffen sind, hängt von den konkreten Umständen, dem Risikoprofil und der Branche des Unternehmens ab. Gewisse Grundfragen stellen sich jedoch für praktisch jedes Unternehmen.

So ist in einem ersten Schritt zu klären, welche Systeme für den Betrieb unverzichtbar sind und welche Daten besonderen Schutz erfordern. Auch externe Dienstleister gehören auf den Prüfstand, insbesondere durch vertragliche Vorgaben zu Sicherheitsstandards und Haftungsregeln. In der Folge müssen Notfallprozesse erstellt und praktisch getestet werden. Schliesslich braucht es klare Verantwortlichkeiten: Wer setzt die Massnahmen um, und wer entscheidet im Krisenfall?

Eine saubere Dokumentation zeigt im Haftungsfall, dass der Verwaltungsrat das Risiko erkannt und sich damit auseinandergesetzt hat, und kann helfen, das Haftungsrisiko zu minimieren. Die identifizierten Risiken und Massnahmen müssen jedoch nicht nur umgesetzt, sondern auch regelmässig neu beurteilt werden.

Der Verwaltungsrat muss kein IT-Spezialist sein. Er muss die Risiken aber erkennen und die nötigen Schutzmassnahmen anordnen, soweit nötig unter Beizug von Spezialisten, bevor es zum Vorfall kommt.

André Brunschweiler ist Partner bei der Wirtschaftskanzlei Lalive in Zürich. Die Kanzlei berät von ihren Standorten in Zürich, Genf und London aus Unternehmen, Behörden sowie Private in komplexen, vorwiegend internationalen Sachverhalten und Streitigkeiten. Lalive publiziert regelmässig Rechtskolumnen auf moneyhouse.ch/kmuplus