MME

Cybersicherheit im Verwaltungsrat von KMU

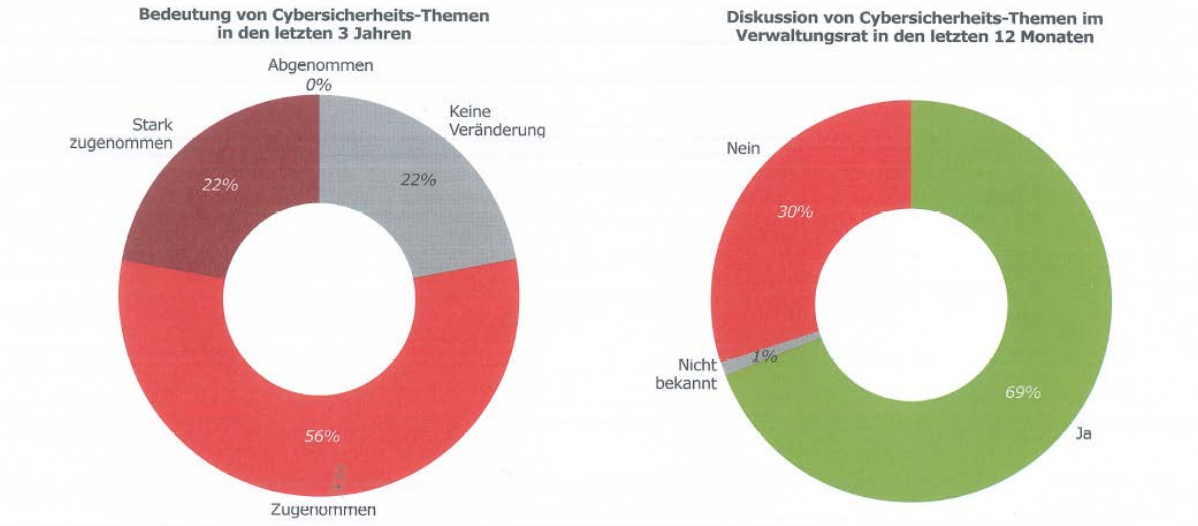
Dr. Martin Eckert
Michael Kunz

Trotz Zunahme von Cyberangriffen auf KMU werden die möglichen Folgen einer mangelhaften Cybersicherheits-Strategie von vielen Unternehmen unterschätzt. Da der Verwaltungsrat die Oberverantwortung für das Risk Management trägt, reicht es nicht aus, die Verantwortung für die Cybersicherheit an den CIO zu delegieren.

Cyberangriffe als Unternehmensrisiko

Ob Privatpersonen, Firmen oder staatliche Institutionen – gegen Cyberangriffe ist niemand gefeit. Auffallend ist, dass Cyberkriminelle vermehrt auch kleine und mittelgrosse Unternehmen angreifen. Wie eine aktuelle Studie des Beratungsunternehmens KMPG zeigt, gaben 88% von 60 befragten Firmen an, im Jahr 2016 einen Cyberangriff erlitten zu haben. Ähnliche Resultate lieferte eine aktuelle Umfrage der Zürich Versicherung, gemäss der bereits 40% der Schweizer KMU Opfer eines Cyberangriffs geworden sind. Diese Zahlen veranschaulichen auf eine eindrückliche Weise, dass ein proaktiver Umgang mit dem Thema Cybersicherheit auch für KMU unerlässlich ist.

Dass dem Thema Cybersicherheit auf strategischer Ebene zunehmend Aufmerksamkeit geschenkt wird, zeigt eine kürzlich veröffentlichte Umfrage des SwissVR Monitor. Von den insgesamt 464 befragten Verwaltungsratsmitglieder sind 78% der Ansicht, dass die Bedeutung von Cybersicherheits-Themen in den letzten drei Jahren branchenübergreifend zugenommen oder gar stark zugenommen hat. Entsprechend gaben auch über zwei Drittel der Befragten an, das Thema Cybersicherheit in den letzten 12 Monaten im Verwaltungsrat diskutiert zu haben. Aufhorchen lässt insbesondere der Umstand, dass Verwaltungsräte, in denen Cybersicherheits-Themen im letzten Jahr nicht diskutiert worden sind, stärker in KMU (35% der Befragten) als in Grossunternehmen (16%) vertreten sind. Dieses Resultat deckt sich mit einer weiteren Erkenntnis, die von der Umfrage zu Tage gefördert wurde. So gab ein Drittel der gefragten KMU Verwaltungsräte an, trotz gesteigertem Gefahrenbewusstsein über keine klare Strategie bezüglich Cybersicherheit zu verfügen. Dies zeigt, dass die möglichen Folgen von Cyberangriffen von vielen Firmen weiterhin unterschätzt werden.



Quelle: swissVR Monitor II/2017

Was sind die Pflichten des Verwaltungsrates?

Schon seit Jahren weisen Experten darauf hin, dass die Frage nicht lautet ob, sondern wann ein Unternehmen Ziel eines Cyberangriffs wird. Zudem dauert es im Schnitt 200 Tage, bis ein betroffenes Unternehmen bemerkt, dass sich ein Eindringling im System befindet. Die möglichen Konsequenzen eines solchen Dauerangriffs können kaum überschätzt werden. Insbesondere wenn im Rahmen eines Cyberangriffs Kundendaten abhandenkommen, kann die mit dem finanziellen Verlust einhergehende Rufschädigung ein enormes Ausmass annehmen. Im Gegensatz zu vielen anderen Ländern müssen Cyberangriffe gegen Schweizer Unternehmen zwar nicht von Gesetzes wegen gemeldet werden. Dies wird sich allerdings ändern, wenn die im Jahre 2016 in Kraft getretene Datenschutz-Grundverordnung der EU (GDPR), an die sich auch die meisten Schweizer Unternehmen halten müssen, im kommenden Mai offiziell anwendbar wird. Gemäss GDPR können Verstösse gegen die Verordnung mit bis zu 4% des globalen Jahresumsatzes eines Unternehmens gebüsst werden.

Für Unternehmen ist es somit von zentraler Bedeutung, dass die noch bestehenden Lücken in ihrem Cybersicherheits-Dispositiv in den kommenden Monaten geschlossen werden. Dabei geht es um weit mehr als um die Implementierung ausgeklügelter IT-Sicherheitslösungen. Einen absoluten Schutz vor Cyberangriffen kann kein System der Welt bieten. Doch mit der richtigen Vorbereitung kann der potentielle Schaden eines allfälligen Cyberangriffs oder Datenlecks aufs Minimum reduziert werden.

Gefordert ist dabei insbesondere der Verwaltungsrat. Er trägt die Oberverantwortung für das Risk Management und kann die Verantwortung für die Cybersicherheit nicht an den CIO delegieren. Wer als Verwaltungsrat nichts unternimmt, riskiert im Rahmen der Organhaftung persönlich belangt zu werden.

Was muss im Verwaltungsrat eines KMU konkret vorgekehrt werden?

- Cyber-Risiken gehören auf die Traktandenliste des Verwaltungsrates
- Initialisierung der Prüfung von Sofortmassnahmen
- Initialisierung einer Risikoanalyse
- Erarbeitung eines Risikokonzepts (Ziele, Definition von Sicherheitsstandards)
- Kontrolle der Umsetzung von technischen und organisatorischen Massnahmen
- Notfallpläne

Wie kann Sie MME bei der Erfüllung Ihrer Pflichten unterstützen?

In einem halbtägigen Workshop unter Beizug von technischen Spezialisten aus unserem Netzwerk können wir Sie auf Kurs bringen. Im Hinblick auf die persönliche Haftung der Mitglieder des Verwaltungsrats und der Geschäftsleitung ist danach die Dokumentation der entsprechenden Schritte zentral. Hier können wir Sie mit Dokumentenvorlagen bedienen (Cyber Risk Strategie, VR-Beschlüsse, Traktanden GL, GL Beschlüsse, Anpassung Organisationsreglemente, Pflichtenhefte, etc.).

Ihr Team

Dr. Martin Eckert
Legal Partner

martin.eckert@mme.ch

Manuela Eisenhut
Assistentin
+41 44 254 99 70

Dr. Andreas Glarner
Legal Partner

Andreas.glarner@mme.ch

Sabrina Costa Kaufmann
Assistentin
+41 44 726 99 77

Michael Kunz
Legal Associate, LL.M.

Michael.kunz@mme.ch

Manuela Eisenhut
Assistentin
+41 44 254 99 70

Philipp Stadler
Legal Associate

Philipp.stadler@mme.ch

Sabrina Costa Kaufmann
Assistentin
+41 44 726 99 77