Cyber Security:

Was tun als Verwaltungsratsmitglied?

Prinzip 1: Verantwortung für Cyber Resilienz / Widerstandsfähigkeit
Der Verwaltungsrat als Ganzes trägt die oberste Verantwortung für die Überwachung von Cyber-Risiko und Widerstandsfähigkeit. Er kann die Hauptaufsicht an einen bestehenden Ausschuss (z.B. den Risikoausschuss) oder einen neuen Ausschuss (z.B. Ausschuss für Cyber-Resilienz).

Prinzip 2: Beherrschung des Themas
Die Verwaltungsratsmitglieder erhalten bei ihrem Eintritt in den Verwaltungsrat eine Einweisung in die Cyber-Resilienz und werden regelmässig über aktuelle Bedrohungen und Trends informiert, wobei Beratung und Unterstützung durch unabhängige externe Expertinnen und Experten auf Anfrage zur Verfügung steht.

Prinzip 3: Verantwortlicher Beauftragter für Cyber-Resilienz
Der Verwaltungsrat stellt sicher, dass eine oder ein Unternehmensverantwortliche:r für die Berichterstattung über die Fähigkeit der Organisation, die Cyber-Resilienz zu managen, verantwortlich ist. Zudem verfolgt er die Fortschritte bei der Zielumsetzung für die Cyber-Resilienz. Der Verwaltungsrat stellt sicher, dass der oder die Beauftragte:r regelmässig Zugang zum VR hat und über ausreichende Befugnisse, Sachkenntnis, Erfahrung und Ressourcen verfügt, um diese Aufgaben zu erfüllen.

Prinzip 4: Integration der Cyber-Resilienz

Der Verwaltungsrat stellt sicher, dass die Geschäftsleitung die Cyber-Resilienz und die Bewertung von Cyber-Risiken in die allgemeine Geschäftsstrategie und in das unternehmensweite Risikomanagement sowie in die Budgetierung und Ressourcenzuweisung integriert.

Prinzip 5: Risikobereitschaft
Der Verwaltungsrat definiert und quantifiziert jährlich die Risikotoleranz des Unternehmens in Bezug auf die Cyber-Resilienz und stellt sicher, dass diese mit der Unternehmensstrategie und der Risikobereitschaft übereinstimmt. Er wird über das aktuelle und künftige Risikopotenzial sowie über die gesetzlichen Anforderungen und Branchen-/Gesellschafts-Benchmarks für die Risikobereitschaft informiert.

Prinzip 6: Risikobewertung und Berichterstattung
Der Verwaltungsrat verpflichtet die Geschäftsleitung, eine quantifizierte und verständliche Bewertung von Cyber-Risiken, -Bedrohungen und -Ereignissen vorzunehmen und dies als kontinuierlicher Tagesordnungspunkt bei Verwaltungsratssitzungen aufzugreifen. Er validiert diese Bewertungen mit seiner eigenen strategischen Risikobewertung unter Verwendung des Board Cyber Risk Framework.

Prinzip 7: Resilienz-Pläne

Der Verwaltungsrat stellt sicher, dass die Geschäftsleitung der oder die Verantwortliche für die Cyber-Resilienz bei der Erstellung, Umsetzung, Prüfung und laufenden Verbesserung von Cyber-Resilienzplänen unterstützt, die auf das gesamte Unternehmen abgestimmt sind. Der oder die Verantwortliche muss die Leistung überwachen und dem Verwaltungsrat regelmässig Bericht erstatten.

Prinzip 8: Gemeinschaft

Der Verwaltungsrat ermutigt die Geschäftsleitung, mit anderen Interessengruppen zusammenzuarbeiten, soweit dies relevant und angemessen ist, um die systemische Cyber-Resilienz sicherzustellen.

Prinzip 9: Überprüfung

Der Verwaltungsrat stellt sicher, dass jährlich eine formelle, unabhängige Überprüfung der Cyber-Resilienz der Organisation durchgeführt wird.

Prinzip 10: Effektivität

Der Verwaltungsrat überprüft regelmässig die eigene Leistung bei der Umsetzung dieser Grundsätze oder holt unabhängigen Rat ein, um sich kontinuierlich zu verbessern.

St.Gallen, im August 2023

Zusammengefasst von Rolf Brunner, Partner und VR-Mitglied bei CONTINUUM AG

Quellen:

Universität St.Gallen WORLD ECONOMIC FORUM DREAMLAB