Ist Ihr Unternehmen für Cyber Security Reporting gerüstet?

Jacqueline Etter, Senior Consultant IRF Communications AG

Investoren wollen vermehrt Klarheit haben, ob Unternehmen sich dieser Risiken bewusst sind und entsprechende Prozesse und Massnahmen zur Verhinderung von Cyber-Gefahren implementiert sind.

Cybersicherheit ist und bleibt eine der grössten Gefahren für Unternehmen weltweit.[1] Dies überrascht wenig, liegen Finanzprodukten und -dienstleistungen meist internetbasierte Systeme zu Grunde, die laufende Vernetzung unterschiedlicher Plattformen und Zusammenarbeit mit Drittanbietern tragen das ihre zu weiteren operationellen Risiken und Abhängigkeiten bei.

Photo by Hannah Joshua on Unsplash

Die Ende 2018 erschienene Untersuchung «PRI – Stepping up Governance on Cyber Security 2018» von 100 Unternehmen zeigt Handlungsbedarf: Während die meisten Firmen «Cyber Security» als Risiko wahrnehmen, informieren erst wenige darüber, ob und welche Richtlinien, Führungsstrukturen und Prozesse vorhanden sind, um Cyber-Gefahren abzuwenden.

[1] Nachzulesen beispielsweise im Jahresbericht der US-Regierungsbehörde **Financial Stability Oversight Council (FSOC)**.

Gemäss der Studie

- lieferte nur ein Fünftel der Unternehmen Informationen zu zwei oder weniger der 14 bewerteten Indikatoren (siehe Checkliste),
- gaben über 30% nicht explizit an, dass sie den Anforderungen von Datenschutz- und Cybersicherheitsgesetzen entsprechen,
- erwähnten fast 60% nicht, dass der Verwaltungsrat bzw. ein Komitee für die Cybersicherheit zuständig sind,
- gaben weniger als zwei Drittel kaum oder gar keine Auskunft über die Häufigkeit und die Kanäle für die Kommunikation mit dem Verwaltungsrat,
- gaben nur 15% der Unternehmen an, dass sie für alle Mitarbeiter ein Cybersicherheitstraining anbieten, und nur wenig mehr - 17% - teilten mit, dass sie auch regelmässige Audits durchführen.

Unternehmen sollten bedenken, dass nicht nur internationaler Vorgaben zunehmen, sondern auch der Informationsbedarf der Investoren wächst. Ein paar Beispiele:

- Das «**BIS Committee on Payments and Market Infrastructures»** und der Vorstand der «**International Organization of Securities Commissions»** haben bereits im Juni 2016 Leitlinien zur Cyber-Resilienz für Finanzmarktinfrastrukturen (FMIs) herausgegeben.
- Eine Analyse der **Bank für Internationalen Zahlungsausgleich (BIZ)** zeigt 2017 auf, dass Banken im Cyberspace zwar am stärksten exponiert sind und die Bankenaufsicht sich sehr für die Sicherheit interessiert, jedoch erst in wenigen Ländern wie Hongkong, Singapur, Grossbritannien und den USA spezifische regulatorische und überwachende Initiativen existieren. Dies dürfte sich jedoch bald ändern, wie zum Beispiel die Einführung von neuen Analyseinstrumenten wie das Cybersecurity Assessment Tool der FFIEC zeigt: Es wird nicht nur zur Risikoerkennung eingesetzt, sondern gibt auch darüber Auskunft wie resilient bzw. gut vorbereitet ein Unternehmen ist.
- Die im Mai 2018 in Kraft getretene allgemeine Datenschutzverordnung der Europäischen Union GDPR harmonisiert die bestehenden Datenschutzgesetze in ganz Europa. GDPR verlangt von den Unternehmen ein angemessenes Mass an Aufsichts-, Sicherheits- und Meldeprotokollen im Falle von Datenverstössen und anschliessenden Korrekturmaßnahmen. Davon bleibt auch die Schweiz nicht unberührt.

Machen Sie sich fit

Evaluieren Sie regelmässig verschiedene Kriterien: die Abwehr von potenziellen Angriffen, die internen Kontrollmechanismen, der Umgang mit Vorfällen sowie die Planung bzw. die Simulation von Ernstfällen. Sie erhalten damit einen guten Überblick über mögliche Bedrohung und vor allem über allfällige Schwachstellen. Vor allem informieren Sie Ihre Investoren über implementierte Prozesse!

>>> Nutzen Sie die Checkliste (PDF)