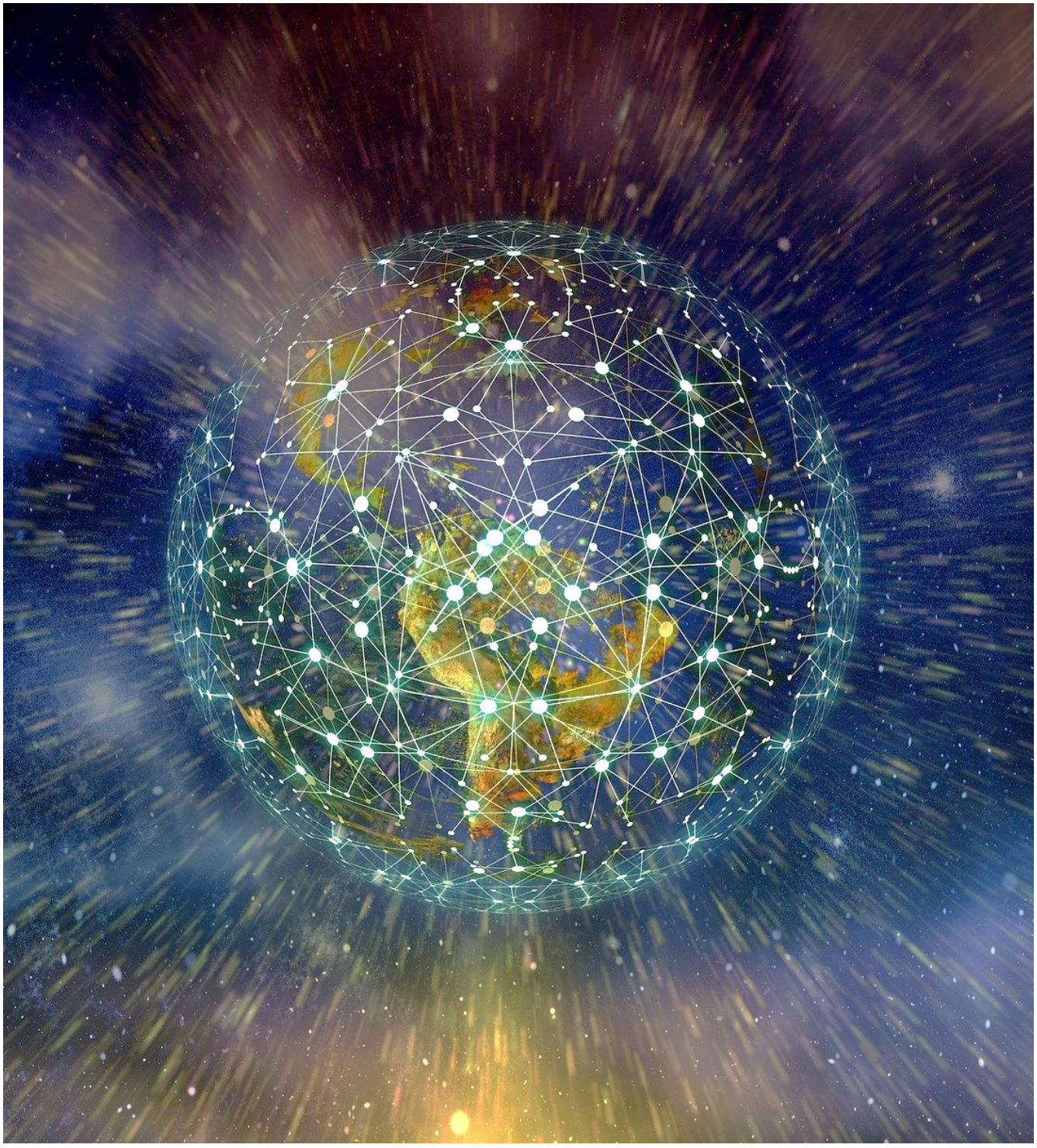
swissVR

swissVR Impuls III/2020
August 2020



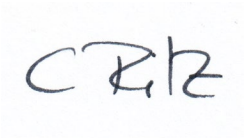
Impuls für KMU-Verwaltungsräte: Cyber-Resilienz

Vorwort

Die letzten Monate haben gezeigt, dass auch vermehrt Schweizer Firmen in den Fokus von Cyberkriminellen geraten und Schaden durch Online-Betrug und Ransomware-Attacken erleiden. Dabei spielt die Grösse des Unternehmens keine Rolle.

Wie können Sie die Widerstandsfähigkeit gegen Cyber-Risiken in Ihren Unternehmen erhöhen und welche Rolle sollte der Verwaltungsrat dabei einnehmen?

Zu diesen Fragen soll Ihnen der vorliegende swissVR Impuls als Hilfestellung dienen. Wir wünschen Ihnen eine erfolgreiche Umsetzung und dass Sie von erfolgreichen Angriffen verschont bleiben.



Cornelia Ritz Bossicard
Präsidentin swissVR

Dr. Matthias Bossardt
Leiter Cyber Security and Technology Risk Consulting
KPMG

Dieser swissVR Impuls wurde von swissVR zusammen mit KPMG ausgearbeitet.

Autorenschaft:

Cornelia Ritz Bossicard, unabhängige Verwaltungsrätin, Präsidentin swissVR (cornelia.ritz@swissvr.ch) und

Dr. Matthias Bossardt, Leiter Cyber Security und Technology Risk Consulting, KPMG (mbossardt@kpmg.com)

Titelseite: pixabay.com/Gerd Altmann

Dieser Text soll betroffenen und interessierten Unternehmen, namentlich KMU, als mögliche Orientierungshilfe dienen. Er gibt die Erkenntnisse der Autoren wieder und beinhaltet weder die Meinung noch konkrete Empfehlungen der Vereinigung swissVR an ihre Mitglieder. Die Autoren, swissVR und KPMG übernehmen keine Verantwortung, Garantie oder Haftung für die Korrektheit und Angemessenheit der Massnahmen und lehnen jede Haftung für allfällige direkte oder indirekte finanzielle oder sonstige Schäden ab, die sich ergeben, wenn eine Person aufgrund dieser Informationen eine Handlung vornimmt oder unterlässt.

swissVR ist eine Vereinigung für Verwaltungsrats–mitglieder in der Schweiz, von Verwaltungsräten für Verwaltungsräte – attraktiv – unabhängig – fokussiert. Mit ihrem Angebot trägt sie zur Professionalisierung der Verwaltungsräte in der Schweiz bei. swissVR fördert den Erfahrungs-austausch unter Verwaltungsrätinnen und Verwaltungsräten von Unternehmen aller Branchen und bietet seinen über 900 Mitgliedern ein bedürfnisspezifisches Informations- und Weiter-bildungsangebot. swissVR richtet sich exklusiv an Personen mit einem aktiven Verwaltungsrats-mandat.

Für weitere Informationen zu swissVR und zur Mitgliedschaft: www.swissvr.ch

swissVR, Suurstoffi 1, 6343 Rotkreuz
info@swissvr.ch, +41 41 757 67 11

(Version vom 12. August 2020)

Tipps für KMU-Verwaltungsräte zur Cyber-Resilienz

Cyber-Risiken haben sich in den letzten Jahren einen prominenten Platz auf den Traktandenlisten vieler Verwaltungsräte ergattert. Zu Recht: Die jüngsten Cybervorfälle hatten schwerwiegende Auswirkungen auf die betroffenen Unternehmen. Sie litten unter Geschäftsunterbrüchen, Datenschutzverletzungen, finanziellen Verlusten sowie Reputations- und Vertrauensproblemen. In einigen Fällen wirkten sich die Vorfälle erheblich auf den Unternehmenswert aus, bis hin zum Konkurs. Wie der umfangreichen Medienberichterstattung zu entnehmen ist, können sowohl grosse als auch kleine Unternehmen gleichermassen Opfer von Cyber-Angriffen werden.

Neben den offensichtlichen operationellen Risiken erkennen fortgeschrittenere Unternehmen, dass Cyber-Resilienz eine strategische Chance ist, sich von der Konkurrenz abzuheben. Verantwortungsbewusstes Management von Cyber-Risiken und sogar ein gut gemanagter Cyber-Vorfall können das Vertrauen der Stakeholder eines Unternehmens stärken, seien dies Kunden, Investoren, Lieferanten oder Aufsichtsbehörden. Darüber hinaus kann ein cyber-resilientes Unternehmen digitale Technologien wie Datenanalyse, künstliche Intelligenz und Cloud Computing mit Zuversicht und nachhaltig nutzen, um seine Wettbewerbsposition zu verbessern.

1. Cyber-Risiken sind nicht technische, sondern operationelle Risiken

Cyber-Risiken werden von Unternehmen oft als eine nicht greifbare, fast schon unreale Bedrohung angesehen. Dies nicht zuletzt, weil solche Angriffe oft hochkomplexe, technische Schwachstellen ausnutzen. Daraus zu schliessen, dass es sich folglich bei Cyber-Risiken um technische Risiken handeln muss, die von der IT-Organisation zu bewältigen sind, ist allerdings ein Trugschluss.

Zieht man die möglichen Folgen eines Cyberangriffs in Betracht, wird klar, dass es sich um operationelle Risiken handelt, mit denen Verwaltungsräte und Geschäftsführungen vertraut sein müssen:

Datenlecks
- Datenschutzverletzungen
- Offenlegung von geistigem Eigentum und vertraulichen Unternehmensinformationen

Abfluss von Vermögenswerten
- Unautorisierte oder durch Täuschung ausgelöste Zahlungen
- Lösegeldzahlungen

Betriebsunterbruch
- Stillstand der Produktion
- Ausfall der Logistik

Fehlfunktion von Produkten und fehlerhafte Dienstleistungen

Eigene Organisation als Einfallstor für Cyberangriffe auf Kunden

Diese direkten Folgen von Cyber-Angriffen können in Schäden resultieren wie:

- Verlust von Reputation und Kundenvertrauen
- Umsatzeinbrüche
- Administrative Kosten für Ersatz und Wiederherstellung
- Rechtskosten und Bussen
- Haftung, Schadenersatz, Kompensationszahlungen für Verspätungen
- Zeitverlust, verspäteter Markteintritt

2. Die Rolle des Verwaltungsrats

Die vier Hauptaufgaben des Verwaltungsrats beziehen sich auf Strategie, Systeme, Mitarbeitende und Überwachung[1]. Daraus leiten sich direkt Aufgaben im Zusammenhang mit der Cyber-Resilienz des Unternehmens ab.

Strategie: Abnahme einer Cyberstrategie als Teil der Unternehmensstrategie
- Geschäftstreiber
- Betriebsmodell
- Produkte/Dienstleistungen

Systeme: Ausgestaltung des Risiko- und Krisenmanagements
- Identifikation und Behandlung von Cyberrisiken im Unternehmenskontext
- Krisenmanagement, das auch im Falle von Cyberkrisen greift

Mitarbeitende: Bestellung der Geschäftsführung
- Der Verwaltungsrat stellt bei der Ernennung der mit der Geschäftsführung betrauten Personen sicher, dass die Geschäftsführung über ein genügendes Verständnis zu operationellen Risiken verfügt, um Cyber-Risiken angemessen zu managen

[1] Best Practice im KMU, www.ccg.ifpm.unisg.ch

Überwachung: Oberaufsicht über die Geschäftsführung und Einhaltung von Gesetzen und Weisungen
- Compliance mit Regulationen zu Datenschutz, Informationssicherheit, Produktsicherheit, internen Weisungen etc.
- Cyber-Reporting

Um diese Aufgaben im Zusammenhang mit der Cyber-Resilienz wahrzunehmen, gilt es im Unternehmen eine Governance zu etablieren, die Cyber-Massnahmen dem Risiko entsprechend umsetzt.

3. Cyber-Grundschutzmassnahmen rigoros umsetzen

Während in der Vergangenheit der Fokus, ähnlich einer mittelalterlichen Stadtbefestigung, auf technische Massnahmen zur Verhinderung eines Eindringens von Angreifern in das Unternehmen lag (Stichwort: Firewall), ist eine moderne Cyber-Strategie breiter abgestützt. Dies weil davon ausgegangen werden muss, dass mit der zunehmenden Vernetzung und Integration zwischen Unternehmen, Lieferanten und Kunden, ein Angreifer in geschützte Bereiche eindringen kann und wird.

Eine moderne Strategie, ist deshalb darauf ausgelegt, diese Eindringlinge zeitnah zu erkennen, sie daran zu hindern, Schäden anzurichten und so die Widerstandsfähigkeit eines Unternehmens gegenüber Cyber-Angriffen zu erhöhen.

Aus diesem Grund spricht man im Zusammenhang mit dem Management von Cyber-Risiken vermehrt von Cyber-Resilienz.

Entsprechend teilt das weltweit verbreitet NIST Cyber-Framework[2] Cyber-Massnahmen in fünf «Funktionen» ein: Identify, Protect, Detect, React, und Recover.

Im Unternehmen gilt es, mit Cyber-Massnahmen eine gute Balance zwischen den fünf Funktionen zu erzielen. Ebenfalls ist darauf zu achten, dass Cyber-Resilienz nicht mit technischen Massnahmen allein, sondern nur in Ergänzung mit organisatorischen / prozessorientierten (z.B. Vieraugenprinzip) und den Menschen betreffende Massnahmen (z.B. Sensibilisierung und Training) erreicht werden kann.

Der Verwaltungsrat sollte darauf achten, dass die folgenden Grundschutzmassnahmen rigoros umgesetzt sind:

Identifizieren («Identify»)
- Zuweisen von Aufgaben, Kompetenzen und Verantwortlichkeiten
- Kennen der unternehmenskritischen Daten UND Geschäftsprozesse
- Inventarisieren der IT-Systeme und Software (auch Internet der Dinge)

Schützen («Protect»)
- Sensibilisierung und Training der Mitarbeitenden
- Identitäts- und Zugriffsmanagement, inklusive Aufzeichnungen
- Regelmässiges «Patching» aller IT-Systeme
- Durchsetzung von Sicherheitsmassnahmen bei der Zusammenarbeit mit Dritten

Entdecken («Detect»)
- Malware Erkennung
- Segmentierung und Überwachung des Netzwerks
- Periodische/kontinuierliche technische Sicherheitstests, auch in der Software- und Produktentwicklung

Reagieren («React»)
- Entwicklung und Testen/Üben der Cyber-Notfallpläne

Wiederherstellen («Recover»)
- Back-up

4. Fragen für den Verwaltungsrat

Das Verständnis des Verwaltungsrats für die Cyber-Bedrohung und die Mitwirkung an der Ermittlung der Reaktion sind sowohl im Hinblick auf die Rolle des Verwaltungsrats als Unternehmensstratege als auch auf seine Aufsichtsfunktion von entscheidender Bedeutung. Der Verwaltungsrat sollte Klarheit über die folgenden Themen erlangen.

1. Welches sind die neuen **Cyber-Bedrohungen und -risiken**; inwiefern betreffen diese unsere Organisation?
2. Genügt unser **Cyber-Resilienz-Programm** den Herausforderungen, die sich aus der heutigen und zukünftigen Cyber-Bedrohungslage ergeben?
3. Verstehen wir unsere **heutigen Schwachstellen** (auch in Bezug auf unsere Lieferanten und Dienstleister) und welche **Prozesse** haben wir, um die identifizierten Cyberrisiken zu adressieren?
4. Ist unsere Organisation genügend vorbereitet, um auf einen **Angriff angemessen reagieren** zu können?
5. Welche **Indikatoren von Schlüsselrisiken** (Key Risk Indicators) und **Leistungskennzahlen** (Key Performance Indicators) sollen wir auf VR-Ebene beobachten, um unsere Aufsichtsfunktion wahrnehmen zu können?
6. Hält unsere Organisation ihre **gesetzlichen und regulatorischen Verpflichtungen** zur Sicherung von Daten ein (z.B. Datenschutz)?
7. Ist Cyber-Resilienz **Teil der strategischen Besprechungen im VR** und wann haben wir uns das letzte Mal mit der Cyberbedrohung befasst?
8. Wie entwickeln wir unsere Organisation von einer **reaktiven zu einer antizipierenden** Herangehensweise in Bezug auf die Cyber-Bedrohung?
9. Ist uns die **Konkurrenz** voraus? Falls ja, ist dies ein **Wettbewerbsvorteil** für sie?

[2] https://www.nist.gov/cyberframework

5. Cyber-Reporting für den Verwaltungsrat

Viele Verwaltungsräte tun sich schwer damit, von ihren Managementteams eine adressatengerechte Berichterstattung über Cyber-Risiken und den Stand der Cyber-Resilienz des Unternehmens zu erhalten. Oft handelt es sich bei solchen Berichten um detaillierte technische und mit Jargon belasteten Übersichten zum Stand der Kontrollen, ohne dass ein klarer Zusammenhang mit operationellen Cyber-Risiken und den möglichen Auswirkungen auf das Geschäft hergestellt wird. Folglich ist es dem Verwaltungsrat nur schwer möglich, seinen Pflichten im Zusammenhang mit Cyberrisiken nachzukommen.

Eine gute Berichterstattung ermöglicht es dem Verwaltungsrat

1) zu verstehen, wie sich Cyber-Risiken auf die Fähigkeit des Unternehmens auswirken, seine Geschäftsstrategie umzusetzen und

2) Cyber-Risiken gegen andere operationelle und strategische Risiken zu positionieren und Ressourcen entsprechend zu priorisieren.

Als Ausgangspunkt sollten regelmässige Cyberberichte an den Verwaltungsrat die folgenden Themen enthalten.

Strategische Bedrohungslage
- Angriffsvektoren, Angreifer
- (Branchen-)Trends

Cybervorfälle im Unternehmen
- Erkenntnisse und Handlungsbedarf

Übersicht Cyber-Toprisiken
- Schadenspotential (insbesondere in Bezug auf geschäftskritische Prozesse und Daten)
- Trends

Cyber-Resilienz-Massnahmen
- Abdeckung und Wirksamkeit in Bezug auf die Cyber-Toprisiken
- Abdeckung und Wirksamkeit der unternehmensweit anzuwendenden Grundschutz-Massnahmen
- Compliance mit regulatorischen Anforderungen, Industrienormen, internen Weisungen

Cyberstrategie/-programm
- Stand der Umsetzung
- Auswirkung auf Toprisiken

Handlungs-/Investitionsbedarf

6. Fazit

Cyber-Risiken sind operationelle Risiken, die den Fortbestand eines Unternehmens gefährden können und mit denen sich der Verwaltungsrat im Rahmen seiner gesetzlichen Aufgaben zu befassen hat. Der Verwaltungsrat sollte darauf achten, dass das Unternehmen seine Cyberstrategie auf Resilienz ausrichtet. Dazu gehört, dass die Cyber-Grundmassnahmen rigoros umgesetzt werden.

Um Klarheit über den Stand der Cyber-Risiken und -Resilienz des Unternehmens zu haben, ist ein adressatengerechtes Cyber-Reporting notwendig.

Neben dem Management von Cyber-Risiken, sollte der Verwaltungsrat zusammen mit der Geschäftsführung auch analysieren, inwiefern sich die Cyber-Resilienz als Unterscheidungsmerkmal und Wettbewerbsvorteil nutzen lässt.

Ergänzende Links

- National Cyber Security Center
  https://www.ncsc.admin.ch/melani/de/home.html
- Werkzeuge für KMU
  https://gcatoolkit.org/de/kmu
- NIST Cyber Framework
  https://www.nist.gov/cyberframework
- Password Breaches
  https://haveibeenpwned.com/
- KPMG
  https://home.kpmg/xx/en/home/services/advisory/risk-consulting/cyber-security-services.html

  https://www.kpmg.ch/cyber