Cyber-Resilienz – Steigende Bedeutung für Verwaltungsräte

swissVR Monitor II/2023
September 2023

swissVR®

Deloitte.
Global Boardroom Programme | Switzerland

HSLU Hochschule Luzern

Inhaltsverzeichnis

Über die Umfrage
Der vierzehnte swissVR Monitor basiert auf einer Befragung von 400 Schweizer Verwaltungsrätinnen und Verwaltungsräten. Die Umfrage erfasst die Einschätzungen der Verwaltungsratsmitglieder zu Konjunktur- und Geschäftsaussichten sowie zu Fragen der Corporate Governance. Zudem greift sie jeweils ein aktuelles Thema auf – dieses Mal die Cyber-Resilienz von Unternehmen.

Die Umfrage für den vorliegenden swissVR Monitor wurde von swissVR in Zusammenarbeit mit dem Beratungsunternehmen Deloitte und der Hochschule Luzern im Zeitraum vom 22. Mai 2023 bis zum 8. Juli 2023 durchgeführt. Die 400 Teilnehmenden repräsentieren sowohl Verwaltungsratsmitglieder von börsenkotierten Unternehmen als auch von kleinen und mittelgrossen Unternehmen (KMU) und stammen aus allen relevanten Branchen der Schweizer Wirtschaft. 32% der Teilnehmenden sind Verwaltungsratsmitglieder in grossen, 35% in mittelgrossen und 33% in kleinen Unternehmen.

Zweck des swissVR Monitors ist es einerseits, aktiven Verwaltungsratsmitgliedern eine Orientierung zu bieten, indem die eigene Einschätzung zu Verwaltungsratsthemen mit jener von anderen Verwaltungsratsmitgliedern verglichen werden kann. Andererseits wird der breiten Öffentlichkeit aufgezeigt, wie Verwaltungsratsmitglieder Fragen rund um ihre Tätigkeit und die aktuelle wirtschaftliche Situation einschätzen.

Hinweis zur Methodik
Beim Vergleich mit den Umfrageresultaten der vorhergehenden Studien gilt es zu beachten, dass die Zahl und die Zusammensetzung der Umfrageteilnehmenden jeweils unterschiedlich sind. Die Prozentzahlen sind so gerundet, dass die Summe der Antworten jeweils 100 Prozent ergibt. Die Unternehmensgrösse wurde über den Personalbestand ermittelt: Kleinunternehmen (1 bis 49 Mitarbeitende), mittelgrosse Unternehmen (50 bis 249 Mitarbeitende) und Grossunternehmen (250 und mehr Mitarbeitende).

Vorwort

Geschätzte Leserinnen und Leser

Wir freuen uns, Ihnen den swissVR Monitor II/2023 zu präsentieren. Für die vorliegende Ausgabe haben wir 400 Mitglieder von Schweizer Verwaltungsräten befragt. Die Resultate bilden deren Einschätzungen zu Konjunktur-, Branchen- und Geschäftsaussichten sowie Meinungen zu relevanten Themen ihrer VR-Tätigkeit ab.

Vor dem Hintergrund der über die vergangenen Jahre gestiegenen Bedeutung der Cyber-Resilienz greift der aktuelle swissVR Monitor dieses Fokusthema wie bereits in der Ausgabe II/2017 wieder auf. Aufgrund der über die letzten Jahre zunehmenden Anzahl von Cyber-Angriffen auf Unternehmen ist es auch für Verwaltungsräte wichtig, sich in ihren Mandaten mit der Cyber-Resilienz auseinandersetzen und in diesem Zusammenhang ein klares Verständnis der eigenen Rolle und der damit verbundenen Aufgaben zu entwickeln. Der aktuelle swissVR Monitor thematisiert deshalb unter anderem die möglichen Folgen von Cyber-Angriffen auf Unternehmen, die Selbsteinschätzung des Verwaltungsrats betreffend die Cyber-Resilienz und das Cyber-Reporting der Geschäftsleitung an den Verwaltungsrat.

Neben den Befragungsergebnissen bietet der swissVR Monitor II/2023 auch Interviews zum Fokusthema mit:

- Maya Bundt, Vorsitzende des Nominations- und Vergütungsausschusses der Valiant Bank sowie Verwaltungsratsmitglied von Bâloise und APG|SGA
- Florian Schütz, Delegierter des Bundes für Cybersicherheit und Leiter des Nationalen Zentrums für Cybersicherheit (NCSC), ab 1. Januar 2024 Direktor des Bundesamtes für Cybersicherheit
- Sonja Stirnimann, Vorsitzende des Prüfungsausschusses der Glarner Kantonalbank und Verwaltungsratsmitglied von Apiax

Wir bedanken uns herzlich bei den Interviewpartnern sowie bei allen VR-Mitgliedern, die an der Befragung teilgenommen haben. Wir wünschen Ihnen, geschätzte Leserinnen und Leser, eine interessante Lektüre.

Cornelia Ritz Bossicard
Präsidentin swissVR

Reto Savoia
CEO Deloitte Schweiz

Dr. Mirjam Durrer
Dozentin IFZ / Hochschule Luzern

Wichtigste Ergebnisse in Kürze

24%
der befragten VR-Mitglieder erwarten für die Schweizer Wirtschaft in den nächsten 12 Monaten eine ositive Konjunkturentwicklung.

Wirtschaftsaussichten leicht optimistischer als am Jahresanfang
Die befragten Verwaltungsratsmitglieder schätzen die Konjunktur-, Branchen- und Geschäftsaussichten für die nächsten 12 Monate insgesamt leicht optimistischer als im letzten swissVR Monitor am Jahresanfang ein. In allen drei Aussichtskategorien (Konjunktur, Branche und Geschäft) gehen jeweils mehr Befragte von einer positiven als von einer negativen Entwicklung aus. Es bleiben Unsicherheitsfaktoren wie geopolitische Risiken, eine unklare Energielage für den Winter 2023/2024 und ein sich als beständig erweisender, überdurchschnittlich hoher Teuerungsdruck.

42%
der Opfer eines Cyber-Angriffs geben einen Betriebsunterbruch als Folge für ihr Unternehmen an.

Cyber-Angriffe können gravierende Folgen für Unternehmen haben
Die Befragten, deren Unternehmen Opfer (mindestens) eines Cyber-Angriffs geworden ist, berichten von teilweise gravierenden Folgen auf die operativen Vorgänge. Am häufigsten kommt es in diesem Zusammenhang zu einem Unterbruch des Betriebs. Als weitere mögliche Konsequenzen eines Cyber-Angriffs werden Datenlecks sowie die Fehlfunktion von Produkten oder Dienstleistungen genannt. Folgeangriffe auf Kunden oder Abflüsse von Vermögenswerten sind vergleichsweise seltener der Fall.

55%
sehen eine starke Zunahme der Bedeutung von Cyber-Resilienz-Themen in den letzten drei Jahren.

Deutliche Zunahme der Bedeutung der Cyber-Resilienz
Fast alle befragten Verwaltungsratsmitglieder sind der Meinung, dass die Bedeutung von Cyber-Resilienz-Themen für ihr Unternehmen in den letzten drei Jahren zugenommen hat. Eine Mehrheit sieht sogar eine starke Zunahme – in Grossunternehmen noch häufiger als in Kleinunternehmen. Keine Veränderung der Bedeutung der Cyber-Resilienz gab es nur für eine kleine Minderheit der Befragten und gar eine Abnahme wurde von keinem einzigen Verwaltungsratsmitglied angegeben.

46%
der Unternehmen haben eine Versicherung für Cyber-Risiken.

Geteiltes Bild bei Versicherungen für Cyber-Risiken
Trotz der gestiegenen Bedeutung der Cyber-Resilienz und der teilweise gravierenden Folgen von Cyber-Angriffen verfügt lediglich knapp die Hälfte der Unternehmen über eine Versicherung für Cyber-Risiken. Überdurchschnittlich häufig versichern sich Firmen aus dem Finanzbereich, dem verarbeitenden Gewerbe und der Chemie sowie aus dem Baugewerbe. Die Unternehmensgrösse hat in diesem Zusammenhang nur einen geringen Einfluss.

56%
der VR-Gremien erhalten von der Geschäftsleitung ein Reporting zu Cyber-Vorfällen im Unternehmen.

Regelmässiges Cyber-Reporting an den Verwaltungsrat ausbaufähig
Laut Aussage der Befragten erhält etwas mehr als die Hälfte der Verwaltungsräte von der Geschäftsleitung ein regelmässiges Reporting zu Cyber-Vorfällen im Unternehmen oder zum Handlungs-/Investitionsbedarf bei der Cyber-Resilienz. In etwas weniger als der Hälfte der Fälle erfolgt eine Berichterstattung bezüglich der allgemeinen Bedrohungslage oder bezüglich Cyber-Resilienz-Massnahmen. Lediglich circa ein Drittel der Verwaltungsräte wird regelmässig durch die Geschäftsleitung über die Top-Cyber-Risiken oder die Cyber-Strategie/Programm informiert.

43%
bilden im Verwaltungsrat Ausschüsse.

Ausschüsse vor allem in Grossunternehmen und in der Finanzindustrie
Knapp die Hälfte der Verwaltungsräte bildet Ausschüsse zu verschiedenen Themen. Bei Grossunternehmen sind es drei Viertel, bei Kleinunternehmen ein Fünftel. Hinsichtlich der Branche werden insbesondere in der Finanzindustrie Ausschüsse gebildet: Drei Viertel haben hier mindestens einen Ausschuss. In den meisten anderen Branchen gibt es in weniger als der Hälfte der Verwaltungsräte einen Ausschuss. Jedoch werden in vielen VR-Gremien einzelnen Mitgliedern Ressorts oder Spezialthemen zugewiesen.

Aussichten

Konjunktur-, Branchen- und Geschäftsaussichten

Bei den **Konjunktur-, Branchen- und Geschäftsaussichten** für die nächsten 12 Monate setzt sich nach Ansicht der befragten Verwaltungsratsmitglieder die Wellenbewegung der letzten Jahre fort (siehe Abbildung 1): von einem durchschnittlichen Niveau im Jahr 2019 trübten sich die Aussichten im Jahr 2020 aufgrund der Corona-Krise ein, bevor sie sich im Folgejahr (2021) wieder deutlich verbesserten. Nach einem erneuten Abschwung der Erwartungen in Folge des Ausbruchs des Ukraine-Kriegs im Jahr 2022 geben die befragten Verwaltungsratsmitglieder aktuell wieder etwas optimistischere Wirtschaftsaussichten für die nächsten 12 Monate an. Es bleiben jedoch viele Unsicherheitsfaktoren für die Schweizer Wirtschaft bestehen, wozu beispielsweise anhaltende geopolitische Risiken, eine unklare Energielage für den Winter 2023/2024 und ein sich als beständig erweisender, überdurchschnittlich hoher Teuerungsdruck zählen.

Die **Konjunkturaussichten** der Verwaltungsratsmitglieder sind im Gegensatz zum Meinungsbild von vor einem halben Jahr (vgl. swissVR Monitor I/2023) in der Summe leicht optimistisch: 24 Prozent der Befragten mit einer positiven Konjunkturerwartung für die nächsten zwölf Monate stehen 10 Prozent mit einer negativen Einschätzung gegenüber. Der Grossteil der Verwaltungsratsmitglieder (66%) geht von einer neutralen Konjunkturentwicklung aus. Das aktuelle Meinungsbild deckt sich mit anderen derzeitigen Prognosen, die ein geringes Wachstum der Schweizer Wirtschaft voraussagen.

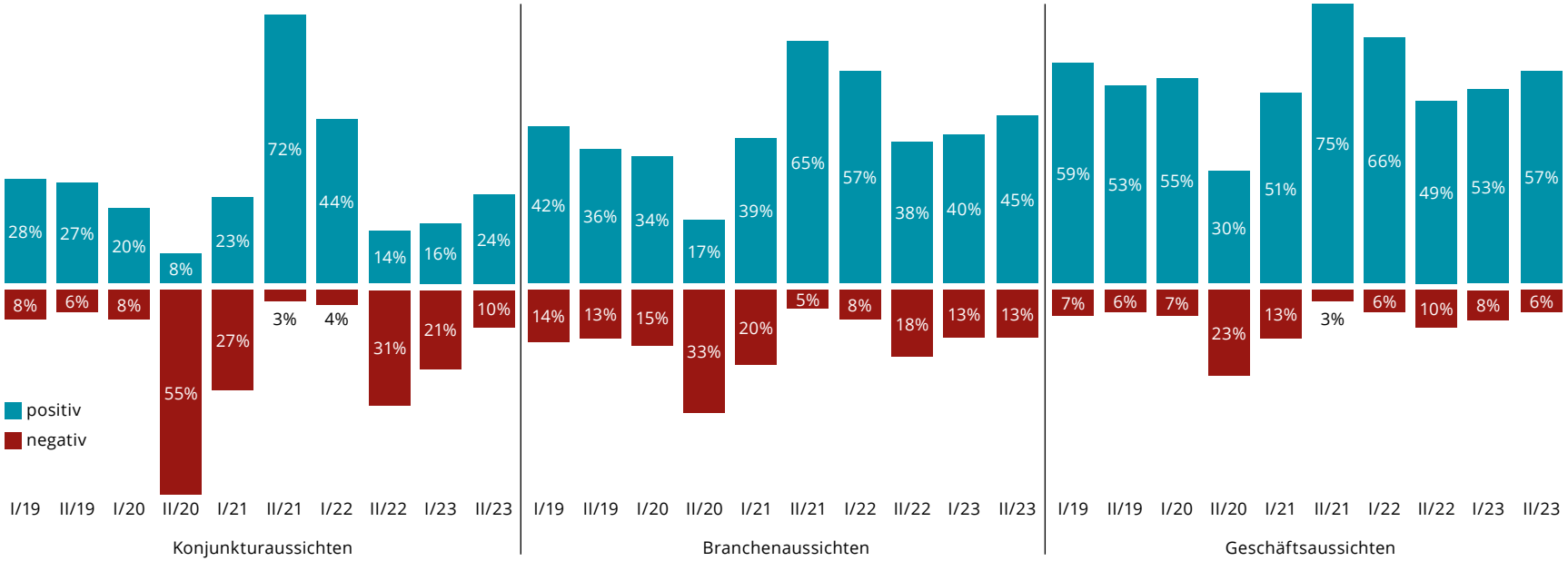
Die **Branchenaussichten** werden im Vergleich zu vor einem halben Jahr ebenfalls etwas optimistischer bewertet. 45 Prozent der befragten Verwaltungsratsmitglieder sind positiv gestimmt und 13 Prozent negativ. Optimistisch zeigen sich vor allem Befragte aus der Branche der Informations- und Kommunikationstechnik (81% positiv versus 0% negativ), was mit den anhaltenden Digitalisierungsbestrebungen der Schweizer Wirtschaft zusammenhängen könnte. Hingegen pessimistisch sind allen voran VR-Mitglieder aus dem verarbeitenden Gewerbe und der Chemie (24% negativ versus 22% positiv). Dieses Ergebnis ist zu einem wesentlichen Teil auf den

voraussichtlich weiterhin anhaltenden Teuerungsdruck bei Rohstoffen und Vorprodukten sowie auf die unsichere internationale Nachfragesituation zurückzuführen.

Die **Geschäftsaussichten** werden ebenfalls leicht optimistischer als vor einem halben Jahr bewertet. Etwas mehr als die Hälfte der befragten VR-Mitglieder (57%) schätzt die eigene Geschäftsentwicklung in den nächsten zwölf Monaten positiv ein, während lediglich 6 Prozent negativ gestimmt sind. Besonders optimistisch zeigen sich erneut Verwaltungsratsmitglieder von Unternehmen aus der Branche der Informations- und Kommunikationstechnik (83% positiv versus 0% negativ). Am verhaltensten unter allen befragten Branchen ist die Stimmung im verarbeitenden Gewerbe und in der Chemie (32% positiv versus 22% negativ).

Abb. 1 Beurteilung der Aussichten in den nächsten 12 Monaten [swissVR Monitor I/2019 bis II/2023]

Frage: Wie beurteilen Sie die Konjunkturaussichten / Branchenaussichten / Geschäftsaussichten in den nächsten 12 Monaten?
Anmerkung: Die Differenz zu hundert Prozent sind neutrale Antworten.



Fokusthema: Cyber-Resilienz – Steigende Bedeutung für Verwaltungsräte

Cyber-Angriffe auf Unternehmen und andere Organisationen haben in den vergangenen Jahren in ihrer Quantität und Qualität stark zugenommen. Ein entscheidender Treiber in diesem Zusammenhang war die Corona-Pandemie, während derer ein höherer Anteil der Beschäftigten als je zuvor seine Arbeit von zu Hause aus verrichtete und die IT-Infrastruktur von Firmen dadurch eine vergleichsweise starke Vulnerabilität aufwies. Auch die Medien berichteten über die letzten Jahre hinweg vermehrt über Fälle von grossen, namhaften Unternehmen, die Opfer von Cyber-Angriffen und infolgedessen operativ und wirtschaftlich beeinträchtigt wurden. Darüber hinaus ist zukünftig vor dem Hintergrund der anhaltenden Digitalisierung und der voranschreitenden Entwicklung der künstlichen Intelligenz von einer noch höheren Frequenz und einem stärkeren Ausmass von Cyber-Angriffen auszugehen. Aus den beschriebenen Gründen ist es auch für Verwaltungsräte wichtig, sich mit der Cyber-Resilienz ihrer Unternehmen auseinanderzusetzen und ein klares Verständnis ihrer Rolle sowie Aufgaben in diesem Themengebiet zu entwickeln.

Vorfälle und Folgen von Cyber-Angriffen

Eine Minderheit von 28 Prozent der befragten Verwaltungsratsmitglieder gibt an, dass ihr Unternehmen in der Vergangenheit **Opfer eines Cyber-Angriffs geworden** ist (siehe Abbildung 2). Im Umkehrschluss verneinen dies 72 Prozent beziehungsweise sind sich dessen nicht bewusst. Die Anzahl an betroffenen Unternehmen könnte tatsächlich um einiges höher sein, da die vorliegende Befragung gezeigt hat, dass die Verwaltungsratsmitglieder nicht immer ein regelmässiges Reporting über Cyber-Vorfälle von der Geschäftsleitung erhalten (lediglich in 56% der Fälle, siehe Abbildung 7).

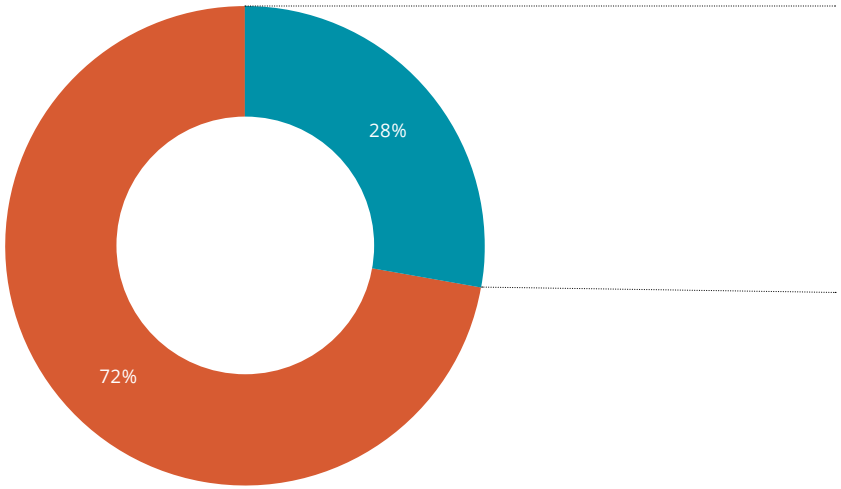
Einen entscheidenden Einfluss hat in diesem Zusammenhang die Unternehmensgrösse: Während in Kleinunternehmen lediglich 18 Prozent der Befragten (mindestens) einen Cyber-Angriff auf das eigene Unternehmen angeben, tut dies fast jedes zweite Verwaltungsratsmitglied (45%) eines Grossunternehmens. Dieser Unterschied könnte beispielsweise entweder

an einer Korrelation zwischen der Unternehmensgrösse und der Anzahl von Cyber-Attacken (je grösser, desto mehr Angriffe) oder an einer höheren Informiertheit in Bezug auf Cyber-Angriffe von Verwaltungsratsmitgliedern in Grossunternehmen liegen (siehe Abschnitt «Der Verwaltungsrat und die Cyber-Resilienz»).

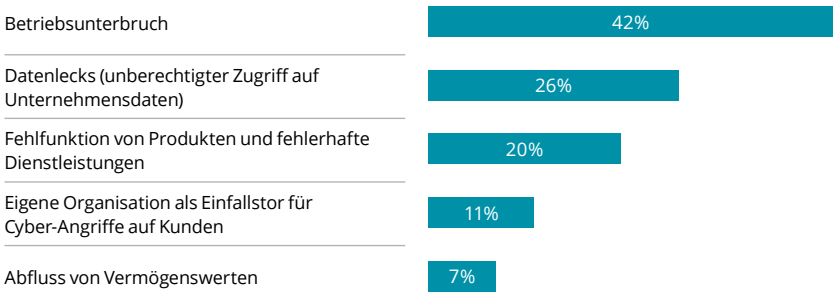
Betrachtet man die Folgen von Cyber-Angriffen auf Unternehmen (siehe ebenfalls Abbildung 2), so sticht der **Betriebsunterbruch** (42%) als mit Abstand meistgenannte Antwort hervor. Vor allem in der Branche der Informations- und Kommunikationstechnik erwähnen Verwaltungsratsmitglieder den Betriebsunterbruch in Folge von Cyber-Attacken besonders häufig (69%). Insgesamt betrachtet folgen an zweiter und dritter Stelle **Datenlecks** (26%) und die **Fehlfunktion von Produkten oder Dienstleistungen** (20%). An der häufigen Nennung von Betriebsunterbrüchen und Fehlfunktionen ist ersichtlich, dass Cyber-Angriffe häufig konkrete Konsequenzen auf operative Vorgänge im Unternehmen haben. Als weitere Folgen werden **Cyber-Angriffe auf Kunden** (11%) und der **Abfluss von Vermögenswerten** (7%) genannt.

Abb. 2 Vorfälle und Folgen von Cyber-Angriffen in Unternehmen

Frage: Wurde Ihr Unternehmen Ihres Wissens bereits einmal Opfer eines Cyber-Angriffs (z. B. nicht autorisierter Zugriff auf Daten; Eingriff in die Kundenkommunikation; Störung der Webseite, etc.)?



Frage: Welche Folgen hatte(n) der/die Angriff(e) auf Ihr Unternehmen? Bitte geben Sie alle zutreffenden Aspekte an. [n=113]



Bedeutung von Cyber-Resilienz-Themen

Für Unternehmen hat die Bedeutung der Cyber-Resilienz und verwandter Themen in den vergangenen Jahren gemäss der Einschätzung der Befragten deutlich zugenommen (siehe Abbildung 3). Die Mehrheit der Verwaltungsratsmitglieder sieht eine **starke Zunahme** (55%), 40 Prozent eine **Zunahme** und ein geringer Rest **keine Veränderung** (5%). Keiner der Befragten gibt eine **Abnahme oder starke Abnahme** an.

Auch in diesem Zusammenhang spielt die Unternehmensgrösse eine nicht unwesentliche Rolle: Bei Kleinunternehmen sind 43 Prozent der Auffassung, dass die Bedeutung der Cyber-Resilienz stark zugenommen hat (45% vertreten die Meinung, dass die Bedeutung zugenommen hat). Hingegen beschreiben 70 Prozent der Befragten aus Grossunternehmen eine starke Zunahme (29% beschreiben eine Zunahme der Bedeutung des Themas). Dieses Ergebnis mag wohl erneut an einer Korrelation zwischen der Unternehmensgrösse und der Anzahl von Cyber-Attacken oder auch an einer stärkeren Institutionalisierung von Cyber-Themen in Grossunternehmen liegen (zum Beispiel in Form einer IT-Abteilung oder in der Funktion eines Chief Information Security Officers, CISO).

Unter den Branchen ist die grösste Zunahme der Bedeutung von Cyber-Resilienz-Themen im verarbeitenden Gewerbe und in der Chemie festzustellen (starke Zunahme: 65%). Über alle Branchen hinweg erklärt sich die zunehmende Bedeutung für viele Unternehmen wohl auch durch neue Geschäftsmodelle und die wachsende Vernetzung von Menschen, Maschinen, Produkten, Systemen und Unternehmen (Internet of Things, IoT).

Versicherung für Cyber-Risiken

Wenn es darum geht, ein Unternehmen für Cyber-Risiken zu versichern, ergibt sich ein geteiltes Bild unter den Befragten (siehe Abbildung 4). Die knappe Hälfte (46%) gibt an, dass ihr Unternehmen über eine solche **Versi-**

Abb. 3 Bedeutung von Cyber-Resilienz-Themen für Unternehmen

Frage: Wie hat sich die Bedeutung von Cyber-Resilienz-Themen für Ihr Unternehmen in den letzten drei Jahren verändert?

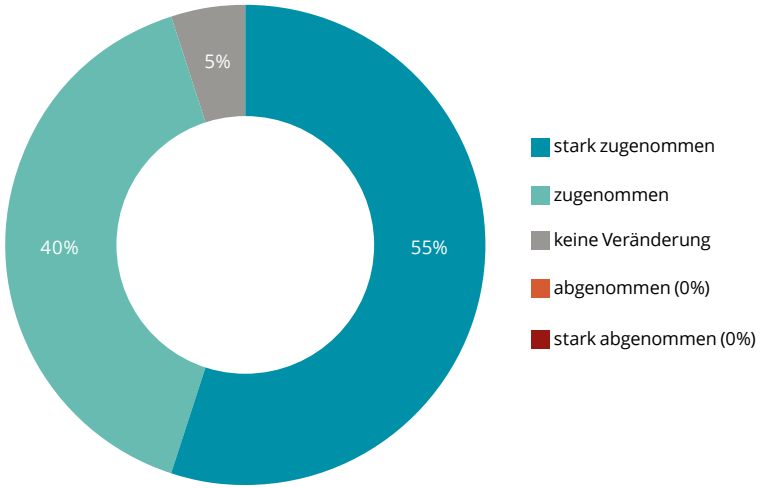
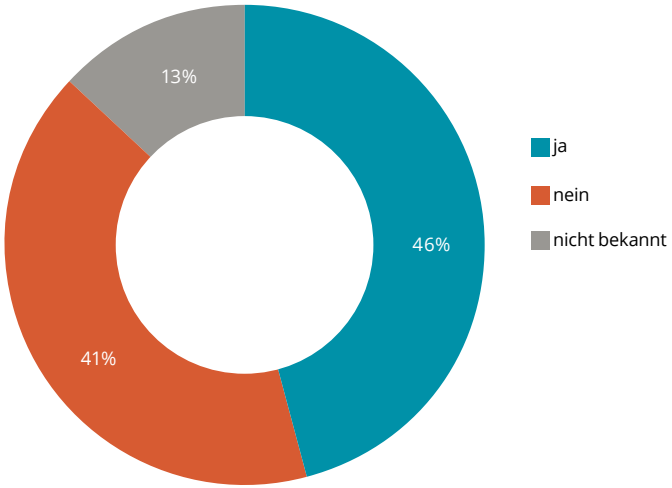


Abb. 4 Versicherung für Cyber-Risiken

Frage: Hat Ihr Unternehmen eine Versicherung für Cyber-Risiken?



cherung verfügt; bei fast genauso vielen (41%) ist dies nicht der Fall. Etwa jedes achte Verwaltungsratsmitglied (13%) macht hierzu **keine Aussage**.

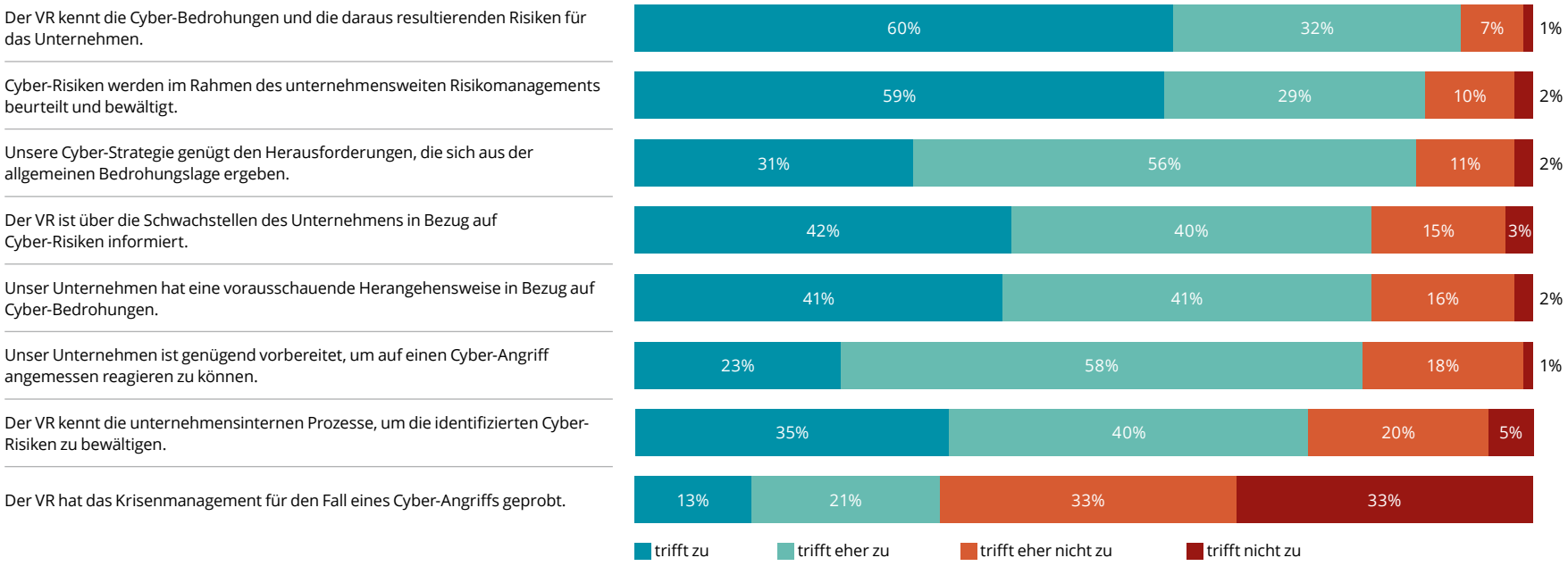
Hinsichtlich der Branchen versichern sich Unternehmen aus dem Finanzbereich (58%), dem verarbeitenden Gewerbe und der Chemie (54%) sowie dem Baugewerbe (51%) mehrheitlich für Cyber-Risiken. In den restlichen Branchen tut dies eine Minderheit der Firmen. Bezüglich der Unternehmensgrössen sind die Unterschiede hingegen gering.

Der Verwaltungsrat und die Cyber-Resilienz

Die Verwaltungsratsmitglieder schätzen sich selbst und ihre Unternehmen bei der Cyber-Resilienz mehrheitlich als kundig und gut vorbereitet ein (siehe Abbildung 5). So geben mehr als neun von zehn Befragten (92%) an, dass ihr **VR-Gremium die Cyber-Bedrohungen und die daraus resultierenden Risiken für das Unternehmen grossmehrheitlich kennt**. In ähnlich vielen Fällen würden **Cyber-Risiken im Rahmen des unternehmensweiten Risikomanagements zumindest teilweise beurteilt und bewältigt** (88%) und **genüge die Cyber-Strategie in der Regel den Herausforderungen, die sich aus der allgemeinen Bedrohungslage ergeben** (87%).

Abb. 5 Selbsteinschätzung des Verwaltungsrats bei der Cyber-Resilienz

Frage: Inwiefern treffen die folgenden Aussagen auf Ihren VR zu?



Ausserdem sind Verwaltungsratsmitglieder überwiegend der Meinung, dass ihre **VR-Gremien über die Schwachstellen des Unternehmens in Bezug auf Cyber-Risiken zumindest partiell informiert** sind (82%), ihre Unternehmen meistens **eine vorausschauende Herangehensweise in Bezug auf Cyber-Bedrohungen** haben (82%) und **auf einen Cyber-Angriff zum Teil angemessen reagieren können** (81%). Drei von vier Befragten (75%) stimmen der Aussage, ihr Verwaltungsrat kenne die unternehmensinternen Prozesse, um die identifizierten Cyber-Risiken zu bewältigen, vollständig oder eher zu.

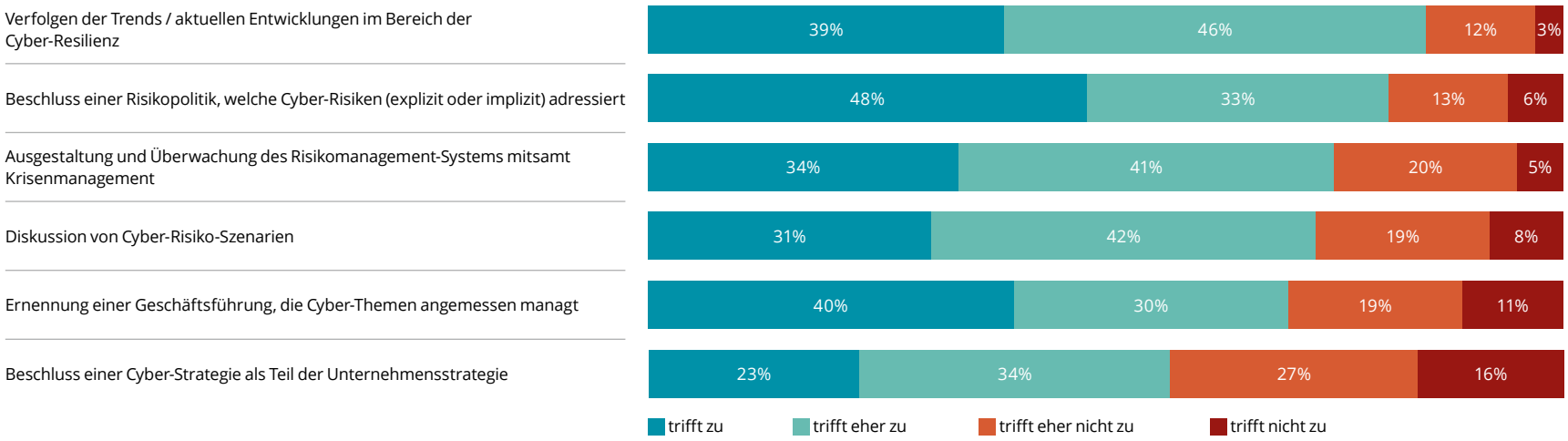
Bei allen beschriebenen Aussagen ist die Tendenz zu erkennen, dass die Zustimmungsraten der Befragten aus Grossunternehmen überdurchschnittlich hoch und diejenige aus Kleinunternehmen im Umkehrschluss etwas niedriger als im Mittel sind. Dies weist auf eine höhere Institutionalisierung und Systematisierung der Cyber-Resilienz in Grossunternehmen und deren VR-Gremien hin.

Lediglich jedes dritte Verwaltungsratsmitglied (34%) bestätigt, das eigene Gremium habe **das Krisenmanagement für den Fall eines Cyber-Angriffs zumindest teilweise geprobt**. Ein solches Krisentraining wird häufiger von Befragten aus Grossunternehmen (45%) als aus Kleinunternehmen (26%) angeführt. In der Finanzindustrie gibt dies fast die Hälfte der Verwaltungsratsmitglieder (45%) an, während es in der Branche der Unternehmensdienstleistungen nur circa ein Viertel (24%) beziehungsweise im Handel und in der Konsumgüterindustrie lediglich etwa ein Fünftel (19%) sind.

In Bezug auf die Aufgaben und Rollen des Verwaltungsrats bei der Cyber-Resilienz zeigt sich ebenfalls ein grösstenteils positives Bild (siehe Abbildung 6). Eine sehr grosse Mehrheit der Befragten bejaht, dass ihr VR-Gremium **Trends und aktuelle Entwicklungen im Bereich der Cyber-Resilienz** in der Regel verfolgt (85%) und grundsätzlich **eine Risikopolitik beschliesst, die Cyber-Risiken (explizit oder implizit) adressiert** (81%).

Abb. 6 Aufgaben/Rollen des Verwaltungsrats bei der Cyber-Resilienz

Frage: Inwiefern nimmt Ihr VR die folgenden Aufgaben/Rollen bei der Cyber-Resilienz wahr?



Die **Ausgestaltung und Überwachung des Risikomanagement-Systems mitsamt Krisenmanagement** (75%), die **Diskussion von Cyber-Risiko-Szenarien** (73%) sowie die **Ernennung einer im Cyber-Management kompetenten Geschäftsführung** (70%) sind weitere Aufgaben, welche die meisten Verwaltungsratsmitglieder zumindest teilweise wahrnehmen. Wenn es um den **Beschluss einer Cyber-Strategie als Teil der Unternehmensstrategie** geht, bestätigen dies lediglich etwas mehr als die Hälfte (57%) der Befragten. Erneut zeigen sich bei den Aussagen tendenziell höhere Zustimmungsraten bei Verwaltungsratsmitgliedern aus Grossunternehmen als aus Kleinunternehmen.

Der Verwaltungsrat erhält von der Geschäftsleitung zu verschiedenen Cyber-Themen ein regelmässiges Reporting beziehungsweise Berichte (siehe Abbildung 7). Etwas mehr als die Mehrheit der Befragten gibt dies in Bezug auf **Cyber-Vorfälle im Unternehmen** (56%) und betreffend den **Handlungs-/Investitionsbedarf** (53%) an. Eine Berichterstattung zur **allgemeinen Bedrohungslage** (43%), zu **Cyber-Resilienz-Massnahmen** (42%), eine **Übersicht der Top-Cyber-Risiken** (33%) oder die **Cyber-Strategie/Programm** (32%) erhält laut eigener Aussage lediglich eine Minderheit der Verwaltungsratsmitglieder. Wieder zeigt sich die Tendenz, dass Befragte aus Grossunternehmen in Bezug auf das Cyber-Reporting/Berichte höhere Zustimmungsraten beziehungsweise Häufigkeiten angeben als Befragte aus Kleinunternehmen. Bezüglich der Branchen sind die Unterschiede hingegen weniger stark ausgeprägt.

Abb. 7 Cyber-Reporting/Berichte an den Verwaltungsrat

Frage: Zu welchen der folgenden Aspekte erhält ihr VR ein regelmässiges Cyber-Reporting/Berichte von der Geschäftsleitung? Bitte geben Sie alle zutreffenden Aspekte an.

Organisationsthemen im Verwaltungsrat

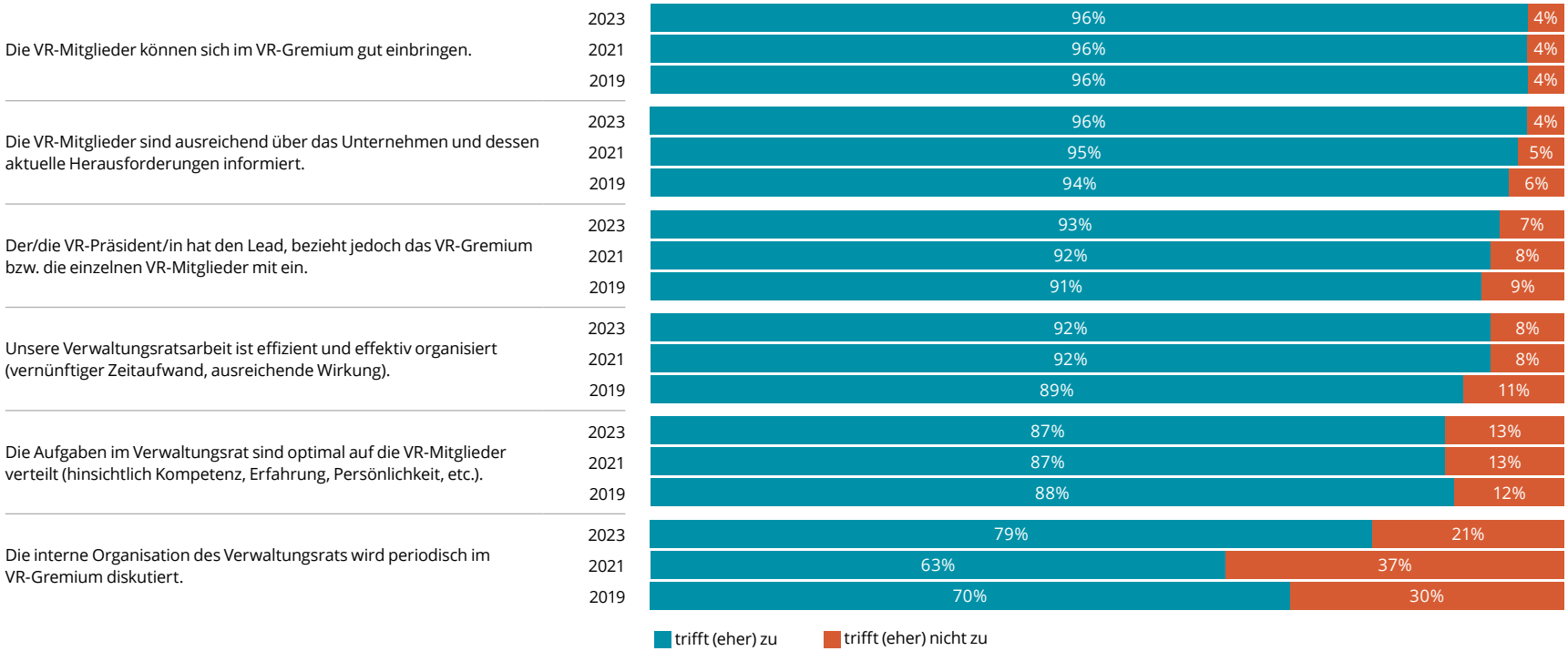
Interne Organisation im Verwaltungsrat

Die interne Organisation des Verwaltungsrats beinhaltet insbesondere die Aufgabenverteilung und den Einfluss einzelner VR-Mitglieder im Gremium. Alles in allem bewerten die Befragten die Lage in ihren Verwaltungsräten bezüglich der internen Organisation positiv (siehe Abbildung 8), wie es ebenfalls bei den gleichen Erhebungen vor zwei und vier Jahren der Fall war (swissVR Monitor II/2019 und II/2021). Die Einschätzungen der Verwaltungsratsmitglieder sind insgesamt betrachtet sehr ähnlich wie in den Vorjahren und bilden damit ein über die Zeit hinweg robustes Bild ab.

In den Augen fast aller Befragten (96%) können sich die **VR-Mitglieder gut ins Gremium einbringen**. Gleich viele Verwaltungsratsmitglieder (96%) sind der Meinung, dass sie und ihre Kollegen **ausreichend über das Unternehmen und dessen aktuelle Herausforderungen informiert** sind. Geringfügig weniger (93%) stützen das Statement, wonach der/die **VR-Prä-**

Abb. 8 Interne Organisation im Verwaltungsrat

Frage: Welche dieser Aussagen treffen zu:



sident/in den Lead hat, jedoch auch die anderen Mitglieder mit einbezieht. Ebenfalls sehr hohe Zustimmungsraten erhalten die Aussagen, **die VR-Arbeit sei effizient und effektiv organisiert** (92%) und die **Aufgaben seien optimal auf die Mitglieder verteilt** (87%).

Vergleichsweise wenige Befragte (79%) geben an, dass die **interne Organisation periodisch im VR-Gremium diskutiert** wird. Jedoch ist bei diesem Statement ein deutlicher Anstieg in der Zustimmung gegenüber den Jahren 2019 und 2021 auszumachen, was auf eine Verbesserung der Situation hindeutet. Bei allen beschriebenen Aussagen sind die Unterschiede zwischen den Unternehmensgrössen und Branchen gering.

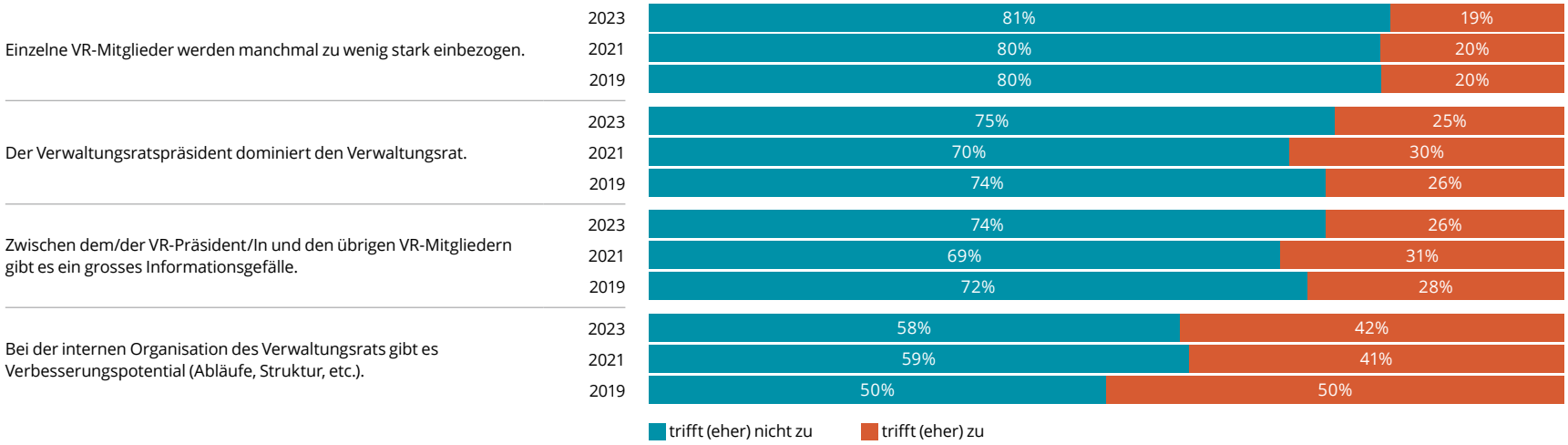
Herausforderungen im Verwaltungsrat

Bei der Zusammenarbeit im Verwaltungsrat können eine Reihe von Herausforderungen auftreten. Die Ergebnisse zu diesen Herausforderungen bestätigen einerseits das positive Meinungsbild zu den vorangegangenen Aussagen bezüglich der internen Organisation, weisen jedoch auch auf gewisse Optimierungspotenziale hin (siehe Abbildung 9).

Ähnlich wie bereits in den Befragungen vor zwei und vier Jahren (swissVR Monitor II/2019 und II/2021) ist ein knappes Fünftel der Verwaltungsratsmitglieder (19%) der Meinung, dass sie oder einzelne ihrer VR-Kollegen **teilweise nicht genügend einbezogen** werden. Jeweils etwa ein Viertel der Befragten sieht in der **Dominanz des VR-Präsidenten beziehungsweise der VR-Präsidentin** (25%) oder dem **Informationsgefälle zwischen dem/der VRP und den übrigen Mitgliedern** (26%) eine nennenswerte Herausforderung. Mit einem Ergebnis von 42 Prozent besteht für einen vergleichsweise hohen Anteil der Verwaltungsratsmitglieder ein **Verbesserungspotenzial bei der internen Organisation** (Abläufe, Strukturen etc.). Vor dem Hintergrund dieser Resultate zeigt sich trotz einer positiven Grundeinschätzung auch ein gewisser Optimierungsbedarf bei der Organisation und Zusammenarbeit innerhalb der Verwaltungsräte. Auch diese Ergebnisse sind über die verschiedenen Unternehmensgrössen und Branchen hinweg relativ ähnlich.

Abb. 9 Herausforderungen im Verwaltungsrat

Frage: Welche dieser Aussagen treffen zu:



Ressorts und Ausschüsse

Etwa zwei Drittel der Befragten (63%) geben an, dass in ihren VR-Gremien einzelnen Mitgliedern **Ressorts oder Spezialgebiete** zugewiesen werden (siehe Abbildung 10). Dieser Wert ist praktisch gleich hoch wie jener vor zwei und vor vier Jahren (swissVR Monitor II/2019: 59%, swissVR Monitor II/2021: 62%).

Der Anteil der VR-Gremien, in denen Ressorts oder Spezialgebiete gebildet werden, hängt unter anderem von der Unternehmensgrösse ab. In Grossunternehmen erfolgt dies in sieben von zehn Fällen (70%), während in Kleinunternehmen lediglich etwas mehr als die Hälfte der Verwaltungsräte (58%) einzelnen VR-Mitgliedern spezielle Aufgaben zuweisen. Dies liegt insbesondere an der höheren Mitgliederanzahl von Verwaltungsräten in Grossunternehmen im Vergleich zu Kleinunternehmen (7 versus 4 Mitglieder). Hinsichtlich der Branche werden Ressorts oder Spezialgebiete besonders häufig im Handel und in der Konsumgüterindustrie (76%) und unterdurchschnittlich oft im verarbeitenden Gewerbe und in der Chemie (51%) gebildet.

Etwa vier von zehn Befragten (43%) geben an, dass ihr Verwaltungsrat über **Ausschüsse oder Committees** verfügt. Dieser Anteil ist ebenfalls praktisch gleich hoch wie jener vor zwei und vor vier Jahren (swissVR Monitor II/2019: 41%, swissVR Monitor II/2021: 43%).

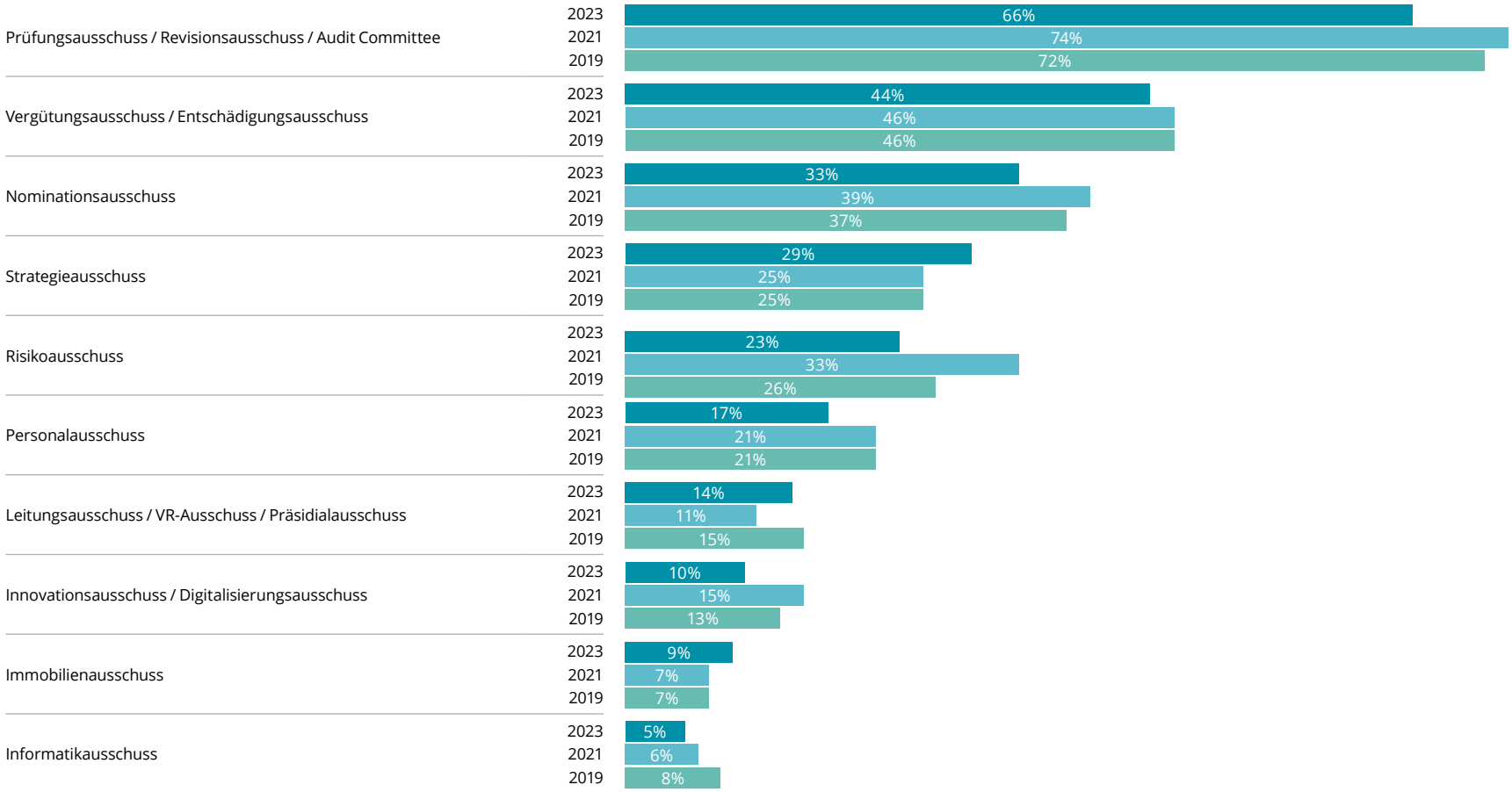
Abb. 10 Ressorts / Spezialgebiete und Ausschüsse / Committees

		Wir haben einzelnen Verwaltungsratsmitgliedern Ressorts/ Spezialgebiete zugewiesen	Wir haben im Verwaltungsrat Ausschüsse/ Committees gebildet
Total II/2023		63%	43%
Total II/2021		62%	43%
Total II/2019		59%	41%
Nach Unternehmensgrösse (II/2023)	Kleinunternehmen	58%	20%
	Mittelgrosse Unternehmen	63%	35%
	Grossunternehmen	70%	75%
Nach ausgewählten Branchen (II/2023)	Unternehmensdienstleistungen	56%	18%
	Handel / Konsumgüterindustrie	76%	41%
	Finanzdienstleistungen	65%	75%
	Pharma / Life Sciences/ Medtech / Gesundheitswesen	65%	43%
	Verarbeitendes Gewerbe / Chemie	51%	38%
	Informations- und Kommunikationstechnik	65%	15%
	Baugewerbe / Immobilien	60%	35%

Bei den Ausschüssen zeigen sich hinsichtlich der Unternehmensgrösse und Branche noch prägnantere Unterschiede als bei den Ressorts und Spezialgebieten. So bilden in Grossunternehmen drei von vier Verwaltungsräten (75%) Ausschüsse, während dieser Anteil in Kleinunternehmen bei lediglich etwa einem Fünftel (20%) liegt. Im Hinblick auf die verschiedenen Branchen sind insbesondere in der Finanzindustrie Ausschüsse vorzufinden (75%), was unter anderem dadurch zu erklären ist, dass die FINMA Banken ab einer bestimmten Unternehmensgrösse einen Prüf- und Risikoausschuss vorschreibt. Im Gegensatz dazu bilden Verwaltungsräte aus den Branchen der Unternehmensdienstleistungen (18%) und der Informations- und Kommunikationstechnik (15%) relativ selten Ausschüsse.

Abb. 11 Arten von Ausschüssen

Frage: Welche Ausschüsse sind vorhanden? [Mehrfachantwort möglich, n=170]

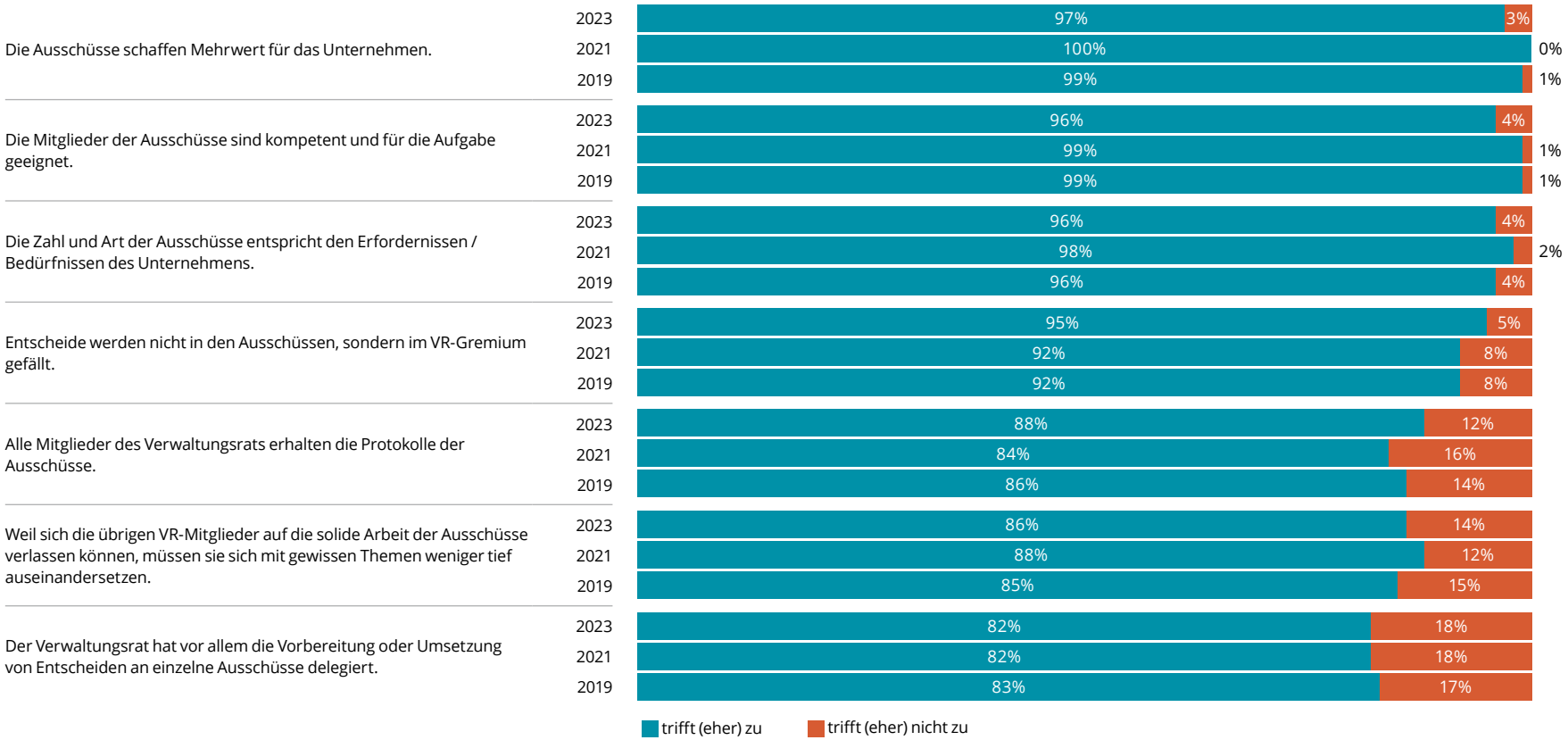


Von den Verwaltungsräten, die über mindestens einen Ausschuss verfügen, geben zwei Drittel (66%) an, ein **Audit Committee** (Prüfungs- beziehungsweise Revisionsausschuss) zu haben (siehe Abbildung 11). Dies ist mit Abstand der am meisten verbreitete Ausschuss, was einerseits mit dem verbundenen Arbeitsumfang, andererseits mit der Empfehlung bezüglich Good Governance von börsenkotierten Unternehmen (zum Beispiel Economiesuisse) und auch mit den Vorschriften der Regulatoren (zum Beispiel FINMA) zusammenhängen dürfte. Ähnliches gilt für **Vergütungsausschüsse** (44%), die bei börsenkotierten Unternehmen gesetzlich vorgeschrieben sind. Darüber hinaus gibt bei den gebildeten Ausschussarten eine hohe Diversität, die die verschiedenen Bedürfnisse der einzelnen Unternehmen und ihrer Verwaltungsräte abbilden.

Die Anteile der einzelnen Ausschussarten in den Verwaltungsräten sind alles in allem relativ ähnlich wie jene vor zwei und vor vier Jahren. Nennenswert erscheint die deutliche Abnahme von **Risikoausschüssen** (23%) im

Abb. 12 Bewertung von Ausschüssen

Frage: Welche Aussagen betreffend VR-Ausschüsse treffen zu: [n=170]



Vergleich zur Erhebung aus dem Jahr 2021 (33%). Diese Entwicklung mag einerseits erstaunen, widerspricht sie doch der wachsenden Bedeutung des Risikomanagements, sei es beispielsweise im Cyber-Bereich (siehe Abbildung 3) oder in Bezug auf geopolitische Entwicklungen (siehe swissVR Monitor II/2022), heisst andererseits, dass das Risikomanagement weniger in einen Ausschuss delegiert, sondern vermehrt im Gesamtverwaltungsrat adressiert wird.

Ferner bewerten die Verwaltungsratsmitglieder die Arbeit der Ausschüsse insgesamt sehr positiv (siehe Abbildung 12). Fast alle Befragten (97%) sind der Meinung, dass die Ausschüsse in ihrem Verwaltungsrat einen **Mehrwert für das eigene Unternehmen schaffen**. Ähnlich hoch ist die Zustimmung (jeweils 96%) bei der **Kompetenz und Eignung der Ausschussmitglieder** sowie bei der **Übereinstimmung von Ausschussanzahl/-art und den Bedürfnissen des Unternehmens**.

Laut der Angabe fast aller Verwaltungsratsmitglieder (95%) werden **Entscheide nicht in den Ausschüssen, sondern im VR-Gremium gefällt**. Dieses Resultat entspricht den gesetzlichen Vorgaben, dass der Verwaltungsrat lediglich «die Vorbereitung und die Ausführung seiner Beschlüsse oder die Überwachung von Geschäften Ausschüssen oder einzelnen Mitgliedern zuweisen kann» (OR 716a/2).

Wenn es um das **Erhalten von Protokollen aus den Ausschüssen** (88%), das **Verlassen/Vertrauen auf eine solide Ausschussarbeit** (86%) und das **Delegieren der Vorbereitung oder Umsetzung von Entscheiden an einzelne Ausschüsse** (82%) geht, sind die Zustimmungsraten etwas geringer, jedoch trotzdem auf hohem Niveau. Insgesamt bewerten die Befragten die Ausschussarbeit sehr ähnlich wie in den Jahren 2019 und 2021, wodurch der swissVR Monitor ein über die Zeit hinweg zuverlässiges und solides Barometer der Einschätzungen von Verwaltungsratsmitgliedern darstellt.

Interviews

Cyber-Resilienz und die Rolle des Verwaltungsrats

Maya Bundt, Vorsitzende des Nominations- und Vergütungsausschusses der Valiant Bank sowie Verwaltungsratsmitglied von Bâloise und APG|SGA

«Es ist wichtig, dass der Verwaltungsrat Cyber- oder digitale Risiken nicht nur in die IT-Ecke stellt, sondern sie als unternehmensweite und strategierelevante Themen anerkennt. Grosse strategische Entscheidungen haben nämlich fast immer einen Einfluss auf den Cyber-Fussabdruck der Unternehmung.»

swissVR Monitor: Welches sind die neusten Entwicklungen und Trends bei Cyber-Angriffen auf Unternehmen?

Maya Bundt: Wenn man sich die Statistik des NCSC (Nationales Zentrum für Cyber-Sicherheit) anschaut, findet man Betrug mit grossem Abstand ganz oben auf der Liste. Das betrifft sowohl Einzelpersonen als auch Unternehmen und ist seit Jahren der absolute Dauerbrenner.

Medial viel stärker im Fokus sind allerdings andere Angriffe. Seit ein paar Jahren stehen da vor allem Ransomware-Attacken mit oder ohne Datendiebstahl im Vordergrund. Dabei verschlüsseln die Verbrecher mit Hilfe von Schadsoftware, sogenannter Ransomware, Daten im Unternehmen und verlangen dann Lösegeld. Neuerdings werden im gleichen Zug häufig auch noch Daten entwendet und dann wird mit der Veröffentlichung dieser Daten gedroht. Dadurch steigt der Druck auf die Unternehmen zu zahlen.

Maya Bundt ist eine erfahrene Verwaltungsrätin mit einer Leidenschaft für Cyber-Themen, Innovation und Menschen. In fast 20 Jahren bei dem globalen Rückversicherer Swiss Re hatte sie bis 2022 eine Vielzahl von Funktionen in den Bereichen IT, Strategie und Rückversicherung inne. Ab 2014 war sie für die Entwicklung der Cyber-Versicherungsstrategie verantwortlich und baute erfolgreich die Funktion und das Team für Cyber- und digitale Lösungen auf; ausserdem leitete sie den Swiss Re Cyber Council. Sie unterstützt eine Reihe von nationalen und internationalen Initiativen rund um die digitale Wirtschaft und Cyber-Risiken und hat mehrere Artikel zu diesen Themen veröffentlicht. Sie engagiert sich in der Community als Vorsitzende des Cyber Resilience Chapters der Swiss Risk Association, als Mitglied des Cybersecurity Committees von digitalswitzerland, als Mitwirkende am Geneva Dialogue und als Partnerin für Governance of Digital Risks am International Center for Corporate Governance.

Und schliesslich sind in letzter Zeit auch wieder DDoS-Attacken (Distributed Denial of Service) publik geworden. Dabei werden zum Beispiel öffentliche Web-Seiten mit massiven Datenanfragen bombardiert, so dass sie für Kunden nicht mehr erreichbar sind. Das konnten wir im Juni 2023 beobachten, als diverse Dienste des Bundes und der SBB für einige Stunden ausfielen.

swissVR Monitor: Welche Rolle kommt dem Verwaltungsrat beim Thema Cyber-Resilienz zu?

Maya Bundt: Generell legt der Verwaltungsrat die Grundzüge der nachhaltigen Unternehmensführung im Sinne der Eigentümer fest. Dazu gehört auch die Cyber-Resilienz. In diesem Zusammenhang muss der VR die Chancen und Risiken der Digitalisierung für das Unternehmen und die Geschäftstätigkeiten abschätzen. Dabei ist wichtig: Es gibt keine 100-prozentige Sicherheit! Das heisst, dass neben klassischen Schutzmassnahmen auch solche Massnahmen ergriffen werden müssen, die das Aufspüren von Eindringlingen ermöglichen. Zudem muss man sich für den Ernstfall vorbereiten, um möglichst schnell und unbeschadet aus einer Krisensituation herauskommen zu können.

Der Verwaltungsrat ist dafür verantwortlich, dass Risikomanagement, Organisation und Budget so ausgestaltet sind, dass sich das Unternehmen dem Geschäftsmodell angemessen gegen Cyber-Risiken schützen kann und vorbereitet ist, einen Cyber-Vorfall zu überdauern.

swissVR Monitor: Welche Massnahmen empfehlen Sie Verwaltungsräten, wenn es um Cyber-Resilienz geht?

Maya Bundt: Es ist wichtig, dass der Verwaltungsrat Cyber- oder digitale Risiken nicht nur in die IT-Ecke stellt, sondern sie als unternehmensweite und strategierelevante Themen anerkennt. Grosse strategische Entscheidungen haben nämlich fast immer einen Einfluss auf den Cyber-Fussabdruck der Unternehmung, sei es die Expansion in einen neuen Markt, M&A-Aktivitäten, die Teilnahme an einem digitalen Ökosystem, oder ganz generell die fortschreitende digitale Transformation.

Zudem muss der Verwaltungsrat verstehen, wo im Unternehmen die grössten Cyber-Risiken liegen, wie gross diese sind und wie sie vermieden, vermindert oder transferiert werden können. In diesem Zusammenhang ist es auch wichtig, den Risikoappetit festzulegen, denn nur so können faktenbasierte Entscheidungen getroffen werden, wie die Cyber-Sicherheit im Unternehmen ausgestaltet werden soll oder ob zum Beispiel eine Cyber-Versicherung abgeschlossen werden sollte.

Ich plädiere immer dafür, dass der Verwaltungsrat die für die Informationssicherheit verantwortliche Person, gewöhnlich den oder die CISO (Chief Information Security Officer), kennt. Das hat gleich mehrere Vorteile: Erstens gibt es eine oder einen CISO und damit kümmert sich jemand hauptamtlich um die Sicherheit des Unternehmens. Zweitens rücken auch die strategischen und operativen Themen um die Cyber-Sicherheit stärker in den Mittelpunkt, wenn der oder die CISO regelmässig an den VR-Sitzungen teilnimmt. Drittens kann der Verwaltungsrat so eine Beziehung zu dieser Schlüsselperson aufbauen. Das finde ich ähnlich wichtig wie die Beziehung zur obersten Risiko- oder zur obersten Personalleitung.

Der Verwaltungsrat sollte sich auch Gedanken machen, wie die Cyber-Expertise im Gremium gestärkt werden kann, zum Beispiel in Form Cyber-affiner Mitglieder oder durch die Weiterbildung des bestehenden Gremiums. Ein gewisses Cyber-Wissen gehört meiner Meinung nach heutzutage zur Grundausstattung eines Verwaltungsrats. Vertieftes Wissen und vor allem auch das Interesse an der Sache führen zusätzlich dazu, dass das Thema in der verwaltungsrätlichen Themenflut nicht untergeht und immer jemand die relevanten Fragen stellt.

swissVR Monitor: Wie sieht aus Ihrer Sicht eine adäquate Berichterstattung an den Verwaltungsrat zur Cyber-Resilienz aus?

Maya Bundt: Viele Firmen behandeln Cyber-Risiken vor allem in einem Ausschuss, meist dem Risiko-Ausschuss; manchmal gibt es aber auch einen Technologie- und Cyber-Ausschuss. Das ist wichtig, weil in den Ausschüssen meist mehr Diskussionszeit zur Verfügung steht als im Gesamt-VR und sich die entsprechenden Ausschuss-Mitglieder noch tiefer mit der Materie befassen können.

Generell muss die Berichterstattung relevant, verständlich und für den VR angemessen sein. Dabei ist es oft nützlich, wenn sich der oder die CISO nicht in technischen Details verliert, sondern die Risiken und den Umgang mit ihnen aus einer Geschäftssicht darstellt. Neben unternehmensspezifischen Informationen und KPIs (Key Performance Indicators) sind auch oft ein allgemeines Lagebild und Benchmarks zu anderen Unternehmen für den Verwaltungsrat interessant und hilfreich.

swissVR Monitor: Was ist Ihre Meinung zu Versicherungen gegen Cyber-Risiken? In welchen Fällen sind diese sinnvoll?

Maya Bundt: Zunächst ist anzumerken, dass Cyber-Versicherungen einen Teil des Cyber-Risikomanagements darstellen, aber das Cyber-Risikoma-

nagement nie ersetzten können. Mir läuft es kalt über den Rücken, wenn ich Aussagen höre wie: «Wir müssen uns nicht um unsere Cyber-Sicherheit kümmern. Wir können ja eine Versicherung abschliessen.» Das geht gar nicht. Ich behaupte auch, dass heutzutage keine Versicherung einem solchen Unternehmen eine Police anbieten würde, wenn nicht ein Mindestmass an Cyber-Sicherheitsmassnahmen implementiert ist.

Zum Risikomanagement gehört, Risiken zu vermeiden, zu vermindern, zu transferieren oder zu akzeptieren. Um eine Versicherung sinnvoll abschliessen zu können, muss man also die Risiken verstehen und sie zu einem gewissen Mass quantifiziert haben, bevor man entscheidet, ob man einen Teil des Residualrisikos an eine Versicherung abgeben möchte. Transferiert wird, was nach den risikomindernden Massnahmen immer noch über dem gewählten Risikoappetit liegt. Es gibt aber auch Firmen, die sich diese Überlegungen machen und dann entscheiden, dass sie keine Cyber-Versicherung abschliessen möchten.

Cyber-Versicherungen beinhalten oft auch Dienstleistungen, die den Versicherten im Ernstfall konkrete Hilfe leisten. Wenn ein Unternehmen zum Beispiel von einer Ransomware-Attacke betroffen ist, kann es eine Notfallnummer anrufen und bekommt schnell die nötige Unterstützung, um diese Krisensituation zu meistern. Das kann für manche Unternehmen durchaus ein Argument für eine Cyber-Versicherung sein.

Cyber-Bedrohungen im Jahr 2023 und Massnahmen für Unternehmen

Florian Schütz, Delegierter des Bundes für Cybersicherheit und Leiter des Nationalen Zentrums für Cybersicherheit (NCSC), ab 1. Januar 2024 Direktor des Bundesamtes für Cybersicherheit

«Grundsätzlich sind alle Unternehmen, unabhängig von ihrer Grösse oder Branchenzugehörigkeit, gefährdet. Bei vielen KMU stellt sich jedoch das Problem, dass aufgrund knapper finanzieller und personeller Ressourcen das für die Cyber-Sicherheit notwendige Know-how und die nötige Infrastruktur nur sehr beschränkt oder gar nicht vorhanden sind.»

Florian Schütz, Delegierter des Bundes für Cybersicherheit, ist zuständig für die Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken und der Koordination aller Cyber-Aktivitäten der Bundesverwaltung. Er dient bei Cyber-Fragen als Ansprechperson für Kantone, Wirtschaft und Wissenschaft und steht dem Kompetenzzentrum des Bundes, dem Nationalen Zentrum für Cybersicherheit (NCSC), vor. Florian Schütz verfügt über einen Master in Computerwissenschaft sowie einen Master of Advanced Studies in Sicherheitspolitik und Krisenmanagement der ETH Zürich und hat mehr als 10 Jahre Führungserfahrung im Bereich der IT-Sicherheit in der Privatwirtschaft.

Bildquelle: Keystone-SDA / Gaëtan Bally

swissVR Monitor: Wie hat sich die Bedeutung der Cyber-Resilienz für Unternehmen in den letzten Jahren verändert? Und wie schätzen Sie die allgemeine Bedrohungslage im Jahr 2023 ein?

Florian Schütz: Das Bewusstsein für Cyber-Sicherheit ist in den letzten Jahren gestiegen und viele Unternehmen sind sich der Cyber-Risiken bewusst. Zwischen den Unternehmen gibt es jedoch grosse Unterschiede: Einige nehmen die Cyber-Sicherheit sehr ernst und setzten die nötigen Schutzmassnahmen um, andere kümmern sich jedoch kaum darum.

Der Meldungseingang zu Cyber-Vorfällen beim NCSC bewegt sich aktuell mit durchschnittlich rund 700 Meldungen pro Woche auf hohem Niveau. Dies führen wir einerseits auf die gestiegene Sensibilität der Bevölkerung zurück. Wir nehmen aber auch eine leichte Steigerung der Cyber-Angriffe wahr. Aktuell werden Betrugsfälle besonders häufig gemeldet. So machen angebliche Drohmails von Strafverfolgungsbehörden, sogenannte Fake-Extortion-E-Mails, ca. einen Drittel der beim NCSC eingegangen Meldungen aus.

Auch bei den Ransomware-Angriffen beobachtet das NCSC eine leichte Zunahme der Angriffe in den letzten Wochen. Es ist davon auszugehen, dass sich diese Angriffe in Zukunft häufen werden. Dies ist unter anderem darauf zurückzuführen, dass der Ukrainekrieg die Ransomware-Angriffe eher gebremst hat, weil einige der Hackergruppen damit begonnen haben, sich für den Krieg zu engagieren und daher keine Zeit mehr für Erpressungsversuche im Ausland hatten. Nun ist aber damit zu rechnen, dass Ransomware-Angriffe wieder intensiver werden, da die Gruppierungen sehr wahrscheinlich neue finanzielle Mittel generieren müssen.

swissVR Monitor: Die Cyber-Resilienz kleiner und mittelständischer Unternehmen (KMU) erhält weniger mediale Aufmerksamkeit. Sind KMU seltener von Cyber-Angriffen betroffen?

Florian Schütz: Grundsätzlich sind alle Unternehmen, unabhängig von ihrer Grösse oder Branchenzugehörigkeit, gefährdet.

Bei vielen KMU stellt sich jedoch das Problem, dass aufgrund knapper finanzieller und personeller Ressourcen das für die Cyber-Sicherheit notwendige Know-how und die nötige Infrastruktur nur sehr beschränkt oder gar nicht vorhanden sind.

Ausserdem stellen auch Angreifer Kosten-/Nutzenrechnungen an. Sie wollen mit möglichst wenig Aufwand, möglichst viel erreichen. So gesehen, stehen KMU eher im Fokus der Angreifer, weil Angriffe auf komplexe IT-Infrastrukturen von Grossunternehmen oft mit einem grossen Aufwand seitens der Angreifer verbunden sind.

Viele KMU entscheiden sich zudem nach einem Cyber-Angriff gegen den Gang an die Öffentlichkeit. Oft spielen hier Befürchtungen bezüglich eines drohenden Reputationsschadens eine grosse Rolle. Bei grösseren Unternehmen hat diesbezüglich ein Umdenken stattgefunden und so sind in der jüngsten Vergangenheit einige Unternehmen an die Öffentlichkeit gegangen und die Medien haben dies entsprechend thematisiert.

swissVR Monitor: Welche Massnahmen empfehlen Sie Unternehmen, die ihre Cyber-Resilienz auf- oder ausbauen möchten?

Florian Schütz: Cyber-Sicherheit ist Chefsache! Sie muss auf Geschäftsleitungsebene thematisiert werden und ein Risikomanagement bezüglich Cyber-Vorfälle muss in jedem Unternehmen etabliert sein. Allfällige Restrisiken müssen gegenüber der Geschäftsleitung ausgewiesen werden. Die Unternehmensleitung muss die Restrisiken kennen und schriftlich festhalten. Die Finanzierung der wichtigsten Massnahmen muss festgelegt, und für deren Umsetzung gesorgt werden. Die dazu benötigten Investitionen scheinen gross. Aber nicht alle Massnahmen müssen auf einmal umgesetzt werden. Eine Priorisierung ist wichtig. Erste Priorität hat das Aktuell-Halten der Systeme. Die meisten erfolgreichen Ransomware-Angriffe nutzen bekannte Schwachstellen aus, für die es bereits Patches gibt.

Neben den technischen Massnahmen zum Grundschutz, dem Erstellen von Backups und dem Einspielen von Updates, spielt auch die Sensibilisierung der Mitarbeitenden eine wichtige Rolle. Denn oftmals zielen Cyber-Angriffe in einer ersten Phase nicht auf die Infrastruktur, sondern gelten einer Person, die für das Unternehmen arbeitet. Mit so genanntem «Social Engineering» wird versucht, Mitarbeitende so zu beeinflussen, dass sie beispielsweise einen schadhaften E-Mail-Anhang öffnen oder ein Passwort bekanntgeben.

swissVR Monitor: Inwiefern unterstützt der Bund respektive das Nationale Zentrum für Cybersicherheit (NCSC) Unternehmen beim Thema Cyber-Resilienz?

Florian Schütz: Das NCSC stellt auf seiner Website zahlreiche Anleitungen und Checklisten zur Verfügung, die aufzeigen, wie man sich vor Cyber-Angriffen schützen kann und was zu tun ist, wenn ein Angriff erfolgt ist. Ausserdem informiert das NCSC laufend über seine Kanäle wie die Website und über LinkedIn zu neuen Angriffsformen, Sicherheitslücken usw.

Die nationale Sensibilisierungskampagne S-U-P-E-R, die der Bund mit diversen Partnern durchführt, thematisiert die fünf Punkte «sichern», «updaten», «prüfen», «einloggen» und «reduzieren» und gibt zahlreiche Tipps, wie man sich vor Cyber-Bedrohungen schützen kann.

swissVR Monitor: Das neue Datenschutzgesetz tritt am 1. September 2023 ohne Übergangsfristen in Kraft. Was verändert sich dadurch für Unternehmen in puncto Cyber-Resilienz?

Florian Schütz: Das neue Datenschutzrecht stellt die Vereinbarkeit der Schweizer Gesetzgebung mit dem europäischen Recht sicher. Dies ist wichtig, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig ohne zusätzliche Anforderungen möglich bleibt. Für den Wirtschaftsstandort und die Wettbewerbsfähigkeit der Schweiz ist dies zentral.

Die verschiedenen Massnahmen wie beispielsweise das rasche Melden eines Cyber-Vorfalls an den EDÖB (Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten), wenn die Datensicherheit verletzt wurde, sind ein wichtiger Beitrag zur Erhöhung der Cyber-Resilienz.

Der Faktor Mensch beim Thema Cyber-Resilienz

Sonja Stirnimann, Vorsitzende des Prüfungsausschusses der Glarner Kantonalbank und Verwaltungsratsmitglied von Apiax

«Das Territorium «Cyber» ist mindestens 40 Jahre alt und im Vergleich zu anderen operationellen Risiken für viele Verantwortliche noch «Neuland». Was ich erlebe, ist, dass dieses aktuelle Tabu-Thema den Schrecken verliert, wenn es in einem geschützten Rahmen mit Gleichgesinnten auf Stufe Verwaltungsrat und Geschäftsleitung diskutiert werden kann.»

swissVR Monitor: Viele Unternehmen scheinen beim Thema Cyber-Resilienz nicht wirklich Handlungsbedarf zu sehen, bis sie Opfer eines Cyber-Angriffs werden. Unterschätzen respektive verdrängen Firmen oftmals Cyber-Risiken?

Sonja Stirnimann: Noch sehe ich, dass sehr oft die Thematik zu stark den IT-Verantwortlichen zugeschanzt und weniger als strategischer Pfeiler wahrgenommen wird. Dies aus meiner Sicht zu Unrecht, da die Thematik einen so massiven Stellenwert einnimmt, wenn es darum geht die Vermögenswerte, Reputation und Handlungsfähigkeit von Unternehmen und deren Verantwortlichen zu schützen. Die Cyber-Resilienz ist einer der wichtigsten Wettbewerbsvorteile für ein Unternehmen (und deren Verantwortlichen) – auch diese Perspektive wird aktuell noch zu wenig berücksichtigt, wenn es darum geht, präventive Massnahmen für den Ernstfall zu ergreifen.

Ob es sich um bewusstes Verdrängen oder Unterschätzen handelt, möchte ich mir nicht anmassen zu beurteilen, jedoch ist es menschlich, dass Themen, in denen man sich selbst noch nicht so versiert bewegt, gerne vermieden werden. Dieses (unbewusste) Verhalten kann im Kontext der Cyber-Resilienz fatale Folgen haben. Wenn wir das nun aus Sicht der Verantwortung eines Verwaltungsrats betrachten, ist es unabdingbar, dass wir der Thematik die notwendige Beachtung schenken.

Sonja Stirnimann ist als unabhängiges Verwaltungsratsmitglied und Vorsitzende der Prüfungsausschüsse mehrerer privater und börsennotierter Unternehmen tätig. Sie ist Ökonomin, dipl. Wirtschaftsprüferin, hält einen eMBA Financial Services & Insurance der HSG, das Board of Director Diploma des IMD und ist Certified Fraud Examiner (CFE). Als Expertin im Bereich Governance, Risk und Audit ist sie für Unternehmen im Einsatz, wenn es um Unternehmensintegrität und Krisenmanagement im Zusammenhang mit Non-Compliance, Wirtschafts- und Cyber-Kriminalität geht. Sonja Stirnimann verfügt über mehr als drei Jahrzehnte Berufserfahrung und arbeitete für globale Unternehmen wie LafargeHolcim, UBS, Deloitte und EY in ihrem Fachgebiet. Sie unterrichtet an verschiedenen globalen Institutionen, Universitäten, Berufsverbänden sowie für international tätige Unternehmen. Ihr Buch *Der Mensch als Risikofaktor bei Wirtschaftskriminalität. Handlungsfähig bei Non-Compliance und Cyberkriminalität.* ist in der 2. Auflage bei Springer erschienen.

swissVR Monitor: Welche Rolle spielt der (Risiko-)Faktor Mensch beim Thema Cyber-Resilienz?

Sonja Stirnimann: Im Gegensatz zur Resistenz, welche sehr viel stärker die Themen der IT-Sicherheit, die IT-Infrastruktur, die Abwehrdispositive inklusive Monitoring betrifft, ist die Resilienz eines Unternehmens essenziell, wenn es darum geht, wie schnell wir in welcher Form wieder für unsere Stakeholder handlungsfähig sind.

Nicht selten wird die Handlungsfähigkeit akut gefährdet. Diese Handlungsfähigkeit ist enorm stark abhängig von der Reaktion der Verantwortlichen in dieser doch meist ausserordentlichen Situation. Nicht alle Verantwortlichen und somit deren Unternehmen sind auf solche Ernstfälle professionell vorbereitet. Diese Sicherstellung der Handlungsfähigkeit gehört auch auf Stufe Verwaltungsrat und Geschäftsleitung implementiert und ist Teil unserer Verantwortung. Es schadet auch nicht, diesen Ernstfall zu üben und die Kenntnisse daraus verbessernd in den Prozess einfliessen zu lassen.

Cyber-Resilienz – wie wir den Begriff im Sprachgebrauch verwenden – bezieht sich auf die Fähigkeit einer Organisation, Cyber-Angriffe zu erkennen, darauf zu reagieren, sich davon zu erholen und ihre Betriebsfähigkeit aufrechtzuerhalten. Der Unterschied zwischen Resistenz und Resilienz, wenn wir uns etwas vertiefter mit der Thematik auseinandersetzen, sehen wir am Lebenszyklus cyberkrimineller Vorfälle.

Die Resistenz konzentriert sich darauf, Angriffe zu verhindern oder zu stoppen, um Schäden zu vermeiden. Dies umfasst die Implementierung von Sicherheitsmassnahmen wie Firewalls, Intrusion Detection Systems und Sicherheitsrichtlinien. Während die Resistenz wichtig ist, kann sie dennoch nicht garantieren, dass ein Angriff vollständig verhindert wird. In der heutigen Zeit müssen wir davon ausgehen, dass wir alle laufend angegriffen werden. Die Resistenz umfasst präventive Massnahmen zur Absicherung / Minimierung des Risikos.

Resilienz bezieht sich auf die Fähigkeit einer Organisation, nach einem Angriff oder einer Störung schnell zu reagieren, sich zu erholen und ihre Geschäftstätigkeit fortzusetzen. Resilienz beinhaltet die Erkennung von Angriffen, die rasche Reaktion, die Wiederherstellung der Systeme und den kontinuierlichen Betrieb des Unternehmens. Es geht darum, die Auswirkungen und somit meist den Schaden von Angriffen zu begrenzen und sich schnell wieder zu erholen, anstatt nur auf Prävention (Resistenz) zu setzen. Und hier spielt die Handlungsfähigkeit die wesentliche Rolle.

swissVR Monitor: Unternehmen sprechen nicht immer offen über Cyber-Vorfälle. Wie kommen Firmen weg von dieser Tabueinstellung und hin zu mehr Transparenz?

Sonja Stirnimann: Das Territorium «Cyber» ist mindestens 40 Jahre alt und im Vergleich zu anderen operationellen Risiken für viele Verantwortliche noch «Neuland». Was ich erlebe, ist, dass dieses aktuelle Tabu-Thema den Schrecken verliert, wenn es in einem geschützten Rahmen mit Gleichgesinnten auf Stufe Verwaltungsrat und Geschäftsleitung diskutiert werden kann. Dazu bedarf es wie erwähnt den geschützten Rahmen und den Willen, Erfahrungen zu teilen und zu lernen. In der Praxis zeigt sich, dass die Verantwortlichen diesen Austausch schätzen und enorm viel voneinander lernen können. Diese Austausche sind gerne auch industrieübergreifend.

swissVR Monitor: Wen geht das Thema Cyber-Resilienz im Unternehmen etwas an respektive wo sollte es angesiedelt sein?

Sonja Stirnimann: Da es sich für viele Unternehmen noch nicht (oder noch nicht lange) um ein Thema handelt, mit welchem sie sich konfrontiert sehen, erachte ich es als wichtig, dass dieses als eines der operativen Risiken auf Stufe Verwaltungsrat und Geschäftsleitung Beachtung findet und auch dort angesiedelt ist. Dies zusammen mit der Cyber-Resistenz, welche der Resilienz vorgelagert ist. Je nach Maturitätsgrad der jeweiligen Unternehmen und deren Gremien bedarf es auch eine mehr oder weniger steile Lernkurve. Verwaltungsrat und Geschäftsleitung wirken als Vorbild («Role Model») und das gilt bei der Thematik der Cyber-Resilienz genauso.

swissVR Monitor: Sie empfehlen Unternehmen die initiale Massnahme der Sensibilisierung. Was bedeutet dies im Kontext der Cyber-Resilienz?

Sonja Stirnimann: Sensibilisierung beginnt dort, wo über das Thema aktiv gesprochen, informiert und ausgebildet wird – auf sämtlichen Hierarchie-Ebenen. Wir lernen durch Praxisfälle, die analysiert und besprochen werden und können diese für unsere eigene Risikoidentifikation nutzen. Das Bedarf Offenheit der Thematik gegenüber und Einsicht, dass auch wir alle betroffen sein werden, früher oder später. Oft beginnen genau diese Diskussionen erst im Nachgang statt bereits präventiv. Ich sehe gute Erfolge – im Sinne vom Schutz der Vermögenswerte – bei denjenigen Unternehmen, die sich bereits im Vorfeld diese strategischen, unternehmerischen Gedanken machen und ihren Wettbewerbsvorteil ausbauen und sichern wollen.

Kontakte und Autoren

swissVR

Cornelia Ritz Bossicard
Präsidentin swissVR
+41 41 757 67 11
cornelia.ritz@swissvr.ch

Dr. Brigitte Maranghino-Singer
Geschäftsführerin swissVR
+41 41 228 41 19
brigitte.maranghino@swissvr.ch

Deloitte AG

Reto Savoia
CEO Deloitte Schweiz
+41 58 279 60 00
rsavoia@deloitte.ch

Dr. Michael Grampp
Chefökonom & Leiter Research
+41 58 279 68 17
mgrampp@deloitte.ch

Dr. Daniel Laude
Ökonom Research Team
+41 58 279 64 35
dlaude@deloitte.ch

Hochschule Luzern

Dr. Mirjam Durrer
Dozentin für Normatives Board Management, Institut für Finanzdienstleistungen Zug IFZ
+41 41 228 41 73
mirjam.durrer@hslu.ch

swissVR engagiert sich für die Professionalisierung, Vernetzung und die Wahrnehmung der Interessen von Verwaltungsräten. swissVR ist eine unabhängige Vereinigung für Verwaltungsratsmitglieder in der Schweiz, von Verwaltungsräten für Verwaltungsräte. Mit ihrem Angebot trägt swissVR zur Professionalisierung der Verwaltungsratstätigkeit bei, fördert den Erfahrungsaustausch unter Verwaltungsrätinnen und Verwaltungsräten von Unternehmen aller Branchen und bietet seinen über 1'200 Mitgliedern ein bedürfnisspezifisches Informations- und Weiterbildungsangebot. swissVR richtet sich exklusiv an Personen mit einem aktiven Verwaltungsratsmandat. Weitere Informationen finden Sie unter www.swissvr.ch.

Deloitte AG ist eine Tochtergesellschaft von Deloitte NSE LLP, einem Mitgliedsunternehmen der Deloitte Touche Tohmatsu Limited («DTTL»), eine «UK private company limited by guarantee» (eine Gesellschaft mit beschränkter Haftung nach britischem Recht). DTTL und ihre Mitgliedsunternehmen sind rechtlich selbständige und unabhängige Unternehmen. DTTL und Deloitte NSE LLP erbringen selbst keine Dienstleistungen gegenüber Kunden. Eine detaillierte Beschreibung der rechtlichen Struktur finden Sie unter www.deloitte.com/ch/about. Deloitte AG ist eine von der Eidgenössischen Revisionsaufsichtsbehörde (RAB) und der Eidgenössischen Finanzmarktaufsicht FINMA zugelassene und beaufsichtigte Revisionsgesellschaft.

Die **Hochschule Luzern** ist die Fachhochschule der sechs Zentralschweizer Kantone. Mit aktuell rund 8'300 Studierenden in der Ausbildung und über 5'200 in der Weiterbildung, 400 aktuellen Forschungsprojekten und rund 2'000 Mitarbeitenden ist sie die grösste Bildungsinstitution im Herzen der Schweiz. Das Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern – Wirtschaft hat einen Themenschwerpunkt Governance, Risk and Compliance, in dem es auch Weiterbildungen für Verwaltungsratsmitglieder und insbesondere den Zertifikatslehrgang «CAS Verwaltungsrat» anbietet. Weitere Informationen finden Sie unter www.hslu.ch/ifz-verwaltungsrat / www.hslu.ch/cas-vr / www.hslu.ch/ifz

swissVR®

Deloitte.

Global Boardroom Programme | Switzerland

HSLU Hochschule Luzern