# Wie der Verwaltungsrat die Cyber-Resilienz stärkt

swissVR Monitor II/2026
September 2026

swissVR®

Deloitte.

Global Boardroom Programme | Switzerland

HSLU Hochschule Luzern

# Inhaltsverzeichnis



**Über die Umfrage**
Der 20. swissVR Monitor basiert auf einer Befragung von 281 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.

Die Umfrage für den vorliegenden swissVR Monitor wurde von swissVR in Zusammenarbeit mit dem Beratungsunternehmen Deloitte und der Hochschule Luzern im Zeitraum vom 26. Mai 2026 bis zum 5. Juli 2026 durchgeführt. Die 281 Teilnehmenden repräsentieren sowohl Verwaltungsratsmitglieder von börsenkotierten Unternehmen als auch von kleinen und mittelgrossen Unternehmen (KMU) und stammen aus allen relevanten Branchen der Schweizer Wirtschaft. 38% der Teilnehmenden sind Verwaltungsratsmitglieder in kleinen, 28% in mittleren und 34% in grossen 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), mittlere Unternehmen (50 bis 249 Mitarbeitende) und Grossunternehmen (250 und mehr Mitarbeitende).

# Vorwort

**Geschätzte Leserinnen und Leser**

Wir freuen uns, Ihnen den swissVR Monitor II/2026 zu präsentieren. Für die vorliegende Ausgabe haben wir 281 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 in den vergangenen Jahren merklich gestiegenen Häufigkeit und Professionalität von Cyber-Angriffen widmet sich der aktuelle swissVR Monitor – wie bereits die Ausgabe II/2023 – erneut dem Fokusthema Cyber-Resilienz. Aufgrund der potenziell erheblichen Schäden für Unternehmen ist es für Verwaltungsräte unabdingbar, sich im Rahmen ihrer Mandate mit der Cyber-Resilienz auseinanderzusetzen und ein klares Verständnis der eigenen Rolle und der damit verbundenen Aufgaben zu entwickeln. Der aktuelle swissVR Monitor beleuchtet deshalb unter anderem die möglichen Folgen von Cyber-Angriffen, die von Unternehmen umgesetzten Massnahmen und das Cyber-Reporting der Geschäftsleitung an den Verwaltungsrat.

Die Ergebnisse des swissVR Monitors II/2026 zeigen: Der Anteil an Unternehmen, die Cyber-Angriffen zum Opfer gefallen sind, ist seit 2023 deutlich angestiegen. Gleichzeitig bereitet sich nur eine überschaubare Minderheit auf Angriffe vor, die sich die Technologie der künstlichen Intelligenz zunutze machen. In Verwaltungsräten besteht der grösste Handlungsbedarf darin, das Krisenmanagement im Fall eines Cyber-Angriffs zu proben, die nötige Expertise für das VR-Gremium sicherzustellen und ein umfassendes Cyber-Reporting durch die Geschäftsleitung zu etablieren. Kleinere Unternehmen weisen bei diesen drei Aspekten tendenziell grösseren Verbesserungsbedarf auf als Grossunternehmen.

Neben den Befragungsergebnissen bietet der swissVR Monitor II/2026 auch Interviews mit:

- Marc Ruef, Head of Research von scip und Lead Architect von VulDB
- Sandra Emme, Industry Leader Cloud Enterprise von Google und Verwaltungsratsmitglied von Belimo und Zehnder Group International
- Frank Desiere, CEO und Verwaltungsratsmitglied von CorTec

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

**Isabelle Amschwand**
Präsidentin swissVR

**Reto Savoia**
CEO Deloitte Schweiz

**Prof. Dr. Mirjam Gruber-Durrer**
Dozentin IFZ / Hochschule Luzern

# Wichtigste Ergebnisse in Kürze

**16%**
**der befragten VR-Mitglieder erwarten für die Schweizer Wirtschaft in den nächsten 12 Monaten eine positive Konjunkturentwicklung.**

**41%**
**geben an, dass ihr Unternehmen in der Vergangenheit Opfer eines Cyber-Angriffs geworden ist.**

**74%**
**verfügen aktuell nicht über eine Strategie, die KI-basierte Cyber-Angriffe berücksichtigt.**

### Leichter Aufwärtstrend bei den Wirtschaftsaussichten

- Die Konjunktur-, Branchen- und Geschäftsaussichten für die kommenden 12 Monate haben sich im Vergleich zu den beiden Vorausgaben leicht verbessert.
- Die Risiken und Unsicherheitsfaktoren für die Schweizer Wirtschaft, darunter die Spannungen am Persischen Golf sowie die Möglichkeit neuer Zölle auf Importe aus der Schweiz in die USA, bleiben jedoch bestehen.

### Die Bedeutung der Cyber-Resilienz nimmt zu

- Der Anteil an Unternehmen, die bereits mindestens einmal Opfer eines Cyber-Angriffs geworden sind, ist seit 2023 um fast die Hälfte gestiegen.
- Zu den häufigsten Folgen von nicht abgewehrten Angriffen gehören Betriebsunterbrüche und unberechtigte Zugriffe auf Unternehmensdaten (Datenlecks).

### Mehrheit der Unternehmen nicht auf KI-basierte Cyber-Angriffe vorbereitet

- Lediglich knapp ein Fünftel der Unternehmen verfügt über eine Strategie gegen KI-basierte Cyber-Angriffe und informiert den Verwaltungsrat über deren Implementationsstatus und Effektivität.
- In über der Hälfte der Unternehmen existieren entweder keine Pläne zur Wiederherstellung der IT nach einem schweren Cyber-Angriff oder wurden diese Pläne noch nicht getestet.

**68%**
**der Verwaltungsräte fehlt ein Mitglied mit Cyber- beziehungsweise IT-Expertise.**

**33%**
**sehen die Effizienzsteigerung und Optimierung interner Prozesse als wichtiges Thema für die kommenden 12 Monate.**

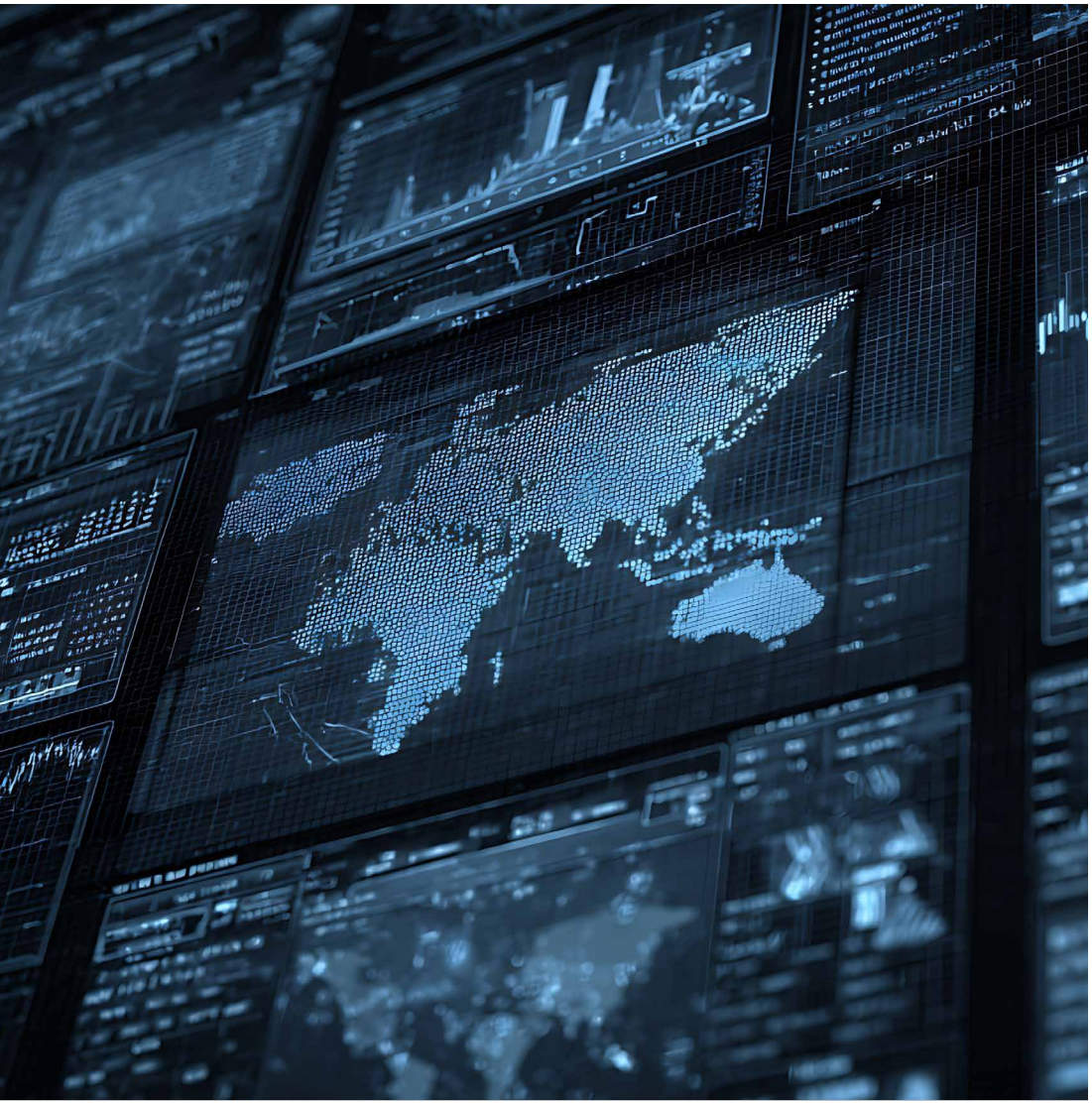
### Verwaltungsräte mit Handlungsbedarf bei der Cyber-Resilienz

- Nur etwa die Hälfte der Verwaltungsräte probt das Krisenmanagement für den Fall eines Cyber-Angriffs.
- Die Hälfte der VR-Gremien wird nicht regelmässig von der Geschäftsleitung über Cyber-Vorfälle im Unternehmen informiert.
- Über ein Mitglied mit Cyber- beziehungsweise IT-Expertise verfügt lediglich ein Drittel der Verwaltungsräte.

### Veränderungen bei den Fokusthemen im Verwaltungsrat

- Bei den Top-Themen der Verwaltungsräte für die kommenden 12 Monate steigen die Effizienzsteigerung und Optimierung interner Prozesse von Rang zwei in der Vorausgabe auf aktuell Rang eins.
- Das Risikomanagement fällt von Platz eins auf zwei und die Themen Digitalisierung, Robotik und Automatisierung steigen von Platz sechs auf drei.

# Konjunktur-, Branchen- und Geschäftsaussichten



Die Konjunktur-, Branchen- und Geschäftsaussichten für die kommenden 12 Monate haben sich im Vergleich zu den vergangenen zwei Ausgaben des swissVR Monitors leicht verbessert (siehe Abbildung 1). Es scheint sich ein leichter Aufwärtstrend abzuzeichnen – fürs Erste in einem verhaltenen Ausmass. Dies ist insofern bemerkenswert, als dass nach wie vor zahlreiche Risiken und belastende Faktoren für die Schweizer Wirtschaft bestehen: Spannungen am Persischen Golf, die Möglichkeit neuer Zölle auf Importe aus der Schweiz in die USA, eine weitere Aufwertung des Schweizer Frankens gegenüber anderen Währungen sowie die weiterhin schwächelnde Konjunktur in wichtigen Auslandsmärkten.

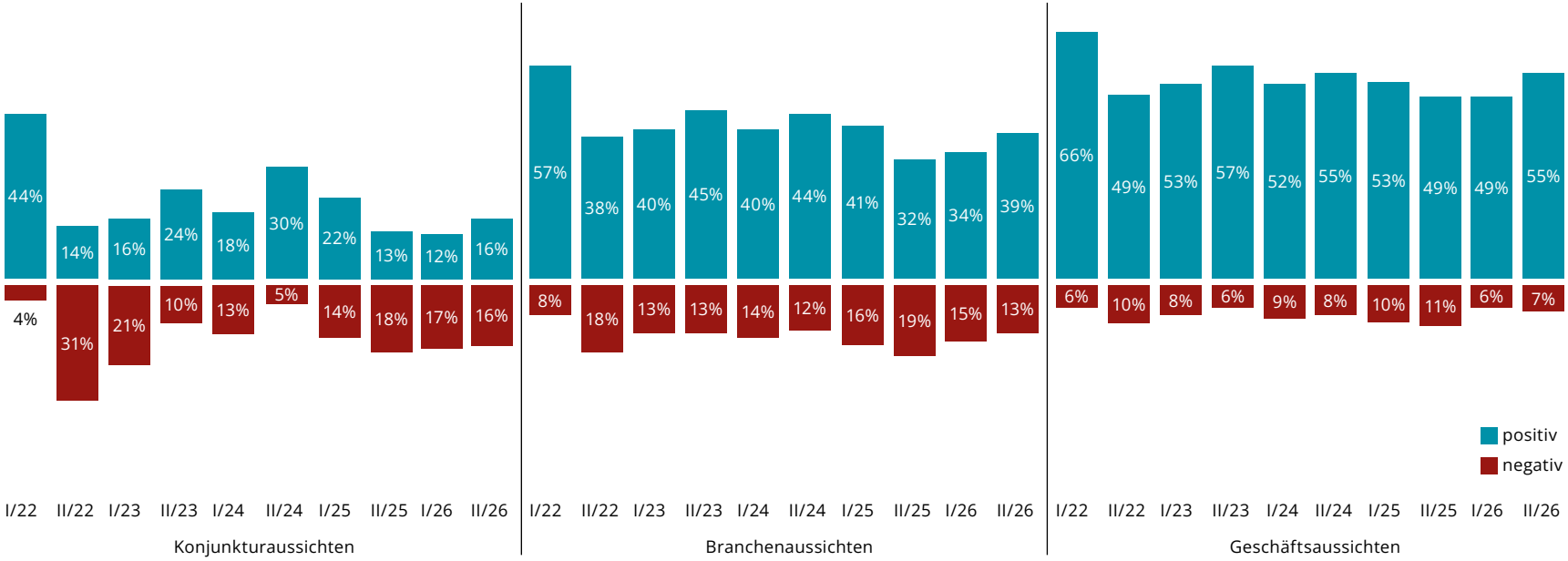
Etwa zwei Drittel der befragten Verwaltungsratsmitglieder (68%) gehen davon aus, dass sich die Konjunktur über die nächsten 12 Monate neutral entwickeln wird. Der Saldo aus positiven und negativen Erwartungen ergibt null und damit ebenfalls ein neutrales Stimmungsbild (16% positiv versus 16% negativ). Dieses Resultat deckt sich mit anderen derzeitigen Prognosen, die für 2026 und 2027 zwar ein leichtes Wachstum der Schweizer Wirtschaft voraussagen, jedoch eines, das deutlich unter dem langjährigen Durchschnitt liegt.

Knapp die Hälfte der Verwaltungsratsmitglieder (48%) erwartet auch in der eigenen Branche für die nächsten 12 Monate eine neutrale Entwicklung. Gleichzeitig überwiegen positive Branchenaussichten (39%) deutlich gegenüber negativen Erwartungen (13%). Überdurchschnittlich optimistisch sind die Aussichten unter Verwaltungsratsmitgliedern in der Informations- und Kommunikationstechnik (58% positiv versus 3% negativ), was auf diese Branche aufgrund der Themenkonjunktur der künstlichen Intelligenz in den letzten Jahren öfters zutrifft, jedoch aktuell besonders stark der Fall ist. Unterdurchschnittliche Erwartungen zeigen sich hingegen im verarbeitenden Gewerbe und der Chemie (20% positiv versus 28% negativ). Dies dürfte mit der hohen Exportorientierung dieser Branche beziehungsweise der Zollsituation, dem starken Franken und der verhaltenen Auslandsnachfrage zusammenhängen.

Für das eigene Unternehmen erwartet mehr als die Hälfte (55%) der Verwaltungsratsmitglieder in den kommenden 12 Monaten eine positive Entwicklung. Ebenfalls ein beträchtlicher Anteil von 38 Prozent hat neutrale Geschäftsaussichten und nur wenige Befragte sind pessimistisch für die kommenden 12 Monate (7%). Die grösste Zuversicht für ihr Unternehmen äussern Verwaltungsratsmitglieder in der Branche der Informations- und Kommunikationstechnik (73% positiv versus 3% negativ) sowie der Pharma- und Gesundheitsbranche (68% positiv versus 0% negativ). Unterdurchschnittliche Geschäftsaussichten zeigen sich im verarbeitenden Gewerbe und der Chemie (24% positiv versus 16% negativ), wobei der sinkende Saldo aus positiven und negativen Erwartungen zusätzlich auf einen (noch) weniger optimistischen Ausblick für jene Unternehmen im Vergleich zur vorigen Ausgabe des swissVR Monitors hinweist.

**Abb. 1 Beurteilung der Aussichten in den nächsten 12 Monaten [swissVR Monitor I/2022 bis II/2026]**

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

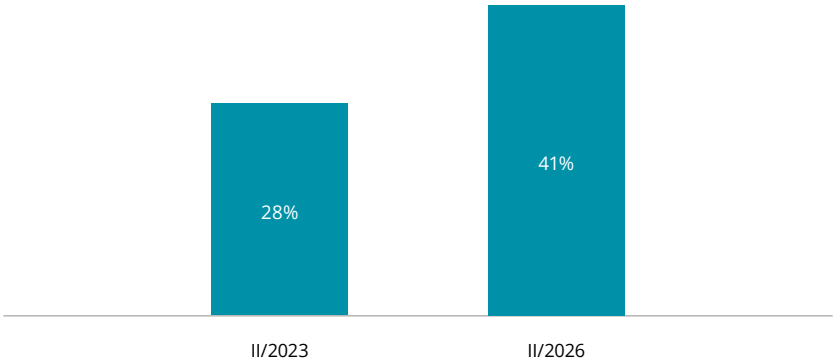


# Fokusthema: Wie der Verwaltungsrat die Cyber-Resilienz stärkt


Cyber-Angriffe auf Unternehmen und andere Organisationen haben in den vergangenen Jahren in ihrer Häufigkeit und Professionalität stark zugenommen. Ein wesentlicher Treiber für diese Entwicklung ist die wachsende Abhängigkeit von stark vernetzten und komplexen digitalen Systemen wie Cloud-Services und Lieferketten. Ausserdem trägt die rasante Weiterentwicklung der künstlichen Intelligenz mit regelmässig neuen Modellen und leistungsfähigeren Agenten dazu bei, dass Cyberangriffe einfacher, schneller und in grösserem Umfang durchgeführt werden können als bisher. Vor dem Hintergrund dieser technologischen Entwicklung ist zukünftig von einer noch höheren Frequenz und einem stärkeren Ausmass von Cyber-Angriffen auszugehen. Daher steigt für Verwaltungsräte weiterhin die Bedeutung, sich mit der Cyber-Resilienz ihrer Unternehmen auseinanderzusetzen und diese im Rahmen der eigenen Rolle und Aufgaben zu stärken.

**Abb. 2 Unternehmen mit schadhaften Vorfällen von Cyber-Angriffen**

*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.)?*



## Vorfälle und Folgen von Cyber-Angriffen

Vier von zehn Verwaltungsratsmitgliedern (41%) geben an, dass ihr Unternehmen ihrer Kenntnis nach in der Vergangenheit Opfer eines Cyber-Angriffs geworden ist (siehe Abbildung 2). Damit ist dieser Anteil innert drei Jahren – zuletzt im swissVR Monitor II/2023 erhoben – um 13 Prozentpunkte respektive bezogen auf den Ausgangswert von 28 Prozent um fast die Hälfte (46%) angestiegen.

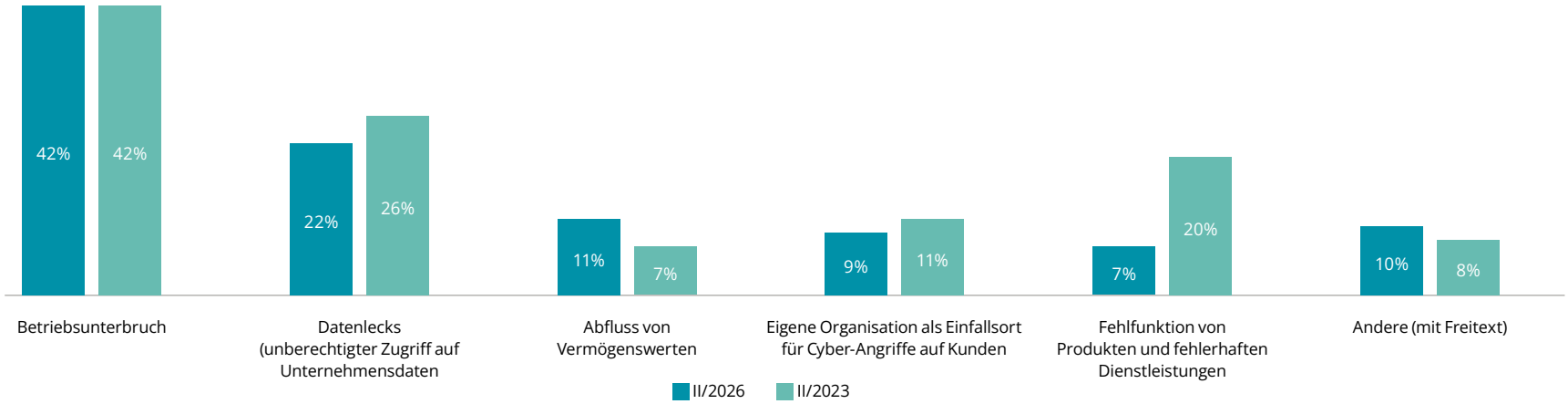
Diese Zunahme ist insofern bemerkenswert, als dass trotz der von vielen Unternehmen in den vergangenen Jahren in Cyber-Resilienz getätigten Investitionen der Anteil an Unternehmen, die Cyber-Angriffen zum Opfer gefallen sind, nach wie vor steigt. Zusätzlich dürfte es eine nicht zu vernachlässigende Dunkelziffer bei Cyber-Vorfällen geben, da die vorliegende Befragung ebenfalls gezeigt hat, dass lediglich jeder zweite Verwaltungsrat hierzu ein regelmässiges Reporting von der Geschäftsleitung erhält (siehe Abbildung 9).

Zurückzuführen ist die Zunahme über die vergangenen drei Jahre darauf, dass mehr kleine und mittelgrosse Unternehmen Cyber-Angriffen zum Opfer gefallen sind. So hat sich der Anteil dieser Unternehmen von 20 auf 37 Prozent fast verdoppelt, während er bei Grossunternehmen praktisch konstant geblieben ist (II/2026: 48%, II/2023: 45%). Zwar sind Letztere auf Grund ihrer Grösse nach wie vor mehr exponiert, jedoch fallen auch immer mehr kleine und mittelgrosse Unternehmen Cyber-Angriffen zum Opfer. Damit ist die Bedeutung der Cyber-Resilienz nicht abhängig von der Unternehmensgrösse, sondern für alle Unternehmen existenziell entscheidend.

Die Bedeutung einer hoch ausgeprägten Cyber-Resilienz zeigt sich ebenfalls in den vielfältigen Folgen, die nicht abgewehrte Angriffe mit sich bringen (siehe Abbildung 3). Dort sticht wie vor drei Jahren der Betriebsunterbruch (42%) als mit Abstand meistgenannte Antwort hervor, gefolgt von Datenlecks (22%) an zweiter Stelle. Die restlichen Folgen kommen relativ selten vor. Mit Ausnahme der Fehlfunktion von Produkten und Dienstleistungen treten alle Folgen praktisch gleich häufig auf wie in der Erhebung vor drei Jahren.

**Abb. 3 Folgen von Cyber-Angriffen in Unternehmen**

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



## Künstliche Intelligenz, Minimal Viable Company und Massnahmen für Mitarbeitende

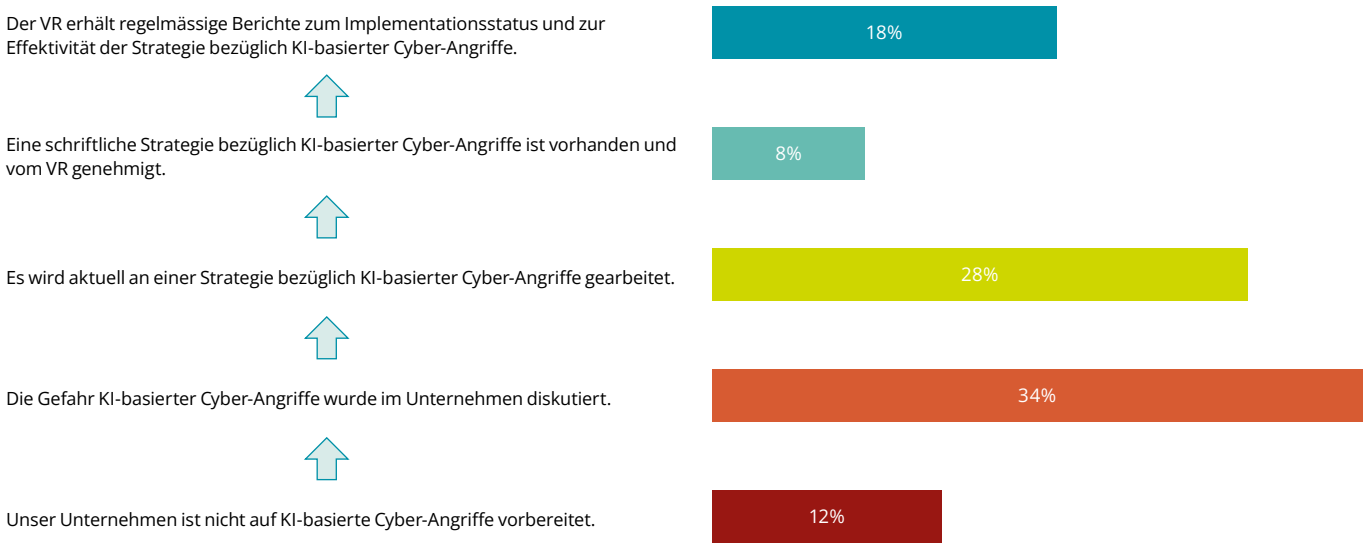
Wie eingangs beschrieben tragen die Entwicklungen in der künstlichen Intelligenz dazu bei, dass Angreifer einfacher und schneller grosse Schäden anrichten können. Daher stellt sich die Frage, wie Unternehmen spezifisch auf diese zusätzliche Gefährdung vorbereitet sind (siehe Abbildung 4).

Etwa drei Viertel (74%, untere drei Balken kumuliert) verfügen aktuell nicht über eine schriftliche Strategie, die KI-basierte Cyber-Angriffe berücksichtigt. Vom restlichen Viertel hat ein Teil der Unternehmen eine solche Strategie (8%), während bei den meisten Unternehmen dieser Gruppe der Verwaltungsrat zusätzlich über den Implementationsstatus und die Effektivität der Strategie informiert wird (18%). An dieser Stelle ist es wichtig anzumerken, dass das Vorhandensein einer Strategie für KI-basierte Cyber-Angriffe sowie ein entsprechendes Effektivitätsreporting an den Verwaltungsrat keine direkte Aussage darüber zulassen, ob ein Unternehmen im Ernstfall tatsächlich in der Lage ist, solche Angriffe abzuwehren.

Auch beim Vorbereitungsgrad spielt die Unternehmensgrösse eine entscheidende Rolle: Während in Kleinunternehmen lediglich 18 Prozent über eine Strategie für KI-basierte Cyber-Angriffe verfügen, liegt dieser Anteil in Grossunternehmen bei 40 Prozent. Dieses Ergebnis könnte auf einen Zusammenhang zwischen der Unternehmensgrösse und der Anzahl von Cyber-Attacken oder auf eine stärkere Institutionalisierung von Cyber-Themen in Grossunternehmen zurückzuführen sein (zum Beispiel in Form einer IT-Abteilung oder in der Funktion eines Chief Information Security Officers, CISO).

**Abb. 4 Vorbereitungsgrad auf KI-basierte Cyber-Angriffe**

*Frage: Mit Hilfe künstlicher Intelligenz (KI) lassen sich grosse Cyber-Schäden anrichten. Wie bereitet sich Ihr Unternehmen auf KI-basierte Cyber-Angriffe vor?*



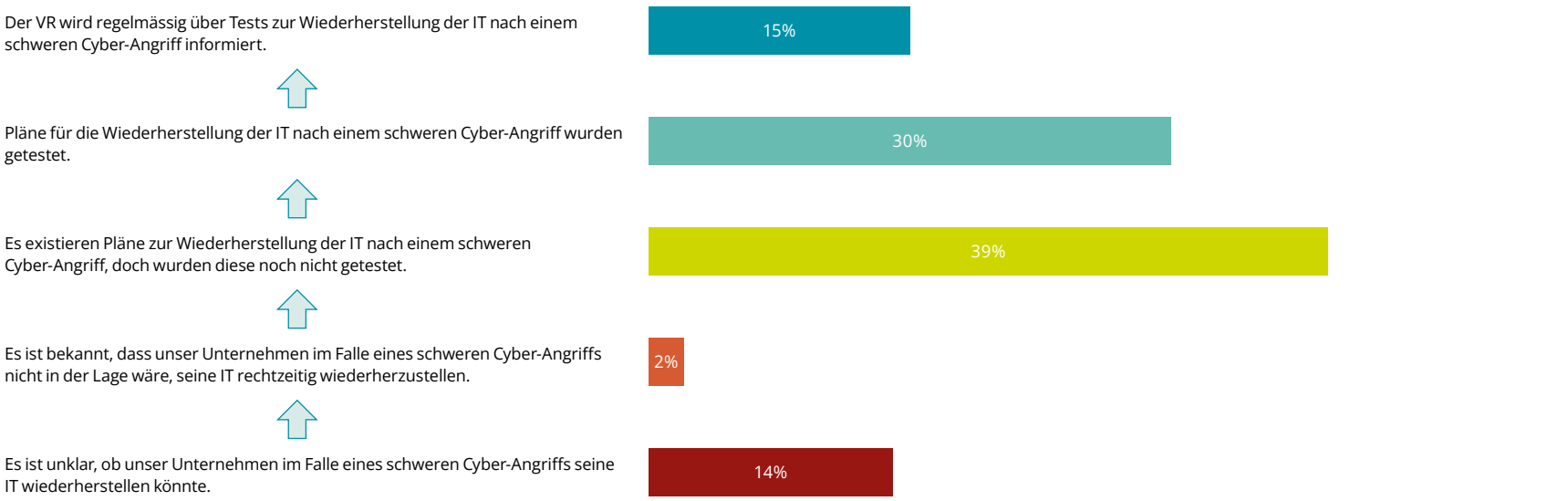
Wenn es wie oben beschrieben nicht möglich ist, einen Cyber-Angriff abzuwehren, stellt sich in der Folge die Frage, ob die wichtigen IT-Kernprozesse – die sogenannte «Minimal Viable Company» – schnell genug wiederhergestellt werden können, bevor das Unternehmen dauerhaften Schaden trägt (siehe Abbildung 5). In mehr als der Hälfte der Unternehmen (55%, untere drei Balken kumuliert) existieren entweder keine Pläne zur Wiederherstellung der IT nach einem schweren Cyber-Angriff oder wurden diese noch nicht getestet.

Im Umkehrschluss haben 45 Prozent ihre Pläne für eine Minimal Viable Company getestet und ein Drittel hiervon rapportiert die Testresultate auch an den Verwaltungsrat (15%). In diesem Zusammenhang ist darauf hinzuweisen, dass das Vorhandensein von getesteten Plänen sowie ein Reporting an den Verwaltungsrat nicht bedeuten, dass eine Wiederherstellung der IT in allen dieser Fälle garantiert ist.

Erneut zeigt sich der Einfluss der Unternehmensgrösse deutlich: Grossunternehmen (60%) verfügen etwa doppelt so häufig über getestete Pläne für eine Minimal Viable Company wie kleine Unternehmen (32%). Unter den verschiedenen Branchen sind in Bezug auf die Wiederherstellung der IT nach einem Cyber-Angriff insbesondere Unternehmen, die Finanzdienstleistungen anbieten, mit entsprechenden Plänen vorbereitet (70%). Dies lässt sich durch den besonders hohen Stellenwert eines funktionierenden IT-Systems für Finanzunternehmen erklären, der im Vergleich zu anderen Branchen wie zum Beispiel dem Baugewerbe oder Tourismus noch ausgeprägter ist, sowie dadurch, dass der Finanzsektor zur kritischen Infrastruktur eines Staates zählt und branchenspezifische Standards entsprechend stärker etabliert sind.

**Abb. 5 Minimal Viable Company im Fall eines Cyber-Angriffs**

*Frage: Könnten die wichtigsten Kernprozesse – die sogenannte «Minimal Viable Company» – im Fall eines Cyber-Angriffs wiederaufgebaut werden, bevor Ihr Unternehmen inakzeptable Kosten oder Schäden hinnehmen müsste?*



Vor dem Hintergrund der teilweise schwerwiegenden Folgen von Cyber-Angriffen stehen Unternehmen eine Reihe von Massnahmen zur Verfügung, damit sich Mitarbeitende im Cyberspace nicht fahrlässig verhalten (siehe Abbildung 6). So geben jeweils etwa neun von zehn Verwaltungsratsmitgliedern (89%) an, dass die Rollen und Verantwortlichkeiten für Cyber-Sicherheit im Unternehmen klar definiert sind oder eine positive Sicherheitskultur aktiv gefördert wird. Cyber-Schulungen sind etwas weniger weit verbreitet (83%), Awareness-Programme in circa drei von vier Fällen (74%) und die Wirksamkeit von Schulungen wird gemäss sechs von zehn Verwaltungsratsmitgliedern gemessen (61%).

In kleinen Unternehmen werden die aufgeführten Massnahmen merklich seltener umgesetzt als in Grossunternehmen. So sind Awareness-Programme wie zum Beispiel Phishing-Tests lediglich in der Hälfte der kleinen Unternehmen (54%) vorhanden. Ob Cyber-Schulungen wirksam sind, untersucht gar nur ein Drittel der kleinen Unternehmen (36%). Ab einer Unternehmensgrösse von 1000 Mitarbeitenden werden alle aufgeführten Massnahmen praktisch von jedem befragten Unternehmen umgesetzt.

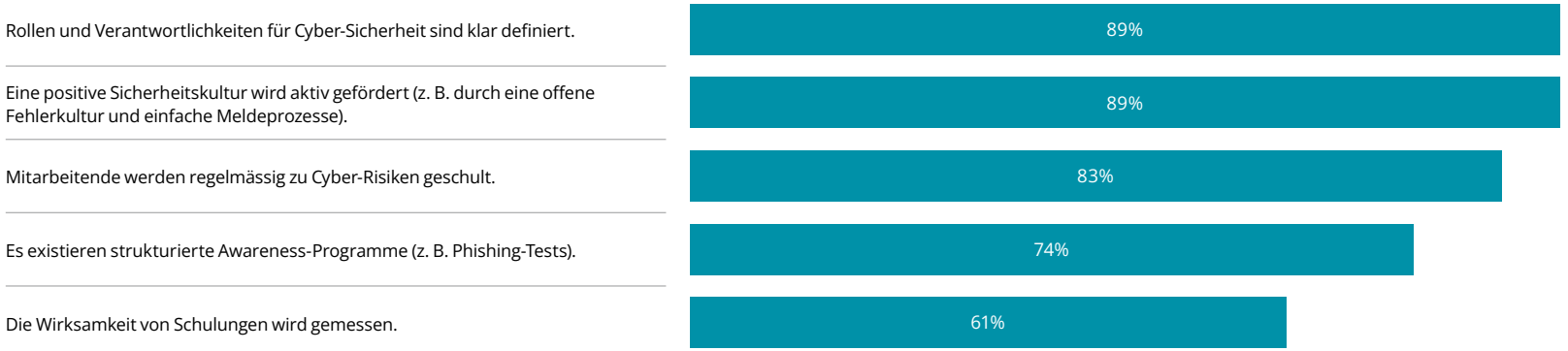
Vor dem Hintergrund der Bedrohung durch KI-basierte Cyber-Angriffe besteht die Aufgabe des Verwaltungsrats darin, von der Geschäftsleitung eine diesbezüglich fundierte Strategie einzufordern sowie deren Implementationsstatus und Effektivität zu überwachen. Ziel des Verwaltungsrats sollte es sein zu beurteilen, ob das Unternehmen im Ernstfall in der Lage ist, solche Angriffe abzuwehren, und gegebenenfalls Verbesserungen der Cyber-Resilienz zu initiieren.

Gleiches gilt für die Sicherstellung der Minimal Viable Company: Auch hier muss der Verwaltungsrat die Pläne zur Wiederherstellung der IT nach einem schweren Cyber-Angriff sowie die Ergebnisse von Testläufen nachvollziehen können. Auf dieser Grundlage kann er beurteilen, ob die Minimal Viable Company sichergestellt ist und ob zusätzliche Massnahmen erforderlich sind.

Weitere Informationen und Empfehlungen zu diesen Themen sind in folgenden Interviews enthalten:
- Marc Ruef über aktuelle Entwicklungen in der Cyber-Resilienz
- Frank Desiere über die Bedeutung von künstlicher Intelligenz bei Cyber-Angriffen

**Abb. 6 Massnahmen zum Verhalten der Mitarbeitenden im Cyberspace**

*Frage: Inwiefern werden folgende Massnahmen, die sich auf das Verhalten der Mitarbeitenden im Cyberspace beziehen, in Ihrem Unternehmen umgesetzt?*



## Der Verwaltungsrat und die Cyber-Resilienz

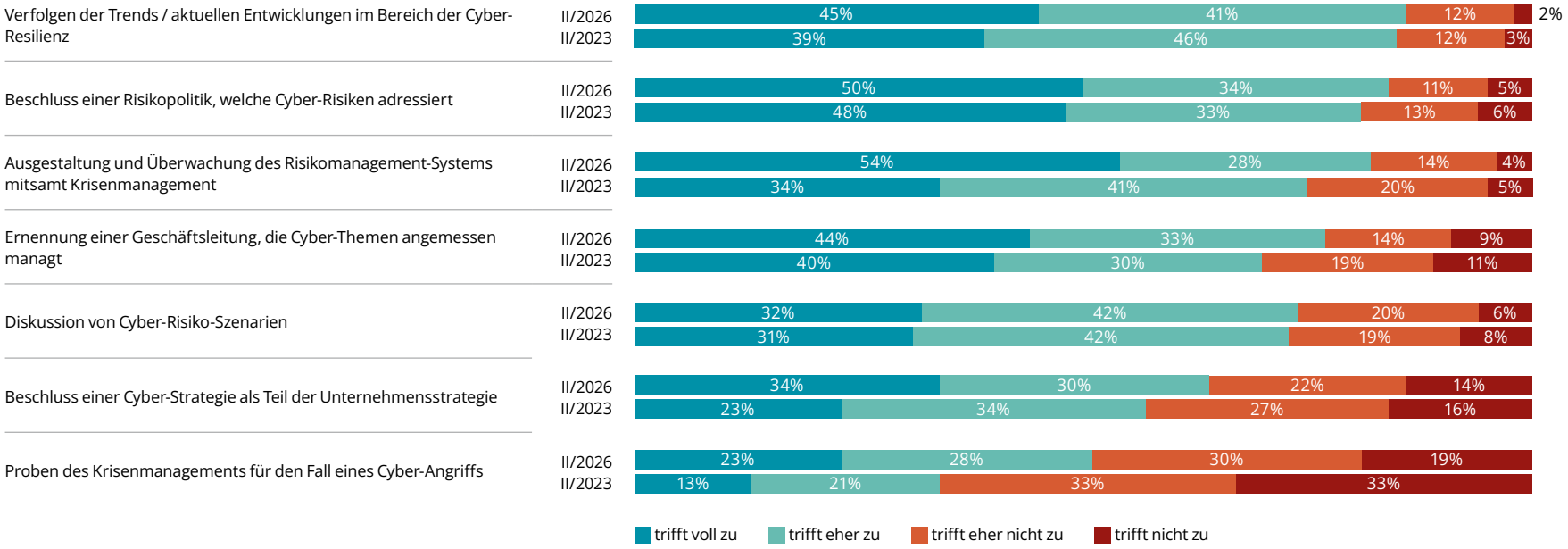
In Bezug auf die Cyber-Resilienz kommen dem Verwaltungsrat verschiedene Aufgaben und Rollen zu (siehe Abbildung 7). Eine sehr grosse Mehrheit der Befragten bejaht, dass ihr VR-Gremium Trends und aktuelle Entwicklungen im Cyber-Bereich verfolgt (86%) beziehungsweise eine Risikopolitik beschliesst, die Cyber-Risiken adressiert (84%).

Weitere Aufgaben, die die meisten Verwaltungsratsmitglieder zumindest teilweise wahrnehmen, sind die Ausgestaltung und Überwachung des Risikomanagement-Systems mitsamt Krisenmanagement (82%), die Ernennung einer im Cyber-Management kompetenten Geschäftsleitung (77%) sowie die Diskussion von Cyber-Risiko-Szenarien (74%). Wenn es um den Beschluss einer Cyber-Strategie als Teil der Unternehmensstrategie geht, bestätigen dies knapp zwei Drittel der Befragten (64%). Verbesserungspotenzial zeigt sich beim Krisenmanagement im Ernstfall eines Cyber-Angriffs: Dies wird lediglich in der Hälfte der Fälle geprobt (51%), wobei im Vergleich zur Erhebung vor drei Jahren ein deutlicher Anstieg zu verzeichnen ist (II/2023: 34%).

Erneut weisen alle Aussagen von Verwaltungsratsmitgliedern aus Grossunternehmen tendenziell höhere Zustimmungsraten auf als jene aus Kleinunternehmen. Ausserdem zeigt der Vergleich mit der Erhebung des swissVR Monitors II/2023, dass sich heute etwas mehr Verwaltungsräte mit der Cyber-Resilienz auseinandersetzen als damals.

**Abb. 7 Aufgaben und Rollen des Verwaltungsrats**

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

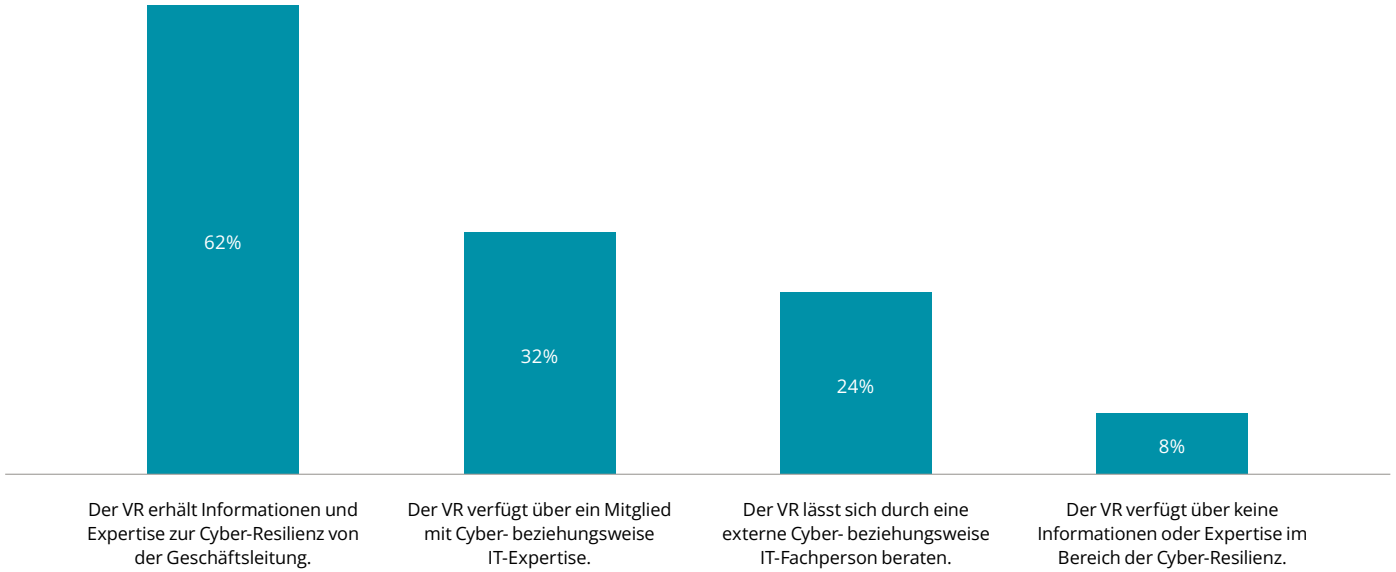


Der Verwaltungsrat kann seine Expertise zur Cyber-Resilienz aus verschiedenen Quellen beziehen (siehe Abbildung 8). Die Mehrheit der Verwaltungsräte ist bei diesem Fachwissen auf die Geschäftsleitung angewiesen (62%). Lediglich ein Drittel der Befragten (32%) gibt an, dass ihr Gremium über ein Mitglied mit Cyber- beziehungsweise IT-Expertise verfügt. In einem Viertel (24%) der Fälle wird eine externe Fachperson zu Rate gezogen und 8 Prozent der Verwaltungsräte weist keine Cyber-Expertise auf.

Da Grossunternehmen tendenziell über grössere Verwaltungsräte als Kleinunternehmen verfügen, überrascht es nicht, dass in ihren Gremien ebenfalls häufiger Mitglieder mit Cyber- beziehungsweise IT-Expertise vertreten sind (41% versus 28%). Im Branchenvergleich sind Mitglieder mit Cyber- beziehungsweise IT-Expertise in Verwaltungsräten besonders häufig in der Informations- und Kommunikationstechnik (53%) sowie in den Unternehmensdienstleistungen (41%) anzutreffen, während das Baugewerbe (20%), das Pharma- und Gesundheitswesen (19%) sowie das verarbeitende Gewerbe und die Chemie (16%) unterdurchschnittliche Werte aufweisen.

**Abb. 8 Cyber-Expertise im Verwaltungsrat**

*Frage: Von wem erhält Ihr VR nötige Informationen und Expertise im Bereich der Cyber-Resilienz? Bitte geben Sie alle zutreffenden Aspekte an.*

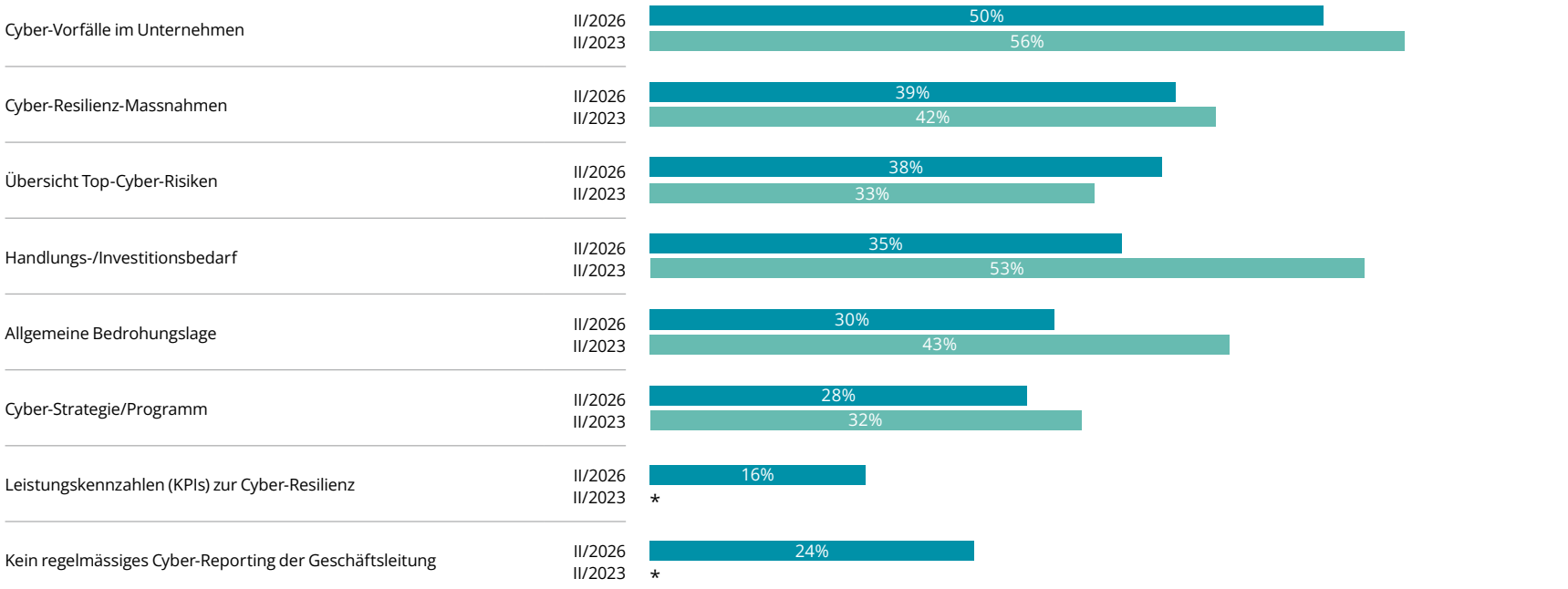


Der Verwaltungsrat erhält von der Geschäftsleitung zu verschiedenen Cyber-Themen ein regelmässiges Reporting beziehungsweise Berichte, dennoch besteht hier Verbesserungspotenzial (siehe Abbildung 9). So wird nur rund die Hälfte der VR-Gremien über Cyber-Vorfälle im Unternehmen informiert (50%). Eine Berichterstattung zu anderen Cyber-Aspekten erfolgt gar jeweils in einer Minderheit aller Fälle und ein Viertel der Befragten (24%) gibt an, der eigene Verwaltungsrat erhalte kein regelmässiges Cyber-Reporting.

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. 9 Cyber-Reporting durch die Geschäftsleitung**

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




* nicht erhoben

Trotz einer steigenden Zahl von Unternehmen, die bereits Cyber-Angriffen zum Opfer gefallen sind, und einer zunehmenden Bedrohung durch KI-basierte Angreifer hat das Reporting zum Handlungs-/Investitionsbedarf (-18 Prozentpunkte) und zur allgemeinen Bedrohungslage (-13 Prozentpunkte) gegenüber der Erhebung des swissVR Monitors II/2023 abgenommen. Dies könnte ein Hinweis darauf sein, dass Cyber-Resilienz in vielen Unternehmen in der Berichterstattung von der Geschäftsleitung an den Verwaltungsrat eher als einmalige Aufgabe und weniger als kontinuierlicher Prozess verstanden wird.

Da das Risiko, dass das eigene Unternehmen einem Cyber-Angriff zum Opfer fällt, weit verbreitet ist, sind Verwaltungsräte gut beraten, das Krisenmanagement innerhalb des Gremiums für einen solchen Ernstfall zu proben. Dazu gehört beispielsweise die Frage, welche Massnahmen in Zusammenarbeit mit der Geschäftsleitung eingeleitet werden müssen, um die Minimal Viable Company sicherzustellen.

Mit Blick auf die Zusammensetzung des Verwaltungsrats empfiehlt es sich, entweder über ein Mitglied mit Cyber- beziehungsweise IT-Expertise zu verfügen oder sich durch externe Fachpersonen auf diesem Gebiet beraten zu lassen, damit das VR-Gremium seine Rolle als Sparringspartner der Geschäftsleitung wahrnehmen und zur Stärkung der Cyber-Resilienz im Unternehmen beitragen kann.

Die Oberaufsichtspflicht des Verwaltungsrats erfordert ebenfalls ein regelmässiges Cyber-Reporting durch die Geschäftsleitung. Eine solche Berichterstattung sollte wichtige Kernelemente wie Informationen über Cyber-Vorfälle im Unternehmen enthalten; fehlen diese, sind sie einzufordern.

Weitere Informationen und Empfehlungen zu diesen Themen sind in folgenden Interviews enthalten:

- Sandra Emme über die Rolle des Verwaltungsrats bei der Cyber-Resilienz
- Frank Desiere über die Bedeutung von künstlicher Intelligenz bei Cyber-Angriffen.

# Strategie- und Strukturthemen im Verwaltungsrat

## Funktionen, Sitzungsanzahl, Zeitaufwand und Organhaftpflichtversicherung

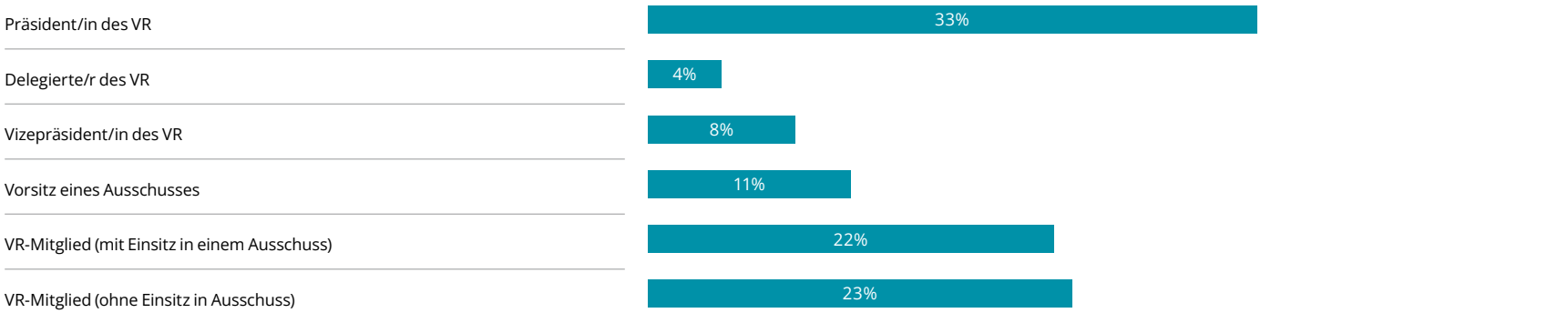
Am swissVR Monitor II/2026 haben Personen mit verschiedenen Funktionen in Verwaltungsräten teilgenommen (siehe Abbildung 10). Verwaltungsratsmitglieder mit und ohne Einsitz in einem Ausschuss stellen zusammen die relative Mehrheit (45%) der Befragten dar. Ein Drittel der in der vorliegenden Befragung teilnehmenden Personen sind VR-Präsidenten/innen (33%). Ausserdem umfasst die Erhebung ebenfalls andere Funktionen wie Ausschussvorsitzende (11%), Vizepräsidenten/innen (8%) oder VR-Delegierte (4%).

Verwaltungsräte können sich bei der Anzahl ihrer Sitzungen pro Jahr – ohne Ausschüsse – stark unterscheiden (siehe Abbildung 11). Fast drei Viertel der VR-Gremien (72%) treffen sich zwischen drei und sechsmal jährlich zu einer Sitzung, etwa ein Viertel (26%) öfter. Tendenziell nimmt die Anzahl an VR-Sitzungen mit der Unternehmensgrösse zu: Während sich Verwaltungsräte von Kleinunternehmen im Median fünfmal im Jahr treffen, finden in Grossunternehmen sechs Zusammenkünfte im gleichen Zeitraum statt. Im Vergleich mit der Ausgabe II/2024 hat sich der Median aller Unternehmen von 5 auf aktuell 6 Sitzungen erhöht.

Neben der Anzahl der Sitzungen variiert auch der jährliche Zeitaufwand für das VR-Mandat stark (siehe Abbildung 12). Inklusive Sitzungen, Ausschüssen, Vorbereitungen, Repräsentation sowie Aus- und Weiterbildungen ergibt sich ein Mittelwert von 22 Tagen und ein Median von 15 Tagen. Dies zeigt, dass einige Verwaltungsratsmitglieder mit einem recht hohen Aufwand nach oben «ausreissen». Jene Ausreisser sind in der Kategorie «> 30 Tage» enthalten und machen circa ein Siebtel (15%) der Befragten aus. Knapp zwei Drittel dieser Untergruppe (61%) stellen VR-Präsident/innen dar. Im Vergleich mit dem swissVR Monitor II/2022 und II/2024 haben sich der Mittelwert und der Median des jährlichen Zeitaufwands für das VR-Mandat nicht nennenswert verändert.

**Abb. 10 Eigene Funktion(en) im Verwaltungsrat**

*Frage: Welche Funktion haben Sie im Verwaltungsrat? [Zutreffende Funktionen ankreuzen.]*



Ein Verwaltungsratsmandat bringt eine grosse Verantwortung mit sich – sowohl für das Unternehmen als auch für die jeweilige Person selbst. Es besteht beispielsweise das Risiko, im Schadensfall durch eine Verantwortlichkeitsklage persönlich belangt zu werden. Um sich gegen die Kosten für die Abwehr von Verantwortlichkeitsklagen, unbegründete Forderungen und allfällige Entschädigungszahlungen abzusichern, können VR-Mitglieder und Unternehmen eine Organhaftpflichtversicherung (D&O Versicherung) abschliessen.

**Abb. 11 Anzahl VR-Sitzungen pro Jahr**

*Frage: Wie viele VR-Sitzungen finden in Ihrem Unternehmen pro Jahr statt (ohne Ausschüsse)?*

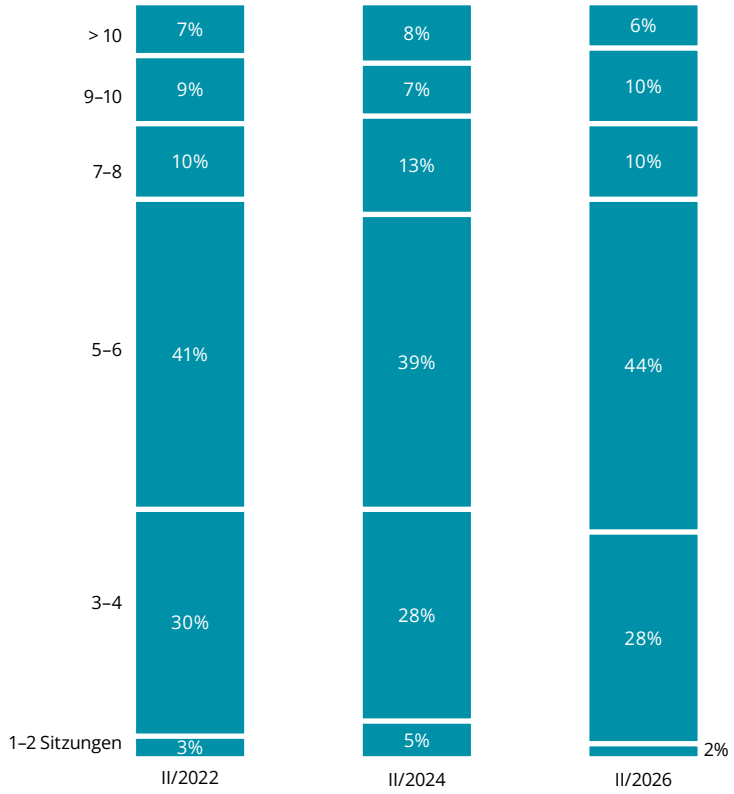
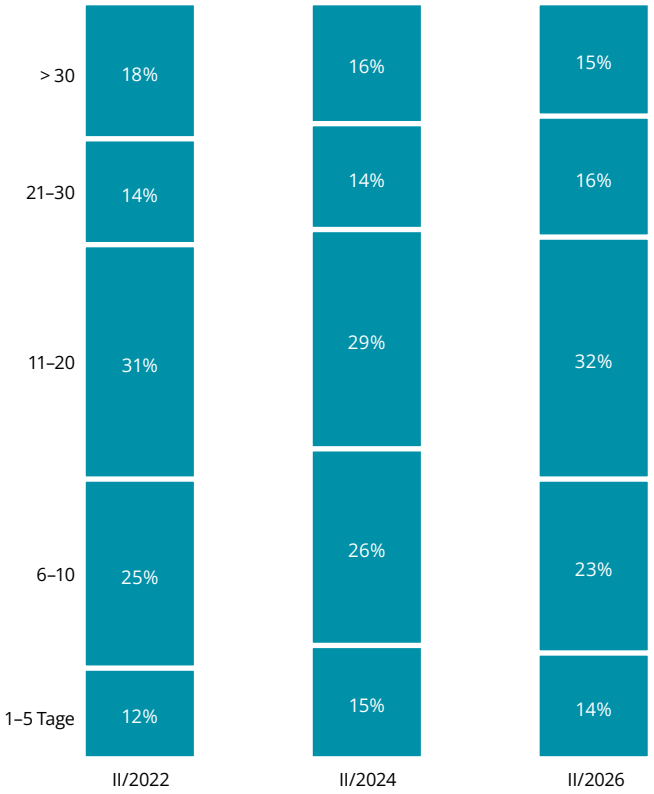



**Abb. 12 Zeitaufwand für VR-Mandat pro Jahr**

*Frage: Wie hoch ist für Sie ungefähr der jährliche zeitliche Aufwand für Ihr VR-Mandat (inkl. Sitzungen, Ausschüssen, Vorbereitungen, Repräsentation, Aus- und Weiterbildung etc.)?*



Vier von fünf Unternehmen (81%) verfügen über eine Organhaftpflichtversicherung für ihre Verwaltungsratsmitglieder und drei Prozent der Befragten haben selbst eine solche Versicherung (siehe Abbildung 13). Jedoch ist zugleich ein Sechstel der Befragten (16%) im Falle einer Verantwortlichkeitsklage nicht durch eine D&O Versicherung geschützt.

In Grossunternehmen verfügen neun von zehn Verwaltungsratsmitgliedern über diesen Schutz (89% über das Unternehmen und 1% persönlich), während er in Kleinunternehmen bei drei Vierteln vorliegt (70% über das Unternehmen und 5% persönlich).

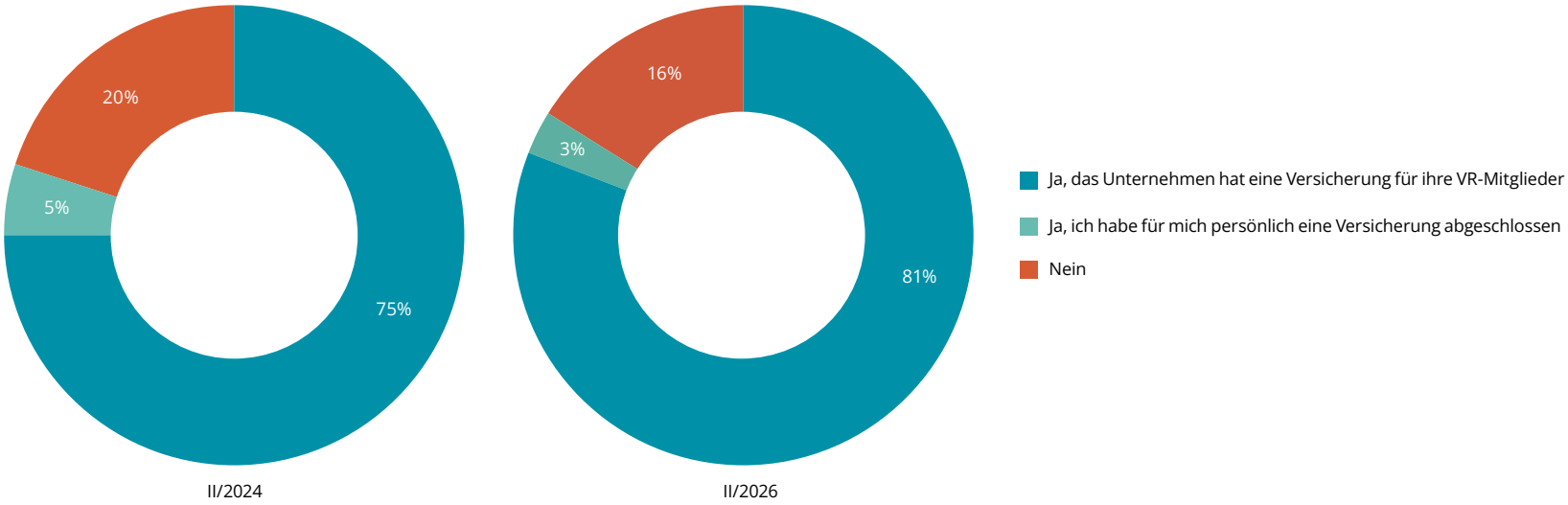
Im Vergleich zur Umfrage im swissVR Monitor II/2024 hat sich das Bild insgesamt leicht verbessert. Dies mag unter anderem dadurch zu erklären sein, dass Verwaltungsratsmitglieder zunehmend eine Organhaftpflichtversicherung von ihren Unternehmen einfordern.

## Wichtige Themen im Fokus des Verwaltungsrats

An erster Stelle der Themen, die Verwaltungsräte in den kommenden 12 Monaten in ihrem Gremium anvisieren möchten, stehen die Effizienzsteigerung und Optimierung interner Prozesse (33%, siehe Abbildung 14). Damit macht dieses Thema im Vergleich zur vorigen Ausgabe drei Ränge gut. Dies hängt – wie in der vorigen Ausgabe ausführlich thematisiert – vermutlich in erster Linie mit der Einführung und Weiterentwicklung der künstlichen Intelligenz in Unternehmen zusammen.

**Abb. 13 Organhaftpflichtversicherung**

*Frage: Haben Sie eine Organhaftpflichtversicherung (D&O Versicherung)?*



Auf Rang zwei und drei der Themenliste folgen das Risikomanagement (29%) sowie die Digitalisierung, Robotik und Automatisierung (28%), die Verwaltungsräte in den kommenden 12 Monaten in ihren Gremien thematisieren möchten. Damit fällt das Risikomanagement um einen Rang und steigen die Digitalisierungsthemen um drei Plätze im Vergleich zur Vorausgabe.

Bemerkenswert ist insbesondere der Aufstieg der IT (19%), des Sicherheitsmanagements inklusive Cyber-Resilienz (18%) und der Go-to-Market-Strategie (18%), welche zuvor allesamt nicht in den Top-10 vertreten waren. Umgekehrt verzeichnet die Erarbeitung einer neuen Unternehmensstrategie den grössten Abstieg in der Rangliste – von Platz zwei auf acht (18%).

**Abb. 14 Top-10-Themen im Fokus des Verwaltungsrates**

*Fragen: Was waren die wichtigsten Themen, mit denen sich Ihr Verwaltungsrat in den letzten 12 Monaten beschäftigt hat? Was werden Ihrer Meinung nach die wichtigsten Themen sein, mit denen sich Ihr Verwaltungsrat in den nächsten 12 Monaten beschäftigen wird?*

| Nächste 12 Monate | | Rang II/2026 | Themen |
|---|---|---|---|
| **1** (33%) | ▲ | **4** (27%) | **Effizienzsteigerung / Optimierung interner Prozesse** |
| **2** (29%) | ▼ | **1** (38%) | **Risikomanagement** |
| **3** (28%) | ▲ | **6** (23%) | **Digitalisierung / Robotik / Automatisierung** |
| **4** (27%) | ▲ | **5** (25%) | **Reaktion auf Marktentwicklung / Wettbewerbsverhalten** |
| **5** (24%) | ▲ | **7** (22%) | **Talent (einschliesslich Recruiting, Retention etc.)** |
| **6** (22%) | ▼ | **3** (28%) | **Personelle Herausforderungen auf Ebene der Geschäftsleitung** |
| **7** (19%) | ▲ | – (15%) | **IT** |
| **8** (18%) | ▲ | – (16%) | **Sicherheitsmanagement, einschliesslich Cyber Resilienz** |
| **8** (18%) | ▲ | – (13%) | **Go to Market (Markt- und Absatzstrategie)** |
| **8** (18%) | ▼ | **2** (36%) | **Erarbeitung einer neuen Unternehmensstrategie** |

«–» bedeutet «nicht in Top-10 vertreten».

# Interviews

## Aktuelle Entwicklungen in der Cyber-Resilienz

**Marc Ruef, Head of Research von scip und Lead Architect von VulDB**

*«Man sollte sich unbedingt die Ruhe und Zeit nehmen, sich für den Krisenfall vorzubereiten. […] Es ist verheerend, sich nicht frühzeitig damit auseinanderzusetzen, denn wenn der Krisenfall eintritt, dann kämpft man je nachdem ums nackte Überleben und hat keine Zeit, besonnen die richtigen Entscheidungen zu treffen, geschweige denn überhaupt etwas zu planen.»*

**swissVR Monitor:** Sie sind ein ausgewiesener Cyber-Experte. Wie hat sich in Ihren Augen die Cyber-Resilienz von Unternehmen in den letzten Jahren entwickelt?

**Marc Ruef:** Die Cyber-Resilienz hat sich grundsätzlich verbessert. Viele Unternehmen verstehen Cybersecurity mittlerweile als wichtigen Bestandteil des Geschäftsrisikos. Mitglieder der Geschäftsleitung beschäftigen sich heute viel mehr mit Risiken und regulatorischen Vorgaben auf digitaler Ebene. Zeitgleich hat jedoch auch eine Professionalisierung der Cyberkriminalität stattgefunden. Ransomware-Gruppen agieren heute wie industrielle Dienstleister mit spezifischen Rollen, Arbeitsteilungen und Geschäftsmodellen. Der Wettlauf besteht also nach wie vor.

**swissVR Monitor:** Gemäss unserer Befragung unter Verwaltungsratsmitgliedern ist mehr als ein Drittel der Unternehmen bis dato einem schadhaften Cyber-Angriff zum Opfer gefallen. Wo sehen Sie Stand heute die grössten Angriffspunkte beziehungsweise Verbesserungspotenziale in Unternehmen?

**Marc Ruef** ist seit Ende der 1990er Jahre im Cybersecurity-Bereich aktiv und hat mit computec.ch das bekannteste deutschsprachige Portal zum Thema Computersicherheit gegründet. Mit 18 Jahren hat er sein erstes Buch herausgegeben. Es folgten unter anderem «Hacking Intern» im Data Becker Verlag und «Die Kunst des Penetration Testing» im C&L Verlag. In den vergangenen 25 Jahren hat er an 16 Büchern mitgewirkt, über 275 Fachartikel in sieben verschiedenen Sprachen publiziert und mehr als 200 Interviews gegeben. Er gilt als einer der meistgelesenen deutschsprachigen Autoren auf seinem Fachgebiet. Zudem ist er Dozent an verschiedenen Universitäten und Fachhochschulen, wie zum Beispiel an der ETH, HWZ, HSLU und IKF. Er ist Mitbegründer der scip AG in Zürich, die seit 2002 Beratungen im Bereich Cybersecurity anbietet. Dort ist er für die Forschungsabteilung zuständig, die in erster Linie unkonventionelle Projekte, wie zum Beispiel Car Hacking oder das Prüfen von Medizinalgeräten, umsetzt.

**Marc Ruef:** Nach wie vor gelten gestohlene Zugangsdaten als das grösste Risiko. Erfolgreiche Angriffe über Phishing, Infostealer und kompromittierte Konten können verheerende Folgen haben. Relativ neu ist das sich festigende Verständnis für die Risiken durch Drittanbieter und Lieferketten. Die zunehmende Vielschichtigkeit moderner Systeme führt Risiken mit sich, die auf den ersten Blick nicht wahrgenommen und deshalb gerne vernachlässigt werden.

**swissVR Monitor:** Vor drei Jahren lag in der gleichen Befragung der Anteil der Unternehmen, die einem Cyber-Angriff zum Opfer gefallen waren, noch bei circa einem Viertel. Wie erklären Sie sich diesen Anstieg vor dem Hintergrund der erhöhten Aufmerksamkeit für Cyber-Angriffe in Unternehmen?

**Marc Ruef:** Diese Zunahme steht nicht im Widerspruch zum verbesserten Verständnis von Cyberrisiken. Grundsätzlich hat aber die Komplexität und damit die Angriffsfläche der Systeme zugenommen. Sie zu schützen, ist also nicht einfacher geworden. Zudem hat sich Cybercrime zu einem Geschäftsmodell entwickelt, das konsequent verfolgt und verfeinert wird. Gegenwärtig sehen wir die ersten, aber sehr konsequenten Effekte von KI im Cybersecurity-Bereich. Sowohl Verteidiger als auch Angreifer profitieren von den neuen Möglichkeiten.

**swissVR Monitor:** Welche Massnahmen sind Ihrer Meinung nach am effektivsten, um Mitarbeitende gegen Cyber-Angriffe vorzubereiten?

**Marc Ruef:** Die erfolgreiche Umsetzung von Cybersecurity beginnt nicht mit der Anschaffung von teurer Technik. Stattdessen diktiert die Sicherheitskultur des Unternehmens die Möglichkeiten und Details in diesem Belang. Das Schulen des Personals ist dabei ein wichtiges Element, um die Angreifbarkeit gering zu halten. Und verschiedene technische Massnahmen, die sich über die Jahrzehnte bewährt haben, können eingesetzt und stetig optimiert werden. Dazu gehören klassische Mechanismen wie Firewalling, Netzwerk-segmentierung, Antivirenlösungen und das Einspielen von Updates.

**swissVR Monitor:** Gemäss unserer aktuellen Befragung ist in mehr als der Hälfte der Unternehmen nicht gesichert, dass die IT-Kernprozesse im Fall eines Cyber-Angriffs wiederhergestellt werden können, ohne inakzeptable Kosten oder Schäden zu verursachen. Wie sollten Pläne für ein solches Szenario konkret aussehen und getestet werden?

**Marc Ruef:** Besonnenheit und Disziplin sind zentrale Voraussetzungen für ein sicheres Unternehmen. Man sollte sich unbedingt die Ruhe und Zeit nehmen, sich für den Krisenfall vorzubereiten. Die Kernprozesse müssen identifiziert, die diese gefährdenden Risiken ausgemacht und Massnahmen zur Eindämmung der Auswirkungen bzw. zur Wiederherstellung ausgearbeitet werden. Es ist verheerend, sich nicht frühzeitig damit auseinanderzusetzen, denn wenn der Krisenfall eintritt, dann kämpft man je nachdem ums nackte Überleben und hat keine Zeit, besonnen die richtigen Entscheidungen zu treffen, geschweige denn überhaupt etwas zu planen.

## Die Rolle des Verwaltungsrats bei der Cyber-Resilienz

**Sandra Emme, Industry Leader Cloud Enterprise von Google und Verwaltungsratsmitglied von Belimo und Zehnder Group International**

*«Vielen Verwaltungsräten ist nicht bewusst, dass sie eine wichtige Rolle haben. […] Die Sicherstellung der Cyber-Resilienz ist keine delegierbare IT-Aufgabe, sondern ein integraler Bestandteil der unentziehbaren Oberleitung des Unternehmens.»*

**swissVR Monitor**: Welche Rolle kommt dem Verwaltungsrat im Allgemeinen zu, wenn es darum geht, die Cyber-Resilienz von Unternehmen sicherzustellen?

**Sandra Emme**: Was mir bei Gesprächen mit Verwaltungsräten oft auffällt: Vielen ist nicht bewusst, dass sie eine wichtige Rolle haben. Da hole ich gerne ein bisschen aus. Die Sicherstellung der Cyber-Resilienz ist keine delegierbare IT-Aufgabe, sondern ein integraler Bestandteil der unentziehbaren Oberleitung des Unternehmens gemäss Art. 716a des Schweizerischen Obligationenrechts.

Der Verwaltungsrat muss Cyber-Risiken, genau wie finanzielle oder operative Risiken, als strategische Geschäftsrisiken behandeln und sie strukturiert in das unternehmensweite Risikomanagement einbinden. Seine Kernaufgabe liegt in der strategischen Steuerung: Er definiert die Risikotoleranz, stellt adäquate finanzielle Mittel bereit und sorgt für eine klare Governance.

Auch muss sich der VR regelmässig über die Bedrohungslage berichten lassen, Sicherheitskennzahlen einfordern und die Wirksamkeit der Notfallpläne überprüfen. Es ist ratsam, diesen Prozess zu dokumentieren, um treuhänderische Verantwortung, Sorgfalt und Kontinuität zu belegen. Wenn es zu einem Vorfall kommt, sind gesetzliche Meldepflichten einzuhalten, die der VR im Rahmen seiner Oberaufsicht überwachen muss.

**Sandra Emme** begann ihre unternehmerische Karriere in Frankreich als Mitgründerin mehrerer IT-Start-ups, die global expandierten und später erfolgreich verkauft wurden. Seit fünfzehn Jahren ist sie bei Google tätig, aktuell als Industry Leader, wo sie Industriefirmen in ihrer Transformations-, Cyber- und Datenstrategie berät. 2018 wurde sie Mitglied des Verwaltungsrats der Panalpina Welttransport Holding AG und 2019 der Metall Zug AG. Aktuell hat sie Verwaltungsratsmandate inne bei der Belimo Holding AG (seit 2018) und der Zehnder Group AG (seit 2022). Sie ist Mitglied im Vorstand von digitalswitzerland, Dozentin für Digital Business Transformation an der IMD und zertifiziert in Corporate Governance (HSG) sowie ESG (Competent Boards).

**swissVR Monitor:** Gemäss unserer Befragung unter Verwaltungsratsmitgliedern probt nur etwa die Hälfte der VR-Gremien das Krisenmanagement für den Fall eines Cyber-Angriffs. Welche konkreten Risiken ergeben sich für die andere Hälfte der Verwaltungsräte?

**Sandra Emme**: Vernachlässigt ein VR das Thema Cyber-Resilienz grundlegend, verletzt er seine gesetzliche Sorgfaltspflicht. Kommt es zu einem schweren Cyberangriff mit massiven finanziellen Schäden, droht dem VR persönliche zivilrechtliche Haftung mit dem Privatvermögen sowie strafrechtliche Konsequenzen, falls gesetzliche Meldepflichten missachtet wurden.

Übrigens: Krisenübungen für den VR dienen ausdrücklich nicht dazu, dass das Gremium im Ernstfall operativ eingreift – das wäre kontraproduktiv und würde den Krisenstab der Geschäftsleitung behin-

dern. Vielmehr geht es darum, zu prüfen, ob die Organisation vorbereitet ist und ob die Informationsflüsse zum VR funktionieren. Wer dies nicht probt, riskiert im Ernstfall strategische Fehlentscheide und massive Zeitverluste.

Die konkreten Risiken umfassen erstens die rechtliche Haftung: Der VR haftet nicht für den Angriff selbst, sondern für mangelhafte Vorbereitung oder strategische Fehler während der Krise, wie etwa die Verletzung von Ad-hoc-Publizitätspflichten oder Datenschutzmeldungen. In solchen Fällen können auch Cyber- und Organhaftpflichtversicherungen (D&O) die Deckung verweigern.

Das zweite Risiko besteht in der Handlungsunfähigkeit im Ernstfall: Ohne Übung weiss der VR nicht, welche strategischen Entscheide er unter enormem Zeitdruck treffen muss (z.B. Freigabe von Sondermitteln, Information von Grossaktionären oder Regulatoren). Als drittes Risiko ist das Lösegeld-Dilemma zu nennen: Ohne Vorab-Diskussion weiss der VR im Moment des Angriffs nicht, ob und wie er auf Lösegeldforderungen eingeht, und hält nicht die dafür notwendigen Mittel bereit.

Das vierte Risiko besteht in Reputations- und Finanzschäden: Ein Cybervorfall führt fast immer zu einem Reputationsschaden – auch bei gutem Krisenmanagement. Ist der VR jedoch unvorbereitet und die Kommunikation unkoordiniert, potenziert sich dieser Schaden massiv und kann insbesondere für KMU existenzbedrohend werden.

Mein Rat: Führen Sie Tabletop-Exercises durch und stellen Sie sicher, dass die Geschäftsleitung einen Incident-Response-Retainer abgeschlossen hat – einen Bereitschaftsvertrag mit externen Experten für sofortige Hilfe. Ein solcher Vertrag wird von Cyber-Versicherungen oft positiv gewertet oder gar vorausgesetzt.

**swissVR Monitor:** Ebenfalls lediglich etwa die Hälfte der Verwaltungsräte erhält von der Geschäftsleitung ein Reporting über Cyber-Vorfälle im Unternehmen. Abgesehen von solchen Vorfällen, über welche Aspekte sollte der Verwaltungsrat ein regelmässiges Cyber-Reporting von der Geschäftsleitung erhalten?

**Sandra Emme:** Ein Reporting, das zum Beispiel nur vergangene Vorfälle auflistet, verfehlt die strategische Flughöhe des VR. Der Fokus muss auf der Risikosteuerung liegen. Der VR muss zu konkreten und fundierten Investitionsentscheidungen kommen. Am besten durch die Quantifizierung von Cyber-Risiken in Schweizer Franken: Was sind wir bereit zu riskieren?

Ein zukunftsgerichtetes Reporting sollte folgende Dimensionen abdecken: Erstens die Top Cyber-Risiken & Mitigation, sprich die Antwort auf die Fragen: Was sind aktuell die grössten Bedrohungen für das Geschäftsmodell und welche Massnahmen ergreift die Geschäftsleitung zur Risikominderung?

In der zweiten Dimension geht es um den Schutz der «Kronjuwelen»: Wie gut sind unsere geschäftskritischsten Systeme und wertvollsten Daten geschützt? Sicherheitskopien müssen zum Beispiel zwingend vom Hauptnetzwerk getrennt sein – und damit vor externer Verschlüsselung geschützt werden.

Die dritte Dimension betrifft die Reaktionsfähigkeit (Resilienz) beziehungsweise Metriken zur mittleren Erkennungszeit – das heisst: Wie lange dauert es intern, bis man merkt, dass das firmeneigene Netzwerk angegriffen wurde? Wie lange braucht es, bis man darauf reagiert hat? Und: Ein externer Hersteller von Software kommuniziert eine Sicherheitslücke – wie lange dauert es, bis das interne Team die kritische Schwachstelle behoben hat?

Die vierte Dimension adressiert Supply Chain & Drittparteien, sprich die Bewertung der Cyber-Risiken entlang der Lieferkette – oft ein grosses Einfallstor. Als fünfte Dimension sind Mensch- & KI-Risiken zu nennen: Resultate von Schulungen sowie die strategische Bewertung der Sicherheit von genutzten KI-Tools.

Die sechste und letzte Dimension umfasst eine unabhängige Aussensicht beziehungsweise Ergebnisse von unabhängigen Cyber-Audits, Penetrationstests oder Reifegrad-Messungen sowie Security-Scores, um ein objektives Benchmark zu erhalten.

**swissVR Monitor:** Die grosse Mehrheit der Verwaltungsräte verfügt nicht über Mitglieder mit Cyber-Expertise. In welchen Fällen sollte ein VR-Gremium eine Person mit Cyber- beziehungsweise IT-Expertise rekrutieren?

**Sandra Emme:** Nicht jeder VR muss ein IT-Experte sein, aber «Tech-Blindheit» im Gesamtgremium birgt enorme strategische Risiken. Eine gezielte Rekrutierung ist insbesondere dann ratsam, wenn, die «Enabling-Lücke» wächst. Der VR benötigt ein Mitglied, das als «Übersetzer» fungiert, um die IT-Aussagen der Geschäftsleitung kritisch zu hinterfragen.

Ein weiterer Grund für eine gezielte Rekrutierung sind tiefgreifende Transformationen: Etwa bei der weltweiten Migration auf neue ERP-Systeme, einer Cloud-First-Strategie oder wenn KI das Kern-Geschäftsmodell disruptiert. Ein VR-Mitglied mit entsprechender Expertise ist ebenfalls unabdingbar, wenn Aufholbedarf im Cyber-Reifegrad besteht. Wenn Cyber-Audits Lücken aufzeigen, dürfen VRs nicht warten, bis das Unternehmen Opfer eines grossen Angriffs wird und Aktionäre personelle Konsequenzen und den Aufbau von Know-How im Gremium einfordern.

Eine gezielte Rekrutierung empfiehlt sich auch im Fall von kotierten Unternehmen, da Investoren und Stimmrechtsberater zunehmend aktiv digitale Kompetenz im VR fordern. Mindestens ein Mitglied sollte ausgewiesene Technologie- und Cyber-Erfahrung mitbringen.

Bei mittelgrossen Unternehmen ist ein Vollzeit-IT-Experte im VR oft schwerer zu finden oder bindet einen von wenigen VR-Sitzen zu spezifisch. Es empfiehlt sich, einen externen Beirat zu bilden oder einen externen CISO als Gastreferenten einzuladen, um die Cyber-Reportings unabhängig zu spiegeln.

**swissVR Monitor:** In welchen Fällen ist es sinnvoll, dass ein Verwaltungsrat einen Cyber- beziehungsweise Informatikausschuss bildet?

**Sandra Emme:** Grundsätzlich entwickelt sich ein solcher Ausschuss zunehmend zur branchenübergreifen- den Best Practice. Zwingend wird die Bildung eines dedizierten IT- oder Cyber-Ausschusses jedoch dann, wenn die Komplexität der IT-Landschaft so hoch ist, dass der Gesamt-VR oder das klassische Audit-Committee nicht die nötige Zeit für ein tiefgehendes Verständnis aufbringen kann. Dies gilt insbesondere im Fall einer OT/IT-Konvergenz. Wenn in produzierenden Unternehmen Produktionsanlagen (Operational Technology) und klassische IT verschmelzen, entstehen hochkomplexe, neue Angriffsvektoren in der Fabrikautomation.

Andere Gründe für einen solchen Ausschuss bestehen, wenn das Unternehmen massive IT-Schulden abbauen muss, stark in KI investiert oder komplexe IT-Integrationen nach Zukäufen bewältigen muss.

Auch für Deep Dives bietet sich ein dedizierter IT- oder Cyber-Ausschuss an: für die Vertiefung von Themen, die besondere strategische Relevanz für ein Unternehmen haben, z.B. SOC-Strategien (Security Operations Center), Schutz der Lieferkette, Cybersecurity- oder KI/IoT-Entwicklungen im Rahmen der Innovationsstrategie.

Noch ein Grund für einen solchen Ausschuss kann regulatorischer Druck sein. Für kotierte oder stark regulierte Unternehmen ist ein «Technology & Cyber Committee» essenziell, um Architekturfragen, grosse IT-Budgets und Security-Audits im «Deep Dive» zu prüfen und dem Gesamt-VR fundierte Empfehlungen abzugeben.

## Die Bedeutung von künstlicher Intelligenz bei Cyber-Angriffen

**Frank Desiere, CEO und Verwaltungsratsmitglied von CorTec**

*«Erhebungen – auch der swissVR Monitor – deuten darauf hin, dass ein erheblicher Teil der Verwaltungsräte kein regelmässiges Reporting zu KI-Einsatz und -Risiken erhält. Ohne dieses Reporting ist Aufsicht schlicht nicht möglich.»*

**swissVR Monitor**: Wie in anderen Anwendungsbereichen wird die künstliche Intelligenz (KI) auch zunehmend für Cyber-Angriffe eingesetzt. Wie hat KI die Qualität und Quantität von Cyber-Angriffen in den letzten Jahren verändert?

**Frank Desiere**: Ich beschreibe es als eine Verschiebung der Ökonomie des Angriffs. Auf der Mengenseite senkt KI die Grenzkosten eines Angriffs gegen null: Aufklärung, Zielrecherche und die Erstellung überzeugender Inhalte lassen sich automatisieren und beliebig skalieren. Was früher ein spezialisiertes Team erforderte, steht heute auch weniger versierten Akteuren zur Verfügung.

Auf der Qualitätsseite ist der Sprung womöglich gravierender. Der IBM «Cost of a Data Breach Report 2025» beziffert, dass bereits rund 16 Prozent der untersuchten Datenschutzverletzungen KI auf der Angreiferseite involvierten – überwiegend KI-generiertes Phishing und Deepfake-Impersonation. Angriffsnachrichten sind nicht mehr an Sprachfehlern erkennbar, sondern individualisiert und kontextgenau; Deepfakes in Stimme und Video machen den klassischen CEO-Fraud überzeugend.

Für den Verwaltungsrat ist die entscheidende Grösse die verkürzte Zeitachse zwischen bekannt gewordener Schwachstelle und ihrer Ausnutzung. Das verschiebt die Verteidigung von «den Perimeter halten» hin zu «schnell erkennen und eindämmen». Cyber ist damit keine reine IT-Frage mehr, sondern eine Resilienzfrage – und die gehört auf die Traktandenliste des Gremiums.

**Dr. Frank Desiere** ist CEO der CorTec und als Non-Executive Director (Verwaltungsrat) tätig. Diese Doppelrolle prägt seinen Blick auf Governance: Er kennt die operative Führungsverantwortung ebenso wie die Aufsichts- und Kontrollaufgabe des Verwaltungsrats – und damit die Nahtstelle, an der wirksame Unternehmensführung entsteht. Mit WE TALK BOARD, seinem Newsletter und Podcast, wendet er sich an Verwaltungsrätinnen und Verwaltungsräte, Präsidien, Führungskräfte und angehende Board-Mitglieder. Im Mittelpunkt stehen Board-Effektivität, verantwortungsvolle Unternehmensführung und die Weiterbildung von Non-Executive Directors – konsequent aus schweizerischer und europäischer Perspektive. Neben seiner Führungs- und Aufsichtstätigkeit hält Dr. Desiere Keynotes und leitet Executive-Sessions zu Governance-Themen, unter anderem im Rahmen des Deloitte Board Program. Sein Anliegen ist praxisnahe, fundierte Orientierung für alle, die im Verwaltungsrat Verantwortung tragen.

**swissVR Monitor:** Wir sind heute beim Übergang vom Zeitalter der Agentic KI zur Multi-Agent-KI. Was bedeutet dieser technologische Fortschritt für die Gefahr von Cyber-Angriffen in der Zukunft?

**Frank Desiere**: Der Unterschied ist qualitativ, nicht graduell. Generative KI hat den Angreifern bessere Werkzeuge gegeben, den Menschen aber im Steuerungskreis belassen. Agentische KI verschiebt genau diese Grenze: Der Agent plant, handelt, beobachtet und passt sich an – weitgehend ohne menschliches Zutun.

Wie real das ist, hat Anthropic im November 2025 offengelegt: die erste dokumentierte, weitgehend KI-orchestrierte Spionagekampagne, nach Einschätzung des Unternehmens durch einen staatsnahen Akteur, bei der die KI rund 80 bis 90 Prozent der operativen Schritte selbst ausführte und Menschen nur an wenigen Entscheidungspunkten eingriffen. Rund 30 Ziele weltweit, ausgeführt in Maschinengeschwindigkeit statt in Handarbeit.

Multi-Agenten-Systeme heben das auf die nächste Stufe: spezialisierte Agenten, die eine Angriffskette arbeitsteilig durchführen und in Echtzeit auf die Abwehr reagieren. Wir bewegen uns auf eine «Maschine-gegen-Maschine»-Dynamik zu, in der rein menschlich getaktete Verteidigung strukturell zu langsam ist.

Die Konsequenz für den Verwaltungsrat: Die Abwehr muss ihrerseits automatisiert werden – und die von uns selbst eingesetzten Agenten, mit ihren Berechtigungen, ihrem Speicher und ihren Werkzeugzugriffen, werden zum eigenständigen Angriffsziel. Das ist die Kehrseite jeder KI-Effizienzinitiative, die das Gremium bewilligt.

**swissVR** Monitor: Unsere Befragung unter Verwaltungsratsmitgliedern zeigt, dass lediglich eine kleine Minderheit von Unternehmen über eine konkrete Strategie gegen KI-basierte Cyber-Angriffe verfügt. Wie schätzen Sie das Risiko für Firmen ein, die Cyber-Angriffe durch die KI noch nicht speziell berücksichtigen?

**Frank Desiere:** Erheblich – aber ich präzisiere, wo das Risiko wirklich liegt, denn es sind zwei Lücken. Die erste: Wer KI-gestützte Angriffe nicht berücksichtigt, verteidigt ein neues Bedrohungsmodell mit Instrumenten von gestern. Signaturbasierte Erkennung greift bei adaptiver Schadsoftware ins Leere, und die Angreiferseite hat ihre Methoden bereits industrialisiert.

Die zweite Lücke ist hausgemacht und wird unterschätzt: der ungesteuerte eigene KI-Einsatz. Der IBM-Report 2025 zeigt, dass rund jede fünfte Datenschutzverletzung mit «Schatten-KI» zusammenhing und solche Vorfälle im Schnitt etwa 670 000 US-Dollar teurer waren; 63 Prozent der betroffenen Unternehmen hatten überhaupt keine KI-Governance-Richtlinie. Das Risiko entsteht hier nicht durch einen Angreifer, sondern durch Mitarbeitende, die Kundendaten oder geistiges Eigentum in externe Modelle geben.

Ich warne zugleich vor Aktionismus. Nicht jedes Unternehmen braucht eine separate «KI-Cyber-Strategie» als eigenständiges Dokument. Entscheidend ist die Integration in das bestehende Risikoframework und die Führung von Cyber als Unternehmens-, nicht als IT-Thema – orientiert an anerkannten Standards wie NIST CSF 2.0 oder ISO 27001. Gerade KMU sind exponiert: mit knapperen Ressourcen, zunehmend aber auch als Ziel über Lieferketten, etwa im Sog der europäischen NIS2-Regulierung. Wer hier abwartet, riskiert, zum Anschauungsbeispiel des nächsten Vorfalls zu werden.

**swissVR** Monitor: Welche konkreten Massnahmen sollten Unternehmen ergreifen, um sich gegen KI-basierte Cyber-Angriffe zu schützen?

**Frank Desiere:** Ich sehe fünf Prioritäten, bewusst in dieser Reihenfolge. Erstens: KI mit KI begegnen. Verhaltens- und anomaliebasierte Erkennung sowie automatisierte Reaktion sind nötig, um überhaupt auf Maschinengeschwindigkeit antworten zu können – laut IBM sparen Organisationen, die KI und Automatisierung breit in der Abwehr einsetzen, im Schnitt rund 1,9 Millionen US-Dollar pro Vorfall und begrenzen Angriffe deutlich schneller.

Zweitens: Zero-Trust mit striktem Identitäts- und Berechtigungsmanagement – ausdrücklich auch für maschinelle Identitäten und KI-Agenten, die zunehmend eigene Zugriffsrechte erhalten. Drittens: Phishing-resistente Authentifizierung, etwa Passkeys, kombiniert mit einem verbindlichen Vier-Augen- und Rückrufprinzip bei Zahlungen und Berechtigungsänderungen. Gegen Deepfake-gestützten CEO-Fraud hilft kein Bauchgefühl, sondern ein Prozess.

Viertens – und oft unterschätzt: der Mensch. Sensibilisierung muss neu kalibriert werden; die Faustregel «auf Tippfehler achten» trägt nicht mehr, wenn Nachrichten sprachlich perfekt sind. Fünftens: Die Grundhygiene bleibt entscheidend – Patch-Management, unveränderliche Backups, Netzsegmentierung und ein regelmässig geübter, nicht nur dokumentierter Incident-Response-Plan.

Zwei Ergänzungen, die auf Geschäftsführungsebene gehören: die Absicherung der Lieferkette und die Governance der eigenen KI-Anwendungen gegen Datenabfluss und Prompt-Injection. Wichtig ist die Reihenfolge – erst das Fundament, dann die Kür. Und der Verwaltungsrat sollte sich zu jedem dieser Punkte den Reifegrad berichten lassen, nicht die blosse Aktivität.

**swissVR Monitor:** Welche Rolle spielt der Verwaltungsrat, um sicherzustellen, dass ein Unternehmen stets auf dem neusten Stand der technologischen Entwicklung beziehungsweise auf die daraus resultierenden Gefahren wie zum Beispiel KI-basierten Cyber-Angriffen vorbereitet ist?

**Frank Desiere:** Cyber- und KI-Risiken sind Sache des Verwaltungsrats – rechtlich wie faktisch. Sie berühren die unübertragbare Oberleitung und die Sorgfaltspflicht nach Art. 716a und 717 OR. Die operative Umsetzung lässt sich an Geschäftsleitung oder CISO delegieren, die Aufsicht nicht; bei einer Pflichtverletzung haftet der Verwaltungsrat persönlich nach Art. 754 OR. Eine D&O-Deckung ersetzt diese Sorgfalt nicht, sie setzt sie voraus.

Der Verwaltungsrat muss dabei nicht die tiefste technische Expertise besitzen, aber genug, um die richtigen Fragen zu stellen und die Geschäftsleitung fundiert zu fordern – und er muss sicherstellen, dass die nötige Kompetenz im Gremium oder über Berater vorhanden ist. Konkret heisst das: klare Zuständigkeit in einem Risiko- oder Prüfungsausschuss; regelmässiges, strukturiertes Reporting statt Berichterstattung erst nach dem Vorfall; ein geübter Krisenplan, in dem auch die Rolle des Gremiums geklärt ist; Ressourcen, die dem Risikoappetit entsprechen; und ein wacher Blick auf den regulatorischen Horizont – revidiertes DSG, NIS2-Ausstrahlung, EU AI Act.

Hier liegt die eigentliche Schwachstelle. Erhebungen – auch der swissVR Monitor – deuten darauf hin, dass ein erheblicher Teil der Verwaltungsräte kein regelmässiges Reporting zu KI-Einsatz und -Risiken erhält. Ohne dieses Reporting ist Aufsicht schlicht nicht möglich.

Mein Grundsatz, als CEO wie als Verwaltungsrat: Unsere Aufgabe ist nicht, Sicherheit selbst zu betreiben, sondern dafür zu sorgen, dass die richtigen Fragen beharrlich gestellt werden und das Unternehmen Cyber als lebendige Resilienz- und nicht als abgeschlossene IT-Frage behandelt. Genau solche Governance-Fragen vertiefe ich regelmässig in meinem LinkedIn-Newsletter «WE TALK BOARD».

# Autoren


## swissVR

**Isabelle Amschwand**
Präsidentin swissVR
+41 41 757 67 11
isabelle.amschwand@swissvr.ch

**Dr. Brigitte Maranghino-Singer**
Geschäftsführerin swissVR
und Dozentin, Institut für
Finanzdienstleistungen Zug IFZ,
HSLU
+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

**Prof. Dr. Mirjam Gruber-Durrer**
Dozentin für Normatives
Board Management, Institut
für Finanzdienstleistungen Zug IFZ,
HSLU
+41 41 228 41 73
mirjam.gruber-durrer@hslu.ch




**swissVR** engagiert sich für die Kompetenz, 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 rund 1'400 Mitgliedern ein bedürfnisspezifisches Informations- und Weiterbildungsangebot. swissVR richtet sich exklusiv an Personen mit einem aktiven Verwaltungsratsmandat. Weitere Informationen finden Sie unter www.swissvr.ch.



Die **Hochschule Luzern** ist die Fachhochschule der sechs Zentralschweizer Kantone und vereinigt die Departemente Technik & Architektur, Wirtschaft, Informatik, Soziale Arbeit, Design Film Kunst, Musik sowie den Schwerpunkt Gesundheit. Mit rund 8'700 Studierenden und rund 13'000 Weiterbildungsteilnehmenden (davon 5'600 MAS, DAS, CAS), 274 neuen Forschungsprojekten und 2'144 Mitarbeitenden ist sie die grösste Bildungsinstitution im Herzen der Schweiz. Das Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern 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.lten.