Wenn die Lichter ausgehen

Warum der Schutz kritischer Infrastruktur und der Umgang mit unberechenbaren Schocks die Verantwortung jedes Verwaltungsrats ist.

Am Nachmittag des 28. April 2025 verlor Spanien innerhalb weniger Sekunden rund 15 Gigawatt Leistung. Dies sind etwa 60 Prozent der üblichen Nachfrage zu diesem Zeitpunkt. Der Ausfall riss Portugal und Teile Südfrankreichs mit: Züge blieben stehen, Zahlungssysteme fielen aus, Millionen Menschen sassen im Dunkeln. Der erste Reflex vieler Beobachter lautete: Cyberangriff. Diese Vermutung erwies sich als falsch. Der Untersuchungsbericht der europäischen Netzbetreiber führte den Zusammenbruch auf ein Zusammenspiel technischer Faktoren zurück: Lücken in der Spannungsregelung, Oszillationen im Netz und kaskadierende Abschaltungen, die sich in Sekundenbruchteilen ausbreiteten.



Für einen Verwaltungsrat steckt darin die unbequeme Erkenntnis, dass Resilienz mehr als die Bewältigung einzelner Risiken ist. Sie beschreibt die Fähigkeit eines Unternehmens, kritische Leistungen auch bei aussergewöhnlichen Störungen aufrechtzuerhalten und rasch zum Normalbetrieb zurückzukehren. Die Ursachen sind dabei nicht entscheidend. Entscheidend hingegen ist, kritische Abhängigkeiten entlang der gesamten Wertschöpfungskette zu kennen, zu steuern und regelmässig auf ihre Widerstandsfähigkeit zu prüfen. Resilienz ist damit eine strategische Führungsaufgabe und zentraler Bestandteil wirksamer Governance.

Schocks lassen sich nicht vorhersagen

Blickt man auf die vergangenen fünf Jahre, reiht sich ein Schock an den nächsten: die Pandemie, die drohende Strommangellage in der Schweiz, der globale Halbleiterengpass, der iberische Blackout oder der extrem heisse und trockene Sommer 2026. Kaum einer davon war in seiner konkreten Form vorhergesagt worden. Genau das ist der Punkt: Ein Verwaltungsrat kann nicht wissen, welcher Schock als Nächstes kommt. Er kann aber die Fähigkeit aufbauen, ihn zu absorbieren.







Die Schweizer Strommangellage der Jahre 2021 und 2022 zeigt das exemplarisch. Als infolge des Kriegs in der Ukraine, ausgefallener französischer Kernkraftwerke und niedriger Füllstände der Speicherseen eine Strommangellage im Winter 2022/23 drohte, aktivierte der Bund seine Notfallplanung. Vorgesehen war eine vierstufige Eskalation: von Spar-Appellen über Verbote einzelner Anwendungen bis zur Kontingentierung der Grossverbraucher. Unternehmen mit mehr als 100 Megawattstunden Jahresverbrauch hätten ihren Bezug um einen festgelegten Prozentsatz drosseln müssen und als letzte Massnahme, rollenden Netzabschaltungen. Unternehmen mussten sich registrieren, ihren Verbrauch modellieren und die Geschäftskontinuität für ein Szenario vorbereiten, das Produktion, Zahlungsverkehr und Alltagsbetrieb getroffen hätte.

Ein milder Winter bewahrte die Schweiz schliesslich vor dem Ernstfall. Doch die Episode war eine Frage der nationalen Sicherheit: Ein wohlhabendes, stabiles Land mit starker Infrastruktur war plötzlich einem Versorgungsrisiko ausgesetzt, das es, abhängig von Importen und einem europäischen Markt unter Druck, nicht allein steuern konnte. Die Verwundbarkeit war da, auch wenn der Schaden ausblieb.

Resilienz: Vom Maschinenraum in den Sitzungssaal

Drei Entwicklungen haben das Thema auf der Agenda des Verwaltungsrats platziert: Erstens erweitert sich der Kreis dessen, was als «kritisch» gilt. Die Schweizer Gesetzgebung definiert kritische Infrastrukturen bewusst funktional als Organisationen, deren Ausfall schwerwiegende Folgen für Wirtschaft oder Bevölkerung hätte. Für die Praxis heisst das: Der kritische Perimeter eines Unternehmens ist fast immer breiter, als der Verwaltungsrat annimmt. Er umfasst nicht nur die eigenen Anlagen, sondern Steuerungstechnik, IT-Dienstleister, Cloud-Plattformen und ganze Lieferketten und somit auch Dritte, deren Ausfall unmittelbar durchschlägt. Zweitens verstärken sich die Risiken gegenseitig. Drittens macht neue Regulierung die Aufsicht persönlich zurechenbar.

«Ein Verwaltungsrat kann nicht wissen, welcher Schock als Nächstes kommt. Er kann aber die Fähigkeit aufbauen, ihn zu absorbieren.»

Ein vernetztes Risiko-Universum

Die wichtigste Botschaft für einen Verwaltungsrat: Die relevanten Risiken treten nicht mehr isoliert auf, sondern greifen ineinander.

Cyber. Stromnetze und andere kritische Systeme gelten als hochattraktive Ziele für kriminelle wie für staatlich unterstützte Akteure. Die grüne und digitale Transformation erhöht durch vernetzte Anlagen, Cloud-Anbindungen sowie die zunehmende Konvergenz von Information Technology (IT)/Operational Technology (OT) die Angriffsfläche. Gleichzeitig erschweren jahrzehntealte Systeme und hohe Verfügbarkeitsanforderungen die Umsetzung von Sicherheitsmassnahmen. OT-Sicherheit wird damit zu einem zentralen Element der operativen Resilienz und Versorgungssicherheit.

Klima und physische Ereignisse. Extremwetter trifft längst nicht mehr nur die Energieinfrastruktur, sondern ganze Wertschöpfungsketten. Als im Sommer 2024 die Rhone nach aussergewöhnlichen Niederschlägen über die Ufer trat, standen die Walliser Aluminiumwerke von Novelis und Constellium in Siders unter Wasser und mussten die Produktion über Monate einstellen. Weil Novelis europäische Automobilhersteller mit Aluminiumblechen beliefert, rechneten Konzerne wie Jaguar Land Rover und Porsche mit spürbaren Produktionsausfällen. Ein einziges, lokal begrenztes Klimaereignis pflanzte sich durch die Lieferkette einer ganzen Branche fort.

Technisch-systemische Instabilität. Mit dem Umbau zu einem erneuerbaren, dezentralen System sinkt die physikalische Trägheit im Netz; kleine Anfangsstörungen können sich, wie auf der iberischen Halbinsel, über Kaskaden aufschaukeln.

Sektorübergreifende Abhängigkeiten. Strom, Telekom, Wasser, Zahlungsverkehr und Gesundheit hängen zusammen. Während des iberischen Blackouts arbeiteten portugiesische Spitäler stundenlang auf Notstrom, digitale Patientendossiers waren nicht abrufbar. Es gab einen Dominoeffekt über Branchengrenzen hinweg. Eine Strommangellage und die Reservierung von Wasserkraftkapazitäten können sich auf diverse andere Sektoren auswirken, so auch in überraschenden Industrien, etwa der Tourismusbranche, mangels Beschneiungskapazitäten in tieferen Lagen.

Geopolitik und Lieferkette. Wie kritisch eine einzige Abhängigkeit sein kann, zeigte der globale Halbleiterengpass von 2021 und 2022: Ganze Produktionsbänder der Automobil- und Maschinenindustrie, beide zentral für die Schweizer Exportwirtschaft, standen still, weil Bauteile im Wert weniger Franken fehlten. Die Fertigung modernster Chips ist auf wenige Unternehmen und Standorte konzentriert; aus einer technischen Abhängigkeit wird so ein geopolitisches Risiko. Sabotage an Kabeln und Pipelines sowie Exportkontrollen wirken in dieselbe Richtung.

Diese Risiken sind nicht additiv, sondern multiplikativ: ein Cybervorfall während einer Hitzewelle, eine Lieferkettenstörung mitten in einer geopolitischen Krise. Wer sie in getrennten Silos betrachtet, Cyber bei der IT, Klima bei der Nachhaltigkeit, Lieferkette beim Einkauf, unterschätzt das Gesamtbild systematisch.

Der Verwaltungsrat ist bereits in der Pflicht

Parallel zur Risikolage hat sich das regulatorische Umfeld verschärft. Im Cyberbereich reicht ein Blick auf die jüngsten Entwicklungen: In der Schweiz gilt seit 2025 eine Meldepflicht für erhebliche Cyberangriffe gegen kritische Infrastrukturen an das Bundesamt für Cybersicherheit (BACS), inzwischen sanktionsbewehrt; in der EU heben Network and Information Security 2 (NIS2) und die CER-Richtlinie die Anforderungen deutlich an und nehmen die Leitungsorgane ausdrücklich in die Verantwortung. Schweizer Unternehmen sind rechtlich nicht an das EU-Regime gebunden, über Netze, Kunden und Lieferketten aber eng damit verflochten. Die Orientierung am strengeren Standard ist damit eine strategische, keine juristische Entscheidung.

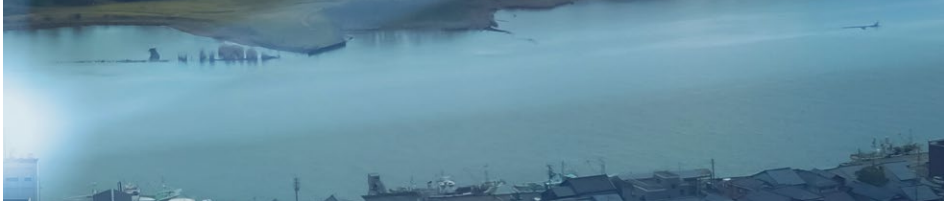
Oft weniger beachtet, aber für den Verwaltungsrat genauso relevant sind die Klima- und Sorgfaltspflichten. Seit dem 1. Januar 2024 ist in der Schweiz die Verordnung zur Klimaberichterstattung in Kraft. Grosse Publikumsgesellschaften, Banken und Versicherer müssen ihre Klimarisiken und -chancen nach den TCFD-Kategorien (Governance, Strategie, Risikomanagement, Kennzahlen und Ziele) offenlegen, inklusive Transitionsplan und Emissionen entlang der gesamten Wertschöpfungskette. Erstmals berichtet wurde über das Geschäftsjahr 2024. Entscheidend für die Governance: Der Bericht über nichtfinanzielle Belange bedarf der Genehmigung und Unterzeichnung durch das oberste Leitungsorgan. Der Verwaltungsrat trägt damit das Risiko einer unvollständigen oder unzutreffenden Berichterstattung.

Diese Pflicht steht nicht allein. Das Schweizer Aktienrecht weist dem Verwaltungsrat unübertragbare Kernaufgaben wie die Oberleitung, Organisation und Überwachung einschliesslich eines wirksamen Risikomanagements zu. Hinzu kommen Sorgfaltspflichten in der Lieferkette. Es entsteht ein Geflecht von Anforderungen (Cyber-Meldung, Klimaoffenlegung, Risikoaufsicht), das an einem Punkt zusammenläuft: Der Verwaltungsrat ist für die Resilienz seines Unternehmens verantwortlich.









Was das für den Verwaltungsrat bedeutet

Resilienz wird damit, unabhängig von der Branche, zu einer Kernaufgabe der Aufsicht. Ob Energieversorger, Bank, Industrieunternehmen, Spital oder Detailhändler: Die Mechanik ist überall dieselbe. Fünf Fragen helfen einem Verwaltungsrat, seinen Reifegrad ehrlich einzuschätzen.

Fünf Fragen für jeden Verwaltungsrat

1. Kennen wir unseren tatsächlichen kritischen Perimeter inklusive der Abhängigkeit von Dritten, Cloudanbietern und Lieferanten?
2. Denken wir Resilienz ganzheitlich, über technologische, physische, klimatische, geopolitische, wirtschaftliche und lieferkettenbezogene Risiken hinweg?
3. Haben wir definiert, was unsere «Minimum Viable Company» ausmacht und welche Ressourcen, Prozesse, Technologien und Drittparteien dafür unverzichtbar sind?
4. Erfüllen wir die wachsenden Melde- und Sorgfaltspflichten?
5. Ist die Aufsicht über Resilienz institutionalisiert, mit fester Reporting-Kadenz, Übungen, Szenarien und klarer Zuständigkeit im Verwaltungsrat?

Zwischen diesen Fragen und der gelebten Praxis liegt oft eine Lücke. Sie zu schliessen heisst, die zunehmenden Pflichten in belastbare Resilienz zu übersetzen, Risikomanagement und Geschäftskontinuität regelmässig zu prüfen, die Klimaberichterstattung verlässlich abzustützen, Cyber- und Lieferkettenrisiken aktiv zu steuern. Das wirksamste Instrument dazu ist die Szenarioplanung. Gerade weil sich der nächste Schock nicht vorhersagen lässt, macht das disziplinierte Durchspielen konkreter Krisenfälle, etwa der Ausfall eines Schlüssellieferanten, ein regionaler Stromausfall oder ein Cybervorfall während einer Hitzewelle, Verwundbarkeiten und Abhängigkeiten sichtbar, bevor sie real werden. Szenarien fügen die einzelnen Fachsilos zu einem Gesamtbild zusammen, das der Verwaltungsrat überblicken und hinterfragen kann.

Szenarien zeigen, wo ein Unternehmen verwundbar ist; die Notfallplanung sorgt dafür, dass es im Ernstfall handlungsfähig bleibt. Sie übersetzt Erkenntnisse in konkrete Fähigkeiten: Geschäftskontinuitätspläne für die kritischen Prozesse, klare Rollen und Entscheidungsbefugnisse, eingespielte Kommunikationswege und Ausweichlösungen für den Ausfall von Strom, IT, Standorten oder Schlüssellieferanten. Novelis etwa verlagerte nach der Überflutung Teile der Fertigung kurzfristig an deutsche Standorte und hielt so die Belieferung der Kunden aufrecht. Entscheidend ist, dass solche Pläne geübt werden: Ein Notfallkonzept, das nur in der Schublade liegt, versagt genau dann, wenn es gebraucht wird. Regelmässige Übungen legen die Lücken offen, solange sie noch folgenlos sind.

Daraus ergibt sich ein Denkansatz, der über jede Branche hinausgeht. Weil sich die Ursache des nächsten Schocks kaum vorhersagen lässt, lohnt es sich, nicht von den Ursachen her zu planen, sondern von den Auswirkungen: Welche Funktionen und Leistungen sind für das Überleben









des Unternehmens unverzichtbar? Was ist unsere «Minimum Viable Company»? Welche Prozesse, Technologien, Daten, Standorte und Drittparteien müssen auch in einem eingeschränkten Betriebsmodus verfügbar bleiben? Wie lange hält das Unternehmen einen Unterbruch aus? Und wie gelingt die rasche Rückkehr zum Normalbetrieb? Ob der Auslöser eine Überschwemmung, ein Cyberangriff oder der Ausfall eines Lieferanten ist, spielt für die Antwort eine geringere Rolle als oft angenommen, denn die Konsequenzen ähneln sich.

Ein Verwaltungsrat, der in diesen Kategorien denkt, stärkt die Widerstandsfähigkeit seines Unternehmens gegenüber einer ungewissen Zukunft, statt es lediglich gegen einen einzelnen, vermeintlich bekannten Feind zu wappnen. Der iberische Blackout dauerte nur Stunden, doch seine Lehre reicht weiter. Kritische Infrastruktur ist heute breiter, vernetzter und stärker reguliert als noch vor wenigen Jahren und Resilienz ist zur Chefsache geworden. Verwaltungsräte, die Resilienz als das begreifen, was sie ist, eine strategische, systemische Führungsaufgabe, verschaffen ihrem Unternehmen einen echten Vorteil: die Fähigkeit, weiterzuarbeiten, wenn andere im Dunkeln stehen.

Autoren



Silvan Jurt
Partner, Leiter Corporate Sustainability Services, Leiter Markets
KPMG Schweiz

+41 58 249 50 25
sjurt@kpmg.com



Nicolas Tinguely
Partner, Cyber and Digital Risk Consulting
KPMG Schweiz

+41 58 249 21 44
ntinguely@kpmg.com

Dieser Artikel ist Bestandteil der KPMG Board Leadership News, unser Newsletter für Verwaltungsrätinnen und Verwaltungsräte.
Er erscheint dreimal pro Jahr.

Über das KPMG Board Leadership Center

Das KPMG Board Leadership Center ist unser Kompetenzzentrum für Verwaltungsrätinnen und Verwaltungsräte. Mit vertieftem Fachwissen und neusten globalen Kenntnissen unterstützen wir Sie in Ihren aktuellen Herausforderungen, damit Sie Ihre Rolle höchst effektiv erfüllen können. Zusätzlich bieten wir Ihnen die Möglichkeit, mit Gleichgesinnten in Kontakt zu treten und sich auszutauschen.

Erfahren Sie mehr unter **kpmg.ch/blc**.

Die hierin enthaltenen Informationen sind allgemeiner Natur und beziehen sich daher nicht auf die Umstände einzelner Personen oder Rechtsträger. Obwohl wir uns bemühen, genaue und aktuelle Informationen zu liefern, besteht keine Gewähr dafür, dass diese die Situation zum Zeitpunkt der Herausgabe oder eine künftige Situation akkurat widerspiegeln. Die genannten Informationen sollten nicht ohne eingehende Abklärungen und professionelle Beratung als Entscheidungs- oder Handlungsgrundlage dienen. Bei Prüfkunden bestimmen regulatorische Vorgaben zur Unabhängigkeit des Prüfers den Umfang einer Zusammenarbeit. Sollten Sie mehr darüber erfahren wollen, wie KPMG AG personenbezogene Daten bearbeitet, lesen Sie bitte unsere Datenschutzerklärung, welche Sie auf unserer Homepage www.kpmg.ch finden.

© 2026 KPMG AG, eine Schweizer Aktiengesellschaft, ist eine Gruppengesellschaft der KPMG Holding LLP, die Mitglied der globalen KPMG-Organisation unabhängiger Firmen ist, die mit KPMG International Limited, einer Gesellschaft mit beschränkter Haftung englischen Rechts, verbunden sind. Alle Rechte vorbehalten.