Cyber-Resilienz

Wettbewerbsvorteile schaffen und Vertrauen fördern

Unternehmen und Arbeitnehmer loben die neue Freiheit des Home Office (oft auch als Remote Work bezeichnet). Die speziellen Umstände der COVID-19-Pandemie haben der Wirtschaft, der Gesellschaft und nicht zuletzt den Schulen und Universitäten einen Digitalisierungsschub beschert, der in dieser Wucht und Geschwindigkeit nicht erwartet worden war. Doch mit der neuen digitalen Arbeitswelt erlebt auch der Missbrauch dieser Datenströme und digitalen Schnittstellen einen Aufschwung. Wer es jedoch schafft, die Widerstandsfähigkeit seines Unternehmens gegen die Cyber-Kriminalität zu stärken und auch auf höchster Führungsstufe eine Sensibilisierung für Cyber-Resilienz zu etablieren, wird einen deutlichen Wettbewerbsvorteil erreichen können.

Vertrauen in unsicheren Zeiten

Jegliches wirtschaftliches Handeln basiert auf Vertrauen. Sowohl Vertrauen in das Gegenüber, aber auch Vertrauen in Produkte, Dienstleistungen, Technologie, Abwicklungssysteme und Intermediäre. Doch eine Krise bringt ebendieses Vertrauen in Schieflage und schafft Unsicherheit. Eine solche ist wiederum der Nährboden für irrationales Verhalten. Diese Tatsache machen sich Cyber-Kriminelle zu Nutze. Der Begriff «Social Engeneering» bezeichnet hinterhältige Betrugsversuche und Phishing-Aktivitäten, bei denen nichtsahnende Nutzer in eine vermeintliche Falle tappen.

Der durch das Remote-Working-Netzwerk getriebene rasante Ausbau der Datenströme bietet Cyber-Attacken eine grosse Angriffsfläche. Denn plötzlich kommen private Geräte von Mitarbeiterinnen und Mitarbeitern im Home-Office zum Einsatz. In aller Eile werden Cloud-Dienstleistungen in Anspruch genommen, Server-Zugriffe über VPN-Tunnels geöffnet oder Videokonferenzen über ungesicherte Datennetzwerke geführt.

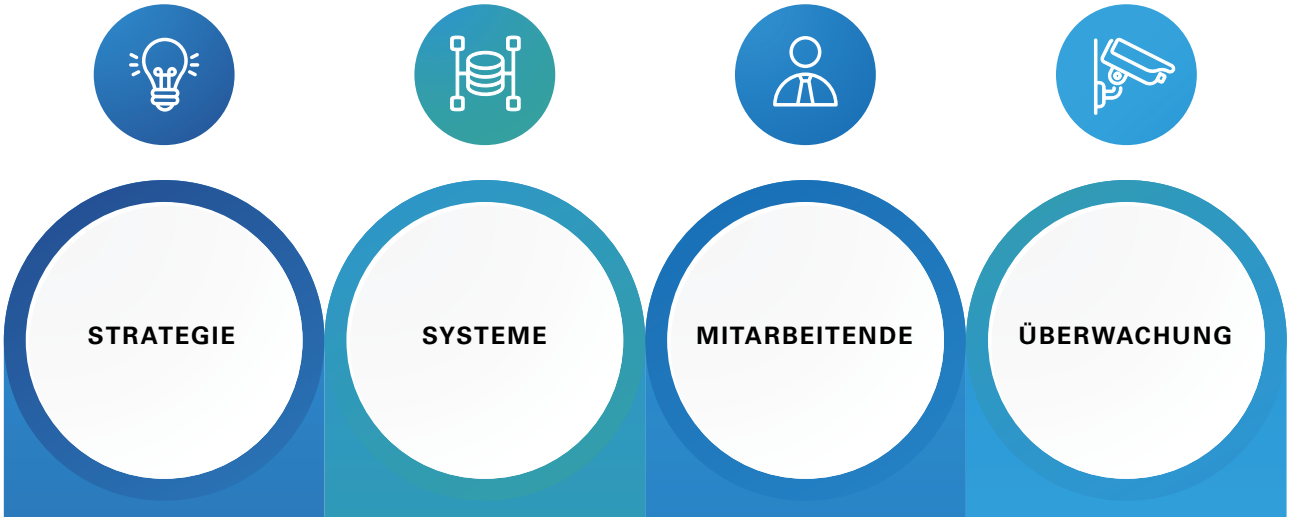
Die direkten Folgen von Cyber-Angriffen sind daher oft dramatisch: wochenlange Betriebsunterbrüche, unautorisierte Zahlungen, Datenlecks und Datenschutzverletzungen, aber auch fehlerhafte Produkte und Dienstleistungen (die im schlimmsten Fall sogar Leben gefährden können). Daraus resultieren, neben dem Verlust von Reputation und Kundenvertrauen, Schäden wie Umsatzeinbrüche, Rechtskosten und Bussen, Zeitverlust im Sinne eines verspäteten Markteintritts, administrative Kosten für Ersatz und Wiederherstellung,

Kosten für Haftung, sowie Schadenersatz und Kompensationszahlungen, von denen sich bekanntlich einige Unternehmen nicht mehr erholen konnten und Konkurs anmelden mussten.

Wissen Verwaltungsrat und Management Cyber-Resilienz als Wettbewerbsvorteil zu nutzen?
Doch wie reagieren Unternehmen und der Verwaltungsrat als oberstes strategisches Führungsorgan auf diese Gefahren, beziehungsweise wie wird die negative Energie in eine positive Kraft der sicheren Unternehmensführung umgeleitet? Neben den offensichtlichen operationellen Risiken erkennen fortgeschrittenere Unternehmen, dass Cyber-Resilienz eine strategische Chance ist, sich von der Konkurrenz abzuheben. Verantwortungsbewusstes Management von Cyber-Risiken und selbst ein gut bewältigter Cyber-Vorfall können das Vertrauen der Stakeholder eines Unternehmens stärken, seien dies Kunden, Investoren, Lieferanten oder Aufsichtsbehörden. Darüber hinaus kann ein cyber-resilientes Unternehmen digitale Technologien wie Datenanalyse, künstliche Intelligenz und Cloud Computing mit Zuversicht und nachhaltig nutzen, um seine Wettbewerbsposition zu verbessern.

Cyber-Risiken werden von Unternehmen häufig als eine nicht greifbare, fast schon unreale Bedrohung angesehen. Dies nicht zuletzt, weil solche Angriffe oft hochkomplexe, technische Schwachstellen ausnutzen. Daraus zu schliessen, dass es sich folglich bei Cyber-Risiken um technische Risiken handeln muss, die von der IT-Organisation zu bewältigen sind, ist allerdings ein Trugschluss. Zieht man die möglichen Folgen eines Cyberangriffs in Betracht, wird klar, dass es sich um operationelle Risiken handelt, mit denen Verwaltungsräte und die Geschäftsführung vertraut sein müssen.

Die Hauptaufgaben des Verwaltungsrats beziehen sich auf die folgenden vier Bereiche: Strategie, Systeme, Mitarbeitende und Überwachung. Daraus leiten sich auch seine direkten Aufgaben im Zusammenhang mit der Cyber-Resilienz des Unternehmens ab:



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

Widerstandsfähigkeit des Unternehmens erhöhen

Während in der Vergangenheit der Fokus, ähnlich einer mittelalterlichen Stadtbefestigung, auf technischen Massnahmen zur Verhinderung eines Eindringens von Angreifern in das Unternehmen lag (Stichwort: Firewall), ist eine moderne Cyber-Strategie breiter abgestützt. Dies, weil davon ausgegangen werden muss, dass mit der zunehmenden Vernetzung und Integration zwischen Unternehmen, Lieferanten und Kunden ein Angreifer in geschützte Bereiche eindringen kann und auch wird. Eine moderne Cyber-Strategie ist deshalb darauf ausgelegt, solche Eindringlinge zeitnah zu erkennen und sie daran zu hindern, Schäden anzurichten und somit die Widerstandsfähigkeit eines Unternehmens gegenüber Cyber-Angriffen zu erhöhen.

Fragen für den Verwaltungsrat

Das Verständnis des Verwaltungsrats für die Cyber-Bedrohung und der damit einhergehenden strategischen Chancen und Risiken, sowie die Einflussnahme bei der Festlegung und Umsetzung strategischer und operativer Massnahmen, sind sowohl im Hinblick auf die Rolle des Verwaltungsrats als Unternehmensstratege als auch auf seine Aufsichtsfunktion von entscheidender Bedeutung. Der Verwaltungsrat sollte dabei Klarheit über die folgenden Themen erlangen:

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

Fazit

Cyber-Risiken sind operationelle Risiken, die den Fortbestand eines Unternehmens gefährden können und mit denen sich der Verwaltungsrat im Rahmen seiner gesetzlichen Aufgaben zu befassen hat. Der Verwaltungsrat sollte darauf achten, dass das Unternehmen seine Cyberstrategie auf Resilienz ausrichtet. Dazu gehört, dass die Cyber-Grundmassnahmen rigoros umgesetzt werden. Um Klarheit über den Stand der Cyber-Risiken und -Resilienz des Unternehmens zu erlangen, ist ein adressatengerechtes Cyber-Reporting notwendig. Neben dem Management von Cyber-Risiken, sollte der Verwaltungsrat zusammen mit der Geschäftsführung auch analysieren, inwiefern sich die Cyber-Resilienz als Unterscheidungsmerkmal und Wettbewerbsvorteil nutzen lässt.

Weiterführende Lektüre

Cyber-Resilienz – Die Rolle des Verwaltungsrats im Umgang mit Cyber-Risiken.
kpmg.ch/blc

Dr. Matthias Bossardt
Partner, Leiter Cyber Security und Technology Risk
KPMG Schweiz

+41 58 249 36 98
mbossardt@kpmg.com

Dieser Artikel ist Bestandteil der KPMG Board Leadership News. Um diesen Newsletter für Verwaltungsrätinnen und Verwaltungsräte dreimal pro Jahr zu erhalten, können Sie sich hier registrieren.

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