Boardroom Questions

Cyber Security - Was bedeutet das für den Verwaltungsrat?

Laut der KPMG Swiss Cyber Security Umfrage 2017 waren 88 Prozent der Umfrageteilnehmer in den letzten 12 Monaten von einer Cyber-Attacke betroffen. Bei 56% der Teilnehmer provozierte der Angriff einen Unterbruch der Geschäftstätigkeit.

Quelle: Clarity on Cyber Security 2017, KPMG Schweiz

In den vergangenen Monaten fielen zahlreiche globale Unternehmen Cyberverbrechen zum Opfer.
Anleger, Regierungen und Regulierungsbehörden üben zunehmenden Druck auf Verwaltungsratsmitglieder aus, bei diesem Thema die gebührende Sorgfalt unter Beweis zu stellen. Die Regulierungsbehörden erwarten den Schutz personenbezogener Daten und Systeme, die sowohl Unfällen als auch geplanten Attacken standhalten können.

Im Verwaltungsrat sollte man sich angesichts dieser Attacken folgende Fragen stellen:
Was sind die Auswirkungen einer Cyberattacke auf den Verwaltungsrat?
Was sollte der Verwaltungsrat bei einer solchen Attacke unternehmen? Ist der Verwaltungsrat vorbereitet?
Welche Arten von Verlusten sind möglich? Wie gross ist das Ausmass?
Wie können wir verstärkt proaktiv, fokussiert und präventiv vorgehen?

Potenzielle Auswirkungen und mögliche Implikationen für den Verwaltungsrat

Verlust von geistigem Eigentum, einschliesslich patentiertes und urheberrechtlich geschütztes Material, Kundenlisten und sensible Geschäftsdaten

Reputationsverlust, führen zu einem Rückgang Ihres Marktwerts; Verlust von Goodwill und des Vertrauens von Kunden und Zulieferern

Sanktionen für rechtliche oder regulatorische Verstösse, z. B. Bussen aufgrund von Datenschutzverletzungen oder Schadenersatzforderungen/ Vertrags-strafen aufgrund von Verzögerungen

Zeitverlust durch Ermittlung des Schadens, die Benachrichtigung der Aktionäre und die Zusammenarbeit mit Aufsichtsbehörden (Finanz-, Steuer- und Rechtsbehörden).

Eigentumsverlust an Produkten oder Informationen können zu Verzögerungen oder gar zu Lieferausfällen führen

Administrative Ressourcen zur Wiederherstellung von Kundenvertrauen, Benachrichtigung der Behörden, Materialersatz und Wiederherstellung der ordentlichen Geschäftsorganisation.

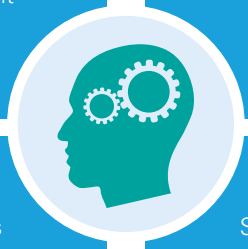
Es ist wichtig, dass sich der Verwaltungsrat auf die folgenden Fragen fokussiert und diese in die Risikostrategie einbindet.

Wie bekommt der Verwaltungsrat dieses Thema in den Griff?

- Erfüllt mein Unternehmen alle seine Verpflichtungen im Zusammenhang mit der Informationssicherung?
- Sind die Daten in meinem Unternehmen sicher?
- Haben wir ein umfassendes Verständnis unserer derzeitigen Schwachstellen?
- Stellen Partner in der Lieferkette ein Risiko für uns dar?
- Erfüllen wir die Anforderungen an die Informationssicherheit, um uns für öffentliche Aufträge bewerben zu können?
- Sind uns unsere Mitbewerber einen Schritt voraus? Und stellt dies für sie gegebenenfalls einen Vorteil dar?
- Wer ist in unserem Unternehmen für die Cybersicherheit zuständig und können diese zusammen mit dem Management-Team die folgenden Fragen beantworten?

Weiss Ihr Management-Team, wie es sich im Falle eines Angriffs verhalten soll?

- Wie sollte unsere Reaktion aussehen?
- Wie wirksam war unsere Reaktion?
- Was wissen Sie über die Personen/Organisationen, die für die Angriffe verantwortlich sind, und ihre Vorgehensweisen?
- Gibt es bei Cyberangriffen irgendwelche Muster, die unsere Informationen und Vermögenswerte zu bestimmten Zeiten verletzungsanfälliger machen?
- Mit wem sollten wir dieses Wissen über Bedrohungen teilen und wie? Wie können wir ein wirksames Security Operation Center einrichten?



Was kann also der Verwaltungsrat in diesem Zusammenhang tun?

KPMG setzt auf fünf Prinzipien, für ein proaktives Bedrohungsmanagement:

- Vorbereitung: Analyse und Verbesserung des aktuellen Stands der Vorbereitungen gegen Cyberattacken.
- Schutz: Entwicklung und Umsetzung einer Infrastruktur zur Abwehr von Cyberbedrohungen.
- Erfassung: Reaktion auf und Untersuchung von Cyberattacken.
- Integration: Einbindung der Cybersicherheit in Kultur und Entscheidungsprozesse.
- Wandel: Organisation und Durchführung eines Komplettprogramms.
- Das Cyber Maturity Assessment (CMA) von KPMG bietet eine detaillierte Überprüfung der Fähigkeit eines Unternehmens zum Schutz seiner Informationen.

Wie kann der Verwaltungsrat proaktiv, fokussiert und präventiv agieren?

Sensibilität im Verwaltungsrat für neue Cyberbedrohungen ist entscheidend. Wissen über Bedrohungen kann Unternehmen dabei helfen, verstärkt proaktiv, fokussiert und präventiv zu agieren.

- Wie können wir uns von Reaktion auf zu Antizipierung von Cyberattacken bewegen?
- Wie können wir uns das Wissen über die uns betreffenden Cyberbedrohungen zunutze machen?
- Wie können wir die Rentabilität der Investitionen in unsere Cybersicherheit belegen?
- Wann wurde die Bedrohung von Cyberattacken zuletzt im Verwaltungsrat erörtert?
- Findet der Cyberbereich Eingang in die strategischen Debatten des Verwaltungsrats?
- Weiss Ihr CIO, wann er reagieren muss und welche taktischen Optionen verfolgt werden sollen? Hat diesen bereits Wirkung gezeigt?

Kontakt

KPMG AG
Badenerstrasse 172
Postfach
8036 Zürich

kpmg.ch/blc

Matthias Bossardt
Partner
Head of Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

Yves Bohren
Director
Cyber Security

+41 58 249 48 95
ybohren@kpmg.com

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.

© 2021 KPMG AG, eine Schweizer Aktiengesellschaft, ist eine Tochtergesellschaft der KPMG Holding AG. KPMG Holding AG ist Mitglied der globalen KPMG-Organisation unabhängiger Firmen, die mit KPMG International Limited, einer Gesellschaft mit beschränkter Haftung englischen Rechts, verbunden sind. Alle Rechte vorbehalten.