swiss BoardForum
sharing experience

# Cyber Risk Management: Bewusstsein allein reicht nicht

**Privat und beruflich erleichtert uns die Digitalisierung den Alltag. Aber die Cyberkriminalität nimmt zu. Unternehmen, die das Cyberrisiko nicht systematisch bearbeiten, gefährden den Betrieb und ihren guten Ruf. Sieben Empfehlungen für ein gutes Cyber-Risikomanagement.**

Die Digitalisierung erlaubt immer vernetztere Geschäftsmodelle. Fragmentierte Wertschöpfungsketten, mehr und mehr Services in der Cloud – Daten werden empfangen und gelesen, bearbeitet und gesendet. Mit diesen Informations- und Kommunikationsprozessen steigt die Abhängigkeit von Lieferanten. Cyberrisiken entwickeln sich zu einem unternehmerischen, aber auch systemischen Risiko oberster Priorität. Denn ohne funktionierende IT steht der Betrieb still.

## Jedes Unternehmen ist Ziel von Cyberattacken

Es ist nicht eine Frage ob, sondern wann ein Unternehmen angegriffen wird. Cyberattacken werden häufiger, und Cyberkriminalität als Geschäft wird lukrativer. Bekannt gewordene Angriffe sind nur die Spitze des Eisbergs, denn die Dunkelziffer ist hoch. Viele Unternehmen möchten Schwachstellen in ihrer IT-Infrastruktur oder ihren Informations- und Kommunikationsprozessen nicht offenbaren und machen Angriffe nicht publik. Erfolgreiche Cyberattacken – in der Versicherungssprache Cyberereignisse genannt – zielen auf die IT. Doch die negativen Auswirkungen strahlen in alle Geschäftsprozesse aus, bis hinein ins Kerngeschäft. Sie gefährden Geschäftsfortführung und Reputation und können Haftpflichtansprüche rund um den Datenschutz nach sich ziehen.

## Die vielen Strategien der Hacker

Zugang verschaffen sich die Angreifer zum Beispiel über Phishing-E-Mails, indem sie Mitarbeitende in die Irre führen (Social Engineering), über offene Ports oder ferngesteuerte Rechner (Botnet). Durch solche Sicherheitslücken wird das IT-System mit Schadsoftware infiziert. Oft werden dabei Daten verschlüsselt, und es kommt zu einer doppelten Lösegeldforderung: Erst nach Bezahlung einer hohen Summe in Bitcoins werden die Daten, wenn überhaupt, wieder zurückgegeben. Mit einer zweiten Zahlung kann das angegriffene Unternehmen verhindern, dass die ausspionierten und gestohlenen geheimen Geschäftsdaten im Dark- oder Internet publiziert werden. Auch Betrugstechniken wie die Manipulation von Rechnungen (Man-in-the-Middle, CEO-Fraud) nehmen zu.

## Kostspielig und nervenaufreibend

Ein Cyberereignis kostet viel Zeit und Nerven: IT-Systeme müssen neu aufgesetzt werden, Daten gerettet und wiederhergestellt, Backups eingespielt sowie eine Notfall- und Krisenorganisation muss hochgefahren werden. Dazu kommen häufig hohe Kosten: finanzielle Verluste durch den Betriebsunterbruch, Wiederherstellungskosten der Infrastruktur, Vermögensschäden bei E-Banking-Betrug und der nicht zu unterschätzende Reputationsschaden nach oft feststellbarem, mangelhaftem Krisenmanagement.

**SwissBoardForum**
Kapellenstrasse 14 | Postfach | 3001 Bern | T: +41 (0)58 796 98 80 | F: +41 (0)58 796 99 03 | sekretariat@swissboardforum.ch
Route de Lac 2 | 1094 Paudex | Case Postale 1215 | 1001 Lausanne | T: +41 (0)58 796 33 00 | F: +41 (0)58 796 33 82 | secretariat@swissboardforum.ch

www.swissboardforum.ch

**Aktiv werden**

Um dieser unsichtbaren und dynamischen Gefahr entgegenzutreten, muss ein Unternehmen zuerst das nötige Verständnis für dieses neue Risiko «Cyber» schaffen. Dies geschieht durch den internen Austausch zwischen den relevanten Anspruchsgruppen sowie eine gemeinsame Antwort auf die Frage, wie stark das Unternehmen von einer funktionierenden IT und sicheren Daten abhängig ist. Vor diesem Hintergrund geht es anschliessend darum, wie mit dem Cyberrisiko umgegangen werden soll. Es gibt – wie bei allen Risiken – vier Handlungsoptionen: Erstens kann das Risiko akzeptiert werden. Das Unternehmen kann zweitens das Risiko mit Massnahmen wie einer Antischadsoftware vermeiden. Das Risiko kann drittens vermindert werden, indem für den Fall einer erfolgreichen Attacke vorgesorgt wird, zum Beispiel mit einem Business Continuity Management. Viertens kann ein Unternehmen das Risiko auf die Versicherung überwälzen. Eine Cyberversicherung unterstützt bei einem Cyberereignis und übernimmt entstehende Kosten.

**Sieben Empfehlungen für den Umgang mit Cyberrisiken**

Was bedeutet dies nun für die Arbeit des Verwaltungsrats? Welche Prozesse müssen angestossen werden, um ein Unternehmen vor Cyberkriminalität effektiv zu schützen? Folgende sieben konkrete, nichtabschliessende Empfehlungen helfen, dem Thema Cybersicherheit das richtige Gewicht zu geben:

1. **Thema in der Risikopolitik verankern:** Kontroll- und Aufsichtsorgane sind gefordert, Cyberrisiken in der Corporate Governance und der Risikopolitik mit Zielen und Grundsätzen zu verankern. Sind diese auch auf operativer Ebene klar und verständlich kommuniziert, tragen sie zu einer Sensibilisierung und einem verstärkten Verantwortungsbewusstsein bezüglich Cyberrisiken bei. Eine Cyber-Risikokultur wird so von den Entscheidungsträgerinnen und -trägern vorgelebt, und es wird deutlich: Cyberrisiken sind Chefsache. Sie gehören in ein unternehmensweites, strategisches Risikomanagement und können nicht einfach von der Unternehmensleitung an die IT delegiert werden.

2. **Verantwortlichkeiten klar zuweisen:** Ist eine oft existenzbedrohende Cyberattacke im Gang, braucht es kompetente, verfügbare Ansprechpersonen: Geschäftsführenden, CFO, Risk Manager und Datenschutzbeauftragten obliegt die organisatorische Verantwortung. Der IT-Security-Dienstleister oder Chief Information Security Officer (CISO) wiederum kennt die Stärken und Schwächen der Informationssicherheit von IT, Netzwerk und Telekommunikation und nimmt die technische Verantwortung wahr. Der Versicherer kann gezielt unterstützen, indem er die Bedrohungslage aufzeigt und nach der Risikoeinschätzung Empfehlungen für Prävention und Cyberresilienz abgibt. Ausserdem kann er dem Unternehmen mit einer geeigneten Versicherungsdeckung und Assistance-Dienstleistungen im Schadenfall (Incident Response, Business Continuity, Krisen- und Reputations-Management) zur Seite stehen, allenfalls gemeinsam mit einem Makler. All diese Verantwortlichkeiten müssen klar geregelt sein.

3. **Durch Risikodialog die Cyberfitness stärken:** Als nächsten Schritt braucht es zwischen diesen Verantwortlichen einen interdisziplinären Diskurs zum Cyberrisiko, bei dem jede verantwortliche Instanz ihr Spezialwissen einbringt. Dieser Risikodialog ist ein kritischer Erfolgsfaktor, damit das Cyberrisiko als Ganzes betrachtet, gesteuert und kontrolliert werden kann. Intern sind IT und Business sowie CISO und Risk Manager gefordert sich abzustimmen, von extern kommen kompetente Partner wie IT-Security-Dienstleister, Versicherer und Makler dazu.

4. **Integration von Cyberrisiken ins unternehmensweite Risikomanagement fördern:** Mit der engen Zusammenarbeit zwischen CISO (technische Cybersicherheit auf Systemebene) und dem betriebswirtschaftlichen unternehmensweiten Risikomanagement entsteht eine gelebte Risk Governance bzw. Risikokultur. Ein strukturiertes Vorgehen hilft in der Identifizierung der digitalen Assets, Beurteilung, Steuerung und Kontrolle der Cyberrisiken bis hin zu Risikoverbesserungsmassnahmen. Ein auf diese Art proaktives und ganzheitliches Risikomanagement unter Berücksichtigung des Cyberrisikos braucht und unterstützt eine klar definierte Governance-Struktur.

5. **Ohne Eigenverantwortung der Unternehmen kein Cyberschutz:** Werden personenbezogene, technische, organisatorische und physische Massnahmen in der Risikoverbesserung gezielt und kontinuierlich umgesetzt, wird die Prävention von Cyberkriminalität gefördert und die Cyberresilienz eines Unternehmens gestärkt. Im Falle einer Cyberattacke ist das Unternehmen vorbereitet und gleichzeitig als Organisation effektiver und wettbewerbsfähiger. Zu den Massnahmen gehört insbesondere die regelmässige Sensibilisierung der Mitarbeitenden – eine lohnende Investition in die Cybersicherheit. Denn oft bestimmen der Faktor Mensch und die organisatorischen Massnahmen, ob ein Cyber-Risikomanagement wirkt. Der Massnahmenmix eines Unternehmens hängt letztlich vom Cyberrisikoverständnis und der Risikoakzeptanz ab. Weil immer ein Restrisiko bleibt, gehört auch die passende Cyberversicherung als komplementäres Element zu einem aktiven Cyber-Risikomanagement dazu. Mit der nötigen Eigenverantwortung können Unternehmen so ihre Cyberrisiken umfassend bewältigen.

6. **Cloud als integraler Bestandteil des Cyber-Risikomanagements:** Gehören Cloud-Services zur IT-Infrastruktur oder sollen diese integriert werden, braucht es auch eine Cloud-Strategie mit entsprechendem Risikomanagement. Für den Betrieb geschäftskritischer Anwendungen werden On-Premise-Lösungen bevorzugt. In Bezug auf die Cybersicherheit sind die Datenhaltung in der Schweiz, die Etablierung einer Datenklassifizierung, der Einsatz von Verschlüsselungstechnologie sowie der bewusste Umgang mit der Abhängigkeit vom Cloud-Dienstleister wichtig.

7. **Vorbereitet für Notfälle durch Planung und Übung:** Im Kontext eines wirksamen Business Continuity Management stellt ein Notfallkonzept unter Berücksichtigung der ausgelagerten Cloud-Dienste im Angriffsfall sicher, dass das Geschäft weitergeführt werden kann. Dessen Effektivität muss durch regelmässige Notfallübungen anhand von Szenarien überprüft werden. Der Versicherer kann hier als Sparringpartner für die Ausarbeitung realistischer Schaden- bzw. Notfallszenarien und als Vermittler zu spezialisierten Dienstleistern unterstützen.

**Quelle:**
Qualifizierte Cyber-Marktstudie 2022; die Mobiliar, Hochschule Luzern, economiesuisse: «Cyber Risk Management in grösseren Schweizer Unternehmen»

**Autor:**
Christoph Clavadetscher ist seit über drei Jahren im Kompetenzzentrum Cyber Risk bei der Mobiliar tätig und bringt 22 Jahre Erfahrung in der Assekuranz in Produktentwicklung und Underwriting mit. Er absolviert zurzeit eine Weiterbildung im Bereich Information und Cyber Security an der Hochschule Luzern.