Cyber Risk Management in Schweizer Unternehmen

Wie ein Schiff ohne Kapitän?

Schweizer Unternehmen integrieren Cyberrisiken zu wenig stark ins Risikomanagement. Das zeigt eine gemeinsame Studie der Hochschule Luzern, der Mobiliar und der Economiesuisse: Zwar sind sich die Leitungsgremien der Gefahren bewusst, behandeln Cyberrisiken aber noch zu oft als reines IT-Problem.

Bild: Cams, Pixabay | Lenz

Aufsichtsorgane sind zunehmend gefordert, ihre rechtlichen Kontroll- und Aufsichtspflichten auch im Umgang mit Cyberrisiken wahrzunehmen. Nebst dieser rechtlichen Verpflichtung gibt es auch aus betriebswirtschaftlicher Sicht gute Gründe, ins Cyber Risk Management zu investieren. Schliesslich können Cyberangriffe einen erheblichen Schaden in Organisationen verursachen. Sie können im schlimmsten Fall hohe Bussen, einen starken Reputationsverlust, den Entzug der Betriebsbewilligung oder gar den Konkurs bedeuten.

Bei vielen Unternehmen scheint ein zentrales Fundament zum Managen von Cyberrisiken grundsätzlich zu fehlen: Keine der befragten Organisationen hat explizit definiert, in welchem Ausmass Cyberrisiken bewusst eingegangen werden sollen, um die Geschäftsziele zu erreichen. «Aus der Sicht des Risikomanagements ist das vergleichbar mit einem Schiff, das keinen Kapitän hat», sagt Stefan Hunziker, Studienautor und Leiter des Kompetenzzentrums Risk & Compliance Management an der Hochschule Luzern (HSLU). Offenbar bereitet das Entwickeln von sogenannten Risikoappetit-Aussagen in der Praxis grosse Mühe.

Wie die HSLU-Studie zeigt, herrscht im Umgang mit Cyberrisiken eine Lücke zwischen der technischen IT-Infrastruktur-Ebene und der organisatorischen Ebene. «Cyber-Risiken werden noch zu stark als reines IT-Thema verstanden. Entsprechend werden sie dezentral und operativ gesteuert und zu wenig in das unternehmensweite Risk Management integriert», erläutert Hunziker. Hier ist eine Diskrepanz der Relevanz des Risikos – respektive Awareness – und der «Risk Governance» feststellbar. «Dieser Umstand verhindert einen konsistenten Vergleich – und damit auch eine sinnvolle Priorisierung – von Cyberrisiken und anderen Risikokategorien auf oberster Führungsebene», stellt der Experte fest.

Als einen ersten Schritt in die richtige Richtung empfiehlt er, die Zusammenarbeit zwischen Chief Information Security Officer (CISO) und Risk Manager zu fördern. «Denn hier wird primär die Brücke zwischen der technischen Cybersicherheit und dem betriebswirtschaftlichen Risk Management geschlagen», erklärt Hunziker.

Risikoursache «Mensch»

Oft werden die einfachsten und gleichermassen wirkungsvollsten Massnahmen im Umgang mit Cyberrisiken noch immer vernachlässigt. «Gegebenenfalls ist die Definition von Cyberrisiken deshalb auch etwas irreführend, da viele Risikoursachen nicht im Cyberraum zu finden sind, sondern in menschlichem Fehlverhalten», so Hunziker. Hilfreich sei die Analogie zur Medizin: Dort wisse man schon lange, dass korrektes menschliches Verhalten die Übertragung von Krankheiten verhindert. Regelmässige Desinfektion, diszipliniertes Händewaschen und Abstand einhalten ist etabliertes Verhalten – spätestens seit Ausbruch der Corona-Pandemie. Die vorliegende Studie bestätigt, dass der «Faktor Mensch», beziehungsweise menschliche Verhaltensweisen im Bereich der Cybersicherheit im Vergleich mit technischen Massnahmen noch zu wenig adressiert wird. «Der Faktor ‹Mensch› macht im kontinuierlichen Verbesserungsprozess der Cybersicherheit zwar nur ein Element aus, jedoch ein sehr wichtiges», führt Hunziker aus. Menschliches Verhalten im Umgang mit der Cybersicherheit sollte so trainiert werden, dass es so selbstverständlich und «normal» wird, wie in die Armbeuge zu niesen.

Cloudmigration – nur mit Strategie

Viele Cyber-Risiken haben ihre Ursache in der Cloud-Nutzung. Umso wichtiger ist es, dass Organisationen den Gang in die Cloud gut planen und mit entsprechenden Massnahmen begleiten. «Das Erstellen einer klaren Strategie steht ganz am Anfang einer gut geplanten Migration in die Cloud», sagt Armand Portmann, Studienautor und Themenfeldverantwortlicher «Information & Cyber Security | Privacy» am Departement Informatik der Hochschule Luzern. Erfreulicherweise verfügt ein Grossteil der befragten Organisationen über ein solches Dokument, das die Rahmenbedingungen zur Einführung und Nutzung von Cloud Services beschreibt. Das lasse den Schluss zu, dass das Thema Cloud Computing inzwischen auch in den Führungsgremien Aufmerksamkeit geniesst. «Es ist ein Bewusstsein vorhanden, dass die Nutzung von Cloud-Diensten mit Risiken verbunden ist», so Portmann.

Hauptrisiken der Cloudmigration

Bei der Benennung der Risiken, die sich bei der Nutzung von Cloud Services ergeben, sind die befragten Organisationen nicht um Antworten verlegen.

«Unter die Top drei fallen der Verlust der Vertraulichkeit, respektive die Verletzung des Datenschutzes, die Abhängigkeit vom Cloud-Diensteanbieter und Fragen der Haftung», führt Fernand Dubler aus, er ist Studienautor und wissenschaftlicher Mitarbeiter an der Hochschule Luzern. Das Thema sei komplex. Deshalb sei es nicht verwunderlich, dass die Massnahmen, die für die Linderung dieser Risiken notwendig sind, nicht einfach auf der Hand liegen. Dubler ergänzt: «Diese Massnahmen sind äusserst vielfältig und müssen individuell aus der konkreten Outsourcing-Situation entwickelt werden. Das stellt die betroffenen Organisationen oft vor sehr grosse Herausforderungen.» ■ *(mgt/HSLU)*

Die Studie steht unter dem nachfolgenden Link zum Download bereit:
https://www.hslu.ch/-/media/campus/common/files/dokumente/h/1-medienmitteilungen-und-news/2022/w/220506-cyber-risk-management-studie-2022.pdf?la=de-ch