

Informationssicherheit in KMU: Noch viel Handlungsbedarf

Eine Firewall allein genügt nicht: Wenn man von Datenschutz und Datensicherheit spricht, geht es längst nicht nur um das, was auf irgendeiner Festplatte gespeichert ist. Informationssicherheit muss umfassend verstanden werden, auch in KMU. Ansätze sind zwar da, diese gelte es zu einem Ganzen zu kitten. So das Fazit eines Roundtable-Gesprächs mit drei Experten.

VON THOMAS BERNER

Täglich werden Informationen erfasst, ausgetauscht und archiviert. Über Netzwerke werden heute Unmengen an Daten verschoben. Die Welt der Information ist definitiv virtuell geworden. Doch vielerorts hinkt das Denken der Realität hinterher: In vielen Unternehmen wird noch zu stark in veralteten Strukturen verharrt, was den Schutz der Informationen betrifft.

Interdisziplinäre Angelegenheit

Jerry Krattiger ist Mitgründer und VR-Präsident von SOLVIS AG und Experte für IT-Sicherheitslösungen. Massnahmen zum Schutz von Informationen sind sein tägliches Brot. Und er kann viel erzählen: «In vielen Unternehmen findet die Wertschöpfung heute im nicht materiellen Bereich, also in der sog. <intellectual property>, dem geistigen Eigentum, statt. Wir staunen deshalb immer wieder, wie fahrlässig mit vertrau-

lichen Daten umgegangen wird. Diese finden sich z.B. unchiffriert auf Laptops. Aber auch ehemalige Mitarbeiter haben häufig immer noch Zugriff auf die Systeme und damit die Daten ihrer alten Arbeitgeber, weil die Deaktivierung der Accounts zu wenig sauber gemacht wurde.» Zwei Aspekte werden hier angesprochen: Einerseits scheinen viele Unternehmen die Kontrolle über ihren Datenfluss verloren zu haben. Andererseits ist Informationssicherheit längst nicht mehr allein eine Frage für die IT-Abteilung. Sie ist heute eine interdisziplinäre Angelegenheit, die selbst vor der Buchhaltung oder dem HRM nicht halt macht.

Datenschutz oft mangelhaft umgesetzt

Und damit nicht genug: Per Gesetz sind die Unternehmen verpflichtet, ihren Daten den grösstmöglichen Schutz zu bieten, damit sie nicht in die Hände Dritter geraten. Die ebenfalls auf IT-Fragen spezialisierte Ju-

ristin Ursula Sury relativiert zwar: «Die Änderungen, welche mit der Revision des Datenschutzgesetzes von 2008 gekommen sind, betreffen das tägliche Geschäftsleben eigentlich nur marginal.» Sie stellt fest, dass die Unternehmen bereits sensibilisiert sind, was die Vertraulichkeit von Daten und ihre Geheimhaltung anbelangt. Vielerorts seien denn auch die technischen Vorkehrungen vorhanden. «Unternehmen sind bestrebt, Firewalls zu installieren, ein Monitoring zu machen darüber, wer alles von aussen auf das Unternehmenssystem Zugriff hat», so Ursula Sury. Lücken ortet sie allerdings woanders: «Die Umsetzung des Datenschutzes im Unternehmen – ich meine damit die Sensibilisierung auf Fragen wie: Darf ich wirklich im Besitz der Daten sein? Darf ich damit das, was ich vorhabe, wirklich tun? Und haben nicht zu viele Leute Zugriff darauf? Oder bewahre ich sie zu lange auf? – ist noch nicht wirklich weit gediehen.»

Denken in überholten Kategorien

Ursula Sury macht noch auf einen weiteren Aspekt aufmerksam. «Heute sind immer mehr Geschäftsprozesse computerisiert. Vieles wird immer virtueller und globalisierter. Es ist nicht mehr so, dass ein Werkstatt-Chef etwa nur darauf achten muss, dass keine Werkzeuge auf die Füsse von Mitarbeitenden fallen, sondern es geht auch um rechtliche Risiken, zum Beispiel um das Risiko, dass Daten verloren gehen können. Und genau diese Risiken gilt es erst einmal bewusst wahrzunehmen.» Gerade in vielen Dienstleistungsunternehmen bilden Informationen das eigentliche Werkzeug. Eine Unmenge an Daten und Informationen wird täglich von verschiedenen Personen bearbeitet. Sind diese Daten personenbezogen, greift das Datenschutzgesetz. Es gibt aber noch Informationen, die darüber hinausgehen, nämlich das geistige Eigentum. Dieses fällt zumeist unter das Immaterialgüterrecht bzw. Urheberrecht, ist aber deshalb nicht weni-

**Informationen hinter
Schloss und Riegel:
Die Realität sieht oft
genug noch anders aus.**



UNSERE GESPRÄCHSPARTNER

Die drei im Text zitierten Experten stehen Ihnen für individuelle Fragen zur Verfügung:



Jerry Krattiger, Executive MBA, Chairman & Director Business Consulting bei SOLVIS AG, Arnold Böcklin-Strasse 35, 4051 Basel & Rue Baudit 6, 1201 Genf.
jerry.krattiger@solvis.ch



Stephan Richard, dipl. Wirtschaftsprüfer und Certified IS-Auditor (CISA) bei der BDO AG, Biberiststrasse 16, 4501 Solothurn.
stephan.richard@bdo.ch



Ursula Sury, Rechtsanwältin und Professorin an der Hochschule Luzern; Die Advokatur Sury GmbH, Alpenquai 4, 6005 Luzern.
ursula.sury@dieadvokatur.ch

ger schützenswert. «An die Grössenordnungen von Datenschutz und Immaterialgüterrecht wird oft noch viel zu wenig gedacht. Vieles davon scheinen wir noch gar nicht begriffen zu haben, da wir noch zu stark in den Kategorien des Sachenrechts denken. Das sieht man beispielsweise bei Unternehmensbewertungen: Diese sind viel einfacher, wenn es nur um Sachwerte geht. Ein Computer hat wohl einen Sachwert, darauf lassen sich aber schnell Abschreibungen machen. Viel wichtiger ist aber, was an Informationen in diesem Computer gespeichert ist», führt Ursula Sury weiter aus und ergänzt, dass rechtliche Risiken, die aus einem Datenverlust entstehen können, oft zu wenig bewusst sind.

Wider die Betriebsblindheit

Rein intuitiv machen die meisten Unternehmen vieles richtig, jedenfalls, wenn es um «klassische» Risiken geht. Technisch sind denn auch viele KMU auf der Höhe der Zeit. «Firewallmässig sind viele Betriebe sehr gut gerüstet», so Jerry Krattiger. Er fügt aber hinzu, dass diese Sicherheit eine trügerische ist. «Die Hauptrisiken für eine Firma kommen weniger von aussen als von innen. Die meisten IT-Schäden werden durch eigene Mitarbeitende verursacht.» Gerade deshalb sei es wichtig, die internen Prozesse festzuschreiben: Wer hat wann zu welchen Informationen Zugang? Wer ist dazu berechtigt? Muss etwa ein Marketingleiter Zugang zu HR-Daten haben?

Dass sich viele Unternehmen womöglich ihrer Sache zu sicher sind, diese Erfahrung macht auch Stephan Richard hin und wieder. Er ist Wirtschaftsprüfer bei der BDO AG und berät Unternehmen in Fragen von Kontrolle und Sicherheit im IT-Bereich. Er sieht bei vielen Geschäftsführern eine gewisse Betriebsblindheit. Sie verschliessen sich und wollen sich auch durch Experten nicht beraten lassen, da sie glauben, alles im Griff zu haben. «Die Führungsebene ist sich zwar häufig der Risiken in ihren Kernprozessen – Einkauf, Produktion, Verkauf – bewusst. Vergessen gehen aber oft die Supportprozesse wie z.B. die Informatik, dies sowohl bei Sicherheit, Verfügbarkeit und Vertraulichkeit als auch in rechtlicher Hinsicht – vielfach deswegen, weil man der Meinung ist, dass ja alles funktioniert. Erst wenn mal etwas passiert, kommt man dann drauf, dass es IT-spezifische Risiken und IT-Abhängigkeiten gibt ... Gerade in solchen Bereichen ist die Beratung von Inhabern, VR oder Managern relativ schwierig, weil in KMU vieles in Personalunion erfolgt», so die Feststellung von Stephan Richard.

IT-Sicherheit interdisziplinär angehen

Schon allein die Tatsache, dass hier Experten aus drei Bereichen zu Wort kommen, ist Beweis genug für die Komplexität des Themas, welches denn auch interdisziplinär angegangen werden sollte. Doch scheinen viele KMU eben damit überfordert.

Dieser Eindruck erscheint wohl auch deswegen, weil die Informationssicherheit bisher stark IT-getrieben war. Jerry Krattiger macht die Erfahrung, dass Projekte für die Informationssicherheit, welche über die IT und die reine Technik hinausgehen, langfristig erfolgreicher sind. Aber es gelte dabei, Hürden zu überwinden: «Viele Organisationen verfügen über eine <Silostruktur>. Die Herausforderung besteht darin, diese einzelnen Silos, die halt oft in eigenen und unterschiedlichen Kategorien denken, an einen Tisch zu bringen und gemeinsam die Benefits zu definieren.» Die meisten dieser Benefits seien immaterieller Natur, doch wenn es um die Vermeidung von Schäden geht, dürfte dies von allen verstanden werden, so Krattiger weiter. «Nur über eine polizeiliche Admin im Stile <gemäss IKS 728 A und B haben Sie dies zu tun> lässt sich ein Projekt nicht unbedingt erfolgreich umsetzen.» Dass interdisziplinär oft auch gleichbedeutend mit zeitintensiv ist, liegt auf der Hand. Dabei besteht wiederum die Gefahr, dass nur die «harten Fakten» verstanden werden und etliche weiche Faktoren auf der Strecke bleiben, «weil man sich nicht einig wird, wer nun mehr profitiert oder weniger», wie Ursula Sury ergänzt und dies als Auswirkung eines zu stark ausgeprägten «Divisionsdenkens» sieht. «Vieles steht und fällt mit einem sauberen Projektmanagement, auch die regelmässige Schulung der Beteiligten gehört dazu», so ihr Fazit.

Informationsbedarf noch nicht gedeckt

Wo können sich Unternehmen jene Informationen beschaffen, die sie benötigen, um ihre Daten zu schützen? Wo finden sie Antworten auf die Frage, welche Sicherheitsmassnahme für sie die richtige ist? Der erste Schritt ist sicher die Klärung der wichtigsten Risiken. Dies muss allerdings innerhalb des Unternehmens geschehen. Zur Informationsbeschaffung rät Stephan Richard zum Kontakt mit Branchenkollegen, z.B. innerhalb eines Verbandes. «Einige Verbände tun bereits sehr viel in diese Richtung», weiss er. Noch nicht alle seien aber so weit, denn jede Branche hat bekanntlich ihre Eigenheiten. Bei einigen, gerade technologiegetriebenen Branchen stehen Fragen der Informationssicherheit eher im Zentrum als bei anderen. Insgesamt scheint aber der Informationsbedarf noch höher zu sein als das Angebot, auch von Bildungsseite. Ursula Sury etwa vermisst niederschwellige Ausbildungsangebote im Bereich Management & Recht. Die Hochschule Luzern ist dabei, einen entsprechenden Ausbildungsgang für KMU anzubieten. «Es gilt zum Beispiel, die komplexen Anforderungen an den Datenschutz in die jeweilige Unternehmenswelt zu transferieren», so die Forderung von Ursula Sury. In der kommenden Ausgabe des ORGANISATORs sollen denn auch einige Massnahmen angesprochen werden, welche KMU zur Informationssicherheit treffen können. ■■■■