Krisenzölibat der Unternehmen

Ganz nach dem Motto «Augen sowie Ohren zu und durch» werden Risiken aus einem Rückspiegelblick dokumentiert und in Form einer Risikobuchhaltung konserviert. Der Erkenntnisgewinn ist gering, denn potenzielle, zukünftige Szenarien werden so ausgeblendet.

Von Richard Werner

Mit anderen Worten: Für Risikobuchhalter liegen diese Gefahren ausserhalb ihrer Vorstellungswelt, abseits von Excel-Spreadsheets und Dashboards. Das Resultat? Pleiten, Pech und Katastrophen. Die Medien sind voll von solchen Beispielen – besonders von renommierten Konzernen, die es aus ihrer Erfahrung heraus besser wissen müssten.

- Der Hackerangriff auf die Server der US-Bank J.P. Morgan Chase & Co war gravierender als bislang angenommen. Erbeutet worden seien bei der Cyberattacke, die Kontaktdaten von 76 Millionen Haushalten und 7 Millionen kleinen Unternehmen, teilte die Bank mit. Die Hacker verschafften sich immer nur für eine kurze Zeit Zugang zu den Servern und stoppten ihre Aktivitäten nach einer Stunde.
- Eine amerikanische IT-Sicherheitsfirma hat den womöglich grössten Datendiebstahl aller Zeiten aufgedeckt. 1,2 Milliarden Login-Daten sollen russische Hacker gestohlen haben. Benutzernamen mitsamt Passwort für alle möglichen Internetdienste, von E-Mails über Social Media bis zu Shopping-Seiten. Experten raten zu einem Passwortwechsel.
- Der Schaden durch den Angriff auf das Playstation-Netz von Sony hatte gewaltige Dimensionen. Hacker haben sich Daten wie Namen, E-Mails, Login-Daten und Adressen von 71 Millionen Nutzern beschafft. Möglicherweise haben sie sogar Kreditkartendaten abgreifen können. Der finanzielle Schaden für Sony wird auf 24 Milliarden US-Dollar geschätzt.
- Beim Softwarehersteller Adobe Systems wurden 100 Millionen Nutzernamen, inklusive der verschlüsselten Passwörter und Passworthinweise gestohlen.

Die Liste wird in Zukunft vor allem bei KMU noch viel schneller wachsen …

Naivität und sorgloser Umgang

Cyberattacken nehmen seit Jahren beständig zu. Empirische Studien zeigen, dass vor allem Ausfälle in der Informa-

tionstechnologie (IT) sich direkt in den Kosten eines Unternehmens niederschlagen. Spannend ist: Man kann sich schützen, aber bei vielen Unternehmen steht das Thema noch nicht auf der Agenda. Die oft beispiellose Naivität von Unternehmen und der sorglose Umgang mit ihren Daten und Sicherungssystemen führen dazu, dass Cyberkriminalität ein «Verbrechen mit Zukunft» ist. Wenn es um Krisenmanagement und die eigene Sicherheit geht, sind die Unternehmen leider oft naiv und wiegen sich in falscher Sicherheit – Wirtschafts- und Cyberkriminalität werden zu oft als «Problem der anderen» angesehen. Dies, obwohl gemäss der aktuellen Studie «Net Losses – Estimating the Global Cost of Cybercrime» des Center for Strategic and International Studies (CSIS) Cyberkriminalität globale jährliche Schäden von über 400 Milliarden US-Dollar anrichtet.

Vor allem in Bezug auf Data Recovery, die Wiederherstellung wichtiger Unternehmensdaten, geht unnötig viel wertvolle Zeit verloren, die durch optimierten Datenschutz, insbesondere bei der Datenwiederherstellung, eingespart werden könnte. Je länger die Ausfallzeiten sind, desto höher sind trivialerweise die damit verbundenen Kosten.

Szenario-orientierte Ansätze

Aber erst wenn sich die Unternehmen vom Rückspiegelblick verabschiedet haben und mit Szenario-orientierten Ansätzen in die Zukunft schauen, bietet Risikomanagement ein solides Navigationsinstrument für Unternehmen. Die wesentlichen Herausforderungen für das Risikomanagement in einem Unternehmen sind die Definition von Szenarien sowie eines «Schlachtplans» für den Krisenfall. Ein solcher Krisenplan ist das wichtigste Werkzeug, mit dem ein Unternehmen auf plötzlich eintretende Angriffe schnell und angemessen reagieren kann. So sollte ein Unternehmen analysieren, welche Probleme dem Unternehmen durch den Datendiebstahl entstehen können, sowie das Ausmass eines möglichen Reputationsverlustes. Es muss eine Strategie vorhanden sein, die definiert, wie im Krisenfall mit den Kunden, der Presse oder der Staatsanwaltschaft umgegangen wird. Oder wie sich das Unternehmen in der Öffentlichkeit verhält und last but not least, wie man sich gegenüber seinen eigenen Mitarbeitern verhält. Die Risikoabwälzung auf die Versicherungsindustrie funktioniert nur bedingt. Dem Versicherungsnehmer muss klar sein, dass nur der finanzielle Schaden über sogenannte Cyberversicherungen abgesichert werden kann. Der eigentliche Schaden, beispielsweise Reputationsverlust, bleibt jedoch weiter bestehen und Aufgabe des Unternehmens.

> Risikomanagement muss sich auf das konzentrieren, was für Unternehmen wirklich zu Krisen führen kann. Insgesamt muss es im Risikomanagement vor allem darum gehen, mehr Zeit und Ressourcen auf das ernsthafte Nachdenken über die wesentlichen kritischen Zukunftsszenarien und Risiken zu lenken. Dies erfordert ein breites Verständnis, interdisziplinäre Zusammenarbeit und auch den Einsatz neuer szenariobasierter Methoden und Werkzeuge.

Tabuthema

Krisenkommunikation gilt in vielen Unternehmen noch immer als Tabuthema. Viele Unternehmen vergessen die Anpassung bestehender Krisenkommunikationspläne auf die neuen Kommunikationskanäle. Was noch wichtiger ist: Nicht selten fehlt die begleitende Neubesinnung in der Unternehmenskultur, die im Krisenfall den offenen, fairen und deeskalierenden Dialog mit wütenden Shareholdern überhaupt erst möglich macht.

Aus Angst vor sich ausbreitenden Protestwellen in den sozialen Medien wird nach dem «Vogel-Strauss-Prinzip» verfahren. Unternehmen verschenken das Kommunikationspotenzial von Twitter, Facebook oder Youtube, weil sie befürchten, nachts um halb drei, wenn die eigene Kommunikationsabteilung schläft, Opfer eines unkontrollierbaren Shitstorms zu werden. Die Überlegung, sich online tot zu stellen, wird zur bewussten Managemententscheidung – im ebenso falschen, wie unumstösslichen Glauben, sich allein durch Nichtpräsenz in den sozialen Medien vor deren Zusammenrottungspotenzial schützen zu können. Dabei sollte der von Greenpeace gegen den Nahrungsmittelkonzern Nestlé gestartete Shitstorm jeder Führungskraft vor Augen geführt haben, dass diese Strategie in der Krise kläglich scheitert. Die Umweltorganisation Greenpeace lancierte im Jahr 2010 eine Kampagne gegen das Nestlé-Produkt Kitkat, da für dieses Produkt Palmöl aus Indonesien eingesetzt wird, welches auf gerodeten Regenwaldflächen angebaut wird. Indonesien weist eine der weltweit höchsten Raten von Urwaldzerstörung auf. Nach dem Start der Greenpeace-Kampagne hatte Nestlé zuerst versucht, den Protest mit anwaltlichen Mitteln aus dem Netz herauszunehmen: eine Strategie der Stärke und des Drohens, wie sie in Druckmedien vielleicht noch hätte erfolgreich sein können. Online aber war dieses Vorgehen zwingend zum Scheitern verurteilt. Am Ende musste Nestlé einlenken und seine Produktion umstellen.

Die Risiko-Weltkarte hat sich in den vergangenen Jahren massiv verändert. Die Zeiten für Risikomanager sind alles andere als langweilig geworden. Unternehmen sollten sich in Zukunft vermehrt mit dem Thema Krisenmanagement auseinandersetzen. Das Krisenmanagementinstrument muss ein «living document» bleiben und Krisenstabsübungen sollten jährlich mindestens einmal mit einem seriös vorbereiteten Szenarien-Drehbuch durchgeführt und gründlich analysiert werden. ■

Quellenangaben: H. Schmitz (2010) «Ausfall der IT-Systeme», F. Romeike (2013) «Erfolgsfaktor Risk Management», R. Werner (2013) «Der effiziente Umgang mit Krisen», Sheffi, Yossi (2012) «Worst-Case-Szenario», L. Steinke (2014) «Shitstorm».

RICHARD WERNER

ist Dr. MBA. Er war mehrere Jahre bei verschiedenen Blue-Chip-Unternehmen und Beratungsfirmen für den Aufbau von Risikomanagementsystemen, Krisenmanagementinstrumentarien und BCM-Projekten verantwortlich. Er ist seit 2003 General Manager der Risk Control RCC GmbH (Schweiz und Europa) und seit 2013 Präsident der Non-Profit-Genossenschaft Private & Confidential Group PnCG, die sich als Sprachrohr und Plattform für sicherheitsrelevante Fragen und Problemstellungen versteht.