Risikomanagement beim Eidgenössischen Bund

Schnittstelle Informationssicherheit

Daten sind ein wichtiges Gut, das optimal geschützt werden muss. Datenraub erspart dem Dieb oft jahrelange Forschung und Entwicklungsarbeit, eröffnet ihm bessere Verhandlungspositionen oder ermöglicht es ihm, ein IT-System zu manipulieren oder Lösegeld zu erpressen. Wie ein neues Beispiel aus der Schweiz zeigt, werden sogar Staatsangestellte erpresst. Wie schätzt man Datenrisiken richtig ein?

Nicole Heyne

In der Schweizer Bankenwelt haben der Diebstahl von Daten und deren Kauf und Auswertung durch Behörden anderer Länder grossen finanziellen Schaden verursacht und die Reputation von Unternehmen gefährdet. Solche Vorfälle können im Extremfall bis zum Konkurs eines Unternehmens führen. Auch der Diebstahl von persönlichen Daten ist nicht zu unterschätzen.

Informationssicherheit

Die Enthüllungen von Edward Snowden haben uns vor Augen geführt, dass tagtäglich unbemerkt Daten entwendet werden. Nicht nur Unternehmen, auch Verwaltungen müssen ihre «Informationen» in den Griff kriegen, andernfalls führt ein «Informationsleck» zu schwerwiegenden Folgen.

Was wird jedoch unter Informationssicherheit verstanden? Je nachdem wird der Begriff unterschiedlich ausgelegt, er führt aber in jedem Fall über eine rein technische Betrachtungsweise hinaus.
Wichtig ist es, dass man jegliche Aspekte, also jene der Mitarbeitenden, der Organisation, der Kultur und der Prozesse untersucht.

In der Bundesverwaltung wird unter Informationssicherheit der Informationsschutz, der Datenschutz, die IKT-Sicherheit, die Personensicherheit und die physische Sicherheit verstanden:
Zwischen den Informationssystemen und Prozessen bestehen allerdings oft grosse Unterschiede. Beispielsweise werden in der Bundesverwaltung die Risikoanalysen für jedes Schutzobjekt der IKT–Anwendungen – Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte – nach der Gefährdungsanalyse durchgeführt (ONR 49002-2:2014).

Dieser Bottom-up-Ansatz steht im Gegensatz zum Top-down-Ansatz des «Risikomanagements Bund», bei dem dank der Szenariomethode eine ganzheitliche Darstellung des Risikos möglich ist.

Die Gefährdungsanalyse konzentriert sich dagegen auf die Details eines Systems oder einer Organisation und ist deshalb prozessorientiert.

Der eigentliche Fokus liegt also auf der operationellen Tätigkeit und nicht auf der strategischen Ebene. Auf einer Risk Map lassen sich die Ergebnisse der beiden Ansätze wie folgt abbilden:

Risiken in der Informations- und Kommunikationstechnik

Die Risiken der Informations- und Kommunikationstechnik (IKT) sind komplex. Wegen des unterschiedlichen Ansatzes bei der Risikoanalyse ist eine Integration der identifizierten IKT-Risiken in das «Risikomanagement Bund» nicht ohne zusätzlichen Aufwand möglich:

Die wesentlichen IKT-Risiken müssen vielmehr nochmals nach der Szenariomethode analysiert werden. Damit diese «Übersetzung» der verschiedenen Methoden gelingt, ist die Zusammenarbeit der verschiedenen Akteure zwingend – insbesondere zwischen Geschäftsprozessverantwortlichen, Risikocoaches sowie Informatiksicherheitsbeauftragten.

Erst durch diesen Schritt wird eine stufengerechte Kommunikation mit der Geschäftsleitung oder dem Verwaltungsrat ermöglicht. Diese Gremien müssen letztlich über die Massnahmen entscheiden, welche die Organisation und die Systeme betreffen.

Besonders der Blick in die Zukunft – mit welchen veränderten Rahmenbedingungen wir in den nächsten Jahren rechnen müssen – ist bei strategischen Entscheidungen miteinzubeziehen.

Neue EU-Datenschutz-Grundverordnung (DSGVO)

Die fortschreitende Digitalisierung stellt auch neue rechtliche Anforderungen an die Unternehmungen. Aktuelles Beispiel ist die am 25. Mai 2018 in Kraft getretene EU-Datenschutz-Grundverordnung (DSGVO). Im Gegensatz zum Informationsschutz, bei welchem es um den allgemeinen Schutz von Informationen geht, ist beim Datenschutz der Schutz der Persönlichkeit und der Grundrechte von Personen zentral. Personenbezogene Daten sind Daten, welche sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

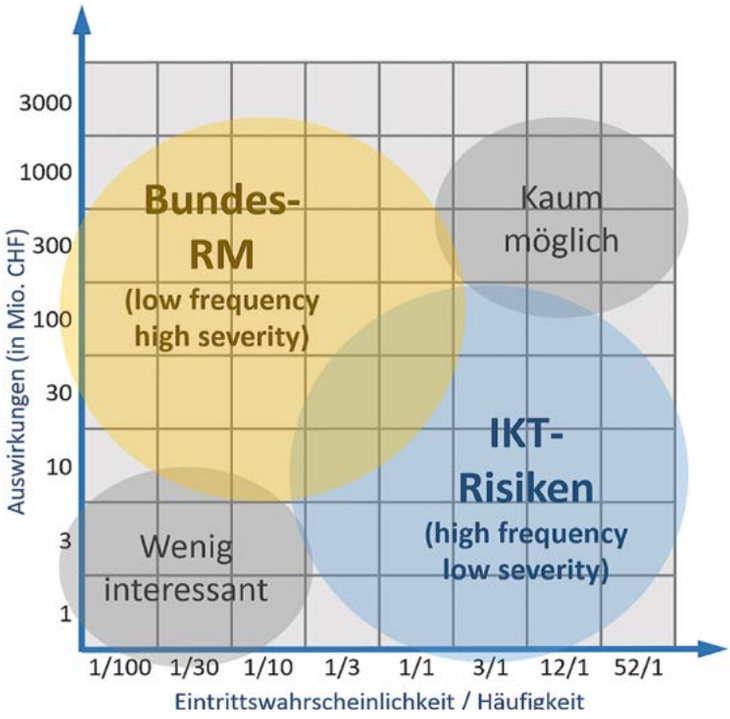
Nicole Heyne ist Co-Sektionsleiterin Risiko- und Versicherungsmanagement (MAS Risk Management/eidg. dipl. Versicherungsfachfrau) und arbeitet in der Eidgenössischen Finanzverwaltung EFV.

Die Informationssicherheit birgt viele Risiken, bietet aber auch Chancen, Wettbewerbsvorteile zu erarbeiten; sie ist eine wichtige Schnittstelle im Management.

Grafik: zVg.

Im Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) werden besonders schützenswerte Personendaten definiert. Darunter fallen gemäss abschliessendem Katalog in Art. 3 Bst. c DSG Daten über die religiösen, weltanschaulichen, politischen und gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre und die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative und strafrechtliche Verfolgungen und Sanktionen.

Besonders schützenswert sind zudem Persönlichkeitsprofile, d.h. Zusammenstellungen von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (Art. 3 Bst. d DSG).



Eine wertvolle Entscheidungshilfe – auf operationeller wie auf strategischer Ebene – beim Schweizer Bund.

Sind alle Prozesse integriert?

Unabhängig vom geltenden Gesetz in der Schweiz sind viele Schweizer Firmen gefordert, die strengere und umfassendere DSGVO zu erfüllen. Obwohl bei der Umsetzung noch viele Fragen offen sind, besteht aus der Perspektive des Risikomanagements erheblicher Bedarf, dieses Thema anzupacken– spätestens seit das Europäische Parlament die DSGVO im April 2016 verabschiedet hat.

Geschäftsprozessverantwortliche und Risikomanager einer Unternehmung müssen analysieren, ob ihre bestehenden Systeme und die Organisation den rechtlichen Anforderungen genügen. In einem wiederkehrenden Prozess müssen die Verantwortlichen der Informationssicherheit kritisch hinterfragen, ob die personenbezogenen Daten mit technischen und organisatorischen Massnahmen ausreichend vor unbefugter Verarbeitung, Zerstörung, Veränderung und Verlust geschützt sind. Die Geschäftsleitung ist verpflichtet, die Vorgaben der DSGVO einzuhalten, sofern die DSGVO auf das entsprechende Unternehmen anwendbar ist.

Eine Delegation der Verantwortlichkeit, beispielsweise an einen Datenschutzbeauftragten, ist nicht möglich, da die Geschäftsleitung letztlich Budget, Strategie und Zweck der Datenverarbeitung vorgibt. Allenfalls kann die Umsetzung der DSGVO übertragen werden.

Im Ereignisfall kommunizieren

Damit bei einem Ereignis richtig gehandelt wird, ist es Aufgabe des Risikomanagements, die Notfallplanung, die Krisenkommunikation und klare Verantwortlichkeiten vorzubereiten. Die Melde- und Analysestelle Informationssicherung MELANI des Bundes empfiehlt im Falle von Datenabflüssen generell eine möglichst hohe Transparenz gegenüber den betroffenen Kunden.

Es ist wichtig, dass die Kommunikation rasch erfolgt. Damit die Massnahmen zur Schadenminderung erfolgreich sind, muss die Organisation allfällige Ereignisse periodisch üben und die Notfallpläne kontinuierlich anpassen und weiterentwickeln.

Von zentraler Bedeutung ist ein ehrliches Risikomanagement, d.h. keines der Risiken kleinzureden oder sich von der Illusion einer Kostenersparnis blenden zu lassen.

Ein unerwünschter Datenabfluss führt nicht nur zu mehr Aufwand und Kosten, sondern kann die Reputation einer Organisation oder Firma nachhaltig schädigen. Darüber hinaus sieht die DSGVO vor, Verstösse mit Geldbussen von bis zu 4 % des gesamten weltweit erzielten Umsatzes im vorangegangenen Geschäftsjahr zu bestrafen.

Fazit: Synergien nutzen

Informationssicherheit und Risikomanagement sind nicht delegierbare Führungsaufgaben, wobei sich ihre Analysenmethoden unterscheiden. Da sich für die Entscheide der Führungsspitze grundsätzlich nur der Top-down-Ansatz eignet, ist der Koordinationsbedarf zwischen beiden Systemen relativ gross. Gelingt jedoch dieses wichtige Zusammenspiel zwischen Informationssicherheit und Risikomanagement, können mehrfache Synergien genutzt und spürbarer Mehrwert erzielt werden: Die Geschäftsleitung empfindet die Instrumente nicht länger als lästige Bürokratie, sondern als wertvolle Entscheidungshilfen.

In einer gemeinsamen Berichterstattung kann so Know-how kombiniert genutzt werden. So kann die Geschäftsleitung effizient und gestützt auf optimalen Grundlagen entscheiden, wie mit den Risiken der Informationssicherheit umgegangen werden soll. ■

Das Datenschutzniveau der Schweiz

Das heute in der Schweiz bestehende Datenschutzgesetz aus dem Jahr 1992 ist weder zeitgemäss noch entspricht es den Anforderungen der EU. Der Bundesrat hat daher Anpassungen an die technologische und gesellschaftliche Veränderung erarbeitet. Aufgrund der Komplexität der Materie wurde die Totalrevision jedoch entschlackt. Deshalb werden zurzeit in der parlamentarischen Beratung die neuen Anforderungen durch das Schengen-/Dublin-System sowie weitere Äquivalenzanforderungen der EU diskutiert (das Recht auf Vergessenwerden; Datenverarbeitung ausschliesslich nach ausdrücklicher Einwilligung der betroffenen Person; das Recht auf Datenübertragbarkeit an einen anderen Dienstleister; das Recht der Betroffenen, bei Verletzung des Schutzes der eigenen Daten darüber informiert zu werden). Ein rasches Handeln des Parlamentes auf diesem Gebiet ist wichtig. Andernfalls könnte die Schweiz u.a. die Anerkennung als Drittstaat mit einem angemessenen Datenschutzniveau in der EU verlieren. (heyne)

Dieser Fachartikel erscheint in einer MQ-Serie, die von Experten und Expertinnen des «Netzwerk Risikomanagement» beigesteuert wird: www.netzwerk-risikomanagement.ch.