Informationssicherheit: Organisation vor Technik!

Zu häufig wird die Informationssicherheit allein mit technischen Lösungen angegangen. Doch dies allein genügt nicht. Informationssicherheit ist in erster Linie eine Frage der Organisation.

VON **HANS HALSTRICK** UND **KARSTEN M. DECKER**

Sie kennen die Situation: Das Unternehmen weiss um seine schützenswerten Informationen und investiert zunächst einmal in Technik. Die IT erhält eine Firewall, Backup-Lösung, Virenschutz und Intrusion Detection müssen her. Das Gebäude bekommt ein Zutrittskontrollsystem, die Eingänge werden mit Video überwacht. Und plötzlich ist das Budget erschöpft. Dabei hat man gar nicht berücksichtigt, dass die Kollegen üblicherweise ihre Projekte auf der Fahrt zum Kunden diskutieren, umweltfreundlich und nervenschonend in der Bahn, aber gefährlich, da es viele unbekannte Zuhörer gibt. Sie nehmen dabei wie selbstverständlich alle Geschäftsdaten auf der lokalen Festplatte ihres Laptops mit – man muss ja die Zeit nutzen und die Funkverbindung ist zu instabil – und die gesamte Kundendatei ist auf dem Smartphone, unverschlüsselt natürlich und ohne Passwortschutz!

Gefährliche Giesskannenpolitik

Natürlich braucht die IT eine Firewall, einen Virenschutz, ein Backup-System etc. Aber inwieweit sich diese technologiegetriebenen Massnahmen angemessen an den Geschäftszielen orientieren und kosteneffizient sind, ist unbekannt, das Budget ist schnell verbraucht und unzählige andere Löcher bleiben offen. Das Schlimme ist, man weiss es nicht einmal, man ahnt es höchstens! Eine solche Giesskannenpolitik ist bei der Informationssicherheit gefährlich und teuer. Die Organisation wird immer weitere Lücken entdecken und immer mehr Geld für deren Beseitigung ausgeben müssen.

Methodik muss sein

Begegnen kann man dem nur mit einer strukturierten, methodischen Vorgehensweise. Die ISO 27002 bietet da Unterstützung. Dieser Standard beschreibt mit Best Practices, wie eine Organisation jeglicher Grösse ein funktionierendes Informationssicherheitsmanagementsystem aufbauen kann. Herzstück des Systems ist ein Risikomanagement. Die Abb. zeigt, dass die organisatorischen Aspekte bei Weitem überwiegen. Die Technik wirkt unterstützend, beseitigt aber keine methodischen Defizite.

VORGEHENSWEISE BEIM AUFBAU EINES ISMS

- Geltungsbereich bestimmen
- ISMS-Politik bestimmen
- Risikobeurteilung durchführen
- Umgang mit Risiken aufzeigen
- Massnahmen für den Umgang mit Risiken definieren
- Verbleibende Risiken formell akzeptieren
- System einführen
- Messen und weiterentwickeln

Informationssicherheit ist Chefsache

Wie auch bei anderen Managementsystemen ist Informationssicherheitsmanagement in der Verantwortung der obersten Leitung der Organisation. Sie muss sicherstellen, dass Informationen bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit angemessen geschützt werden. Im Schadensfall muss die oberste Leitung gemäss Gesetz haften. Die operative Tätigkeit (Aufbau, Überwachung, Überprüfung und Pflege des Systems) wird meist an einen entsprechend ausgebildeten Mitarbeitenden delegiert. Doch wie fängt er das an? Der Aufbau eines Informationssicherheitsmanagementsystems (ISMS) ist grundsätzlich nicht schwierig. Das schematische Vorgehen ist im Kasten «Vorgehensweise beim Aufbau eines ISMS» dargestellt. Besitzt die Organisation bereits ein Managementsystem, kann man darauf aufbauen und die zusätzlichen Massnahmen in die existierenden und erprobten Prozesse einbauen.

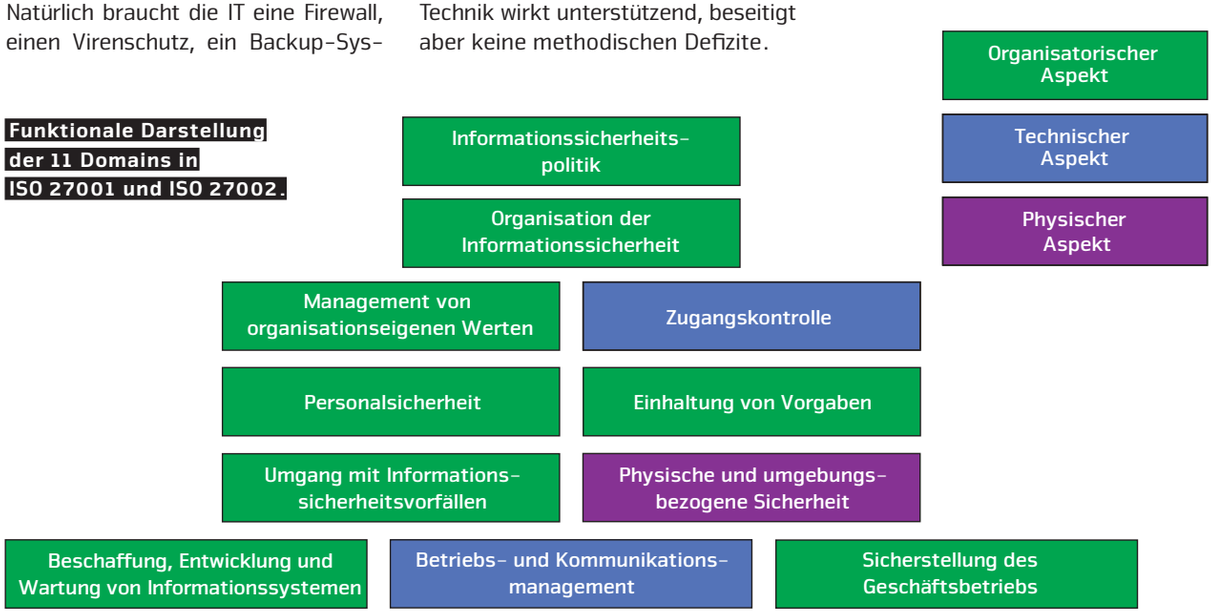
Am Anfang steht der Wert

Zunächst listet man alle organisationseigenen Werte innerhalb des Fokus der Informationssicherheit auf. Dabei muss beachtet werden, dass hier nicht nur die Informationen selber gemeint sind, sondern auch die Informationsträger, z.B.: die Server, die Datenleitung, das Smartphone, der USB-Stick, ausgedruckte Schriftstücke und nicht zuletzt das gesprochene Wort, wobei wir wieder bei unserem Beispiel der Unterhaltung im Zug wären.

Risikobeurteilung

Ist diese Liste erstellt, führt man die verbleibenden Schritte der Risikobeurteilung gemäss Kasten auf Seite 31 (unten) durch. Dabei ist Erfahrung gefragt, denn sonst kommt man gar nicht auf die Idee, was alles passieren kann. Hilfreich ist da der Beizug verschiedener interner Personen mit unterschiedlichem Erfahrungshintergrund oder auch externe professio-

Funktionale Darstellung der 11 Domains in ISO 27001 und ISO 27002.



«Organisatorische Aspekte überwiegen. Die Technik wirkt unterstützend, beseitigt aber keine methodischen Defizite.»

nelle Hilfe. Es ist unerheblich, welche Methode dabei eingesetzt wird, sie muss nur beschrieben und eingehalten werden. Als praktikabel hat sich die «Zurich Hazard Analysis» erwiesen, in der Eintrittswahrscheinlichkeit und Schadensausmass in einem Fünf-Stufen-Schema bewertet und in ein xy-Diagramm übertragen werden. Befinden sich die Risiken in einem Feld jenseits der Schmerzgrenze, muss gehandelt werden. Dabei legt die Organisation selber fest, wo diese Schmerzgrenze liegt. Diese Methode setzt z.B. auch die SUVA ein.

Vertraulichkeit – Integrität – Verfügbarkeit

Die Vertraulichkeit der Daten ist nur eine Sichtweise. Nicht minder wichtig sind die Integrität, also die Unverletzbarkeit, und die Verfügbarkeit der Informationen. In diesem Spannungsfeld bewegt sich die Informationssicherheit. Damit kommt es logischerweise zu Konflikten. Daten, die immer und überall verfügbar sein müssen, sind bezüglich ihrer Vertraulichkeit nur mit grossem Aufwand zu schützen. Sehr häufig ist sogar gerade die Verfügbarkeit das wichtigste Kriterium. Denken wir an einen produzierenden Betrieb, der mit allgemein bekannten Technologien fertigt. Wird die Fertigung durch Feuer oder Wasser zerstört, was immer eine reale Bedrohung ist, findet sich meist ein Lohnfertiger, der die Produktion übernimmt. Der finanzielle Schaden ist in der Regel durch eine Versicherung gedeckt. Werden aber die Daten (z.B. CAD, Maschinendaten) zerstört, dann hat er nichts mehr zu produzieren.

Risikobehandlung: Nullrisiko ist nicht das Ziel

Die erste Frage lautet: Wo sind meine Top-5-Risiken? Und da liegt der entscheidende Vorteil gegenüber dem Giesskannenprinzip. Kaum eine Organisation hat die Mittel, alle zu behandelnden Risiken gleichzeitig auf ein vertretbares Mass zu reduzieren. Also widmet sie sich zunächst den grössten Risiken und behandelt die nächsten anschliessend.

CHECKLISTE INFORMATIONSSICHERHEIT

- Unser Verwaltungsrat sowie die Geschäftsleitung haben die Bedeutung der Informationssicherheit für die Zukunft unseres Unternehmens klar erkannt. Sie nehmen ihre Verantwortung aktiv wahr und stellen die erforderlichen Ressourcen zur Verfügung.
- Alle Mitarbeitenden sind aufgabengerecht für das Thema Informationssicherheit sensibilisiert, ausgebildet und geschult. Sie haben dessen Bedeutung für die Zukunft unseres Unternehmens verstanden, anerkennen die Regelungen, setzen diese im Arbeitsalltag um und behalten sie auch dauerhaft bei.
- Sämtliche Risiken, die bei der Verarbeitung, Speicherung, Archivierung, Übertragung, Versendung, Bearbeitung sowie der Verwendung durch Systeme, Einrichtungen, Geräte, Geschäftsprozesse und unsere Mitarbeitenden entstehen, haben wir aktuell, systematisch und abschliessend bestimmt.
- Sämtliche Massnahmen zum risikogerechten Schutz unserer organisationseigenen Werte im Fokus der Informationssicherheit sind in unsere Geschäftsprozesse integriert.
- Die Risikobeurteilung wird bei uns mindestens einmal pro Jahr überprüft und bei Bedarf angepasst.
- Alle Investitionen zum Schutz unserer IT-Systeme werden ausschliesslich auf der Basis unserer Geschäftsziele unter Verwendung der Risikobeurteilung begründet; technologiegetriebene Investitionen gibt es bei uns nicht.
- Massnahmen zum Schutz von Systemen, die Risiken ausgesetzt sind, die unter den Akzeptanzwerten liegen, werden wissentlich nicht umgesetzt.
- Wenn Sie all diese Punkte bejahen können, ist Ihre Organisation punkto Informationssicherheit bestens aufgestellt.

RISIKOBEURTEILUNG: DIE EINZELNEN SCHRITTE

- Organisationseigene Werte im Fokus der Informationssicherheit bestimmen
- Für jeden dieser Werte Risikoquellen wie Bedrohungen und Schwachstellen systematisch identifizieren
- Für jedes Ereignis, bei dem eine Bedrohung auf eine Schwachstelle einwirkt und damit die Vertraulichkeit, Integrität oder Verfügbarkeit gefährdet, die Eintrittswahrscheinlichkeit und den resultierenden Effekt (das Schadensausmass) abschätzen, und so das dazugehörige Risiko bestimmen
- Die so ermittelten Risiken mit unternehmensspezifischen Richtwerten verglichen, um die Bedeutung der Risiken für das Unternehmen zu bestimmen

«Es gibt nicht das System für das Informationssicherheitsmanagement, es gibt auch keine Branchenlösung.»

Die zweite Frage lautet: Wie reduziere ich die Risiken auf ein vertretbares Mass? Ziel muss es sein, durch geeignete Massnahmen Eintretenswahrscheinlichkeit und/oder den resultierenden Schaden so weit zu reduzieren, dass der Erlebensfall die Organisation nicht substanziell gefährdet. Diese Restrisiken sind wieder zu bewerten. Man sollte sie dann unbedingt von der obersten Leitung des Unternehmens verabschieden lassen, denn Geschäftsleitung und Verwaltungsrat sind im Schadensfall haftbar. Der Verwaltungsrat ist es ja auch, der zunächst einmal die Risikoaversion und den Risikoappetit, der mit Chancen korreliert, definieren muss.

Die bereits erwähnte ISO 27002 gibt uns ebenfalls gedankliche Anstösse für die Risikobehandlung. Z.B. empfiehlt sie, Regeln für den Umgang mit Informationen aufzustellen und das Bewusstsein der Mitarbeitenden für Informationssicherheit zu wecken und kontinuierlich weiterzuentwickeln. So könnte diese Organisation erreichen, dass ihre Mitarbeiter Projekte in der Öffentlichkeit nicht mehr diskutieren.

Massnahmen müssen wirksam sein

Das Umfeld ändert sich kontinuierlich und somit auch die Bedrohungslage, und das in zunehmend höherer Kadenz. Auch die Schwachstellen ändern sich in der Regel. Deshalb muss die Risikobeurteilung ein immer wiederkehrender Prozess sein. Neue Risiken sind zu identifizieren, bestehende neu zu bewerten und die Massnahmen auf ihre Wirksamkeit zu prüfen. Letzteres geschieht am besten durch Audits, interne sowie externe.

Jedes System ist individuell

Es gibt nicht das Informationssicherheitsmanagementsystem, es gibt auch keine Branchenlösung. So wie jede Organisation einzigartig ist, muss auch das Informationssicherheitsmanagementsystem einzigartig sein. Dieses kann dann nach ISO 27001:2005 zertifiziert werden. Durch den risikobasierten Ansatz sind die beiden Standards ISO 27001 und 27002 auf jede Organisation jeglicher Grösse und Branche anwendbar. Die Zertifizierung gibt der Organisation die Sicherheit, durch ihr Risikomanagement und wirksame Massnahmen alles Notwendige zu tun, um Pannen in der Informationssicherheit zu vermeiden.

Wirksames Risikomanagement ist Selbstschutz

Wie oben gesagt gibt es kein Nullrisiko, und es kann immer noch etwas passieren. Dennoch ist die Organisation dann in der besseren Position, denn sie weiss, wie sie reagieren muss: Plan B tritt in Kraft. Und sollte es zu einem Verfahren kommen, können Organisation und oberste Leitung nachweisen, was sie alles unternommen haben, um diese Panne zu vermeiden. Der Vorwurf der Fahrlässigkeit ist dann vom Tisch. ■■■■

Dipl.-Ing. (TU) Hans Halstrick ist Produktmanager ISO 27001 bei Swiss TS Technical Services AG, Wallisellen.
PD Dr. Karsten M. Decker ist CEO von Decker Consulting GmbH, Rotkreuz.