Quelle: shutterstock

Drahtseilakt – ohne Organisation ist alles nichts!

Die Situation ist bekannt: Eine Organisation weiss um ihre schützenswerten Informationen und investiert zunächst einmal in Technik. Doch dies allein reicht noch lange nicht.

HANS HALSTRICK, KARSTEN M. DECKER

Erst erhält die IT 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 ihrem Laptop 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!

Was ist passiert?

Die Organisation hat Schwachstellen identifiziert und diese behoben, wie so oft mit einer technischen Lösung. Natürlich braucht die IT eine Firewall, Virenschutz, Backup-Systeme etc. Aber inwieweit sich diese technologiegetriebenen Massnahmen angemessen an den Organisationszielen 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 methodischen Vorgehensweise. Der Standard ISO/IEC 27001:2005 beschreibt die Anforderungen an ein Managementsystem für Informationssicherheit und stellt auch eine Struktur zur Verfügung, wie man es gründen, implementieren, betreiben, überwachen, überprüfen und kontinuierlich verbessern kann. Herzstück des Systems ist das Risikomanagement der Informationswerte, das mit dem organisationsweiten Risikomanagement koordiniert wird. Dieser risikobasierte Ansatz garantiert, dass Informationen auf eine Weise geschützt aber auch verfügbar gemacht werden, wie dies für die Organisation angemessen ist. Der Ansatz steuert also die Auswahl von Massnahmen und deren Implementierung. Ein Zuviel-des-Guten wird so vermieden. Dadurch wird Informationssicherheit für Organisationen jeglicher Grösse erschwinglich. Mit welchen Massnahmen eine wirksame Informationssicherheit erreicht werden kann, ... beschrieben. Kästchen 1 zeigt, dass die organisatorischen Aspekte bei Weitem überwiegen. Die Technik wirkt unterstützend, beseitigt aber keine methodischen Defizite. A von ISO/IEC 27001:2005 beschrieben.

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 Verantwortung (Gründung, Implementierung, Betrieb, Überwachung, Überprüfung und kontinuierliche Verbesserung des Systems) wird meist an einen entsprechend ausgebildeten Mitarbeitenden delegiert. Doch wie fängt dieser das an?

Wichtig ist zunächst die Integration in die organisationseigenen Abläufe. Verfügt eine Organisation bereits über ein Managementsystem, kann man darauf aufbauen und die zusätzlichen Massnahmen in die existierenden und erprobten Prozesse einbauen. Hat sie das nicht, müssen die Prozesse erst beschrieben werden.

Als Nächstes gilt es, den Geltungsbereich des Informationssicherheitsmanagementsystems (ISMS) ganz genau zu beschreiben und die ISMS-Politik festzulegen, welche die Ziele, Prinzipien und allgemeinen Verantwortlichkeiten für das ISMS beschreibt und regelt. In dieser Politik wird auch festgehalten, welche grundsätzliche Haltung die Organisation zu Risiken im Bereich der Informationssicherheit einnimmt. Bei der Bewältigung dieser beiden wichtigen Punkte ist ISO/IEC 27003:2010 (Anleitung zur Implementierung eines Informationssicherheitsmanagementsystems) behilflich.

Risikobeurteilung in drei Schritten: identifizieren, analysieren, bewerten

Bei der Risikoidentifikation bestimmt man zunächst alle Informationswerte, d.h. die Vermögenswerte von Bedeutung für die Informationssicherheit im Geltungsbereich des ISMS. Dabei muss beachtet werden, dass hier nicht nur Informationen selber inkl. des gesprochenen Worts gemeint sind, sondern auch die Geschäftsprozesse und alles, was zur Verwaltung und Bearbeitung von Informationen jeglicher Art notwendig ist – Server; mobile Geräte aller Art wie Laptops, Notebooks, Smartbooks, Netbooks, Tablet PCs, PDAs und Smartphones; Geräte wie Drucker, Faxmaschinen und Fotokopierer; Datenträger inkl. Papier und Software aller Art; Netzwerkkomponenten wie Modems, Router und Datenleitungen; die Mitarbeitenden, von der Geschäftsleitung bis zum Reinigungspersonal; der Standort inkl. aller Räumlichkeiten und erforderlichen Services und Betriebsmittel.

Identifikation

Ist diese Liste erstellt, ermittelt man die Schwachstellen, die diesen Informationswerten zu eigen sind, sowie alle Bedrohungen, die auf diese Schwachstellen einwirken und diese somit ausnutzen können. Eine Aufstellung aller möglichen Vorfallszenarien, d.h. aller Kombinationen, bei denen Bedrohungen auf Schwachstellen einwirken, sowie eine textuelle Beschreibung der daraus resultierenden Folgen schliessen die Risikoidentifikation ab.

Analyse

Bei der nachfolgenden Risikoanalyse beurteilt man für jedes einzelne Vorfallszenario die Auswirkung auf die Tätigkeit der Organisation, die Häufigkeit des Eintretens und bestimmt das daraus resultierende Risikoniveau. Bei der Analyse der Auswirkung kommen genau definierte Risikoauswirkungskriterien zum Einsatz, die man z.B. dem organisationsweiten Risikomanagement entlehnen kann.

Bewertung

Im abschliessenden Schritt der Risikobewertung werden die zuvor bestimmten Risikoniveaus mit genau definierten Kriterien für die Risikobewertung und die Risikoakzeptanz verglichen. Als Ergebnis liegt nun eine Liste von Risiken vor, die relativ zu den Bewertungskriterien priorisiert sind. Auch bei den Kriterien für die Risikobewertung und -akzeptanz kann man auf diejenigen des organisationsweiten Risikomanagements zurückgreifen, um Konsistenz zu gewährleisten.

Informationssicherheitsmanagement gehört in die Verantwortung der obersten Leitung der Organisation. Quelle: shutterstock

Liste der elf Abschnitte von ISO/IEC 27001:2005, Anhang A

- Sicherheitspolitik
- Organisation der Informationssicherheit
- Management der Informationswerte
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit
- Management der Kommunikation und des Betriebs
- Zugriffskontrolle
- Beschaffung, Entwicklung und Wartung von Informationssystemen
- Management von Informationssicherheitsvorfällen
- Business Continuity Management
- Compliance

Kästchen 1: Massnahmen für eine wirksame Informationssicherheit, die 11Abschnitte von ISO/IEC 27001:2005, Anhang A.

Über die Ausgestaltung der Risikoakzeptanzkriterien steuert man auch, welche Risiken man überhaupt behandeln will. Nullrisiko ist ja nicht das Ziel, denn einerseits kann jede Organisation gewisse Risiken tragen, andererseits gibt es in der Regel nie genügend Mittel, um alle tatsächlich zu behandelnden Risiken gleichzeitig auf ein vertretbares Mass zu reduzieren. Also widmet man sich zunächst den grössten Risiken und behandelt die nächstwichtigeren anschliessend. Dank der methodischen Risikobeurteilung können jeder Entscheid zur Behandlung eines Risikos und die damit verbundene Mittelzuweisung ohne Weiteres mit den Auswirkungen auf die Tätigkeit der Organisation begründet werden. Das ist beim Giesskannenprinzip für die Freigabe einzelner, isolierter technischer Massnahmen völlig unmöglich.

Erfahrung ist wichtig

Bei der Risikobeurteilung ist Erfahrung gefragt, denn sonst kommt man gar nicht auf die Idee, was alles passieren kann. Auch ist die Festlegung der Kriterien für Risikoauswirkung, -bewertung und -akzeptanz in der Regel nicht einfach. Hilfreich ist da, verschiedene interne Personen mit unterschiedlichem Erfahrungshintergrund oder auch externe professionelle Hilfe beizuziehen. Auch das Studium des Standards ISO/IEC 27005:2011 (Informationssicherheitsrisikomanagement) ist hier empfohlen.

Risikobehandlung

Ziel muss sein, durch geeignete Massnahmen die Häufigkeit des Eintretens eines Risikos und/oder den resultierenden Schaden so weit zu reduzieren, dass im Eintrittsfall die Organisation nicht substanziell gefährdet ist. Die aus der Be-

handlung resultierenden Restrisiken sind wieder zu bewerten. Man sollte sie dann unbedingt von der obersten Leitung der Organisation 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.

Massnahmen müssen angemessen und wirksam sein

Bei der Auswahl geeigneter Massnahmen, die zugleich angemessen und wirksam sind, ist wieder Erfahrung gefragt. Darüber hinaus leistet der Standard ISO/IEC 27002:2005 (Leitfaden für das Management der Informationssicherheit) wertvolle Hilfestellung. Um z.B. dem eingangs geschilderten Verhalten in der Öffentlichkeit wirksam zu begegnen, empfiehlt ISO/IEC 27002:2005, eine verbindliche Richtlinie für die Nutzung von mobilen Geräten und Wechseldatenträgern zu verabschieden, das Bewusstsein der Mitarbeitenden für Informationssicherheit zu wecken, kontinuierlich weiterzuentwickeln und die Mitarbeitenden entsprechend auszubilden und zu schulen. So kann eine Organisation erreichen, dass ihre Mitarbeiter Projekte in der Öffentlichkeit nicht mehr diskutieren.

Auch im Zusammenhang mit den heute aggressiv vermarkteten Dienstleistungen wie «Software as a Service» (SaaS), «Platform as a Service» (PaaS) oder «Infrastructure as a Service» (IaaS), häufig salopp unter dem Begriff Cloud Computing zusammengefasst, bietet ISO/IEC 27002:2005 praktische Unterstützung. Grundsätzlich handelt es sich hierbei ja um die Auslagerung eines oder mehrerer Services. Also gilt es, zunächst ein Service Level Agreement (SLA) vertraglich zu vereinbaren. Typischerweise haben die SLAs der Anbieter aber hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität unzureichen-den Detaillierungsgrad und/oder zu wenig Präzision. Mit dem Versprechen eines verschlüsselten Kommunikationskanals oder eines sicheren Authentifizierungsverfahrens ist es nicht getan. Denn was weiss man dann schon über den Betrieb von Netzwerk, Servern oder Anwendungen? Wie ist etwa das interne Netzwerk ausgebildet? Werden hinreichende Kapazitäten zur Verfügung gestellt, und wie werden diese überwacht sowie bei Bedarf aktiv nachgeführt? Wie sind die Verantwortlichkeiten für den Betrieb und die Zugriffsrechte der Administratoren geregelt? Welche Machtkonzentrationen gibt es? Bei all diesen Fragen bietet ISO/IEC 27002:2005 praktische Empfehlungen. Und selbst wenn das SLA all diese Fragen zufriedenstellend adressieren sollte, kann man bestenfalls schliessen, dass seitens des Service-Anbieters angemessene Massnahmen getroffen worden sind. Ob diese auch wirksam sind, weiss man dabei noch lange nicht. Deswegen empfiehlt ISO/IEC 27002:2005, zusätzlich ein entsprechendes Berichtswesen und das Recht zur Durchführung formaler Audits vertraglich zu vereinbaren sowie die Services kontinuierlich zu überwachen, periodisch zu überprüfen und zu auditieren.

Kontinuierliche Verbesserung tut Not

Das Umfeld ändert sich kontinuierlich und somit auch die Bedrohungslage. Und das mit zunehmend höherer Kadenz. Neue Informationswerte kommen hinzu, andere entfallen. Auch die Schwachstellen ändern sich in der Regel. Deshalb müssen die Aktualisierung der Informationswerte, die Risikobeurteilung und die Risikobehandlung ein immer wiederkehrender Prozess sein. Neue Risiken sind zu identifizieren, bestehende neu zu bewerten und die Massnahmen auf ihre Wirksamkeit zu prüfen.

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/IEC 27001:2005 zertifiziert werden. Durch den risikobasierten Ansatz ist ISO/IEC 27001:2005 auf Organisationen jeglicher Grösse und Branchen anwendbar. Die Zertifizierung durch eine anerkannte Zertifizierungsstelle gibt der Organisation die Gewissheit, durch ihr Risikomanagement und wirksame Massnahmen alles Notwendige zu tun, um Pannen in der Informationssicherheit zu vermeiden.

Wirksames Risikomanagement ist Selbstschutz

Wie beschrieben, gibt es kein Nullrisiko, und es kann immer noch etwas passieren. Dennoch ist die Organisation dann in einer besseren Position. Sie ist gut vorbereitet und weiss genau, 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.

Der Mitinhaber und Geschäftsführer eines mittelgrossen und nach ISO/IEC 27001:2005 zertifizierten Unternehmens beantwortete die Frage nach dem Warum so: «Ich will nachts ruhig schlafen können.» Ein nachvollziehbarer Grund. ■

Die Autoren: Hans Halstrick, Zertifizierter ISO/IEC 27001:2005 Lead Auditor, ist Produktmanager ISO 27001 bei der Swiss TS Technical Services AG, Wallisellen. PD Dr. Karsten M. Decker, Zertifizierter ISO/IEC 27001:2005 Lead Auditor und akkreditierter Trainer für Informationssicherheit, ist CEO der Decker Consulting GmbH, Rotkreuz.

DIGICOMP

Drive your life.

SECURITY
Powered by Digicomp

Security Zertifizierungen – Wie sicher ist Ihre berufliche Zukunft?

Zertifizieren Sie Ihr Wissen mit einem international anerkannten Abschluss mit Sicherheit bei Digicomp.
Bei Digicomp gibt es neu die gesamte Security Zertifizierungspalette aus einer Hand. Das bedeutet: Sicherheit für Ihre Bildung!

HAK	Hackerfähigkeiten für Systemadministratoren (HAK)	31.10.11	16.01.12 (ZH od. BE)
CEH	Certified Ethical Hacker (CEH)	08.–14.12.11	28.03.–03.04.12 (ZH od. BE)
CHFI	Computer Hacking Forensic Investigator (HFI)	30.09.–06.10.11	16.–22.12.11 (ZH, BE)
LPT	EC-Council Certified Security Analyst/Licensed Penetration Tester (ESA)	16.–22.11.11	02.–08.05.12 (ZH, BE)

Checkpoint und Jupiter Kurse bald verfügbar!

www.digicomp.ch/security

Digicomp Academy AG, Telefon 0844 844 822, www.digicomp.ch
Zürich, Bern, Basel, St. Gallen, Luzern, Genève, Lausanne, Bellinzona

EDUQUA