Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 80 (2002)

Heft: 9

Artikel: Service Management und Sicherheit

Autor: Oswald, Philipp / Schwyter, Fredy

DOI: https://doi.org/10.5169/seals-877237

Network Solution

Service Management und Sicherheit

Das Bewusstsein für Informationssicherheit ist in den meisten Betrieben innerhalb des letzten Jahres stark gestiegen. In Chefetagen wird offen über Verbesserungen der Informationssicherheit im Unternehmen gesprochen.

Der Wille zur Verbesserung ist vorhanden. Wie soll das Vorhaben nun möglichst wirkungsvoll und vollständig umgesetzt werden?

PHILIPP OSWALD UND
FREDY SCHWYTER

Die Unternehmens-Ressource «Information»

Informationen sind im heutigen Geschäftsumfeld eine genauso elementare Ressource wie Mitarbeiter oder Finanzen. Dabei hat der Verlust von Informationen mindestens so gravierende Auswirkungen wie eine Einschränkung in der Verfügbarkeit anderer Ressourcen. Aber Informationen sind oft grösseren, unsichtbaren Risiken ausgesetzt. Die Zuständigkeit für angepasste Massnahmen zum Schutz der Informationen wurde auch gesetzlich geregelt. Der Gesetzgeber hatte zwar bei der Schaffung der entsprechenden Gesetze nicht in erster Linie den Schutz der Informationen im Auge, sondern den Schutz von Arbeitnehmern und Investoren. Da aber die Informationssicherheit untrennbar mit dem Geschäftserfolg verbunden ist, gilt die Verantwortung auch für den Schutz der Informationen. In diesen Gesetzen wird die Verantwortung von Verwaltungsrat und Geschäftsleitung klar festgehalten.

Was sagen die Gesetze?

OR 754: Die Mitglieder des VR und der GL sind für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.
Abs. 2: Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.

IT-Sicherheit oder Informationssicherheit?

In Diskussionen mit Topmanagern wird sehr oft das hohe Sicherheitsniveau der IT-Infrastruktur hervorgehoben. Im Gespräch merkt der Experte, dass damit die IT-Sicherheit gemeint ist. Informationssicherheit ist aber wesentlich mehr und umfasst nebst der mehr technisch orientierten IT-Sicherheit in erster Linie die strategisch-konzeptionellen Aspekte. Hierfür ist es notwendig, die Geschäftsprozesse, die Organisation und die Mitarbeiter in die Untersuchungen mit einzubeziehen. Gut definierte und dokumentierte Geschäftsprozesse helfen dabei enorm. Aufwändiger werden Risikoanalysen, wenn keine diesbezügliche Dokumentation darüber existiert. Bei den Analysen muss primär auf die Aussagen von beteiligten Mitarbeitern abgestellt werden, und dabei sind die eigene Interpretation und Zuverlässigkeit kritische Faktoren. Grundsätzlich müssen Geschäftsprozesse in dem Sinn gesichert werden, dass die betroffenen Informationen geschützt werden. Deshalb ist das Wissen um die relevanten Geschäftsprozesse unabdingbar.

Ausarbeitung einer Sicherheitsstrategie

Die Festlegung einer Sicherheitsstrategie ist Aufgabe des Verwaltungsrats und der Geschäftsleitung. Erfahrene Spezialisten, welche die Branche, die Gefahren und

Bild 1. Unsere Gesellschaft basiert in weiten Bereichen auf dem sicheren Funktionieren von Telekommunikations-Einrichtungen.

das Geschäftsumfeld kennen, können dazu wertvolle Hilfe leisten.
Folgende Aufgaben sollten nicht an subalterne Stellen delegiert werden:
- Das Formulieren klarer Zielsetzungen
- Die Definition der Wege zum Erreichen des Ziels
- Das Abschätzen der notwendigen Budgets und der personellen Ressourcen
- Das Bestimmen des notwendigen Controllings, um die Einhaltung der Sicherheitsstandards zu überwachen

Die Sicherheitsstrategie muss in einer glaubwürdigen Form an die Mitarbeiter kommuniziert werden. Dies ist nicht zuletzt dann ein ausschlaggebender Faktor, wenn es um das Engagement und die Motivation der Mitarbeiter geht. Zur Umsetzung der Sicherheitsstrategie bedarf es klarer Richtlinien, die anwendbar und überprüfbar sind. Dabei darf ohne weiteres ein Vorgehen in mehreren Schritten und eine Priorisierung der Etappen gewählt werden. Es ist aber wichtig, dass nicht ein Stückwerk von isolierten Bereichen eingeführt wird, sondern eine ganzheitliche Sicherheitsstrategie. Eine Konzentration auf einzelne Informationssicherheitsbereiche führt unweigerlich zu Sicherheitslücken, die meistens schwierig zu lokalisieren und zu eliminieren sind.

Systematik durch Systems Engineering

Systems Engineering ist eine weltweit anerkannte Problemlösemethodik. Sie hilft, Probleme und Aufgaben systematisch und strukturiert zu analysieren und sinnvolle Lösungsvarianten zu erarbeiten. Systems Engineering wird an der ETH Zürich unterrichtet.
Eine umfassende Systematik ist auch im Sicherheitsbereich von elementarer Bedeutung. Der «Systems Engineering Approach» bildet dazu eine gute Grundlage. Systems Engineering ist eine systematische Anwendung von Methoden und kann kein Ersatz für Ausbildung und Erfahrung sein. Die wichtigsten Schritte im klassischen Systems Engineering sind wie folgt:
- Situations-Analyse
- Zielformulierung
- Lösungssuche
- Lösungsentwicklung
- Umsetzung

Effektives Management heisst führen

In der Praxis der Informationssicherheit hat es sich bewährt, dass das Management klar führt. Dazu gehören einige wichtige Punkte, ohne die eine Verantwortung nicht wahrgenommen werden kann:
- Auf Konsistenz in den Richtlinien achten
- Die Übereinstimmung mit den Firmenzielen im Auge behalten
- Die Richtlinien gutheissen
- Die Richtlinien unterschreiben
- Die Umsetzung der Sicherheitsrichtlinien veranlassen
- Die Umsetzung der Sicherheitsrichtlinien kontrollieren

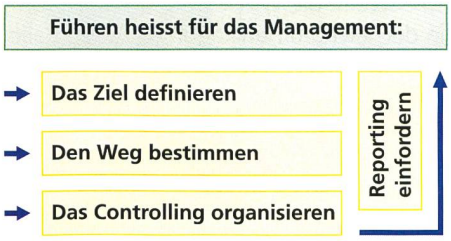

Bild 2. Effektives Management heisst Führen.

Inhalt von Sicherheitsrichtlinien

Die Sicherheitsrichtlinien (Security Policy) bilden den Kern der Informationssicherheit in einem Unternehmen. Darin sind konkrete und umsetzbare Aufgaben und Ziele beschrieben, die Zuständigkeiten für die verschiedenen Verantwortlichkeiten definiert. Zudem ist darin enthalten, über welche Informationskanäle was rapportiert werden muss. Die Sicherheitsrichtlinien sind für alle Mitarbeiter verbindlich und sollten dementsprechend verständlich formuliert sein. In den Ausführungsbestimmungen müssen alle wesentlichen Bereiche abgedeckt und konkrete Massnahmen verbindlich ausformuliert sein. Die Mitarbeiter müssen sich schriftlich verpflichten, die Richtlinien einzuhalten.

Beschluss des Managements

Wer soll Verantwortung für die Umsetzung der Informations-Sicherheitsstrategie übernehmen? Gemäss den gesetzlichen Anforderungen, kann sich der Verwaltungsrat und die Geschäftsleitung dieser Verantwortung nicht entziehen. Die Umsetzung erfordert in den meisten Fällen eine Ergänzung in der Organisation, da selten die notwendigen Kontrollorgane vorhanden sind. Das Topmanagement muss also genügend Ressourcen und Budget zur Verfügung stellen und für die Einführung einen erfahrenen Projektleiter einsetzen. Dieser hat in erster Linie die Aufgabe, die erforderlichen Kontrollstrukturen und Reporting-Mechanismen zu entwickeln und umzusetzen sowie die nötige Ausbildung für das gesamte Kader zu planen und zu veranlassen. Im Idealfall wird dieser die Rolle des Sicherheitsbeauftragten übernehmen. Nur wenn alle notwendigen Vorkehrungen getroffen sind, kann sich das Management entlasten.

Wichtige Aspekte für einen reibungslosen Betrieb

Zu den organisatorischen Voraussetzungen gehören ein Sicherheitsverantwortlicher und eine Kontrollinstanz (internes Kontrollsystem, IKS). Das IKS ist für die laufende Überwachung der Sicherheitsmechanismen verantwortlich. Der Sicherheitsverantwortliche stellt einerseits die Kommunikation zum Topmanagement sicher, andererseits ist er Ansprechpartner für das IKS und für alle Mitarbeiter, wenn es um Meldungen von sicherheitsrelevanten Vorkommnissen geht. Der Sicherheitsverantwortliche plant und organisiert die sicherheitsrelevante Aus- und Weiterbildung für alle Mitarbeiter. Er hat klare Verantwortlichkeiten mit einem definierten Aufgabenkatalog im Rahmen der Sicherheitsrichtlinien. Bedingt durch den erhöhten Aus- und Weiterbildungsbedarf werden wiederum zusätzliche Ressourcen belegt. Das Budget ist den entsprechenden Aufgaben und Verantwortungen anzupassen. Die Sicherheitsorganisation ist als integraler Bestandteil der operationellen Organisation zu betrachten. Das IKS kann aber niemals ein Ersatz für ein sporadisches «Auditing» sein. Dieses hat den Zweck, die Funktionalität und Wirksamkeit der Sicherheitsmassnahmen zu überprüfen.

Regel zur Limitierung von Kosten

Ein bekannter Killer für fortschrittliche Informations-Sicherheitskonzepte ist die Perfektion. Dabei weiss jeder Eingeweihte, dass es hundertprozentige Sicherheit nicht gibt. In fast jeder Projektleiterausbildung wird heutzutage erwähnt, dass 80% einer möglichen Lösung für Informationssicherheit 20% der finanziellen Aufwände einer hypothetisch hundertprozentigen Sicherheit kosten. Zwischen 80 und 100% steigen die Kosten exponentiell. Wenn nun (wie fast überall) mit beschränkten Budgets ein Optimum an Sicherheit erreicht werden soll, dann ist es ratsam zu überlegen, wo

Sieben Tipps zur erfolgreichen Umsetzung

- Setzen Sie Spezialisten auf ihren Spezialgebieten ein. Schlecht ausgebildetes Personal ist dort gefährlicher als gar keines.
- Lassen Sie sich Sachverhalte erklären, bis Sie diese beurteilen können.
- Legen Sie Wert auf einen gut organisierten Betrieb.
- Erwarten Sie nicht, dass Technik allein Informationssicherheit bewirkt.
- Erkundigen Sie sich, wie viel Ihre geschäftskritischen Informationen wert sind.
- Verlangen Sie bei neuen Projekten integrierte Informations-Sicherheitskonzepte mit logischen Übersichten sowie Kosten-, Nutzen- und Ausbildungsaufstellungen.
- Glauben Sie nicht, dass Fehler verschwinden, wenn man nichts ändert.

die Sicherheit ohne Funktionseinbusse reduziert werden kann. Ähnliche Überlegungen stellen sich übrigens heute alle erfolgreichen Automobilhersteller.

Branchenspezifische Risiken und Benchmarks

Die Führungsübungen zum Schutz kritischer Informationsinfrastrukturen von Infosurance haben gezeigt, dass viele Risiken gewissen Geschäftsbereichen zugeordnet werden können. Somit ist es oft sinnvoll, vor der Realisierung grösserer Projekte einen Benchmark über die Lösungen bei vergleichbaren Unternehmen zu erstellen. Die Sache hat nur einen Haken: In solchen Benchmarks wird meist die gegenwärtige Situation erfasst. Wenn nun in einer Branche tief greifende Technologieveränderungen anstehen, wie beispielsweise die Wireless-Kommunikation in der Telekommunikation, dann sind alle Verantwortlichen gut beraten, wenn sie die Risiken solcher Veränderungen in den Benchmarks mit berücksichtigen.

Unterstützung durch Ausrüster

Für zukünftige Projekte ist es sinnvoll, den Leistungsumfang der Ausrüster genau zu beachten. Alcatel Schweiz AG beispielsweise liefert neu bei jeder grösseren Offerte einen Informationssicherheitsteil mit. Dieser beinhaltet als integralen Bestandteil ein Angebot zu einer Risikoanalyse mit einem sich daraus ergebenden Informations-Sicherheitskonzept. Dieses basiert auf der ISO-Norm 17799: «Code of practice for information security management». Interessant dabei ist, dass sich das Risk Assessment über die technologischen Sicherheitsaspekte ihrer Produkte hinaus auf die betroffenen Geschäftsprozesse des Kunden erstreckt und nicht nur auf zu liefernde Systemeinheiten. [4]

Philipp Oswald, *Dipl.-Ing., TS, NDS FH, Head of Security Solutions, Alcatel Schweiz AG, Leiter des Security Circel Telecom bei InfoSurance, Dozent an der «Swiss Network Academy», Zürich.*

Fredy Schwyter, *Dipl.-Ing., HTL, Präsident von Cosit AG, CISA, Mitglied bei FGSec, ACM SIGSAC, ISACA, SICTA und InfoSurance, Gründungsmitglied von «Swiss Network Academy», Dozent an der «Swiss Network Academy», Zürich.*