Service Management and Security **(Umfang 2 Doppelseiten)**
Publiziert in Comtec 4, 2003

Informations-Sicherheit

Systematisches Vorgehen bei der Einführung

Das Bewusstsein für Informationssicherheit ist in den meisten Betrieben innerhalb des letzten Jahres stark gestiegen. In Chefetagen wird offen über Verbesserungen der Informations-Sicherheit im Unternehmen gesprochen. Der Wille zur Verbesserung ist vorhanden. Wie soll das Vorhaben nun möglichst wirkungsvoll und vollständig umgesetzt werden?

Fredy Schwyter und Philipp Oswald

Die Unternehmens-Ressource „Information“

Informationen sind im heutigen Geschäftsumfeld eine genauso elementare Ressource wie z.B. 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 Informations-Sicherheit 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?

z. B. 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 Ueberwachung die nach den Umständen gebotene Sorgfalt angewendet hat.

Halbseitiges Bild: Telecom und Sicherheit im Hintergrund (im Original)
Text: Je mehr Werte im Spiel sind, desto höher müssen die Sicherheitsmassnahmen und der Ausbildungsstand der Mitarbeiter sein.

Unterschied zwischen IT-Sicherheit und Informations-Sicherheit

In Diskussionen mit Top-Managern wird sehr oft das hohe Sicherheitsniveau der IT-Infrastruktur hervorgehoben. Im Gespräch merkt der Experte, dass damit die IT-Sicherheit gemeint wird. Informations-Sicherheit 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. Aufwendiger werden Risiko-Analysen, wenn keine diesbezügliche Dokumentation darüber existiert. Bei den Analysen muss primär auf die Aussagen von beteiligten Mitarbeitern abgestellt werden, und dabei sind eigene Interpretation und Zuverlässigkeit kritische Faktoren.

Grundsätzlich müssen Geschäftsprozesse in dem Sinne 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 VR und der GL. Erfahrene Spezialisten, welche die Branche, die Gefahren und das Geschäftsumfeld kennen, können dazu wertvolle Hilfe leisten.

Nicht an subalterne Stellen zu delegierende Aufgaben:
- Klare Zielsetzungen zu formulieren
- die Definition der Wege zur Ziel-Erreichnung
- das Abschätzen der notwendigen Budgets und der personellen Ressourcen
- das Bestimmen des notwendige Controllings, um die Einhaltung der Sicherheitsstandard zu überwachen

,

Die Sicherheitsstrategie muss anschliessend in einer glaubwürdigen Form an die Mitarbeiter kommuniziert werden. Dies ist nicht zuletzt dann ein auschlaggebender Faktor, wenn es um das Engagement und die Motivation der Mitarbeiter geht. Zur Umsetzung der Sicherheitsstrategie bedarf es klarer Richtlinien, welche 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 Informationssicherheits-Bereiche führt unweigerlich zu Sicherheitslücken, welche meistens schwierig zu lokalisieren und zu eliminieren sind.

Systematik durch Systems Engineering

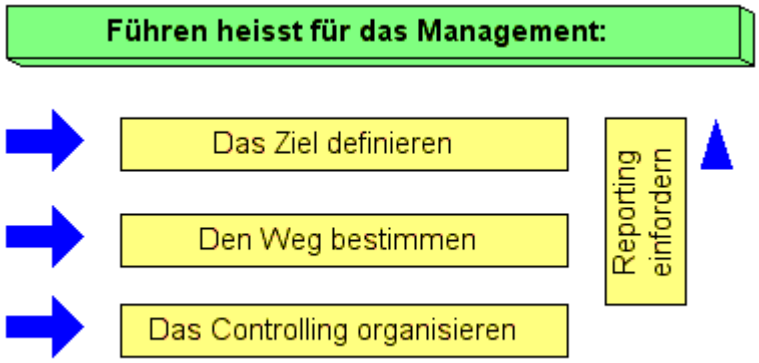
Eine umfassende Systematik ist auch im Sicherheitsbereich von elementarer Bedeutung. Der „Systems Engineering Approach“ bildet dazu eine gute Grundlage. Systems Engineering ist eine systematische Anwendung von Methoden, und kann kein Ersatz für Ausbildung und Erfahrung sein. Die wichtigsten Schritte im klassischen Systems Engineering sind wie folgt:

- Situations-Analyse
- Ziel-Formulierung
- Lösungssuche
- Lösungs-Entwicklung
- Umsetzung

Warum Systems Engineering?
Systems Engineering ist eine weltweit anerkannte Problemlöse-Methodik. Sie hilft, Probleme und Aufgaben systematisch und strukturiert zu analysieren und sinnvolle Lösungsvarianten zu erarbeiten. Systems Engineering wird an der ETH Zürich unterrichtet.

Effektives Management heisst führen
In der Praxis der Informations-Sicherheit hat es sich bewährt, dass das Management klar führt. Dazu gehören einige wichtige Punkte, ohne die eine Verantwortung nicht wahrgenommen werden kann. Dazu gehören:

- Auf Konsistenz in den Richtlinien achten
- Auf Übereinstimmung mit den Firmenzielen achten
- Die Richtlinien gutheissen
- Die Richtlinien unterschreiben
- Die Umsetzung der Sicherheits-Richtlinien veranlassen
- Die Umsetzung der Sicherheits-Richtlinien kontrollieren



Inhalt von Sicherheitsrichtlinien (Security Policy)
Die Sicherheits-Richtlinien bilden den Kern der Informations-Sicherheit in einem Unternehmen. Darin sind konkrete und umsetzbare Aufgaben und Ziele beschrieben, die Zuständigkeiten für die verschiedenen Verantwortungen, und über welche Informationskanäle was rapportiert werden muss. Die Sicherheits-Richtlinien sind für alle Mitarbeiterinnen und Mitarbeiter verbindlich und sollten dementsprechend verständlich formuliert sein. In den Ausführungsbestimmungen müssen alle wesentlichen Bereiche abgedeckt sein und konkrete Massnahmen sind darin verbindlich ausformuliert. 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 VR und die GL dieser Verantwortung nicht entziehen. Die Umsetzung erfordert in den weitaus meisten Fällen eine Ergänzung in der Organisation, da selten die notwendigen Kontroll-Organe vorhanden sind. Das Top-Management 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 organisatiorischen Voraussetzungen gehören einerseits ein Sicherheits-Verantwortlicher und eine Kontroll-Instanz (IKS: Internes Kontroll-System). Das IKS ist

für die laufende Überwachung der Sicherheitsmechanismen verantwortlich. Der Sicherheits-Verantwortliche stellt einerseits die Kommunikation zum Top-Management sicher, andererseits ist er Ansprechpartner für das IKS und für alle Mitarbeiter für Meldungen von sicherheitsrelevanten Vorkommnissen. Der Sicherheits-Verantwortliche 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.

80-20% Regel zur Limitierung von Kosten

Ein bekannter Killer für fortschrittliche Informations-Sicherheitskonzepte heisst: Perfektion! Dabei weiss jeder Eingeweihte: 100%-ige Sicherheit gibt es nicht! In fast jeder Projektleiter-Ausbildung wird heutzutage erwähnt, dass 80% einer möglichen Lösung für Informations-Sicherheit 20% der Kosten einer (hypotetisch) 100%-igen 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 die Sicherheit ohne Funktionseinbusse reduziert werden kann. (Ähnliche Überlegungen stellen sich übrigens heute alle erfolgreichen Automobilhersteller!)

Branchenspezifische Risiken und Benchmarks

Die Führungs-Übungen zum Schutze kritischer Informations-Infrastrukturen 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 tiefgreifende Technologieänderungen anstehen, wie z.B. Wireless-Kommunikation in der Telekommunikation, dann sind alle Verantwortlichen gut beraten, wenn sie die Risiken solcher Veränderungen in den Benchmarks mitberücksichtigen.

7 Tips zur erfolgreichen Umsetzung

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

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 Informations-Sicherheits-Teil mit. Dieser beinhaltet im wesentlichen 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 über die betroffenen Geschäftsprozesse des Kunden erstreckt und nicht nur auf zu liefernden Systemeinheiten.

Fredy Schwyter, dipl. Ing. HTL, Präsident von Cosit AG, CISA.
Mitglied bei FGSec, ACM SIGSAC, ISACA, SICTA und Infosurance,
Gründungsmitglied von „Swiss Network Academy“
Philipp Oswald, dipl.Inf. TS, NDS FH, Head of Security Solutions, Alcatel Schweiz AG, Leiter des Security Circels Telecom bei Infosurance.

Beide sind Dozenten an der „Swiss Network Academy“ in Zürich.