

Ist Informationssicherheit ein technisches Problem?

Karsten M. Decker

Die Grenzen technischer Lösungen

Schenkt man den Herstellern und Verkäufern von Virenschutzprogrammen, Spamfiltern, Intrusion Detection, Firewalls, Virtual Private Network Lösungen, etc. Glauben, ist ein Unternehmen nach Installation ihrer Software oder Hardware in jeder Hinsicht bestens geschützt. Häufig können zwar so einzelne technische Sicherheitslücken geschlossen werden. Eine grundlegende Verbesserung der Sicherheitslage wird so aber nicht erreicht, da entscheidende Aspekte einer integrierten und effizienten unternehmensweiten Informationssicherheit nicht berücksichtigt werden:


- Der Bezug zur Unternehmenspolitik fehlt; die Risikofähigkeit des Unternehmens wird so bestenfalls intuitiv berücksichtigt. Die Investitions- und Unterhaltskosten können somit nur schwer begründet werden. Zudem wird durch ein technologiefokussiertes Vorgehen die Geschäftstätigkeit häufig mehr behindert als das Sicherheitsprobleme umfassend gelöst werden.
- Organisatorische und personelle Aspekte bleiben völlig unberücksichtigt. Mit Blick auf die Gefährdung der Informationssicherheit aus dem Firmennernen, die wachsende Zahl und Qualität von Angriffen über die menschliche Schiene von aussen und die zunehmende Mobilisierung der Mitarbeiter unter Verwendung von Laptops, Mobiltelefonen, PDAs oder Smartphones eine grobe Unterlassung.

Zudem sind die Einzellösungen oft nicht hinreichend aufeinander abgestimmt, sodass es zu kostspieligen Überschneidungen kommt.

Informationssicherheit mit System

Worauf es tatsächlich ankommt, wenn man Information erfolgreich schützen will, zeigt der internationale Standard ISO/IEC 27001:2005 - Anforderungen an ein Informationssicherheitsmanagementsystem:

- Die Sicherheitspolitik, -ziele und -massnahmen werden individuell auf die Unternehmensziele und -strategien zugeschnitten.
- Die Risikoüberlegungen zur Informationssicherheit werden in das unternehmensweite Risikomanagement integriert.
- Organisatorische, personelle und technische Aspekte werden ganzheitlich betrachtet.


- 
- Das gesamte Personal sowie alle Lieferanten und Geschäftspartner werden regelmässig und funktionsgerecht für die Fragen der Informationssicherheit sensibilisiert, zu neuen Bedrohungen ausgebildet und über Neuerungen bei den organisatorischen Regeln und Verfahren informiert.
 - Die Informationssicherheit wird gemäss dem Plan - Do - Check - Act (PDCA) Zyklus regelmässig überwacht, überprüft, wo möglich gemessen und verbessert.
 - Das Management übernimmt nicht nur die rechtlich zugewiesene Gesamtverantwortung, sondern engagiert sich auch nachweislich, indem es die erforderlichen Ressourcen für den PDCA Zyklus sowie die Aus- und Weiterbildung des Personals zur Verfügung stellt und das Informationssicherheitsmanagementsystem mindestens einmal im Jahr auf Tauglichkeit, Angemessenheit und Effektivität überprüft.

Unternehmenskultur als Fundament

Eine effiziente Informationssicherheit, die darüberhinaus optimal auf die Bedürfnisse des Unternehmens abgestimmt ist, muss bereits in der Unternehmenskultur verankert werden. Über die Beschreibung entsprechender Normen, Wertvorstellungen, Denk- und Arbeitshaltungen beim Umgang mit Information im Unternehmen definiert man eine Sicherheitskultur und legt so ein solides Fundament für alle personellen Aspekte und Massnahmen einer integrierten Informationssicherheit. Eine gelebte Sicherheitskultur bietet den besten Schutz vor dem Erschleichen von Information durch soziale Manipulation (Social Engineering) bei gleichzeitig niedrigen Kosten.

Unternehmenspolitik als Leitplanken

Als nächstes gilt es auf Ebene Unternehmenspolitik die Rahmenbedingungen und Leitlinien für den Umgang mit Information im Unternehmen zu bestimmen und nachfolgend in der Sicherheits- und Risikopolitik auszuformulieren. Dabei werden die Unternehmensziele und -strategien, die Anforderungen von Gesetzen und Verordnungen am Sitz des Unternehmens und der Zielmärkte, die Bedürfnisse von Eigentümern, Kunden und anderen Anspruchstellern, die Einzigartigkeit sowie der Innovationsgrad der Produkte oder Services, die Wettbewerbssituation und allfällige Besonderheiten der Branche berücksichtigt.



Es ist offensichtlich, dass die Entscheidungskriterien für das Abwägen von Risiken für einen Produzenten einfacher Konsumgüter in einem wettbewerblich geschützten, lokalen Markt gänzlich anders aussehen, als für einen weltweiten Anbieter hoch innovativer Produkte mit Mitbewerbern und Kunden aus verschiedenen Kulturkreisen. Sicherheits- und Risikopolitik sind daher für jedes Unternehmen unbedingt individuell auszuformulieren.

Das Riskomanagement als Regler

Die Risikopolitik setzt wiederum die strategischen Rahmenbedingungen für das Risikomanagement, damit im Speziellen auch für die Analyse, Evaluation, Behandlung und Akzeptanz aller Risiken, die sich aus dem Umgang mit Information ergeben. Das Risikomanagement steuert den Umfang der Massnahmen zur Gewährleistung der Sicherheit im Allgemeinen und der Informationssicherheit im Speziellen. Es wirkt gleichsam als Regler, mit der die Gegenpole Risiko und Sicherheit ausbalanciert werden. Ist dieser Regler entsprechend gesetzt, ist die strategische Einbettung des Informationssicherheitsmanagementsystems in das Unternehmen im Sinne eines ``top-down'' Ansatzes abgeschlossen.

Technische Massnahmen

Ist die Gesamtstruktur vorhanden, kann man sich um die Implementierung einzelner technischer Massnahmen kümmern. Wie man das prozess-, service- und kundenorientiert machen kann, ist im Standard ISO/IEC 2000-1:2005 – Anforderungen an das IT Service Management - und der IT Infrastructure Library (ITIL) als der dazu gehörigen Best Practice beschrieben.

Feinabstimmung

Abschliessend gilt es die Auswirkungen der Methoden und Massnahmen zur Gewährleistung der Informationssicherheit auf operativer Ebene zu verifizieren. Geschäftsprozesse, die im Umgang mit Information nicht tragbare Sicherheitsrisiken in Kauf nehmen, müssen angepasst werden. Wird die Geschäftstätigkeit hingegen unangemessen behindert, müssen im Sinne eines ``bottom-up'' Ansatzes auf einer oder mehrerer der übergeordneten Ebenen Korrekturen angebracht werden.

Die Vorteile

Die Vorteile eines systematischen ``top-down'' Vorgehens für eine schlagkräftige Informationssicherheit, die Massnahmen zur Sicherung von Vertraulichkeit und Integrität von Information sorgfältig und sparsam verwendet, um zu gewährleisten, dass Information immer zur Verfügung steht, wenn Sie gebraucht wird, liegen auf der Hand:

- Umfang und Qualität sämtlicher Massnahmen werden aus den Geschäftsanforderungen bedarfsgerecht abgeleitet und können mit diesen einfach und nachvollziehbar begründet werden.
- Lücken oder kostspielige Überlappungen werden vermieden. Sicherheit wird integral und kosteneffizient.
- Durch den PDCA Zyklus wird die fortwährende Verbesserung der Informationssicherheit optimal mit der Entwicklung des Unternehmens abgestimmt.

Fazit

Informationssicherheit ist immer aus der spezifischen Unternehmenssicht heraus zu sehen und zu planen. Nur wenn wie beschrieben vorgegangen wird, besitzt man schliesslich klare Entscheidungsgrundlagen für die gezielte Realisierung technischer Schutzmassnahmen, die auch in Einklang mit der Kultur und Politik des Unternehmens stehen. So genannte Standardprodukte aus den Regalen der Software- und Hardware-Hersteller bieten eine gewisse Hilfe, aber nur dann, wenn ihr Einsatz im Rahmen der unternehmensweiten Informationssicherheit gezielt geplant wird. Entscheidend sind sie nicht.

Über den Autor

Dr. habil. Karsten M. Decker studierte Physik, Informatik und Chemie und ist Geschäftsführer der Decker Consulting GmbH. Er ist ISO/IEC 27001:2005 zertifizierter Lead Auditor, Experte für IT Service Management und internationales Projektmanagement sowie Dozent an der Hochschule für Technik+Architektur Luzern.

Decker Consulting GmbH

prüfen, bewerten, optimieren -
Decker Consulting GmbH hilft Unternehmen, Informationssicherheit und IT strategisch und operativ optimal in ihre Geschäftstätigkeit zu integrieren.