Informationssicherheitsrichtlinien

Nach dem Aufbau, dem Unterhalt und der stetigen Pflege des ISMS sind wir beim Anhang angelangt. Im ersten Teil (A.5) werden Anforderungen an Informationssicherheitsrichtlinien gestellt.

Während beim Aufbau des ISMS (27001) jede Anforderung mit «Muss» formuliert wurde, wird bei ISO 27002 (entspricht dem Anhang A.5 – A.18 von ISO 27001) «Sollte» verwendet. Hier hat ein Unternehmen etwas mehr Spielraum. Jedoch werden Anforderungen sehr schnell auch zu Muss-Anforderungen, wenn ein Unternehmen die entsprechende Massnahme umsetzt. Aus meiner langjährigen Erfahrung können nur wenige Bereiche ausgeklammert werden: zum Beispiel Lade- und Anlieferungszonen oder die eigene (Software-)Entwicklung. Daher ist es empfehlenswert, bei jedem sogenannten Control genau zu prüfen, ob dieser umgesetzt werden muss oder nicht.

Um die richtigen Anforderungen zu definieren, entscheidet das Unternehmen in einem ersten Schritt, welche Richtlinien überhaupt aufgestellt werden sollen. Dies ist abhängig von der Grösse und der Branche des Unternehmens. Bei einem grösseren Unternehmen sind vermutlich mehr Punkte zu regeln als bei einem kleineren.

Im Minimum gilt es, die IS-Politik auf höchster Ebene zu verabschieden. Sie gibt den Rahmen vor. Ich vergleiche dies gerne mit einer Autobahn. Die Richtung ist klar vorgegeben, welche Spur ich nutze, ist mir aber überlassen. Dies ist der Handlungsspielraum für die nachfolgenden Stufen der Dokumentation.

Von der Definition her wird folgende Abstufung gemacht:

1. Politik: sie ist auf oberster Ebene definiert und verabschiedet. Darin wird festgehalten, dass die Informationssicherheit für das Unternehmen wichtig ist. Das Management unterstützt das Security Team mit vollem Support. Weiter ist darin die Verpflichtung enthalten, Prozeduren, Guidelines und Baselines einzuhalten. In der Politik können strategische und taktische Sicherheitswerte definiert werden sowie spezifische Sicherheitsaspekte.
2. Baselines: darin ist das minimale Sicherheitslevel für das Unternehmen festgehalten. Damit soll garantiert werden, dass die Security einheitlich implementiert und gelebt wird. Bei Systemen kann dies bereits sehr ins Detail gehen. Eine Empfehlung bei Systemen ist das Center for Internet Security, zu finden unter www.cisecurity.org, welches kostenlose Konfigurationsempfehlungen für diverse Betriebssysteme, Applikationen und Geräte veröffentlicht (Registrierung notwendig).
3. Guidelines: hier wird die Methode, wie etwas gemacht wird, beschrieben.
4. Prozeduren: zuunterst in der Hierarchie sind dann die Prozeduren. Es sind detaillierte Step-by-Step-Beschreibungen, wie etwas gemacht wird, sprich Anleitungen.

Die Norm vermischt übrigens die Begriffe «Politik» und «Richtlinien». In der Fussnote wird dann erwähnt, dass die Politik auf oberster Ebene zu definieren ist, die Richtlinien darunter einzuordnen sind. Gemäss der vorherigen Definition gehören Baselines, Guidelines und Prozeduren zu diesen. Erwähnt wird weiter, dass auch Ausdrücke wie «Normen», «Richtlinien» oder «Regeln» für diese Dokumente verwendet werden.

Nebst den bereits erwähnten Punkten gehören folgende Elemente in die Politik:

- Definition der Informationssicherheit: was versteht das Unternehmen darunter?
- Ziele: Welche (messbaren) Ziele sollen damit erreicht werden? Zum Beispiel Reduktion von IS-Vorfällen, Erhöhung der Awareness bei den Mitarbeitenden, Verbesserung des Images usw.
- Grundsätze: welche Grundsätze möchte das Unternehmen leben? Zum Beispiel Clear Desk (aufgeräumter Arbeitsplatz), Gäste sind immer zu begleiten usw.
- Verantwortlichkeiten: wer ist für was verantwortlich (Stichworte: Ressourcenplanung, Umsetzung ISMS, Schulungen, Umgang mit Schwachstellen, Lieferanten und Partner)? Wer

rapportiert wem (Berichterstattung)? In welchen Abständen sind welche Kontrollen durchzuführen usw.?
– Umgang mit Abweichungen und Ausnahmen: ein ganz wichtiger Punkt. «Unverhofft kommt oft», sagt der Volksmund. Auf diese Abweichungen muss mit einem Prozess reagiert werden können. Ein typischer Satz ist: «Der CISO entscheidet über Ausnahmen.» Doch sollte der CISO bereits im Vorfeld einen Kriterienkatalog haben, der ihn bei seinen Entscheiden unterstützt.

Wichtig ist, dass alle Mitarbeitenden die Politik verstehen. Sie sollte also Jargon-frei (das heisst keine technischen Details oder Fachwörter) und in kurzen, einfachen Sätzen geschrieben sein. Weiter ist das Dokument stellenunabhängig, betrifft also von der Geschäftsleitung bis zum Hauswart alle. Alle müssen die Wichtigkeit der Politik verstehen und befolgen! Aussagen wie: «Ich dachte, diese Politik gilt nicht für mich», dürfen nicht vorkommen.

Die IS-Politik sollte weiter so geschrieben sein, dass diese auch externen interessierten Stellen zur Verfügung gestellt werden kann. Daher dürfen keine vertraulichen Details darin enthalten sein. Falls dies nicht möglich ist, sollten zwei Versionen des Dokuments erstellt werden: eine interne und eine öffentliche Politik.

Wie wird nun die Politik verteilt? Bei der Neueinstellung wie auch bei Wiederangestellten während des Einstellungsprozesses. Ideal ist es, wenn dieses Dokument gleich einen Anhang zum Arbeitsvertrag darstellt. So wird die Wichtigkeit nochmals unterstrichen. Zudem sollte sie im Intranet veröffentlicht werden. Die Schulung kann mittels Videos, WBT (Web Based Trainings), Postern, Booklets oder anderen Hilfsmitteln erfolgen.

Auch die Politik unterliegt Änderungen. Daher sollte diese, wie auch die anderen Richtlinien, in regelmässigen Abständen überprüft werden. Die Norm selber definiert keinen Zeitraum. Es hat sich aber ein jährlicher Rhythmus als ideal herausgestellt. Bei grösseren Veränderungen muss natürlich auch in kürzeren Intervallen reagiert werden. Die Norm verlangt bei jedem Dokument eine verantwortliche Person zu bestimmen, die die Enwicklung, Überprüfung und Bewertung durchführt. Die Richtlinien sind stets durch das Management zu verabschieden.

In der ISO-Norm sind 16 Richtlinien erwähnt, die ein Unternehmen erarbeiten sollte. Darunter zum Beispiel das Backup-Konzept, Mitarbeiter-Weisungen, Handhabung von technischen Schwachstellen und weitere. Diese Richtlinien werden in den folgenden Beiträgen detailliert behandelt. Daher wird auf eine vollständige Aufzählung verzichtet.

Mit der IS-Politik kann das Gerüst beziehungsweise die Rahmenbedingungen für den Aufbau, die notwendigen Ressourcen, die kontinuierliche Verbesserung sowie die Verantwortlichkeiten klar geregelt werden. Die Politik ist somit das Fundament für die nachfolgenden Richtlinien.