ISO 27001: Führung

Der dritte Teil geht auf das Normenkapitel 5 Führung ein. Es genügt nicht mehr, dass die Geschäftsleitung zwar den Auftrag gibt, aber nicht aktiv mitarbeitet und die Umsetzung nicht unterstützt. Im BSI 100-1 steht sogar: «Wenn Zielvorgaben aufgrund fehlender Ressourcen nicht erreichbar sind, sind hierfür nicht die mit der Umsetzung betrauten Personen verantwortlich, sondern die Vorgesetzten, die unrealistische Ziele gesetzt beziehungsweise die erforderlichen Ressourcen nicht bereitgestellt haben.» Dies zeigt klar, welche Verantwortung von der Führung erwartet wird.

Im Punkt 5.1.a wird verlangt, dass die Führung die Informationssicherheitspolitik und die Informationssicherheitsziele festlegt. Diese müssen natürlich auf die strategische Ausrichtung des Unternehmens abgestimmt werden. Der Auftrag kann an eine interne Person erteilt werden, die Führung segnet diese schlussendlich ab.

Unter 5.1.b wird verlangt, dass die Informationssicherheit in allen Geschäftsprozessen im Anwendungsbereich des ISMS berücksichtigt wird (Anmerkung: dies sollte gleich für das gesamte Unternehmen gelten). Dazu passt auch die Anforderung aus A.6.1.5 Informationssicherheit im Projektmanagement. Jedes (neue) Projekt muss die Informationssicherheit berücksichtigen. In der Praxis kann ein zusätzliches Feld auf dem Projektantrag angebracht werden: IS-relevant. Von Vorteil wird auch gleich noch DS-relevant (Datenschutz, speziell DS-GVO) ergänzt werden. Wurde ein Häkchen gesetzt, gilt es eine Risiko-Analyse durchzuführen: welche Daten werden erfasst/bearbeitet? Welche Systeme sind involviert? Welche Prozesse werden tangiert? Wer und Wie muss darauf zugegriffen werden? Welche Kritikalität ist damit verbunden? usw. Mehr zur Risiko-Analyse folgt im nächsten Blog-Beitrag.

Projektplan mit klaren Zielen

Der dritte Punkt 5.1.c verlangt die bereits in der Einleitung erwähnte Zuteilung der notwendigen Ressourcen. Ressourcen sind nicht nur Zeit, das kann auch die richtigen Personen, Finanzen oder externe Unterstützung enthalten. Idealerweise wird auch ein Projektplan mit klaren Zielen erstellt.

Beim Punkt 5.1.d wird die Bedeutung und Wichtigkeit beschrieben. Allen muss klar sein, um was es geht, was die Ziele dieses Projektes sind, warum dies für das Unternehmen wichtig ist und wie das ISMS umgesetzt wird. Nur was bekannt ist, kann auch gelebt werden.

Eigentlich ist Punkt 5.1.e selbstverständlich, aber halt doch nicht so einfach umzusetzen. Es geht darum, dass das beabsichtigte Ergebnis auch erreicht wird. Beim Etablieren des ISMS ist es noch einfach. Alle sind in einer Euphorie, kennen die Gründe und das Ziel und die Umsetzung geht flott voran. Sobald das ISMS etabliert, allenfalls auch zertifiziert ist, kommt das Alltagsgeschäft und schlägt wieder zu. Die notwendigen und definierten Kontrollen und Tätigkeiten werden mehr und mehr vernachlässigt. Darum ist es wichtig, dass das Management auch danach immer noch dahintersteht und klare Resultate/Ergebnisse fordert.

Der nächste Punkt 5.1.f verlangt das Anleiten und das Unterstützen, damit alle zur Wirksamkeit beitragen. Regelmässige Awareness und Sensibilisierungen helfen dabei, dass alle immer wieder auf die richtige Spur gebracht werden.

Der Punkt 5.1.g ist bereits in e erwähnt, denn nur mit fortlaufender Verbesserung kann die Informationssicherheit am vorhandenen (und wechselnden) Risiko angepasst werden. Neue Technologien kommen dazu, neue Stellen werden geschaffen, neue Dienstleistungen angeboten. Dies gilt es alles zu beachten. Wenn Fehler und Schwächen erkannt werden, gilt es diese auszumerzen und so das ISMS laufend zu verbessern. Dies wird auch unter Kapitel 10 der Norm verlangt.

Spannend ist auch der Punkt 5.1.h: es wird verlangt, dass auch andere Führungskräfte ihrer Rolle bewusst sind. Also nicht nur die für die IT-verantwortliche GL-Person kümmert sich um das ISMS, nein, es geht alle an. Es darf nicht sein, dass sich nur ein Teil an die Vorgaben hält, der oberste Chef aber eine ganz andere Meinung hat.

Die Politik gibt die Leitplanken vor

Das Kapitel 5.2 beschreibt die Anforderungen an die Informationssicherheitspolitik. Sie wird von der obersten Leitung festgelegt. Was darin enthalten sein könnte, wird in A.5 ausführlich beschrieben. Mögliche Inhalte folgen in einem späteren Artikel. Die Anforderungen verlangen, dass die Politik dem Zweck der Organisation entspricht. Eigentlich selbstverständlich, aber doch nicht so einfach. Wichtig ist, dass es keinen Widerspruch zu den Firmenzielen gibt. Die Politik gibt die Leitplanken vor und geht nicht auf Details ein. Es sind Spielregeln, an die sich alle halten müssen. Sie sollten aber nicht so eng gefasst sein, dass keine Innovation mehr möglich ist. In der Politik werden die Ziele der Informationssicherheit beschrieben. Dies auf einem High-Level. Es macht keinen Sinn, hier Details zu fordern, wie «es darf maximal drei Incidents geben, deren Behandlung mehr als drei Tage dauerte», sondern «Incidents müssen entsprechend der Kritikalität innert kürzester Zeit behandelt werden». Was dies nun im Detail für die einzelnen Kategorien bedeutet, wird zu einem späteren Zeitpunkt definiert. Der dritte Punkt 5.2.c verlangt eine Verpflichtung

Bild: Archiv

Die Geschäftsleitung sollte aktiv an Aufträgen mitarbeiten und an der Umsetzung mitwirken.

zur Erfüllung und Punkt 5.2.d eine Verpflichtung zur fortlaufenden Verbesserung. Somit ist allen bekannt, um was es geht und meine Mitwirkungspflicht ist unmissverständlich gefordert.

Weiter fordert dieser Abschnitt, dass dies schriftlich gemacht wird und intern allen, wie aber auch allen externen interessierten Parteien zur Verfügung gestellt wird. Da keine sensiblen Informationen in die Politik gehören, kann das Dokument sogar auf der Firmenhomepage veröffentlicht werden. Es zeigt allen, uns ist es ernst mit der Informationssicherheit.

Der dritte Abschnitt verlangt von der obersten Leitung, dass die Verantwortlichkeiten und Befugnisse für alle im Bereich der Informationssicherheit zugewiesen und bekannt gemacht werden. Im Intranet kann beispielsweise die Rolle CISO beschrieben und einer Person zugeteilt werden. Für den CISO könnte dies wie folgt aussehen:

- Aufbau und Betrieb eines Managementsystems zur Informationssicherheit (ISMS)
- Aufbau und Betrieb einer Organisationseinheit zur Umsetzung der Sicherheitsziele
- Identifikation sicherheitsrelevanter Unternehmensprozesse
- Erarbeitung und Definition der sicherheitsrelevanten Objekte, der Bedrohungen und Risiken und den daraus abgeleiteten Sicherheitszielen
- Ausarbeitung, Anpassung von Sicherheitsrichtlinien und IT-Sicherheitszielen, inkl. Definition von KPIs
- Aufsicht über die Einhaltung von Vorschriften
- Auditierung der Funktionseinheiten zum Stand der Umsetzung und Weiterentwicklung der Sicherheitsvorschriften
- Beaufsichtigung des Identity- und Access-Managements
- Bewusstsein der Mitarbeiter durch Trainings und Awareness-Kampagnen schaffen
- Zusammenarbeit mit anderen Führungskräften zur Etablierung eines Desaster-Recovery- und BCM
- Reporting der KPIs an den Verwaltungsrat/Geschäftsleitung

Explizit wird aufgeführt, dass sichergestellt sein muss, dass die Anforderung der ISO-Norm 27001 und der 114 Controls erfüllt werden. In einem externen Audit wird dies auch sehr genau überprüft. Ebenfalls wird überprüft, dass die Berichterstattung an die oberste Leitung funktioniert. Der Autor hat gute Erfahrungen damit gemacht, wenn der CISO ein Zeitfenster in jedem GL-Meeting erhält. So ist sichergestellt, dass Rückmeldungen oben ankommen und auch Massnahmen zeitnah getroffen werden können.

Informationen regelmässig austauschen

Interessant ist die Anmerkung: Die oberste Leitung kann verlangen, dass Informationen auch innerhalb der Organisation geteilt werden. Dies gilt sowohl für Konzerne wie auch für kleinere Firmen. An das Zielpublikum angepasste Informationen sollten regelmässig ausgetauscht werden. Wenn sich ein Vorfall ereignet, zum Beispiel ein Einbruch, wissen alle, was passiert ist, wie reagiert und welche Schritte eingeleitet wurden. Vielleicht kommen dann sogar Rückmeldungen, wie «das könnte auch beim Eingang B passieren, der ist auch nicht optimal geschützt».

Alle können dazu beitragen, dass die geforderte Verbesserung des ISMS erfolgt. Wenn die Rahmenbedingungen aus der Politik sowie die Ziele bekannt sind, kann das ISMS stetig verbessert und damit die Informationssicherheit nachhaltig erhöht werden.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch