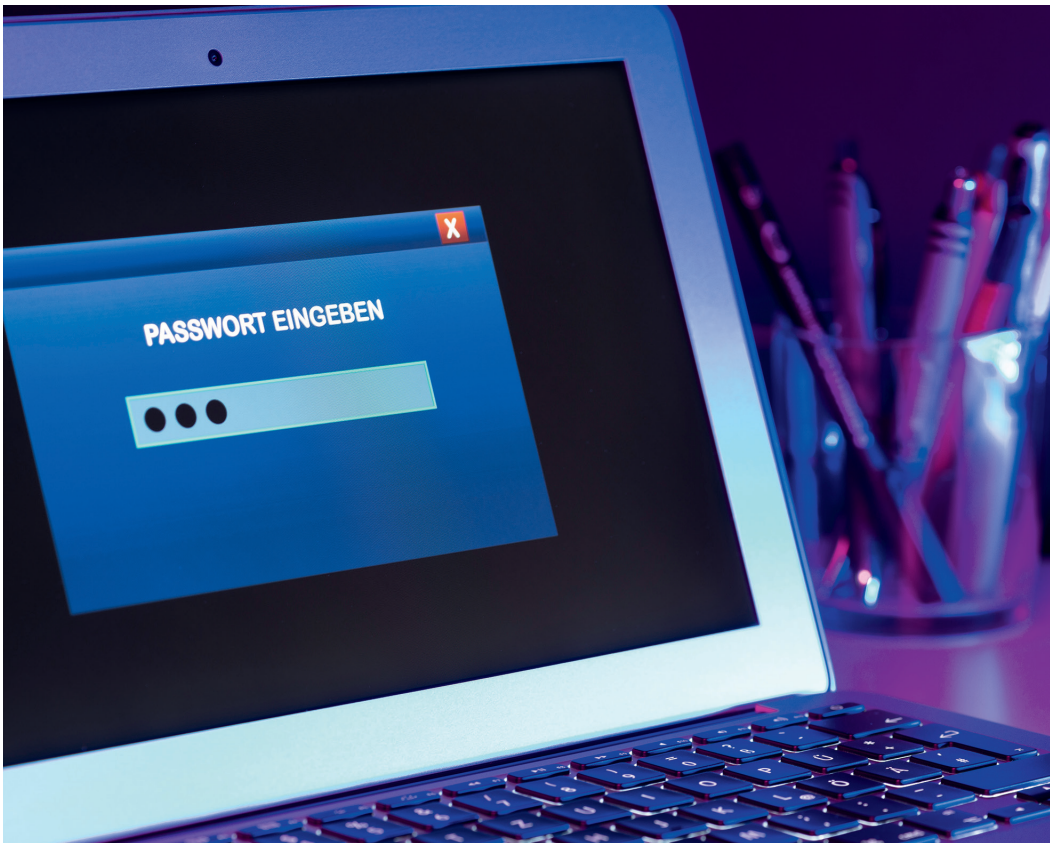

Bild: Archiv

Stetig verändert sich die Bedrohungslage und neue Schwachstellen werden erkannt.

Umsetzung eines ISMS

Viele Unternehmen sind daran ein Informationssicherheitssystem aufzubauen und damit die IT-Sicherheit nachhaltig zu erhöhen. Doch der Start stellt sich oft sehr harzig dar. Wo soll man nur beginnen? Welche Reihenfolge macht Sinn? Nur die ISO 27001 Norm zu lesen bietet zwar eine gute Übersicht und Einführung in die Thematik, doch was genau bei jedem Punkt verlangt wird, ist nicht immer auf den ersten Blick klar. Die ISO 27003 kann hier eine gute Unterstützung sein.

In den maschinenbau-Ausgaben 4/2018 bis 12/2019 wurden die verschiedenen Kapitel der ISO 27001 (Aufbau des Managementsystems) und ISO 27002 (notwendige Massnahmen) behandelt. Die ISO 27003 ergänzt das erstgenannte Dokument optimal und bietet einen vertieften Einblick in den Aufbau und den Unterhalt des ISMS. Die internationale Norm mit dem offiziellen Titel «Information technology – Security techniques – Information security management systems – Guidance» wurde im März 2017 in der Version 2 veröffentlicht. Der Aufbau entspricht 1:1 dem der ISO 27001. Ist dieses Dokument bereits bekannt, kann direkt gestartet werden. Auf 41 Seiten werden zusätzliche Gedanken und Hilfestellungen zu den Schlüsselkomponenten Policy, Rollen und Verantwortlichkeiten, Risiko-Management, Awareness, dem PDCA-Zyklus sowie Verbesserungen und notwendiger Dokumentation gezeigt. Jeder Norm-Punkt der Kapitel 4 bis 10 beschreibt die notwendigen Aktivitäten, Erklärungen, Detail-Informationen und Beispiele sowie weiterführende Quellen.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

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

Etablierung von Informationssicherheitsrichtlinien

Das Kapitel 4 verlangt die Beschreibung des Kontexts des Unternehmens. Dazu gehören die externen und internen Einflüsse, die auf ein Unternehmen einwirken. Dies können unter anderem das soziale Umfeld, politische oder vertragliche Anforderungen, die finanzielle Situation, eingesetzte Technologien oder die Wettbewerbsfähigkeit sein. Dies zu dokumentieren ist zwar optional gefordert, lohnt sich aber, um das ISMS ganzheitlich abzustützen und den notwendigen Rahmen zu definieren. Weiter gilt es die interessierten Parteien zu definieren. Die Norm gibt zu externen und internen einige Beispiele. Mit diesen Angaben kann in der Folge der Anwendungsbereich definiert werden.

Zu Kapitel 5 erhält die/der Lesende Informationen, wie die Norm den Begriff «Top Management» definiert und welche Verpflichtungen dieses hat, nicht nur in Bezug auf die Unterstützung der notwendigen Massnahmen. Ein wichtiger Punkt ist dabei die Etablierung von Informationssicherheitsrichtlinien. Auf einem hohen Level wird der Rahmen für die weiteren Dokumente gesteckt, Ziele definiert und die Kommunikation sichergestellt. Weiter definiert das Top Management die involvierten Rollen inklusive deren Verantwortlichkeiten.

Das Kapitel 6 nimmt einen grossen Stellenwert ein. Hier geht es darum, ein umfassendes Risiko-Management zu etablieren. Risiken müssen erkannt und bewertet werden. Die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit helfen dabei. Die Risiken können auf strategischer, taktischer oder operativer Ebene sein. Die notwendigen Schritte dazu sind ausführlich im Unterkapitel 6.1.2 aufgeführt. Risiken können aus vergangenen oder möglichen Ereignissen entstehen, in Workshops erfasst und besprochen werden. Die Bewertung kann dabei qualitativ sein (zum Beispiel Hoch, Mittel, Gering), quantitativ (das heisst mit erfassten Kosten und Wahrscheinlichkeiten) oder ein Mix beider Methoden umfassen. Nach der Bewertung wird definiert, ob Massnahmen ergriffen oder das Risiko akzeptiert wird. Darauf geht das Unterkapitel 6.1.3 im Detail ein. Der letzte Teil umfasst die Definition von Zielen, wie diese umgesetzt, gemessen und verbessert werden.

Notwendige Ressourcen

Im Kapitel 7 geht es um die Unterstützung. Dies umfasst die notwendigen Ressourcen wie involvierte Personen, den Zeitbedarf, finanzielle Aufwendungen, externe Unterstützung, aber auch die Infrastruktur. Ebenfalls werden das notwendige Wissen, die Bewusstsein, die Kommunikation gegen innen und aussen sowie die

Anforderungen an die Dokumentation ausführlich beschrieben.

Auf das Kapitel 8 wird in diesem Beitrag nicht näher eingegangen. Hier wird der in Kapitel 6 definierte Risiko-Prozess umgesetzt. Die Schritte basieren auf den gemachten Definitionen. Was umgesetzt wird, muss auch gemessen und bewertet werden. Auf diesen Umstand geht das Kapitel 9 ein. Es ist wichtig zu wissen, wie die Performance und die Effektivität des ISMS sind. Das Kapitel 9.1 zeigt, wie man KPI's (Key Performance Indicator, zu Deutsch Leistungskennzahl) definiert und diese regelmässig misst. Die notwendigen Schritte für das interne Audit werden in Kapitel 9.2 beschrieben. Hier geht es darum, durch das ganze ISMS zu gehen, inkl. den 114 Massnahmen aus ISO 27002. Es wird verglichen, ob die geforderten Punkte umgesetzt sind und auf welchem Maturitätslevel sich diese bewegen. Die Norm hilft auch dabei, wie ein Audit-Programm über das gesamte Jahr erstellt werden kann. Dazu können Resultate aus Penetration Tests, Security Audits, Code Reviews, Phishing-Angriffe und viele weitere Kontrollen beigezogen werden. Die Norm hilft ebenfalls, wie ein Audit-Team zusammengestellt werden kann, welches Wissen vorhanden sein muss und welche Anforderungen an den Audit-Bericht gestellt werden. Der letzte Teil umfasst das Management Review. Wie bereits eingangs erwähnt, ist es wichtig, dass das (Top) Management den genauen Stand des ISMS kennt und die notwendigen Steuerungsmassnahmen ergreifen kann. Läuft es nicht wie gewünscht, können frühzeitig die Weichen gestellt und Verbesserungen geplant werden.

Informationssicherheit ist keine einmalige Sache

Auf diesen Umstand geht das Kapitel 10 ein. Im ersten Unterkapitel wird gezeigt, wie Abweichungen, sogenannte Nonconformities erfasst und bewertet werden müssen. Die Norm gibt Beispiele und Hinweise, wie diese erkannt werden können. Danach gilt es angepasste Massnahmen zur Korrektur einzuleiten und die Wirkung der ergriffenen Massnahmen zu überprüfen. Der letzte Normpunkt, die 10.2, ist in der ISO 27001 ein einziger Satz. Aber dieser hat es in sich. Es geht darum, das ISMS stetig weiter zu verbessern. Welche Schritte dies umfassen sollte, kann in diesem Kapitel nachgelesen werden.

Informationssicherheit ist keine einmalige Sache oder etwas, was nur für die Zertifizierung gemacht wird. Stetig verändert sich die Bedrohungslage, neue Schwachstellen werden erkannt, das Unternehmen wandelt sich, Mitarbeiter stossen dazu oder verlassen das Unternehmen, neue Techniken werden eingeführt und vieles mehr. Ein sauber strukturiertes ISMS kann diese Punkte erfassen, die Risiken neu bewerten und adäquat darauf reagieren. Damit kann die Informationssicherheit immer auf einem hohen, für das Unternehmen passenden Niveau gehalten werden. Die ISO 27003 hilft dabei mit vielen Tipps und Tricks, dies effektiv umzusetzen.