Compliance – Einhalten von Gesetzen und Verträgen

Das letzte Kapitel der ISO-Norm A.18 beschreibt Anforderungen an die Richtlinienkonformität. Damit sollen Verstösse gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Verpflichtungen mit Bezug auf Informationssicherheit und gegen jegliche Sicherheitsanforderungen vermieden werden.

Bevor gestartet werden kann, müssen die anwendbaren Gesetze und vertraglichen Anforderungen erfasst und dokumentiert werden. Folgende Gesetze für ein Unternehmen können dabei einen Einfluss haben: ZGB, OR, StGB, GeBüV, DSG und VDSG, URG, UWG, MSchG, KG, SchKG, VASR, MWSTG oder AHVG. Unter www.kmu.admin.ch/kmu/de/home/aktuell/gesetzesaenderungen-mit-auswirkungen-fuer-kmu.html sind Gesetzesänderungen mit Auswirkungen für KMU abrufbar. Diese Seite gilt es regelmässig zu besuchen. Wenn sich diese Gesetze oder eigene Verträge ändern, gilt es die Unterlagen immer auf dem aktuellsten Stand zu halten.

Eigentumsrechte

Der zweite Punkt umfasst die geistigen Eigentumsrechte. Die Norm geht explizit auf den Schutz dieser Rechte ein, bezieht sich auf die vertraglichen Abmachungen, wie auch auf urheberrechtlich geschützte Software. So sollten intern Richtlinien zum Umgang mit urheberrechtlich geschützten Medien erstellt werden. Es darf nicht sein, dass fremde Texte, Bilder, Videos oder Musik ohne entsprechende Rechte verwendet werden. Auch sollten Medien nur aus seriösen Quellen beschafft werden. Bei Verletzungen kann der Disziplinarprozess zum Einsatz kommen (siehe Maschinenbau 1/19). Lizenzen (inkl. deren Bedingungen), Originaldatenträger und Handbücher sollten aufbewahrt werden. Erfahrungsgemäss macht es auch Sinn, die Original-Rechnung aufzubewahren, um einen Beweis für die Richtigkeit zu haben. Insbesondere Lizenz-Rechte gilt es einzuhalten. Aber auch für vollständige oder auszugsweise Kopien von Büchern, Artikel, Berichte oder anderen urheberrechtlich geschützten Werken gelten die Regeln. Bei einer Kontrolle könnten unangenehme Schadensersatzforderungen die Folge sein.

Verschiedene Gesetze fordern das Speichern von Informationen über einen gewissen Zeitraum. Diese Aufzeichnungen gilt es vor Verlust, Zerstörung, Fälschung, aber auch unbefugtem Zugriff oder Veröffentlichung zu schützen. Es gilt auch die Klassifizierungs-Anforderungen über die gesamte Dauer einzuhalten (siehe Maschinenbau 2/19). Beachten Sie auch, dass Daten auf Datenträgern verloren gehen können. CDs, Tapes wie auch Festplatten habe eine begrenzte Lebensdauer. Darauf gespeicherte Daten sollten daher regelmässig überprüft und auf neue Medien kopiert werden, um sich vor einem Datenverlust zu schützen. Die Norm empfiehlt dazu die Erstellung von Leitfäden zur Aufbewahrung, Lagerung, Handhabung und Entsorgung von Aufzeichnungen und Informationen.

Schützenswerte Daten

Neben den Firmendaten gilt es auch die Privatsphäre und den Schutz von personenbezogenen Informationen gemäss den relevanten Gesetzen und Vorschriften zu schützen. Im Datenschutzgesetz sind für besonders schützenswerte Daten, und da gehören Mitarbeiterdaten dazu, klare Anforderungen definiert. In der Verordnung zum Datenschutzgesetz (VDSG) sind vor allem (aber nicht nur) die Artikel 8, 9 und 10 einzuhalten. Es handelt sich im vierten Abschnitt um vorzunehmende Technische und Organisatorische Massnahmen (TOMs), wie sie auch die DSGVO der EU verlangt.

Gerade für kryptographische Techniken gelten separate Anforderungen. Verschiedene Länder verbieten den Export, aber auch den Import von solchen Produkten. Dies gilt es im Vorfeld genau abzuklären, um nicht mit gewissen Regierungsstellen grosse Probleme zu bekommen. Die Norm hat unter A.18.1.5.d noch eine spezielle Anforderung: «verpflichtende oder freiwillige Methoden für den Zugriff der Behörden des Landes auf hardware- oder softwareseitig verschlüsselte Informationen zur Gewährleistung der Vertraulichkeit der Inhalte.» Hier werden Backdoors gefordert, die ich als sehr heikel betrachte. Ein gewisses Verständnis für diese Massnahme bei der Terrorbekämpfung ist verständ-

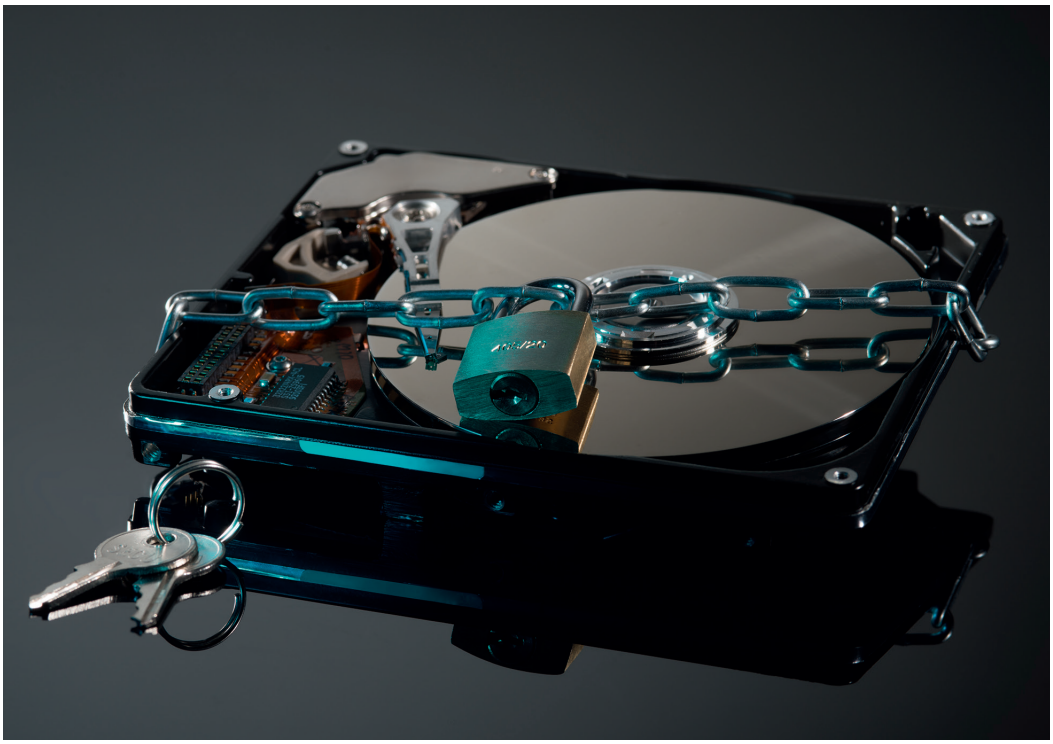

Bild: Archiv

Informationen gilt es vor Verlust, Zerstörung, Fälschung, aber auch unbefugtem Zugriff oder Veröffentlichung zu schützen.

lich, aber generelle Hintertüren können keine Lösung dafür sein. Für Lieferungen in bestimmte Länder sind diese Anforderungen abzuklären und geeignete Massnahmen zu treffen oder nicht in solche Länder zu liefern.

Das zweite Kapitel beschreibt Anforderungen an die Überprüfung der Informationssicherheit. Dies hatten wir bereits in Maschinenbau 10/18 angesprochen. Die Kontrollen sollten durch eine unabhängige Stelle durchgeführt werden. Dies kann eine interne Person sein, aber auch externe Spezialisten können beigezogen werden. Dazu sollte im Vorfeld ein Auditprogramm zusammengestellt werden. Was sind wichtige Punkte? Welche Bereiche gilt es in welchen Abständen zu überprüfen? Gibt es Schlüssel-Lieferanten oder -Partner, die Einfluss auf das eigene ISMS haben, zu überprüfen? Werden Abweichungen in Audits festgestellt, müssen diese erfasst, bewertet, geeignete (Gegen-)Massnahmen definiert und dem Management präsentiert werden. Nach der Freigabe können diese Abweichungen behandelt und geschlossen werden.

Sicherheitsanforderungen überprüfen

Die letzten beiden Punkte umfassen die Einhaltung von Sicherheitsrichtlinien, -standards und technischen Vorgaben. Leitende Angestellte sollten regelmässig die Einhaltung der Sicherheitsrichtlinien, Standards und jeglicher Sicherheitsanforderungen überprüfen. Dazu können auch automatische Werkzeuge zum Einsatz kommen. Werden Abweichungen festgestellt, gilt es die Ursache festzustellen, mögliche Massnahmen zu erarbeiten und zu bewerten sowie Korrekturmassnahmen umzusetzen. Für jede getroffene Massnahme gilt es die Wirksamkeit zu überprüfen und allenfalls Anpassungen vorzunehmen.

Mit der Etablierung eines ISMS und der Umsetzung der 114 Controls kann in einem Unternehmen die Informationssicherheit nachhaltig verbessert, überwacht und gesteuert werden. Für Kunden, Lieferanten, Partner und Anteilseigner existiert mit einer Zertifizierung ein allgemein anerkannter Nachweis. Trotz hohem Initial-Aufwand steht ein wirkungsvolles Werkzeug zur Verfügung, das schlussendlich Zeit und Geld sparen hilft, indem klare Vorgaben und Prozesse existieren. Gleichzeitig ist das eigene Unternehmen auf einen möglichen Vorfall vorbereitet.

Dies ist der letzte Teil der ISO-27001- und -27002-Reihe, welche mit der Ausgabe Maschinenbau 4/18 gestartet ist. Die nachfolgenden Artikel werden auf die weiteren Normen der 27000er-Reihe eingehen und Details zum Inhalt und der Umsetzung liefern.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

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