Informationssicherheit als Teil der Unternehmenskultur

Informationssicherheit ist mehr als nur IT, sie umfasst sämtliche Informationen, die für wichtige Geschäftsprozesse in einem Unternehmen unentbehrlich sind. Aus den klassischen Werten werden Informationswerte.

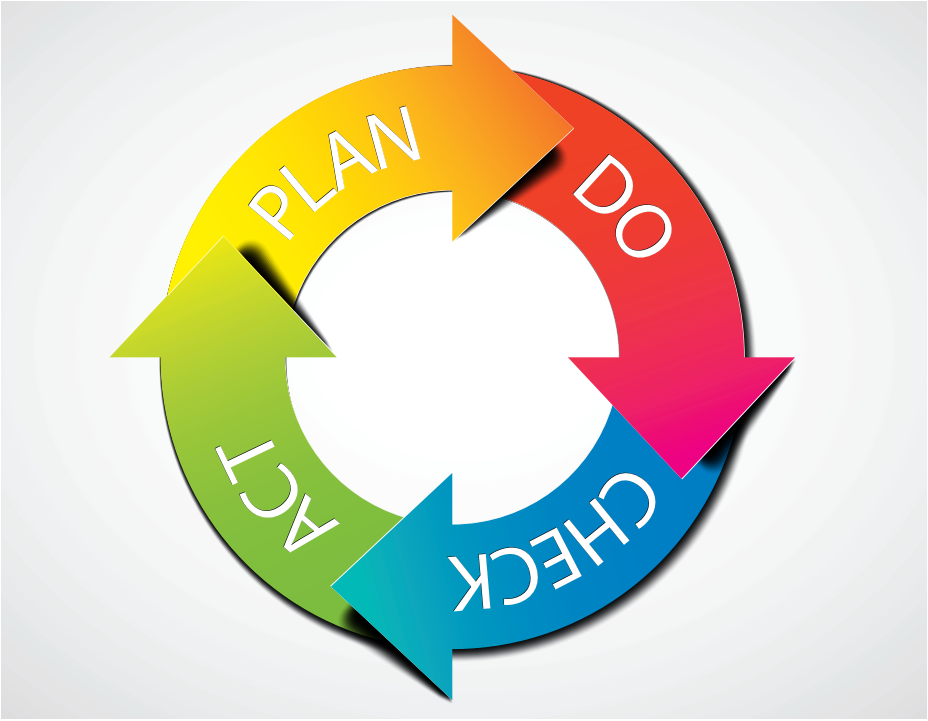
Von Almut Eger und Walter Rüegg

Ein System der Informationssicherheit geht selbstredend weit über Dinge wie Virenschutz hinaus, denn es sollen alle wichtigen Prozesse, Elemente und deren Verbindungen berücksichtigt werden: Informationen zu den wesentlichen Prozessen wie Produktion, Wartung, Änderung und Störungsbeseitigung sowie alle internen und externen Kontakte, Patente und Assets. Speziell der Handhabung der Informationen durch die Mitarbeitenden kommt grosse Bedeutung zu.

Wofür steht das Kürzel ISMS?

ISMS ist die Abkürzung für ein dokumentiertes Informations-Sicherheits-Management-System zur sicheren Handhabung von Informationen gemäss ihrer Bedeutung für das Unternehmen. Die Norm ISO/IEC 27001 spezifiziert die Anforderungen für dieses System und dessen Aufbau, Einführung, Betrieb, Überwachung, Wartung und Verbesserung. Eine ähnliche, speziell auf Informationstechnologie (IT) fokussierte Vorgabe hat das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) gesetzt: Mit dem sogenannten «IT-Grundschutz» wird eine systematische Vorgehensweise zum Identifizieren und Umsetzen von Sicherheitsmassnahmen der unternehmenseigenen IT eingefordert. Das Ziel ist, ein mittleres, angemessenes und ausreichendes Schutzniveau für IT-Systeme aller Firmen in Deutschland zu erreichen.

Für ein solches System werden Verfahren und Regeln innerhalb einer Organisation erarbeitet, um dann zum PDCA-Lifecycle-Management der Informationssicherheit überzugehen (PDCA steht für: Plan – Do – Check – Act).



© depositphotos

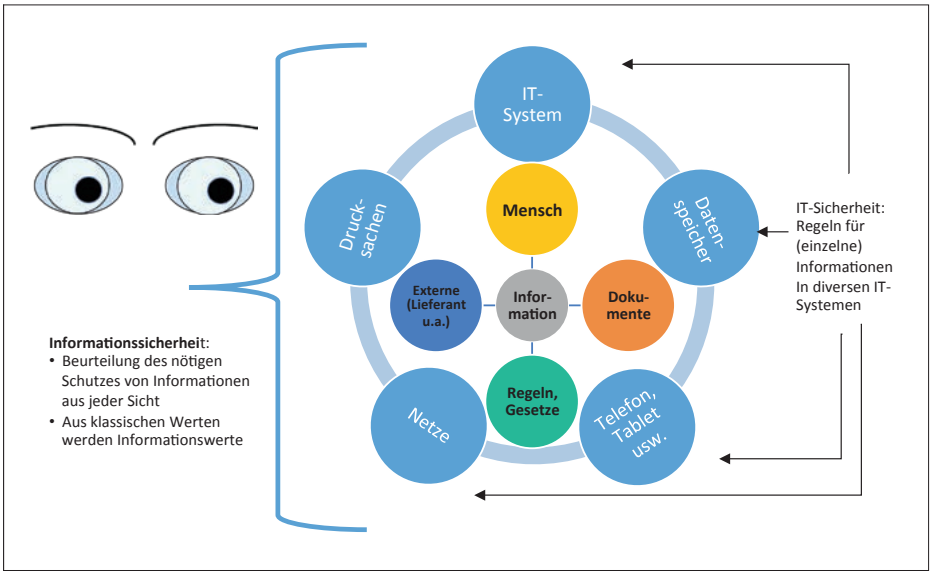
Informationssicherheit als kontinuierlicher Prozess im PDCA-Zyklus.

Mit ISMS wird die Informationssicherheit nicht nur aus der IT-Warte heraus betrachtet, sondern «integriert» auf alle relevanten Elemente bezogen. Der Vorteil eines integrierten Managementsystems ist das systematische Disziplinen übergreifende Vorgehen, um technische Sicherheitsmassnahmen in der IT, Schutzmassnahmen in der Datenverwendung, Sicherheitsanforderungen in Bereichen der Infrastruktur, Organisation und Personelles miteinander verwoben zu betrachten. Es geht also um Einzelanforderungen genauso wie um Schnittstellen und End-to-End-Betrachtungen von Verantwortung und IT-Sicherheit.

Welches ist der Nutzen für KMU?

Durch Einführung eines ISMS gewinnt ein KMU in relativ kurzer Zeit die Sicherheit, mit Informationen nach verlässlichen Schutzregeln umzugehen: nicht das Rad selbst erfinden, sondern Anwendung von bereits erprobten Mechanismen umsetzen. Schnell werden Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit, Authentizität, Verantwortlichkeit und Verlässlichkeit verbessert. Der bewusste Umgang mit Unternehmenswerten wird «State of the Art», die geltenden Regeln sind definiert und für alle verbindlich. Mit Schnelligkeit und Transparenz einen höheren Schutz der eigenen Informationswerte zu erreichen, das ist der grosse Nutzen von ISMS für ein KMU.

Ein weiterer Nutzen ist die Analyse der Anforderungen an die Sicherheit von Informationen und Werten und zum Beispiel die Gegenüberstellung zu vorhandenen Vorkehrungen. So wird oft ein grosser Teil des IT-Budgets für den Betrieb redundanter Systeme investiert, in der An-



© 4m2s

ISMS – ein ganzheitlicher Ansatz.

nahme, dass dadurch die Sicherheit massgeblich gesteigert werden kann. Eine Analyse der Anforderungen kann – um ein Beispiel zu nennen – aufzeigen, dass ein redundantes IT-System für die Sicherheit der spezifisch kritischen Prozessleistung gar keine Relevanz hat, folglich der IT-Service gar nicht notwendig ist. Konkret ergibt sich daraus eine erhebliche Einsparung der Redundanz – ausgelöst durch eine kleine einmalige Investition in die Analyse der Anforderungen gemäss ISMS. Und zusätzlich zu dieser finanziellen Einsparung kann das Unternehmen nun fachliche Prozesse zielgerichtet mit IT-Investitionen optimieren.

Was haben grosse international tätige Firmen davon?

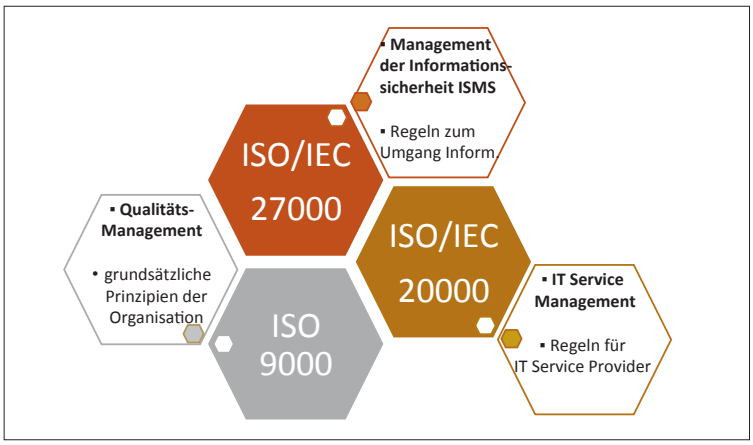
Internationale Normen wie ISO 27001 haben den Vorteil, dass sie rund um den Globus angewendet werden können. Die lokale Zertifizierung kann so nach einheitlichen Kriterien erfolgen. Das Regelwerk ist in allen Teilen der Unternehmung gleich, der Umgang mit und die Klassifizierung von Informationen ist vereinheitlicht und bietet grösstmöglichen Schutz vor Missbrauch. Bei grossen, internationalen Projekten ergeben sich erhebliche Einsparungen, da die beteiligten Mitarbeitenden aus den unterschiedlichsten Kulturkreisen nach den gleichen Regeln arbeiten und keine Unklarheit bei der Anwendung der Sicherheitsaspekte entsteht.

Mobile Working, eine grosse sicherheitsrelevante Herausforderung seitens IT wie bezüglich des persönlichen Verhaltens, wird nach gleichen Grundsätzen gehandhabt. Innerbetrieblicher Transport von Informationen über Landesgrenzen hinweg ist klar geregelt und folgt den gleichen Standards. Lösungen für etwa die Verschlüsselung von E-Mails, den Versand von vertraulichen Dokumenten oder generell den Umgang mit klassifizierten Informationen folgen nach einmal definierten Regeln und müssen nicht in jeder Niederlassung «erfunden» werden. Arbeitsortwechsel innerhalb der Firma hat somit keine Auswirkungen auf die Handhabung von Informationen.

Gegenüber Kunden kann mit einem etablierten ISMS die Sicherheit gegeben werden, dass dem Lieferanten übergebene schützenswerte Informationen nach einheitlichen Richtlinien behandelt werden. ISMS bildet eine Vertrauensbasis zwischen dem Kunden und Lieferanten, anywhere, anyplace, anytime!

Welchen Vorteil bringt die Umsetzung nach ISO 27001?

Die Anwendung der Norm ISO 27001 bietet Gewähr, dass der Schutz der Informationen umfassend und in allen Bereichen Anwendung findet. Nicht nur IT, sondern auch der Umgang mit portablen Speichermedien, Papierdokumenten und Verhalten der Mitarbeitenden generell stehen im Fokus. Auch gegenüber zweifelhaften Telefonaten und Social Engineering: Gerade hier ist es wichtig, dass allen klar ist, wie mit klassifizierten Informationen umzugehen ist, dass keine Gespräche über innerbetriebliche Vorgänge in öffentlichem Raum abgehalten werden usw., aber es ist ja altbekannt, dass der Mensch die grösste Schwachstelle in dieser Hinsicht ist.



© 4m2s

Aufbau eines ISMS: ISO 9000, ISO 20000, ISO 27000.

Die Regeln des ISO 27001 stellen auch sicher, dass ISMS als Managementsystem lebt und sich mit dem Unternehmen stetig weiterentwickelt, Neuerungen implementiert werden. Kontinuierliche Mechanismen zur Prüfung auf Schwachstellen müssen regelmässig durch das Topmanagement begutachtet werden, Massnahmen daraus abgeleitet und umgesetzt werden. Informationssicherheit wird so Teil der Unternehmenskultur und wird zum langfristigen Erfolgsfaktor.

Welche Rolle spielen Tools bei der praktischen Umsetzung?

Der Einsatz von geeigneten Tools erlaubt speziell in der IT-Landschaft, die Übersicht zu Anforderungen, Systemen und Schnittstellen, kritischen Anwendungen und Daten pflegenden Personen von zentraler Stelle zu bewahren. Im Alltag ist das unter anderem speziell nützlich bei der Zuordnung von Zugriffsrechten, bei der Einführung von neuen Mitarbeitenden in der Unternehmung oder Definition von verschiedenen Profilen für unterschiedliche Aufgabengebiete, projektbezogen, kundenbezogen. Nach einem Ereignis sind diese Informationen sprichwörtlich Gold wert, um den Wiederanlauf nach dem grössten ereignisbezogenen Nutzen etappieren zu können.

Der Einsatz von Werkzeugen empfiehlt sich dann, wenn sie breite Anwendung finden, zum Beispiel bei der stetigen Analyse von Schwachstellen und deren Beseitigung. Das heisst, das eingesetzte Werkzeug soll dann auch die Nachweise für die Fehlerbehebung respektive Weiterentwicklung liefern. Damit wiederum ist die Verfolgung der Umsetzung von Massnahmen möglich und im Gesamtkontext von ISMS kann die Wirksamkeit von Massnahmen und Entwicklungsschritten beurteilt werden.

Werkzeuge können auch einen Workflow/Abläufe vorgeben, womit die Einhaltung von ISMS-Richtlinien sichergestellt werden kann.

Beim Schutz von geistigem Eigentum – sehr wichtig für KMU – ist die Anwendung von Werkzeugen besonders bedeutend. Erfindungen müssen geschützt werden und dürfen nicht zu früh in falsche Hände geraten. Geeignete Ablagen und Verfahren bieten hier Schutz vor Missbrauch oder unerlaubtem Zugang.

Fazit

Mit der Planung gemäss ISMS können sowohl KMU als auch grössere Unternehmen einen Mindeststandard von Informationssicherheit erreichen, der für alle Unternehmenswerte zusätzlichen Nutzen bringt: Für die praktische Umsetzung werden die Anforderungen an Informationssicherheit und Erwartungen aus Sicht der Geschäftsprozesse definiert. Unter Anwendung des internationalen Standards ISO 27001 ergibt sich in effizienten Schritten ein aktuelles Bild der unternehmensspezifischen Situation, womit zielgerichtet und prozessorientiert eine Weiterentwicklung zum Schutz der Unternehmenswerte eingeleitet werden kann. Aus eigener Erfahrung: Es lohnt sich. ■

ALMUT EGER UND WALTER RÜEGG

Senior Consultants und Trainer für Notfall-/Krisenmanagement, BCM und ISMS bei 4m2s – 4 Management 2 Security GmbH Zürich und Frankfurt, Auditoren für TÜV Rheinland.