Die Zeiten ändern sich …

Die Geschichte der internationalen Sicherheitsstandardisierung ist noch relativ jung, ihre Anfänge liegen erst etwa dreißig Jahre zurück. Zu Beginn ging es dabei vor allem um das Schutzziel Vertraulichkeit, der Fokus lag bei der Normung kryptographischen Verfahren. Inzwischen haben wir verstanden, dass technische Mechanismen nur einen Teil des Normungsbedarfs ausmachen, und dass oft weniger mangelnde Technologien denn mangelndes Vertrauen die Einführung bzw. Nutzung neuer Dienste behindern.

Jedem, der sich heute mit Managementsystemen beschäftigt, ist der sogenannte PDCA-Zyklus ein Begriff, der Planung (Plan), Implementierung (Do), Überwachung (Check) und resultierende Verbesserung (Act) umfasst und das Nicht-Nachlassen beim Immer-Besser-Werden zum Ziel hat. Kontinuierlichen Verbesserungsbedarf gibt es dabei auf verschiedenen Ebenen:

- Zunächst natürlich auf Seiten der Normen selbst, die einem regelmäßigen Review und Update-Prozess unterliegen. Ähnlich wie im ISMS-Umfeld macht man übrigens auch hier gelegentlich die Erfahrung, dass das Starten einfacher ist, als das Durchhalten.
- Bei den Standardisierungsprozessen, insbesondere im Hinblick Verschlankung und Beschleunigung.
- Und schließlich bei den Strukturen der Normierungsgremien.

Insbesondere ist das PDCA-Prinzip fester Bestandteil von Sicherheitsmanagementsystemen wie etwa ISO/IEC 27001. Ihre enorm gewachsene Beliebtheit verwundert nicht, versprechen sie doch u.a. eine Verringerung von Geschäftsrisiken, besser strukturierte Prozesse, Wettbewerbsvorteile, und die Vermeidung von Imageschäden.

Lenka Fibíková und Roland Müller zeigen in diesem Zusammenhang auf, wie Informationssicherheit eine wichtige Rolle bei der Modernisierung der Informationstechnik eines Unternehmens spielen kann, wenn Sicherheitsmechanismen und deren Konsequenzen offen diskutiert werden und insbesondere die Informationssicherheitsstrategie stark auf die Geschäftsstrategie eines Unternehmens abgestimmt ist.

Mangelndes Vertrauen führt vielfach dazu, dass Verbraucher, Unternehmen und Verwaltungen elektronische Transaktionen nur zögerlich nutzen. Christoph Thiel und Arno Fiedler beleuchten neben der kritischen Bewertung des Entwurfs einer neuen EU-Verordnung zu Identifizierung, Authentifizierung und Signaturen (eIAS), die Signatur-Standardisierungsaktivitäten bei CEN/CENELEC und ETSI (Mandate 460).

Der Beitrag von Gisela Quiring-Kock setzt sich ebenfalls mit den Stärken und Schwächen des Entwurfes der EU Verordnung eIAS auseinander und schlägt diverse Verbesserungen speziell zum Erreichen der Interoperabilität vor. Sie versteht den Entwurf als Schritt in die richtige Richtung, der u.a. auch in das nationale Gesetz zur Förderung der elektronischen Verwaltung einfließen sollte.

Auch die elektronische Rechnungsstellung ist in der europäischen Standardisierung bereits seit vielen Jahren ein Thema. Der Beitrag von Stefan Engel-Flechsig fasst deren Bedeutung für die Praxis der Unternehmen, die Politik sowie die Rechtssetzung der Europäischen Union und der EU Mitgliedstaaten zusammen und sieht ein Etappenziel erreicht.

In einer Technikwelt, die Aspekte der IT-Sicherheit in einer Vielzahl von Verfahren und Produkten berücksichtigen muss, gewinnt neben dem Erarbeiten von Normen die Branchen und Technologiefelder übergreifende Koordinierung und Auswahl geeigneter Normen in ganz erheblichem Maße an Bedeutung. Der Beitrag von Cord Wischhöfer beschreibt die dazu seit einiger Zeit laufenden Aktivitäten des DIN.

ISO/IEC JTC 1 „Information Technology" hat Ende 2012 sein 25-jähriges Jubiläum gefeiert. Im Gateway berichtet aus diesem Anlass Karen Higgenbottom, Vorsitzende von JTC1, über aktuelle Herausforderungen an die internationale Standardisierung, die sich durch den schnellen technologischen Wandel ergeben.

Die Zeiten ändern sich und bestenfalls gestalten wir diesen Wandel immer aktiv mit. Wir hoffen, das Spektrum der Beiträge in diesem Heft findet Ihr Interesse.

Walter Fumy