Nr. 3, März 2010

ISSN 1862-4375

IT·Grundschutz

Informationsdienst

Praxis und Anwendungen

Grundschutz im Krankenhaus

Seite 7

Quelle: iStock-xchng/fsc2k5

NEWS

19. EICAR-Konferenz in Paris legt Fokus auf ICT Security *Seite 2*

Certgate tritt dem IT-Verband BITKOM bei *Seite 2*

Gefahr für mobile Anwendungen nimmt zu *Seite 2*

Workshops

Windows 7 und die Sicherheit *Seite 3*
Compliance im eHealth verbessern *Seite 9*

Praxis und Anwendungen

Kolumne: Die größte Schwachstelle im System *Seite 6*
Klinikum Braunschweig sichert IT-Infrastruktur *Seite 7*

Studien und Analysen

Wirtschaftskriminalität nimmt zu *Seite 12*
Interview: Freud und Leid mit dem GSTOOL *Seite 14*

Rubriken

Editorial *Seite 2*
Veranstaltungen *Seite 16*
Impressum *Seite 6*

SecuMedia
Der Verlag für Sicherheits-Informationen

Compliance im eHealth verbessern

Basis für die erfolgreiche ISO 27001 Zertifizierung

Judith Balfanz, Vice President Marketing, AuthentiDate International AG

Die zunehmende Digitalisierung geschäftlicher Abläufe führt zu zunehmend komplexen Prozessen. Dies ist, nicht zuletzt durch die elektronische Gesundheitskarte, auch im Gesundheitswesen zu beobachten. Um Compliance-Vorschriften zu genügen ist die Zertifizierung nach ISO 27001 eine gute Lösung.

Ein Dienstleister oder Hersteller im Gesundheitswesen muss sein Unternehmen nicht nur genauso sicher und regelkonform führen wie in einer anderen Branche sondern sogar noch genauer auf die internen und externen Prozesse achten. Viele der Prozesse sind höchst unternehmenskritisch, verlaufen diese unplanmäßig oder fallen gar aus, entsteht ein nur schwer oder gar nicht regulierbarer Schaden für die Organisation. Gleichzeitig steigt aber die Menge der sensiblen, personenbezogenen Daten, die verarbeitet, weitergeleitet und langfristig vorgehalten werden müssen. Für Führungskräfte in Krankenhäusern, Rehabilitationszentren, bei Krankenkassen, Krankenversicherungen, Einkaufsgemeinschaften und auch der Zulieferindustrie wird daher sowohl die Prozess-, als auch Datensicherheit immer schwerer kontrollierbar.

Die Verantwortlichen müssen sicher stellen, dass die Informationssicherheit zu jedem Zeitpunkt gewährleistet ist, um eigene Haftungsrisiken zu minimieren. Hierbei gilt es für die Verantwortlichen nicht nur unbeabsichtigte Fehler zu vermeiden, sondern auch absichtlichen Manipulationen von Prozessen und Daten vorzubeugen. Schäden durch nicht funktionierende Informationstechnologie gehören hierzu genauso, wie die ungewollte Veröf-

fentlichung von sensiblen Patientendaten. In beiden Fällen entsteht der Organisation ein Schaden. In einem Fall dadurch, dass eine Leistung nicht erbracht werden kann, im anderen Fall durch Schadensersatzklagen oder Imageschaden.

Um ein höchstmögliches Maß an Informationssicherheit in allen Facetten sicherzustellen, hat sich in der Praxis der Einsatz von Informations-Sicherheits-Management-Systemen (ISMS) bewährt. Die Vorgehensweise für die Einrichtung eines ISMS ist mittlerweile in internationalen Standards festgeschrieben. Die Konformität mit diesen Standards ist zertifizierbar, so dass hierüber ein Nachweis gegenüber Dritten erbracht werden kann. Ein sehr weit verbreiteter Standard ist ISO/IEC 27001:2005; kurz ISO 27001.

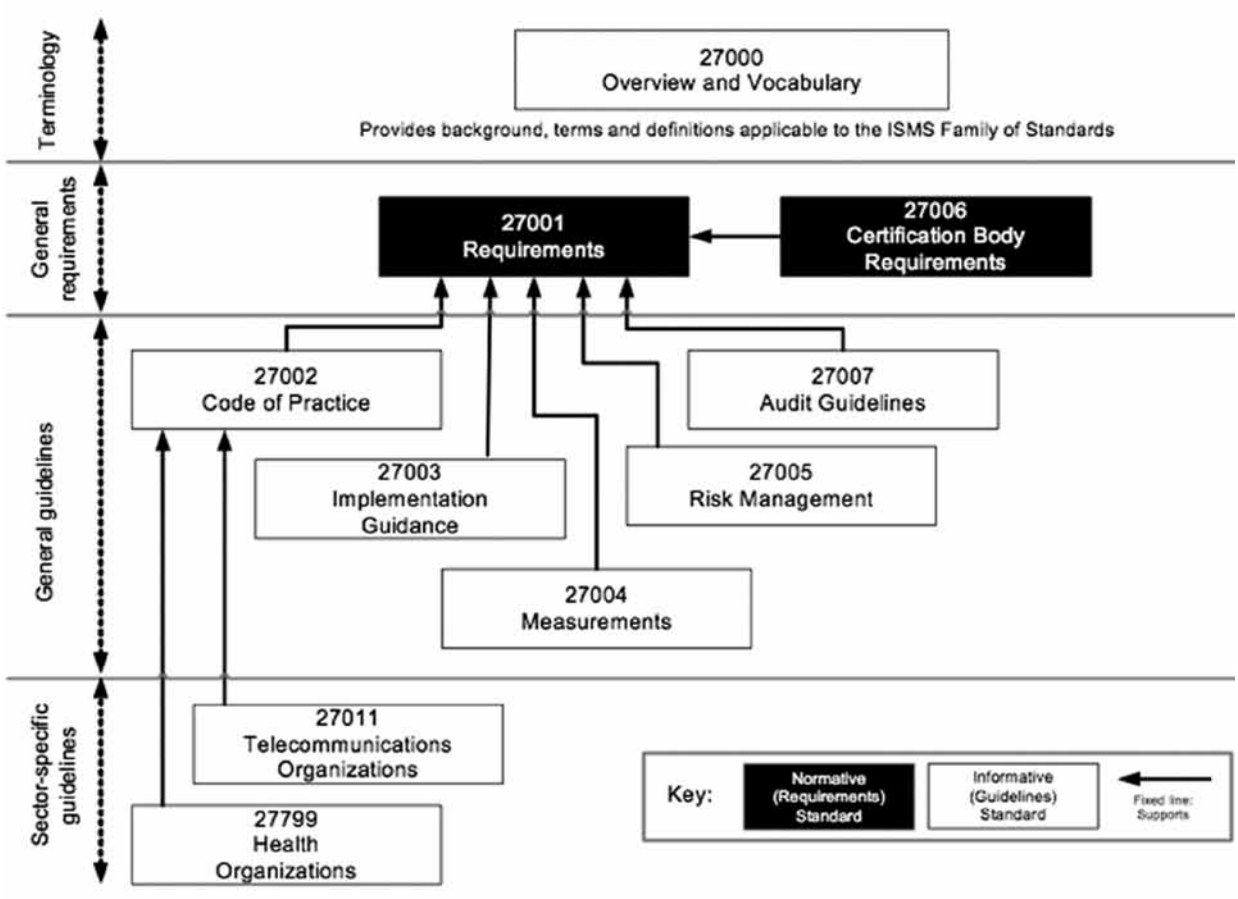
Die Einrichtung eines Information-Security-Management-Systems (ISMS) bietet Verantwortlichen in Unternehmen und Organisationen gleich mehrere Vorteile:

1. Erkennen von bislang verborgenen Sicherheitslücken im Prozess: Bereits während der Einrichtung des ISMS werden Unternehmensprozesse umfänglich erfasst und dokumentiert. Somit können Fehler im Prozess wie ein fehlendes 4-Augen-Prinzip bei einer kritischen Applikation direkt erkannt und behoben werden.

2. Dauerhafte Transparenz für Prozesse: Durch die Prozessdokumentation werden alle Prozesse transparent. Notwendige Prozessänderungen lassen sich schnell umsetzen.

3. Kennzahlen zur schnellen Kontrolle: Bei der Einrichtung eines ISMS werden Kennzahlen zur Prozesskontrolle eingeführt. Die Verantwortlichen müssen nur ein Minimum an Arbeit aufwenden, um die Ordnungsmäßigkeit der Prozesse zu überwachen. Die Kontrolle der Kennzahlen ermöglicht bereits eine gute Prozessüberwachung ohne ins Detail zu gehen.

4. Substanzielle Schadensbegrenzung und -reduzierung durch Früherkennungssystem: Durch die Verwendung von Kennzahlen können Risiken, Prozessfehler, Datenverluste und Manipulationen schneller erkannt und Gegenmaßnahmen ergriffen werden. Zusätzlich werden durch regelmäßige Reviews und Kennzahlenabgleiche über einen längeren Zeitraum unternehmensspezifische Vergleichswerte ermittelt. Das ISMS verbessert somit selbst die Aussagekraft der Kennzahlen, da auch kleinste Abweichungen von den Standards sofort erkannt werden.



Beziehung der ISO 27xxx Standards untereinander

5. Kostenreduktion durch nachweisbare Reduktion von Schadensfällen und Unternehmensrisiken: Da die Einrichtung eines ISMS im Allgemeinen mit einer ISO 27001 Zertifizierung durch unabhängige Dritte abgeschlossen wird, erhält die Organisation einen anerkannten Nachweis zur Sicherstellung der Informationssicherheit. Dieser kann unter anderem gegenüber den Haftpflichtversicherern zur Reduktion von Versicherungspolicen verwendet werden.

6. Positive Außenwirkung: Die ISO 27001 Zertifizierung stellt ein allgemein anerkanntes Gütesiegel dar und eignet sich gegenüber Geschäftspartnern und Kunden als „Verkaufsargument". Bei Ausschreibungen im eHealth Markt wird die Einführung eines ISMS (oder darauf aufsetzend eine ISO 27001 Zertifizierung) häufig als Selektionskriterium verwendet.

7. Reduzierung des Haftungsrisikos für Führungskräfte: Schnelleres Erkennen von Fehlern und demzufolge schnelleres Eingreifen mindert die Haftungsrisiken für Prozessverantwortliche und Führungskräfte. Zusätzlich stellt die Einrichtung eines ISMS und die ISO 27001 Zertifizierung einen Nachweis darüber dar, dass die Führungskraft ihrer Pflicht zur Sicherung der Informationssicherheit bestmöglich nachgekommen ist. Falls dennoch Schadensfälle eintreten sollten, können die Verantwortlichen nachweisen, dass sie ihrer Sorgfaltspflicht nachgekommen sind und bestmöglich Maßnahmen ergriffen haben, um diesen Schadensfall zu verhindern.

Schritte zur ISO Zertifizierung

Der Focus von ISO 27001 liegt darauf, die Rahmenbedingungen zu definieren, nach welchen ein ISMS aufgesetzt und betrieben werden muss, um darauf basierend die ISO 27001 Zertifizierung erfolgreich zu durchlaufen. Der ISO 27001 Standard liefert damit einen Kriterienkatalog für die „Zertifizierung" eines ISMS. Spricht man davon, dass sich ein Unternehmen nach ISO 27001 zertifizieren lassen will, so verbirgt sich dahinter nichts anderes als der Aufbau eines ISMS, welches später von unabhängigen Dritten nach festgelegten Kriterien geprüft und bestätigt wird. Bei erfolgreicher Prüfung und Bestätigung des ISMS ist die ISO 27001 Zertifizierung das Resultat.

Der Aufbau eines ISMS bildet das Herzstück einer ISO 27001 Zertifizierung. Im Zusammenhang mit Informationssicherheit spricht man in der Regel vom ISO 27001 Standard. Dies gibt jedoch genau betrachtet nur einen Teilaspekt wieder. Der Standard ISO 27001 wird durch eine ganze Reihe weiterer Standards ergänzt. ISO 27001 alleine ist im Grunde überhaupt nicht anwendbar. Daher spricht man häufig auch von der ISO 27000 Familie oder von ISO 2700x.

ISO 27001 definiert die Grundanforderungen an ein ISMS. Bei Konzeption und Umsetzung des ISMS fällt schnell auf, dass einige Teilaspekte in weiteren ISO Standards näher spezifiziert sind. Unter anderem existiert ISO 27002, ein Leitfaden zur Implementierung von ISMS. Er definiert verschiedene Zielsetzungen und Kontrollziele, welche durch das ISMS erreicht werden müssen. Aktuell sind sieben Standards für den Aufbau eines ISMS von Bedeutung.

ISO Richtlinien sind grundsätzlich branchenneutral gefasst. Sie definieren aus der Vogelperspektive welche Prozesse, Kennzahlen, Kontrollzahlen und ähnliches herangezogen werden sollen, um die Informationssicherheit langfristig zu gewährleisten. Prozesse und Kennzahlen hingegen sind meist branchenspezifisch geprägt. Daraus ergibt sich, dass jede Branche selbstverständlich auch ihre „eigenen" kritischen Prozesse und Kennzahlen hat. Derjenige, der eine ISO 27001 Zertifizierung leitet und den Aufbau des ISMS realisiert, muss zwingend über umfangreiche ISO-bezogene Branchenkenntnisse verfügen. Dabei ist es wichtig, dass die Personen Kenntnisse und praktische Erfahrungen aus der Umsetzung einer ISO 27001 Zertifizierung in der jeweiligen Branche gesammelt haben. Nur so können die kritischen Prozesse identifiziert und durch das ISMS abgedeckt werden.