Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Informationssicherheit als Motor zur nachhaltigen Qualitäts-verbesserung der gesamten IT

Der Standpunkt von Dr. Simon Hoff greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Informationssicherheit wird oft als ein Overhead empfunden, der die Arbeit eines Entwicklers, Architekten, Administrators oder Nutzers in der IT erschwert. Das Gegenteil kann jedoch der Fall sein, wenn ein sogenanntes Information Security Management System (ISMS) im Sinne von Standards wie ISO 27001 oder BSI IT-Grundschutz richtig umgesetzt wird.

Die Prüfpunkte in einem Sicherheitskonzept eines ISMS beispielsweise für eine Anwendung und die zugehörigen IT-Komponenten decken dabei typischerweise den gesamten Lebenszyklus ab:

- Planung: Wurden nachvollziehbare konzeptionelle Überlegungen angestellt, z.B. in Form einer Architektur dokumentiert, Anforderungen analysiert und dabei Aspekte der Informationssicherheit berücksichtigt? Wurde betrachtet, Daten gemäß ihrem Schutzbedarf bei Verarbeitung, Transport und Speicherung zu sichern?

- Beschaffung und Umsetzung: Wurden Produkte anhand eines Anforderungskatalogs ausgewählt und getestet? Werden die Komponenten gemäß den Vorgaben konfiguriert und wird dies geprüft? Wird die Initialkonfiguration dokumentiert und gesichert?

- Betrieb: Erfolgt die Administration der Komponenten auf eine sichere Weise? Werden die Komponenten überwacht und ist festgelegt, welche Ereignisse protokolliert werden, welche Daten dabei aufgezeichnet werden und wie mit Protokollen umgegangen wird? Werden Changes und Patches systematisch nach einem geregelten Prozess durchgeführt, getestet und dokumentiert? Sind Anwendungen und zugehörige IT-Systeme im Verwundbarkeitsmanagement erfasst und sind Vorgehensweisen bei Sicherheits- und Notfällen festgelegt?

- Außerbetriebnahme: Werden bei Außerbetriebnahme bzw. Weitergabe Daten auf Systemen gelöscht?

Solche Sicherheitskonzepte sind natürlich aufwendig, jedoch geht es hier um nichts geringeres als um durchdachte IT-Architekturen und IT-Konzepte, die geregelte Einführung von IT-Komponenten sowie ordentliche, lebendige und dokumentierte Prozesse für den Betrieb von Anwendungen und IT-Komponenten und natürlich darum, dass hier die Informationssicherheit nicht zu kurz kommt. Wesentlich ist dabei die Integration der Informationssicherheit in die IT-Prozesse insbesondere in den Bereichen Beschaffung, Change Management, Incident Management und Risikomanagement.

Damit ein Sicherheitskonzept nachhaltig ist, ist es außerdem entscheidend, den Sicherheitsprozess als PDCA-Zyklus[1] zu gestalten, der neben den erforderlichen Schnittstellen zu anderen IT-Prozessen eine regelmäßige Prüfung des Stands der Informationssicherheit festschreibt. Solche regelmäßigen Prüfungen des Stands der Umsetzung von Maßnahmen zur Informationssicherheit können in der IT-Revision verankert werden. Der nötige Druck zur Maßnahmenumsetzung kann durch eine Zertifizierung (z.B. nach ISO 27001) verstärkt werden, da Nachlässigkeiten in der Informationssicherheit durchaus zum Entzug eines Zertifikates führen können.

Mit jedem Durchlauf durch den PDCA-Zyklus des ISMS werden IT-Prozesse rundgeschliffen, die Qualität der IT-Dokumentation, des IT-Betriebs und letztendlich der gesamten IT verbessert. Ein ISMS erschlägt also (mindestens) zwei Fliegen mit einer Klappe und in diesem Sinne bringt ein ISMS sehr viel und kostet im Vergleich zu den Schäden, die bei Sicherheitsvorfällen und insbesondere bei unzureichender Betriebsstabilität der IT drohen, wenig. Nebenbei bemerkt: Das ist der eigentliche Business Case der Informationssicherheit.

Egal wie groß oder klein eine Institution ist, es besteht die realistische Möglichkeit, ein ISMS als Motor der Qualitätsverbesserung und Betriebsstabilisierung der IT zu implementieren. Dabei müssen sich natürlich die Leistung und damit verbunden der „Spritbedarf“ des Motors sowie die „Fahrweise“ an den Möglichkeiten der jeweiligen Institution orientieren. Dabei ist es besser mit geringerer Geschwindigkeit langfristig eine Informationssicherheit zu schaffen, als nach einem Sprint keinen Atem mehr zu haben (weniger ist oft mehr, wenn es nachhaltig ist).

[1] PDCA = Plan, Do, Check, Act

Jetzt Leser werden! Wenn Sie aktuelle Artikel kostenlos und zeitnah erhalten möchten, können Sie den Netzwerk-Insider hier abonnieren: www.comconsult-research.de/insider/