Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Nachhaltige Informationssicherheit: Ohne Druck geht es nicht

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.

Seit letztem Jahr wird die Arbeit am neuen IT-Sicherheitsgesetz [1], das Betreiber kritischer Infrastrukturen betreffen wird, in der IT mit besonderer Spannung verfolgt. Im aktuellen Gesetzentwurf heißt es beispielsweise in § 8a unter anderem:

- „(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen."

- „(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen."

Dies ist nichts anderes als die Forderung innerhalb eines gewissen Zeitraums ein sogenanntes Information Security Management System (ISMS) zu implementieren und dessen nachhaltige Umsetzung in regelmäßigen Abständen nachzuweisen.

Wesentliche Standards sind in diesem Zusammenhang neben den BSI-Standards (inklusive der BSI IT-Grundschutz-Kataloge) insbesondere ISO 27001 aber auch COBIT.

Die Umsetzung von Sicherheitskonzepten nach solchen Standards ist zunächst ein aufwendiges Vorhaben, das bis zu einem akzeptablem Umsetzungsgrad durchaus mehrere Jahre in Anspruch nehmen kann. Besonders wichtig ist dabei, dass Sicherheitskonzepte im Rahmen eines geregelten Prozesses erstellt, umgesetzt und gepflegt werden, um mit dem Entwicklungstempo in der IT Schritt halten zu können. Kernelemente hierzu sind unter anderem:

- Schnittstellen zu anderen (IT-)Prozessen, z.B. Beschaffung, Change Management, Configuration Management, Incident Management, Compliance Management und Risikomanagement

- IT-Sicherheitsrisiko-Management für den Umgang mit nicht oder nur teilweise umgesetzten Maßnahmen

- Kennzahlen für die Informationssicherheit zur Erfolgsmessung und entsprechendes Reporting an das Management

- Nachhaltigkeit durch regelmäßige Prüfungen bzw. Audits erzwingen

Gerade der letzte Punkt ist von besonderer Bedeutung, denn ohne Druck wird früher oder später an entscheidenden Punkten in der Informationssicherheit gespart. Innerhalb von kürzester Zeit klaffen so Lücken in den Sicherheitskonzepten und Risikobewertungen, die letztendlich die gesamte bis dahin geleistete Anstrengung fragwürdig machen und zu einem entsprechend großen Schaden für die jeweilige Institution führen können.

Die notwendige regelmäßige Prüfung der Informationssicherheit kann zunächst z.B. von der IT-Revision wahrgenommen werden. Wenn das ISMS auf Basis von ISO 27001 oder der BSI-Standards aufgebaut wird, ist jedoch auch eine Zertifizierung möglich. Für die Aufrechterhaltung solcher Zertifikate sind regelmäßige Audits (z.B. in einem jährlichen Raster) und Re-Zertifizierungen (z.B. alle drei Jahre) erforderlich. Auf diese Weise entsteht ein natürlicher Druck zur Aktualisierung und Vervollständigung von Sicherheitskonzepten und von Risikobetrachtungen für die Bereiche, in denen Maßnahmen nicht angemessen umgesetzt werden konnten.

Es ist von daher eigentlich nicht überraschend, dass eine Zertifizierung im eben angesprochenen IT-Sicherheitsgesetz als Element eines Nachweises der Nachhaltigkeit deutlich genannt wird. Sie wird auch immer häufiger bei der Ausschreibung von Outsourcing-Vorhaben (inklusive Cloud Computing) gefordert. Letztendlich wird in der Zukunft ein anerkannter Nachweis der Qualität der Informationssicherheit ein Normalfall für das IT Business werden. Das IT-Sicherheitsgesetz ist hierzu als treibende Kraft ausgesprochen zu begrüßen!

[1] Siehe **https://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html**