Der Netzwerk Insider

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Informationssicherheit ist ohne Risikomanagement nicht denkbar

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.

Die Komplexität und die Dynamik der modernen IT und der damit verbundenen Gefährdungslagen führen zu ebenso komplexen wie sich stetig ändernden Katalogen von Sicherheitsmaßnahmen. Als Beispiel sei hier der Maßnahmenkatalog für Voice over IP (VoIP) und für Unified Communications & Collaboration (UCC) der in dieser Ausgabe des Netzwerk Insider vorgestellten Technischen Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf des BSI genannt. Alleine für VoIP und UCC werden ca. 80 Maßnahmen genannt, welche die für VoIP und UCC anwendbaren Maßnahmen der BSI IT-Grundschutz-Kataloge bei einem erhöhten Schutzbedarf ergänzen sollen. In Summe kommen hier für VoIP und UCC deutlich mehr als 150 Maßnahmen zusammen.

Eine weitgehende Umsetzung solcher Maßnahmenkataloge ist oft nur bei neu beschafften Anwendungen oder IT-Systemen möglich. Für Bestandssysteme können dagegen diverse Maßnahmen nicht oder nur teilweise umgesetzt werden. Außerdem dauert eine Maßnahmenumsetzung oft seine Zeit (z.B. die Einführung einer Verschlüsselungstechnik oder die Anpassung eines Betriebsprozesses), bis eine vollumfängliche Wirkung der Maßnahme entsteht.

Daher ist ein Kernelement eines Information Security Management System (ISMS) die systematische und regelmäßige Erfassung des Ist-Zustands und die weitere Planung der Maßnahmenumsetzung.

Stellen wir uns hierzu eine Ampelfunktion vor, mit der wir den Umsetzungsgrad von den für die Komponenten in der IT-Landschaft (Prozesse, Anwendungen oder IT-Systeme) vorgesehenen Sicherheitsmaßnahmen bewerten: grün = Maßnahme umgesetzt,

gelb = Maßnahme teilweise umgesetzt, rot = Maßnahme nicht umgesetzt.

Dann scheint sofort klar zu sein, dass es der Idealzustand ist, auf der Statuslandkarte alle anzuwendenden Maßnahmen auf grün gesetzt zu haben. Nun haben wir aber eben gesehen, dass mit recht hoher Wahrscheinlichkeit auch in einer gut organisierten IT ein bunter Flickenteppich entsteht. Außerdem ist diese Landkarte der Informationssicherheit ja in höchstem Maße dynamisch. Was heute grün ist, kann morgen durch einen Change gelb werden und es kommen neuartige Anwendungen und IT-Systeme auf die Landkarte für die der Maßnahmenkatalog ggf. erst erarbeitet und umgesetzt werden muss.

Ist nun eine Statuslandkarte mit ziemlich viel gelb und rot wertlos? Nein, das Gegenteil ist der Fall. Diese Statuslandkarte ist ein fundamentales Instrument, unabhängig davon wieviel gelb und rot einem zu einem Zeitpunkt begegnet, denn auf dieser Basis kann mit den Mitteln des Risikomanagements eine systematische Vorgehensweise geschaffen werden, die den Umgang mit Lücken in der Maßnahmenumsetzung regelt.

Wir haben nämlich in der Informationssicherheit leider oft den Reflex, bei einer erkannten Sicherheitslücke sofort nach einem technischen Werkzeug zu suchen, das diese Lücke vermeintlich schließt und schlagartig materialisiert sich z.B. die nächste Firewall oder eine teure Überwachungslösung. Am Ende haben wir dann dank des neuen Werkzeugs aber oft genug zu viele Probleme in der Stabilität des Betriebs der IT im Vergleich zum Sicherheitsgewinn.

Wir benötigen also ein Instrument, das bei der Bewertung und Priorisierung von Sicherheitslücken bzw. nicht oder teilweise umgesetzten Maßnahmen hilft und unnötige Panikaktionen verhindert. Ein solches Instrument kann über das IT-Risikomanagement geschaffen werden.

Für unzureichend umgesetzte Maßnahmen können dabei folgende Punkte erfasst werden:

- Bewertung der Bedrohungen, die von der unzureichenden Umsetzung einer Maßnahme ausgehen, und der Eintrittswahrscheinlichkeiten von Schadensereignissen
- Planung der weiteren Maßnahmenumsetzung bzw. Angabe der Gründe, warum eine Maßnahmenumsetzung nicht möglich ist
- Analyse möglicher Ersatzmaßnahmen, falls eine Maßnahmenumsetzung nicht oder nicht in adäquater Zeit möglich ist
  Bewertung der Machbarkeit und Schätzung des mit der Umsetzung der Maßnahme bzw. der Ersatzmaßnahmen verbundenen Aufwands

Mit diesen Informationen ist eine Entscheidung über das weitere Vorgehen möglich. Insbesondere sind Priorisierungen möglich, und es kann sogar durchaus die Entscheidung getroffen werden, das Risiko einzugehen und gewisse Maßnahmen zunächst nicht weiter zu verfolgen und es bei dem Status quo zu belassen. Das Ergebnis ist ein sogenannter Risikobehandlungsplan für die oben beschriebene Statuslandkarte der als roter Faden für die Umsetzung von Sicherheitsmaßnahmen dient und entsprechend regelmäßig gepflegt werden muss.

Erst diese bewusste Auseinandersetzung mit Risiken liefert ein Kontrollinstrument, um eine Balance in der Informationssicherheit zwischen Aufwand und Sicherheitsgewinn zu schaffen. Dies ist der wesentliche Grund, warum Standards zum Aufbau eines ISMS wie ISO 27001 oder die BSI-Standards stets die Verwendung von Methoden des Risikomanagements fordern.