Quelle: SIV.AG

Einfache Maßnahmen für ein wirksames IT-Sicherheitsmanagement

*von **Dr. Sebastian Unger**, IT-Sicherheitsbeauftragter der SIV.AG*

Im Juli 2016 schreckte diese Nachricht die Branche auf: Zwei Studenten war es aufgrund „unzureichender Sicherheitskonfigurationen“ gelungen, auf die sensiblen Steuerungssysteme mehrerer deutscher Wasserwerke, Blockheizkraftwerke und Biogasanlagen zuzugreifen. Damit wäre „mit nur mäßigem technischem Aufwand“ jederzeit eine gezielte Sabotage und ein umfassender Datendiebstahl möglich gewesen. Schon einfache Veränderungen der Aufbau- und Ablaufstruktur und eine optimierte IT-Infrastruktur hätten hier nachhaltigen Schutz geboten.

Der Gesetzgeber hat die essentielle Bedeutung der Informations- und IT-Sicherheit für einen sicheren Netzbetrieb erkannt und verpflichtet Betreiber kritischer Infrastrukturen, zu denen u. a. Energie- und Trinkwasserversorger gehören, zur Etablierung geregelter Informationssicherheitsprozesse: Strom- und Gasnetzbetreiber müssen bis zum 31. Januar 2018 eine Zertifizierung nach ISO 27001 und den Vorgaben des IT-Sicherheitskatalogs nachweisen. Betreiber von Trinkwasserversorgungsanlagen, die oberhalb des Schwellenwerts von 500.000 Einwohnern liegen, müssen bis Mai 2018 einen Nachweis gemäß den Anforderungen des § 8 a Abs. 1 BISG erbringen.

Darüber hinaus beschäftigen sich auch Unternehmen der Energie- und Wasserwirtschaft mit dem Thema IT-Sicherheit, die noch nicht den gesetzlichen Nachweispflichten unterliegen. Einen wirksamen Schutz gegen Manipulationen und Datenverlust können diese Unternehmen auch ohne die Einführung eines standardisierten Informationssicherheitsmanagementsystems (ISMS) erreichen: Eine Vielzahl praxisbewährter Maßnahmen steht zur Verfügung, die ohne hohe Kosten kurzfristig effektiv sind und gleichzeitig einen umfassenden Schutz ermöglichen. Aber wo beginnen? Bei Virenschutz, Krypto-Chips oder abhörsicheren Besprechungsräumen? Ein systematisches Vorgehen spart auch hier viel Zeit und Geld.

Erste Orientierung kann ein Cyber-Sicherheits-Check bieten. Er bestimmt den jeweiligen Bedrohungsgrad und identifiziert schnell und stichprobenartig mögliche Schwachstellen und Risiken. Häufig und meist ungewollt geht dabei von den Mitarbeitern das größte Sicherheitsrisiko aus, wie zahlreiche Studien belegen. Das standardisierte Verfahren wurde von ISACA und BSI im Rahmen der Allianz für Cyber-Sicherheit entwickelt.

Weit technischer sind Penetrationstests. Hierbei werden reale Angriffe auf eine IT-Infrastruktur simuliert, um existierende Schwachstellen zu identifizieren und anschließend zu eliminieren. Diese Tests lassen sich automatisiert durchführen, um schnell zu Ergebnissen zu gelangen. Eine gründliche Analyse ist jedoch nur manuell durch einen erfahrenen Tester erreichbar, der zunächst versucht, von außen einzudringen (Off-Site-Test) und bei Bedarf anschließend das Schadenspotenzial bei erfolgreicher Infiltration eruiert (On-Site-Test).

Mit einer detaillierten Gap-Analyse geht es noch einen Schritt weiter. Hier wird bereits nah an der Norm ISO 27001 gearbeitet und es werden dringende Handlungsfelder auf dem Weg zu ihrer Erfüllung identifiziert. Die Ableitungen daraus können einerseits ganz konkrete Handlungsempfehlungen für die Verbesserung der operativen IT-Sicherheit darstellen, andererseits lassen sich die Erkenntnisse auch später für den Aufbau eines effektiven ISMS nutzen.

Darüber hinaus gibt es von unterschiedlichen Anbietern zahlreiche begleitende Seminare und Workshops zur Sensibilisierung und Vertiefung. Auch hier wird mit einfachen Maßnahmen und Umsetzungsempfehlungen auf eine zukünftige umfassende Zertifizierung eingezahlt. ■

Quelle: j-mel – Fotolia.com