Smart-Meter-Gatewayadministration

Einführung eines Informationssicherheitsmanagementsystems nach ISO/IEC 27001

Die Einführung intelligenter Messtechnik beim Endverbraucher bringt große Chancen für Netzsteuerung, bedarfsgerechte Energieerzeugung und transparente Preisgestaltung mit sich. Sie birgt jedoch auch Risiken: Durch den Einsatz von IT-Systemen in unkontrollierter Kundenumgebung sowie der Nutzung öffentlich zugänglicher Netze zur Datenfernübertragung werden Datenschutz und Datensicherung vor neue Herausforderungen gestellt.

Dem Smart-Meter-Gatewayadministrator (GWA) kommt bei der Einführung intelligenter Messtechnik als Informationsknotenpunkt angesichts gebündelter Prozess- und Datenverantwortung eine besondere Bedeutung zu. Von diesem wird durch das Energiewirtschaftsgesetz (EnWG § 21 e) gefordert, »[...] nach aktuellem Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherung zu treffen [...]«. Doch was ist ein ausreichendes Maß an Datenschutz und IT-Sicherheit und wie lässt sich dieses erreichen?

Informationssicherheitsmanagementsystem

Die konkrete Gestaltung der Sicherheitsanforderungen für GWA befindet sich in der technischen Richtlinie TR-03109-6 (TR) des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die zentrale Anforderung darin ist die Planung, Etablierung und Zertifizierung eines Informationssicherheitsmanagementsystems (ISMS). Dieses ist ein effektives Rahmenwerk, um Informationssicherheitsrisiken zu erkennen, zu bewerten und durch Maßnahmen nach Stand der Technik innerhalb eines PDCA-Zyklus (Plan/Do/Check/Act) zu behandeln.

Informationssicherheit ist kein rein technisches Thema. Sie ist gleichermaßen von aufeinander abgestimmten organisatorischen, personellen und technischen Maßnahmen abhängig. Im Vergleich zu bisherigen Sicherheitskonzepten setzt ein ISMS einen Schritt früher an: Am konkreten Beispiel eines GWA bedeutet dies beispielweise, dass vor der Anschaffung einer GWA-IT-Lösung die Anforderungen bezüglich Informationssicherheit

Dem GWA kommt bei der Einführung intelligenter Messtechnik als Informationsknotenpunkt eine besondere Bedeutung zu.

bestimmt worden sein müssen, um ein geeignetes Produkt wählen zu können.

Anforderungen bestimmen

Der erste Schritt für den Aufbau eines ISMS ist die Bestimmung der anwendbaren Gesetze und anderer Auflagen. Dies können sowohl externe Anforderungen, beispielsweise existierende Verträge, als auch interne Anforderungen sein, weil unter Umständen bereits andere Managementsysteme existieren, in die das ISMS integriert werden soll.

Definition des Geltungsbereichs

Die Definition des Geltungsbereichs oder Scopes auf Basis der erkannten Anforderungen legt fest, welche Geschäftsprozesse geschützt werden sollen. Die mindestens zu berücksichtigenden Anwendungsfälle werden in Kapitel 3 der TR beschrieben. Sie sind Grundlage für die im späteren Verlauf zu identifizierenden Systeme, Informationen, Personen und weiteren Ressourcen.

Inventarisierung der Werte

Vor Erstellung einer Schutzkonzeption müssen die schützenswerten Informationen beziehungsweise Werte oder Assets, und darauf aufbauend die zugrunde liegenden IT-Systeme sowie die für den ordnungsgemäßen Betrieb benötigten Ressourcen, erfasst werden. Auch hier bietet die TR eine gute Grundlage, da ebenfalls in Kapitel 3 allen Anwendungsfällen die mindestens benötigten Assets als Daten, Dienste, Anweisungen und Anbindungen zugeordnet wurden.

Sofern für die technische Umsetzung eine fertige GWA-IT-Lösung zum Einsatz kommt oder kommen soll, ist die Bestimmung der an den Kernprozessen beteiligten Systeme meist bereits gut dokumentiert. Zumindest kann angemessene Dokumentation bei der Auswahl einer Lösung im Lastenheft gefordert werden. Für eine ganzheitliche Sicht sollten zusätzlich Räume und Mitarbeiter sowie durch Dienstleister bereitgestellte Leistungen wie Kommunikationsverbindungen oder Energieversorgung inventarisiert werden.

Bestimmung des Schutzbedarfs

Mit dem Ziel, die GWA zu schützen, muss nun für alle erfassten Assets deren Schutzbedarf bestimmt werden. Praktischerweise gibt auch hier die TR in Kapitel 4 sowohl ein mögliches Klassifizierungsschema als auch Mindestvorgaben zu den Assets vor. Darauf aufbauend vererbt sich der Schutzbedarf unter anderem auf die zur Verarbeitung genutzten Systeme und Räume. Die weitere Anforderung der ISO 27001, jedem Asset einen Verantwortlichen zuzuordnen, kann in diesem Schritt mit erledigt werden.

Risikoanalyse

Ausgehend von den identifizierten Assets und deren Schutzbedarf kann nun eine Risikoanalyse durchgeführt werden. Da-

bei wird ein Prozess festgelegt und dokumentiert, der Risiken im Zusammenhang mit dem Verlust von Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität ermittelt. Gleichzeitig müssen Eintrittswahrscheinlichkeit und Schadensschwere eingeschätzt sowie Kriterien für die Risikoakzeptanz oder Risikobehandlung festgelegt werden. Allgemeine Bedrohungen sind in generischen Katalogen zusammengestellt – beispielsweise den Gefährdungskatalogen des IT-Grundschutzes des BSI. Spezifische Bedrohungen für GWA enthält die TR im Kapitel 4.4.

Die Einschätzung der Eintrittswahrscheinlichkeiten und Größe der Schäden kann kategorisiert geschehen, da häufig statistische Informationen für schädigende Ereignisse nicht verfügbar oder repräsentativ sind. Bis zu diesem Schritt reicht die Planphase des PDCA-Zyklus.

Auswahl und Umsetzung der Maßnahmen

Nach Kenntnis und Bewertung der allgemeinen und spezifischen Risiken können angemessene Maßnahmen zum Schutz der Assets ausgewählt und umgesetzt werden. Die Risikobehandlung ist durch Maßnahmen möglich, die die Eintrittswahrscheinlichkeit oder hervorgerufene Schäden verringern sowie durch Umstrukturierung von Prozessen, die Risiken verringern beziehungsweise Risiken transferieren – zum Beispiel Versicherungen. Risiken können bewusst akzeptiert werden, wenn eine andere Behandlung nicht wirtschaftlich oder umsetzbar erscheint. Der Risikobehandlungsplan ist Teil der Pflichtdokumentation und sollte auch Informationen enthalten, wann Maßnahmen umzusetzen sind.

Einen Satz von Mindestmaßnahmen, die umgesetzt werden müssen, befindet sich in Kapitel 4.5 der TR. Diese sind zwar deutlich konkreter formuliert, orientieren sich jedoch an den Mindestmaßnahmen beziehungsweise Controls des Annex A der ISO 27001. Hierbei handelt es sich mehr um einen Leitfaden zu den zu behandelnden Themen, damit keine wichtigen Bereiche übersehen werden.

Wird eine zugekaufte Lösung eingesetzt, sollte bei der Auswahl darauf geachtet werden, dass alle technischen Mindestvorgaben erfüllt werden. Auch wenn gängige Produkte teilweise damit beworben werden, dass keine IT-Expertise auf Seiten des GWA erforderlich ist, muss dennoch vom GWA überprüft werden können, ob alle Vorgaben zur sicheren Nutzung (Konfigurationen usw.) eingehalten werden.

Prüfung der Umsetzung und Bewertung der Maßnahmen

Obgleich die Prüfung, ob alle Maßnahmen eingeleitet wurden, wiederum als Maßnahme bezeichnet werden kann (TR Kap. 4.5.16), ist dieser Schritt im Modell des PDCA-Zyklus der Check-Phase zuzuordnen, wohingegen die Umsetzung von Maßnahmen in die Do-Phase fällt.

Die Wirksamkeit von Maßnahmen setzen frühestens nach der Implementierung ein. Aber auch dann können sie in einem konkreten Fall wirkungslos (geworden) sein. Neben der Revision (Prüfung der Umsetzung) ist daher auch eine Be-

wertung der Maßnahmen unabdingbar (Vollständigkeits- beziehungsweise Aktualisierungsprüfung). Beispielsweise könnte eine verschlossene Tür zum Zugangsschutz ihre Wirkung durch eine andere Maßnahme in Form offener Fluchtwege verlieren. Gleichsam bietet sich durch regelmäßige Kontrolle und Bewertung der Maßnahmen auch Potenzial für Einsparungen, wenn beispielsweise einzelne Maßnahmen durch eine Änderung im Prozess oder die Umsetzung anderer Maßnahmen obsolet geworden sind. Der Umsetzungsstatus jeder Maßnahme muss dokumentiert sein, damit jederzeit die Gesamtsicherheitslage bewertet werden kann. Dies ist neben den eigentlichen Audits, bei denen der Dokumentationsstand aktiv geprüft wird, vor allem bei Änderungen der Rahmenbedingungen sehr hilfreich, zum Beispiel für die Bewertung, ob ein Risiko durch eine neue Gefahrenquelle entsteht oder ausreichende Maßnahmen zum Schutz bereits implementiert wurden.

Korrekturen

Die Reaktion nach Prüfung und Bewertung der Maßnahmen ist, die erforderlichen Korrekturen vorzunehmen (Act-Phase). Falls mehrere Fehler oder Schwachstellen erkannt wurden, sollten die Korrekturmaßnahmen priorisiert geschehen. In jedem Fall müssen erkannte Nichtkonformitäten sowie deren Behandlung dokumentiert werden, um aus den Fehlern der Vergangenheit zu lernen und sicher zu sein, dass alle Sicherheitslücken beseitigt wurden.

Der erste Schritt für den Aufbau eines ISMS ist die Bestimmung der anwendbaren Gesetze und anderer Auflagen.

Verbesserungsprozess

Anforderungen, Prozesse, Bedrohungen, Schadensauswirkungen und Schutzwirkungen von Maßnahmen sind ständigen Veränderungen unterworfen. Informationssicherheit ist ein stetiger Prozess, der auf das Veränderungsbild reagieren muss. Alle erforderlichen Bestandteile des ISMS müssen in geeigneten Intervallen überprüft und bei Bedarf entsprechend angepasst werden.

Zertifizierungsaudit

Wurden alle Schritte durchlaufen, steht dem eigentlichen Zertifizierungsaudit nichts mehr im Weg. Vor Beginn des Audits muss ein Auditor gewählt werden, bei dem die »Chemie« zur eigenen Organisation stimmt.

Das Audit gliedert sich in zwei Phasen und wird jährlich wiederholt: die Dokumentenprüfung (Stufe 1) sowie die Prüfung der Umsetzung der in der Dokumentation beschriebenen Prozesse und Maßnahmen (Stufe 2). Spätestens an dieser Stelle wird von einer durchdachten, verständlichen und angemessenen Dokumentation profitiert, da sich ein Auditor auf der Basis der Dokumenten ein Bild der Abläufe, Risiken und Sicherheitsmaßnahmen – einschließlich deren Bewertung – machen muss. Werden vom Auditor keine grundlegenden Abweichungen festgestellt, endet das Audit mit einem Zertifikat, das die Umsetzung der gesetzlichen Anforderungen bescheinigt.

Häufige Fehler und Unterstützung bei der Implementierung

Managementsysteme werden häufig mit dem Vorurteil belegt, dass sie vor allem bürokratisch seien und unnötige Kosten verursachen. Sicherlich gibt es Beispiele, wo dies zutrifft. Jedoch dienen Managementsysteme nicht dem reinen Selbstzweck, sondern liefern Unternehmen einen Ordnungsrahmen, um Probleme effektiv zu behandeln. Damit ein ISMS seinen Zweck – die Verbesserung der Informationssicherheit – erreichen kann, sind einige Stolperfallen zu beachten.

Informationssicherheit ist kein Thema der IT-Abteilung, sondern spricht jeden einzelnen Mitarbeiter an. Es ist daher wichtig, dass alle Mitarbeiter die Notwendigkeit des Schutzes von Informationen verstehen und sich an diesem Prozess beteiligen. Eine hohe Akzeptanz wird einfacher erreicht, wenn sich neue Regelungen nahtlos in den gelebten Alltag integrieren lassen und verstanden wird, dass dem eventuell zusätzlich entstehenden Aufwand auch ein bedeutender Nutzen entgegensteht.

Informationssicherheit ist generell ein dauerhafter Prozess und kein Produkt, das einmalig gekauft wird. Ein Return on Investment kann demnach nur eintreten, wenn die Sicherheitskonzeption dauerhaft Anwendung findet, gleichermaßen wirksam und angemessen ist, und von jedem Mitarbeiter getragen wird.

Richtig ist, dass ein ISMS eine Dokumentation erfordert, die den aktuellen Stand der Informationssicherheit beschreibt und erkennen lässt, was zur Erreichung dessen getan wurde. Zusätzlich sollte beachtet werden, dass sich die Dokumentation des Managementsystems an der Realität der Organisation orientiert und nicht für eine unerreichbare Zielvorstellung konzipiert wurde.

Weiter spricht nichts dagegen, die Dokumentation auf die wirklich benötigten Informationen zu beschränken und dadurch eine unnötige Bürokratisierung zu vermeiden.

Die Implementierung eines ISMS kann grundsätzlich von den Mitarbeitern einer Organisation allein bewerkstelligt werden, sofern auf die Bereitstellung nötiger Ressourcen und die teilweise benötigte Rollentrennung geachtet wird. Wenn keine oder nur wenig Erfahrung beim ISMS-Aufbau im Unternehmen vorhanden ist, kann professionelle Unterstützung durchaus eine wirtschaftlich günstige Alternative sein. Sie führt in der Regel zu einer schnelleren Implementierung.

Bei der Beraterauswahl sollte unbedingt darauf geachtet werden, dass die Unterstützung bei der Umsetzung individuell an die vorhandene Basis anschließt. In der Regel sind bereits viele Prozesse zum Informationsschutz – teilweise unbewusst – etabliert. Nur so wird eine hohe Akzeptanz und Wirkung erreicht. Auf ein unter Umständen günstigeres Angebot für ein Produkt von der Stange, das lediglich einen allgemeinen Satz Dokumente und Regeln umfasst, dem sich die Organisation unterordnen muss, sollte prinzipiell verzichtet werden. Sonst besteht die Gefahr, dass das ISMS nur kurz vor den Zertifizierungsaudits läuft, was jeweils sehr viel Arbeit erfordert aber keinen Mehrwert für die Sicherheit bringt. Zusätzlich ist die Wahrscheinlichkeit, das Audit nicht zu bestehen, viel größer. Einem Auditor fällt in der Regel auf, dass es sich um nichtgelebte Prozesse handelt. Kleinere Fehler in einem noch nicht perfekten, jedoch gelebten ISMS sind dabei deutlich weniger kritisch, wenn später nachgewiesen werden kann, dass diese Fehler behoben wurden. Dies ist die Hauptaufgabe des ISMS – die Erkennung, Bewertung und Behandlung der Risiken.

Dr. **Deniz Ulucay**,
Berater für Informationssicherheit,
SRC Security Research & Consulting GmbH, Bonn

>> deniz.ulucay@src-gmbh.de

>> www.src-gmbh.de

43080