ISMS-Zertifizierung nach **DIN ISO/IEC 27001**

„Frühzeitig mit dem Thema befassen“

Bis zum 31. Januar 2018 müssen Strom- und Gasnetzbetreiber ein Informationssicherheits-Managementsystems (ISMS) aufgebaut und zertifiziert haben. Die Stadtwerke Schwäbisch Hall haben mit Partnern ein portalbasiertes Angebot entwickelt, das eine schlanke Erfüllung der gesetzlichen Vorgaben verspricht. ew sprach mit Mark Käpplinger, IT-Leiter des Unternehmens, über die Anforderungen des Gesetzgebers und den Lösungsweg der Haller für kleine und mittelgroße Versorger. Wichtige Botschaft: Netzbetreiber sollten das Thema nicht auf die lange Bank schieben.

ew: Herr Käpplinger, als IT-Leiter der Stadtwerke Schwäbisch Hall können Sie aus erster Hand berichten: Wie ernst ist das Thema Cyber-Kriminalität für die Energiewirtschaft?

Käpplinger: Im Zuge der Digitalisierung der Energiewirtschaft hält mehr und mehr Informationstechnologie (IT) Einzug in die Netz- und Anlagensteuerung. Diese IT gerät automatisch auch ins Visier von Cyber-Kriminellen, die mit ihren Attacken potenziell großen Schaden anrichten können. Ein gravierender Blackout der Energieversorgung brächte das öffentliche Leben hierzulande in kürzester Zeit zum Erliegen. Wir müssen – und das verlangt ja auch explizit der Gesetzgeber – die IT-Infrastrukturen in diesem Bereich schützen. Die Bedrohung ist real, wie wir der Presse immer wieder entnehmen können und auch aus eigenem Erleben wissen. Wie massiv die Attacken aus dem Internet mittlerweile sind, macht eine kürzlich von der Telekom kommunizierte Zahl deutlich: Rund 1 Mio. Hackerangriffe wehrt das Unternehmen nach eigener Aussage täglich ab. Das Trommelfeuer der Attacken aus dem Netz erleben auch Energieversorger als immer intensiver.

ew: Bitte kurz mit Ihren Worten: Was verlangt der Gesetzgeber von Energieversorgern zur Verbesserung der Sicherheit von IT zur Anlagensteuerung?

Käpplinger: Hier müssen wir unterscheiden: Übergeordnet gibt es das IT-Sicherheitsgesetz, das die Betreiber kritischer Infrastrukturen (KRITIS) verpflichtet, die IT Sicherheit der Infrastrukturen für die Netzsteuerung nachzuweisen. Dabei handelt es sich um ein Artikelgesetz, das heißt, es ändert andere Gesetze, etwa auch § 11 des Energiewirtschaftsgesetzes. Was dies in der Praxis bedeutet und auf wen die KRITIS-Regeln anzuwenden sind, regelt das BSI-Gesetz. Der KRITIS-Regelschwellenwert liegt bei 500.000 versorgten Personen. Unter die KRITIS-Bestimmungen fallen bundesweit etwa 320 Anlagen.

Alle Unternehmen, die unter diesem Grenzwert bleiben, haben sich den Vorgaben des IT-Sicherheitskatalogs der Bundenetzagentur zu unterwerfen. Dieser verpflichtet Energieversorger zur Einführung und Zertifizierung eines Informationssicherheits-Managementsystems nach DIN ISO/IEC 27001 und ISO/IEC TR 27019 bis zum 31. Januar 2018. Über das zertifizierte ISMS hinaus beschreibt der IT-Sicherheitskatalog beispielsweise weitere Pflichten, etwa das Benennen und Melden eines IT-Sicherheitsbeauftragten bei der Bundesnetzagentur und das Erstellen eines Netzstrukturplans. Der IT-Sicherheitskatalog ist somit das Regelwerk, das die große Mehrheit der Energieversorger betrifft.

ew: Gilt die ISMS-Zertifizierungspflicht lückenlos?

Käpplinger: Grundsätzlich verlangt der IT-Sicherheitskatalog die Sicherstellung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Betroffen sind demnach alle TK- und EDV-Systeme des Netzbetreibers, die direkt Teil der Netzsteuerung sind. Vom Geltungsbereich ausgenommen sind Messsysteme, sofern sie nicht zu netzbetrieblichen Zwecken

eingesetzt werden. Die Verantwortung für die Einhaltung des Katalogs liegt übrigens immer beim Netzeigentümer, auch wenn er den Netzbetrieb einem Dritten anvertraut hat. Jedes Unternehmen muss für sich prüfen, ob es zertifizierungspflichtig ist.

ew: Das klingt keineswegs eindeutig. Was ist direkt Teil der Netzsteuerung und was nicht?

Käpplinger: Da gibt es in Tat Unschärfe in den Definitionen. Eine grobe Orientierung vermitteln drei Kontrollfragen, die wir unseren Kunden bei ISMS-Projekten stellen. Werden Schalthandlungen am Netz unter Verwendung von ITK-Systemen durchgeführt? Würde der Ausfall von ITK-Systemen die Sicherheit des Netzbetriebes gefährden? Sind für die Wiederherstellung der Energieversorgung nach einem Schwarzfall ITK-Systeme erforderlich? Ein dreimaliges Nein deutet darauf hin, dass eine Zertifizierung nicht erforderlich ist. Dass keine IT für die Netzsteuerung eingesetzt wird, muss allerdings per Gutachten bestätigt und bei der Bundesnetzagentur angezeigt werden, um offiziell von der Zertifizierungspflicht befreit werden zu können. Bei der Erstellung dieser Gutachten unterstützen wir selbstredend auch. In einigen Fällen wurden solche Gutachten bereits von der BNetzA genehmigt.

ew: Sie unterstützen mit mehreren Partnern bei der ISMS-Zertifizierung. Wie ist das Angebot organisiert, und an wen richtet es sich?

Käpplinger: Wir, das heißt, die Süd IT AG, ditis Systeme, die International Consulting Group GmbH und die Stadtwerke Schwäbisch Hall, bieten gemeinsam ein umfassendes Dienstleistungspaket an, von der Erstberatung bis zur Zertifizierung etwa durch TÜV, DQS oder DEKRA. Der Service richtet sich vorrangig an kleine und mittelgroße Energieversorger. Diese werden in Gruppen von bis zu fünf Unternehmen, die im Idealfall räumlich benachbart und ähnlich strukturiert sind, gemeinsam durch den Prozess geführt. Das dämpft die Kosten: Bei weitgehend identischem ISMS lassen sich externe und interne Aufwände gegenüber Einzelprojekten um bis zu 50% reduzieren.

ew: Wie läuft eine ISMS-Zertifizierung ab?

Käpplinger: Sofern keine individuellen Beratungsdienstleistungen vorgeschaltet sind, startet das Projekt mit einer Schulungs- und Infoveranstaltung, die über das ISMS und die Pflichten für Energieversorger informiert. Der erste operative Schritt ist ein Kompaktanalyse-Workshop, worin mit Hilfe von Checklisten die Ist-Situation in den Unternehmen detailliert erfasst wird. Auf dieser Basis lassen sich die Informationssicherheit der Unternehmen bewerten und der Projektaufwand schätzen. Im zweiten Schritt folgt die Planung und Umsetzung des ISMS. Ein ISO/IEC 27001-konformes ISMS besteht aus Prozessen, Verfahren und Regeln, Infrastrukturmaßnahmen sowie Dokumenten und Aufzeichnungen, die eingeführt und etabliert werden müssen. Bevor all dies zertifiziert werden kann – so verlangen es die Regeln –, muss das ISMS mindestens neun Monate in der Praxis gelebt werden. Dabei wird das System kontinuierlich gepflegt und verbessert. Bevor die Zertifizierung tatsächlich durchgeführt werden kann, sind interne Audits zur Vorbereitung darauf vorgeschrieben. Die Mitarbeiter von ditis und SÜD IT sind übrigens selbst zertifizierte Auditoren, die wissen, worauf es im Detail ankommt.

ew: Welche Rolle spielen die Stadtwerke Schwäbisch Hall in diesem Team?

Käpplinger: Die Stadtwerke Schwäbisch Hall betreiben ein zertifiziertes Rechenzentrum, in dem das ISMS-Portal gehostet und den Anwendern nach dem Software-as-a-Service- (SaaS-) Prinzip zur Verfügung gestellt werden kann. Das mandantenfähige Portal bietet die komplette Methodik zur ISO-27001-Norm inklusive Risikomethode, Maßnahmenumsetzung und Audit-Planung. Technologisch basiert das ISMS-Portal auf SharePoint, damit die wichtigsten Office-Funktionen, die zur Steuerung des ISMS-Prozesses benötigt werden, möglichst ohne zusätzlichen Lernaufwand genutzt werden können. Das heißt, alle Dokumente und Prozesse sind vorkonfiguriert, lassen sich also komfortabel und effizienzoptimiert nutzen. Die Stadtwerke Schwäbisch Hall sind auch primär für die Vermarktung

des ISMS-Angebots zuständig. Wir vertreiben es gemeinsam mit unserer Mehrheitsbeteiligung Somentec Software GmbH als Teil des gemeinsamen Leistungsportfolios unter der Dachmarke SHERPA-X.

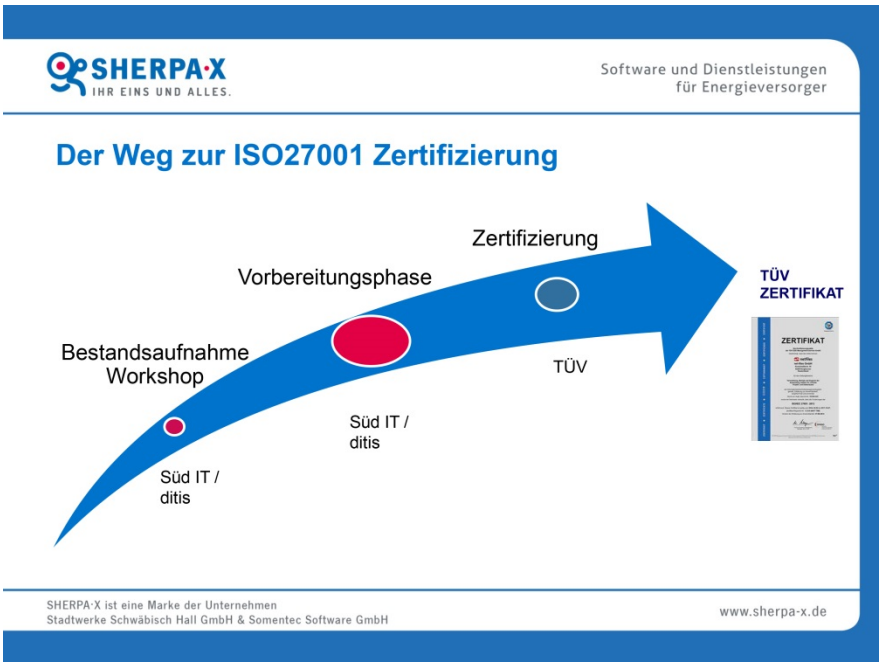
ew: Bis zum 31. Januar 2018 müssen alle Netzbetreiber über ein zertifiziertes ISMS verfügen. Wie eilig sollte man das Projekt starten?

Käpplinger: Rund anderthalb Jahre bis zum Stichtag sind eine trügerische zeitliche Entfernung. Wir kalkulieren mit rund 40 Wochen vom ersten Workshop bis zur Zertifizierung. Wenn man vom 31. Januar 2018 zurückrechnet, landet man im Frühjahr 2017. Das ist aber definitiv zu spät für den ISMS-Projektstart, weil beispielsweise im Endspurt die Kapazitäten der Dienstleister zum Engpass werden können. Man sollte sich also frühzeitig mit dem Thema befassen. Nun könnte man darauf hoffen, dass der Gesetzgeber Übergangsfristen gewährt. Darauf sollte man sich aber nicht verlassen. Im Übrigen liegt es im eigenen Interesse der Netzbetreiber, ihre IT schnellstmöglich vor Hacker-Angriffen sicherer zu machen. Das ISMS ist für die Informationssicherheit der Netz-IT jedenfalls ein starkes Immunisierungsinstrument.

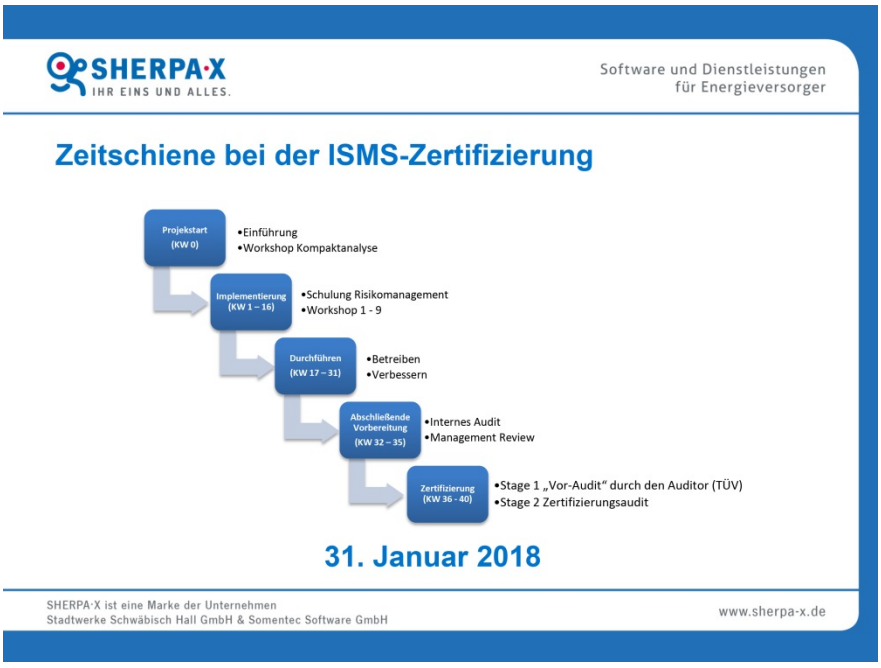
ew: Herr Käpplinger, vielen Dank für das Gespräch.

www.sherpa-x.de
mark.kaepplinger@stadtwerke-hall.de

Mark Käpplinger, IT-Leiter der Stadtwerke Schwäbisch Hall: „Netzbetreiber sollten sich frühzeitig mit dem Thema ISMS-Zertifizierung befassen.“
Bild: Stadtwerke Schwäbisch Hall GmbH



Der Weg zur ISMS-Zertifizierung.



Zeitschiene bei der ISMS-Zertifizierung.