Sicherheit nach Katalog

So gelingt der sicherere Netzbetrieb von Energieversorgern

Angela Recino

Der Ausfall kritischer Infrastrukturen wie z.B. der Energieversorgungsnetze hätte in Hochtechnologieländern wie Deutschland massive Auswirkungen auf Gemeinwesen und Wirtschaft: vom Stillstand der Industrieproduktion über Engpässe bei der Versorgung bis hin zur Gefährdung der öffentlichen Sicherheit. Der speziell an Strom- und Gasversorger gerichtete IT-Sicherheitskatalog, der ab 31. Januar 2018 gilt, zielt darauf ab, solche Szenarien zu verhindern bzw. im Fall eines Falles den Schaden zu begrenzen. Die Stadtwerke Bad Reichenhall gehören zu den ersten Unternehmen, die mit der Auditierung die Grundlage für eine Zertifizierung gemäß IT-Sicherheitskatalog durch TÜV Rheinland erfüllen. Damit ist von unabhängiger dritter Seite bestätigt, dass ihr Informationssicherheits-Managementsystem konform zu den Anforderungen des Katalogs ist.

Die Kreisstadt Bad Reichenhall mit ihren rund 18.000 Einwohnern liegt im Berchtesgadener Land im äußersten Südosten Deutschlands an der Grenze zu Österreich. Ihre Stadtwerke haben Tradition: Sie versorgen die Menschen in der Region seit über 150 Jahren. Heute präsentiert sich das Unternehmen als moderner kommunaler Netzbetreiber mit 95 Mitarbeitern und 12.000 Stromentnahmestellen, 2.700 Gas- und 3.100 Wasserhausanschlüssen sowie jährlich 1 Mio. Stadtbuskunden. Die Nachbargemeinde Bayerisch Gmain mit rund 3.000 Einwohnern gehört ebenfalls zum Versorgungsgebiet. Seit einiger Zeit ergänzt Telekommunikation das Portfolio, die Stadtwerke betreiben hierfür ihr eigenes Glasfasernetz.

Carsten Viell, IT-Leiter und -Sicherheitsbeauftragter der Stadtwerke Bad Reichenhall, nahm die Umsetzung des IT-Sicherheitskatalogs (siehe *Kasten*), der ab 31. Januar 2018 gilt, frühzeitig in Angriff: „Wir haben uns Anfang 2016 erstmals mit den Anforderungen des Katalogs beschäftigt. Der gesamte Prozess bis zur erfolgreichen Zertifizierung dauerte dann ein knappes Jahr." Um festzustellen, wie groß der Handlungsbedarf bei den Stadtwerken ist, nahm er in der Vorbereitung für die Zertifizierung den Istzustand des Unternehmens genau unter die Lupe. Er analysierte die unterschiedlichen Unternehmensbereiche, prüfte die vorhandenen Strukturen und Prozesse und glich sie mit den Kataloganforderungen ab. Betroffene Kollegen wurden eingebunden und z.B. mit Schulungsdokumenten und Workshops fit gemacht für das Thema IT-Sicherheit. Am Ende stand fest: Die Stadtwerke Bad Reichenhall sind gut vorbereitet auf die Zertifizierung.

„Mit einer gründlichen und zielgerichteten Vorbereitung ebnet das Unternehmen den Weg zur erfolgreichen Zertifizierung", erklärt Bernd Kloft von TÜV Rheinland. „Eine Bestandsaufnahme des Istzustandes zeigt dem Unternehmen die notwendigen Maßnahmen auf und spart im Endeffekt Zeit und Kosten ein." Es kann hilfreich sein, einen externen Berater für die Bestandsaufnahme in Anspruch zu nehmen. Gemeinsam werden dann die einzelnen Kapitel der Norm mit den Gegebenheiten im Unternehmen verglichen, um Abweichungen zu identifizieren. Auf diese Weise weiß das Unternehmen, wo Nachbesserungsbedarf besteht. Es erfährt kon-

IT-Sicherheitskatalog

Bis 31. Januar 2018 verlangt die Bundesnetzagentur (BNetzA) von den deutschen Strom- und Gasversorgern mit eigenem Netzbetrieb einen Nachweis über die Zertifizierung nach dem IT-Sicherheitskatalog. Die Vorgabe basiert auf §11 Absatz 1a des Energiewirtschaftsgesetzes und vollzieht sich im Nachgang zur Veröffentlichung des IT-Sicherheitsgesetzes. Damit möchte die Bundesregierung die IT-Systeme und digitalen Infrastrukturen insbesondere in kritischen Infrastrukturen (Kritis) sicherer machen.

Kernvorgabe ist der Betrieb eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 erweitert um die ISO 27019, der von akkreditierten Prüforganisationen bestätigt werden muss. Über die Akkreditierung entscheidet die Deutsche Akkreditierungsstelle Dakks in Berlin. TÜV Rheinland gehört zu den wenigen Prüfdienstleistern, die die Akkreditierungsanforderungen der Dakks erfüllt haben und seit der Erteilung der Akkreditierung durch die Dakks-Audits Zertifizierungen gemäß IT-Sicherheitskatalog durchführen darf.
www.tuv.com/it-sicherheitskatalog

Angela Recino ist Fachjournalistin in Sankt Augustin

kret, auf welche Bereiche sich die Vorgaben auswirken und wo seine Stärken und Schwächen liegen. Letztlich lässt sich der Aufwand für die Vorbereitung auf eine Zertifizierung deutlich verringern. Die Einbindung von Kollegen steigert zudem die Mitarbeitermotivation und ermöglicht Lerneffekte. Voraussetzung ist natürlich immer, dass der Berater die nötige Erfahrung und das entsprechende Fachwissen mitbringt.

Dienstleister zur Einhaltung der Vorgaben verpflichten

Die Stadtwerke Bad Reichenhall ließen sich im Dezember 2016 durch TÜV Rheinland gemäß dem IT-Sicherheitskatalog auditieren. Die Kernforderung des Katalogs besteht in der Implementierung eines ISMS gemäß ISO 27001, das mindestens die TK- und EDV-Systeme umfasst, die für einen sicheren Netzbetrieb notwendig sind. Der Netzbetreiber muss in diesem Zusammenhang auch einen Prozess zur Risikoeinschätzung und -behandlung definiert haben. Außerdem gilt es, einen „Netzstrukturplan" anzufertigen und zu pflegen. Dieser umfasst mindestens die Technikkategorien „Leitsystem und Systembetrieb", „Übertragungstechnik/Kommunikation" und „Sekundär-, Automatisierungs- und Fernwirktechnik". Bis 30. November 2015 musste jedes Unternehmen darüber hinaus einen „Ansprechpartner IT-Sicherheit" an die BNetzA gemeldet haben.

Die Stadtwerke Bad Reichenhall hatten schon vor dem Erscheinen des Katalogs die meisten der geforderten Punkte umgesetzt – wenn auch nicht immer exakt in der vorgeschriebenen Form. Carsten Viell verfügt über viele Jahre IT-Erfahrung und weiß, worauf es bei einem sicheren System ankommt – und auch, dass die Sicherheitsmaßnahmen sich kontinuierlich den Bedrohungen anpassen müssen. Unmittelbar nach seinem Eintritt ins Unternehmen im Jahr 2014 machte er sich daran, mögliche Sicherheitslücken in der IT-Infrastruktur zu schließen. Er überarbeitete u.a. die Netzstruktur und teilte sie in einzelne, physisch getrennte Segmente auf. Zudem etablierte er ein dreistufiges Firewall-Konzept. Die Benutzerregistrierung wurde ebenfalls optimiert; BYOD (Bring Your Own Device), also der Einsatz von Privatgeräten innerhalb des Unternehmensnetzes, ist schlicht verboten. Diese und die anderen Verbesserungen hielten den Aufwand direkt vor dem Zertifizierungsaudit relativ gering. Auch die Forderungen hinsichtlich externer Dienstleister waren in Bad Reichenhall bereits umgesetzt: Der IT-Sicherheitskatalog verlangt von den Gas- und Stromversorgern, dass auch beauftragte Dritte die Vorgaben einhalten. Der Dienstleister, der für die Stadtwerke die Netzleittechnik betreut, muss deshalb IT-Sicherheits- und Datenschutzvereinbarungen unterzeichnen und seine Mitarbeiter regelmäßig schulen. Den Zugang für die Fernwartung schalten die Stadtwerke jedes Mal aufs Neue frei.

Für die Stadtwerke Bad Reichenhall gab es nur wenige Punkte, die im Zuge der Einführung des ISMS überarbeitet oder verbessert werden mussten. Dazu zählt u.a. die Dokumentation. Die technischen Arbeitsabläufe z.B. funktionieren einwandfrei, wurden aber nicht wie gefordert dokumentiert. „Wir prüfen unsere USV-Anlagen wöchentlich, hielten die Prüfung in der Vergangenheit aber nicht schriftlich fest", erklärt Carsten Viell. „Das haben wir jetzt geändert." Auch beim Thema Datenschutz galt es an einigen Stellen nachzubessern, damit personenbezogene Informationen von Kunden oder Mitarbeitern jederzeit zuverlässig geschützt sind.

„Stillstand ist Rückschritt"

Wer die Zertifizierung gemäß dem IT-Sicherheitskatalog noch vor sich hat, dem empfiehlt Carsten Viell, im Vorfeld die Expertise externer Berater einzuholen. Der unabhängige Blick von außen auf den Istzustand des Unternehmens, z.B. durch eine GAP-Analyse, kann wertvolle Impulse geben. Die intensive Auseinandersetzung mit der ISO 27001 sowie der ISO 27019 ist für jeden IT-Sicherheitsbeauftragten trotzdem unumgänglich. Außerdem sollte der IT-Profi des Unternehmens die Zertifizierung gemeinsam mit einem technisch versierten Kollegen in Angriff nehmen. Auf diese Weise lassen sich beide Infrastrukturen in den Blick nehmen: die IT-Infrastruktur sowie das Strom-, Wasser- und/oder Gasnetz. Die beiden Fachleute ergänzen sich mit ihrem Wissen und finden so die besten Lösungen.

Für die Zertifizierung selbst zahlt sich die Zusammenarbeit mit einem renommierten Prüfdienstleister wie TÜV Rheinland aus. Dessen Auditoren sind durch ständige Weiterqualifizierung in Bezug auf digitale Transformation und aktuelle Bedrohungslage stets up to Date. Darüber hinaus verfügen sie über jahrelange Erfahrung und umfassendes Know-how im Bereich kritische Infrastrukturen.

Mit der Umsetzung der Katalogforderungen und der Etablierung eines ISMS haben die Stadtwerke Bad Reichenhall einen wichtigen Schritt hin zu mehr IT-Sicherheit unternommen. Aber Carsten Viell weiß, dass man sich darauf nicht ausruhen darf: „Die Bedrohung durch Cyberattacken nimmt durch die voranschreitende Vernetzung und das Internet der Dinge weiter zu. Selbst ein vernetzter Heizungsregler kann heute Einfallstor für Angreifer sein." Und dann sind da noch die Gefahren, die Unternehmen von innen drohen, z.B. durch infizierte USB-Sticks, die ein Mitarbeiter unbedarft an Firmenrechner anschließt. „Stillstand ist Rückschritt", sagt Carsten Viell. „Wir müssen Wege finden, den neuen Herausforderungen gerecht zu werden." Deshalb werden die Stadtwerke Bad Reichenhall ihre Sicherheitsmaßnahmen weiter ausbauen, z.B. mit regelmäßigen Penetrationstests. Denn, so Viell, „nur so lässt sich ein Ausfall der kritischen Infrastrukturen in Deutschland verhindern und dauerhaft ein verlässlicher Netzbetrieb sicherstellen."

Nach Ablauf von zwölf Monaten sehen sich Carsten Viell von den Stadtwerken Bad Reichenhall und die Auditoren von TÜV Rheinland wieder – zum Überwachungsaudit. Die Laufzeit der Zertifizierung beträgt drei Jahre – bis dahin dürfte in Bezug auf Cyberattacken und IT-Sicherheit eine Menge Wasser die Saalach hinunterfließen – auch in Bad Reichenhall. *(bk)*