ener|gate
con|energy gruppe

2|17
Ausgabe 2
April 2017

e|m|w

Energie. Markt. Wettbewerb.

Prozesse & IKT

Zertifizierung nach IT-Sicherheitskatalog

Von **Dr. Stefan Krempl**, Vorstand, Süd IT AG

ISSN: 1611-2997

Zertifizierung nach IT-Sicherheitskatalog

Die Frist läuft

Ende des Jahres läuft die Frist zur Umsetzung der Anforderungen des IT-Sicherheitskataloges der Bundesnetzagentur (BNetzA) ab. Die darin geforderte Zertifizierung ist, aus Sicht der BNetzA nicht einfach eine erweiterte ISO/IEC 27001-Zertifizierung sondern folgt eigenen, speziellen und im Konformitätsbewertungsprogramm festgelegten Regeln. Für Energieversorger, die bereits eine normale ISO/IEC 27001-Zertifizierung erhalten haben, bedeutet dies voraussichtlich, dass sie eine erneute Zertifizierung durchführen müssen.

Von **Dr. Stefan Krempl**, Vorstand, Süd IT AG

Die Zertifizierung nach dem IT-Sicherheitkatalog können nur Zertifizierungsdienstleister durchführen, die sich für diesen Standard eigens bei der Deutschen Akkreditierungsstelle akkreditiert haben. Auch die eingesetzten Auditoren müssen eine spezielle Schulung nachweisen. Mittlerweile sind einige wenige der großen Zertifizierungs-Dienstleister, wie TÜV Rheinland oder TÜV Süd, bereits zugelassen oder stehen kurz davor. Andere, wie Dekra oder die PÜG, sind gerade im Akkreditierungsprozess. Im Rahmen dessen haben daher bis heute nur einzelne Netzbetreiber in sogenannten Witness-Audits die geforderte Zertifizierung durchgeführt. Es ist aber zu erwarten, dass deren Anzahl im Laufe der kommenden Wochen zunehmen wird. Ausgehend von den Vorgaben der ISO/IEC 27006 werden die meisten Zertifizierungsprozesse zumindest fünf Tage dauern. Wie die jetzt zu erwartenden circa 1.000 Zertifizierungen bis Jahresende durchgeführt werden sollen, ist allerdings mehr als ungewiss. Erschwert wird der Umstand auch dadurch, dass viele der freiberuflichen Auditoren derzeit noch tief in lukrativeren Beratungsprojekten stecken. Wie aus gut informierten Kreisen zu vernehmen ist, werden Netzbetreiber, die aufgrund des zu erwartenden Andrangs keinen rechtzeitigen Termin für eine Zertifizierung erhalten, von der BNetzA eine angemessen Nachfrist erhalten. Netzbetreiber, die bis heute das Thema noch nicht begonnen haben, dürften aber nicht unbedingt mit so viel Nachsicht rechnen.

Eine Zertifizierung gemäß ISO/IC 27001 oder IT-Sicherheitskatalog dauert typischerweise zumindest neun Monate für kleine und mittlere Unternehmen (Tab. 1). Für große Firmen oder Konzerne sind auch Laufzeiten von zwei und mehr Jahren nicht untypisch. Ein Teil der Laufzeit rührt daher, dass ein normgerechtes Informationssicherheits-Managementsystem (ISMS) erst über eine gewisse Zeit gelebt werden muss, bevor es zertifiziert werden kann. In größeren Firmen dauert zumeist die Abstimmung der neu einzuführenden oder zu ändernden Prozesse lange. Im Besonderen, wenn die Interessen der Unternehmensleitung und der Arbeitnehmervertretung zusammen mit den Anforderungen der Norm unter einen Hut gebracht werden müssen.

01 Durchschnittliche Aufwände für kleine und mittlere Netzbetreiber

Projektphase	Arbeitsaufwand externer Berater [Tage]	Arbeitsaufwand interne Ressourcen [Tage]
Ersterfassung	2–4	4–12
Implementierung	25–50	60–150
Zertifizierung Stufe 1	1–2	1–4
Zertifizierung Stufe 2	2–4	4–12
Gesamt	30–60	69–178

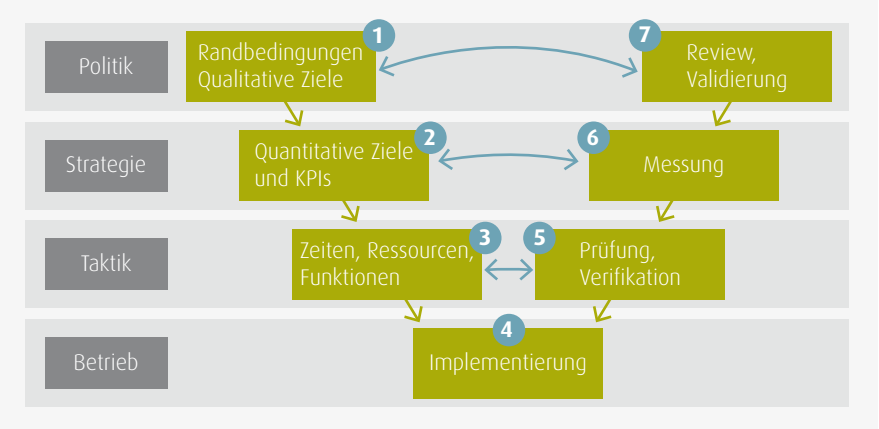
Implementierung des Informationsmanagementsystems

Bei der Vorbereitung auf eine Zertifizierung lassen sich nahezu alle Netzbetreiber von Beratern unterstützen. Gute Berater wissen, worauf es ankommt und führen ihre Kunden zielsicher zu einer erfolgreichen Zertifizierung. Unternehmen, die erst jetzt in den Prozess einsteigen, sollten versuchen, Referenzen zu verlangen, um bei der Auswahl keinen Reinfall zu erleben.

1. Unternehmenspolitik

Die Implementierung eines ISMS gemäß der ISO/IEC 27001 ist selbst in der Norm ISO/IEC 27003 beschrieben. Sie lässt sich in der praktischen Umsetzung auf die im folgenden beschriebenen Schritte herunterbrechen. Wichtig ist dabei, den grundsätzlichen Gedanken der Norm eines gemanagten Prozesses zu verinnerlichen. In früheren Versionen der Norm war noch ausdrücklich der PDCA-Prozess (plan-do-check-act) genannt, der aber – aus guten Gründen – nicht mehr erwähnt wird. Viel treffender lässt sich der Prozess durch ein an das V-Modell der Softwareentwicklung angelehnte Vorgehensmodell beschreiben, das in Abbildung 1 dargestellt ist.

01 Vorgehensmodell



1. Politik

Um überhaupt die Grundlage für ein weiteres Vorgehen zu schaffen, müssen die grundlegenden Randbedingungen des ISMS festgelegt werden. Dazu gehören

- die Art des Geschäftes, das unter dem ISMS durchgeführt werden muss,
- die Ziele des Unternehmens,
- die sonstigen an dem ISMS interessierten Parteien und deren Erwartungen an das ISMS,
- sonstige vertragliche und gesetzliche Vorgaben.

Dieser erste Schritt ist wesentlich, um die Richtung des weiteren Vorgehens festzulegen. Auch können in der späteren Risikoanalyse nur dann Risiken entstehen, wenn bei deren Eintritt gegen eine dieser Festlegungen verstoßen würde. Alles andere kann definitionsgemäß kein Risiko sein. Wichtige Ergebnisse dieses ersten Schrittes sind in den „Leitlinien zur Informationssicherheit“ und „Definition des Geltungsbereichs“ festgehalten. Auch die sogenannte Erklärung zur Anwendbarkeit, bei der festgelegt wird, welche der 114 Controls des Anhangs A der ISO/IEC 27001 anwendbar sind, wird in der Praxis in diesem Schritt zumindest entworfen.

Die Norm kann käuflich erworben werden. Der beschreibende Text der Controls in Anhang A ist relativ knapp gehalten, sodass sich dazu auch die Anschaffung der ISO/IEC 27002 lohnt. In dieser sind die Controls näher erläutert und mit Beispielen versehen. Dazu sollten Sie auch die Norm ISO/IEC TR 27019 kennen, in der zusätzliche Maßnahmenziele für Netzbetreiber enthalten sind. Ergänzend dazu ist es empfehlenswert, sich mit dem BDEW-Whitepaper auseinander zu setzen.

2. Strategie

In dem zweiten Schritt gilt es, die allgemeinen Ziele und Vorgaben weiter herunter zu brechen, um eine Strategie zur Umsetzung des ISMS zu formulieren. Dazu gehört unter anderem eine Risikomanagement-Methode festzulegen sowie zu definieren, was für die Firma geringe oder hohe Risiken sind, sowie quantitativ messbare Ziele (KPI) zur Wirk-samkeit des ISMS. Werden im Rahmen der Risikobewertung Risiken identifiziert, die die festgelegte Akzeptanz-Schwelle überschreiben, so müssen diese behandelt werden, indem geeignete Maßnahmen zur Risikominderung getroffen werden, das Risiko verlagert oder vermieden wird. Zuletzt steht dem Unternehmen auch noch die Möglichkeit offen, Risiken ausdrücklich zu akzeptieren, zum Beispiel, wenn Risiken nicht auf wirtschaftliche Weise weiter reduziert werden können (vgl. Tab. 2).

Anhand der Risikobewertung wird der Maßnahmenkatalog aus Anhang A vervollständigt. Diese Liste gilt es im Weiteren in konkrete Maßnahmen zu überführen und umzusetzen.

3. Taktik

In den ersten beiden Schritten wurden Maßnahmenziele identifiziert und sonstige Maßnahmen definiert. Diese gilt es jetzt in Schritt 3 zu konkretisieren und nachweisbar zu planen. Hier ist der Prozess vollständig auf der Ebene des Projektmanagements angekommen, während zuvor immer noch das Management wesentlich beteiligt war.

4. Betrieb

Schritt 4 liegt im Grunde nicht mehr im Bereich des Managementsystems. Hier ist die schnöde Umsetzung der geplanten Maßnahmen gefragt. Die Norm erwartet hier von der Unternehmensleitung, dass sie die erforderlichen Ressourcen in Form von Geld und Personal bereitstellt.

5. Verifikation

Ist eine Maßnahme umgesetzt, gilt es in Schritt 5 zu prüfen, ob diese gemäß der Vorgaben umgesetzt wurde. Man spricht auch von der Verifikation. Wie immer erwartet ein Auditor später, dass die Schritte Planung und Verifikation anhand von Aufzeichnungen nachvollziehbar sind.

6. Messung

Eine Ebene höher, in der Strategie-Ebene, wird in Schritt 6 die Wirksamkeit des ISMS anhand der festgelegten Indikatoren bewertet. Dies erfolgt über die festgelegten Kennzahlen (KPI) oder die Durchführung von internen Audits.

7. Validierung

In Schritt 7, der Validierung, wird zuletzt bewertet, ob das ganze Vorgehen dazu geführt hat, die Unternehmensziele zu erreichen und den Anforderungen der

02 Bewertung des Risikos anhand von Schadenshöhe und Eintrittswahrscheinlichkeit

	Sehr selten	Gelegentlich	Häufig	Ständig
Kritische Schaden	M	H	K	K
Hoher Schaden	N	M	H	K
Mäßiger Schaden	U	N	M	H
Geringer Schaden	U	U	N	M

Risikohöhe: K – kritisch, H – hoch, M – mittel, N – niedrig, U – unbedeutend

03 Risiko-Akzeptanzkriterien

Kritische Risiken	stellen für das Unternehmen eine existentielle Bedrohung dar und können in keinem Fall akzeptiert werden. Falls das Risiko nicht verringert werden kann, muss der zugrundeliegende Geschäftsprozess eingestellt werden.
Hohe Risiken	sind in der Regel nicht tolerierbar, da sie Betriebsabläufe in Frage stellen. Im Rahmen des Risikobehandlungsplans sind Maßnahmen festzulegen, die das Risiko zumindest auf die Stufe „mittel" reduzieren. Gelingt das nicht, werden sie als Restrisiken eigens aufgeführt und bedürfen der Zustimmung des Managements.
Mittlere Risiken	stellen Betriebsabläufe eventuell in Frage. Für sie sind im Risikobehandlungsplan Maßnahmen festzulegen, die sie auf die Stufe „niedrig" reduzieren, sofern dies wirtschaftlich sinnvoll ist. Gelingt dies nicht, werden sie als Restrisiken eigens aufgeführt und bedürfen der Zustimmung des Managements.
Niedrige Risiken	stellen kein substanzielles Betriebsrisiko dar. Sie sind tolerierbar, ohne dass eine Risikobehandlung oder Restrisikobetrachtung erfolgen muss.
Unerhebliche Risiken	stellen kein Betriebsrisiko dar. Sie sind tolerierbar, ohne dass eine Risikobehandlung oder Restrisikobetrachtung erfolgen muss.

interessierten Parteien gerecht zu werden. Das in der Norm dazu vorgesehene Instrument ist das zumindest jährlich durchzuführende Management-Review. Hier wird die Wirksamkeit des ISMS bewertet, neue Maßnahmen beschlossen und bei Bedarf die Weichen neu gestellt.

Auswahl des Zertifizierers

Parallel zu dem Implementierungsprozess sollte ein geeigneter Zertifizierer gesucht werden. Die Preise zwischen den Anbietern unterscheiden sich dabei nicht wesentlich, auch weil die Anzahl der Audittage durch die ISO/IEC 27006 festgeschrieben sind. Wichtig ist es, einen Zertifizierer zu finden, mit dem eine vertrauensvolle Zusammenarbeit möglich ist. Der Geltungsbereich sollte vorab geklärt werden, er muss den Vorgaben des IT-Sicherheitskatalog und des Konformitätsbewertungsprogramms entsprechen. Aufgrund des zu erwartenden Engpasses ist es ratsam, den Zertifizierungstermin so früh wie möglich fest zu vereinbaren. Auch ist es erfahrungsgemäß dem Projektfortschritt durchaus förderlich, wenn ein fester Endtermin frühzeitig feststeht.

Endspurt zur Zertifizierung

Hat die Organisation alle Schritte von 1 bis 6 weitgehend durchgeführt und dabei alle von der Norm geforderten Dokumente und Aufzeichnungen erstellt, so folgen die letzten Wochen zu der Zertifizierung immer dem gleichen Schema:

In einem geplanten internen Audit wird die Umsetzung des ISMS geprüft. Dazu sollte nach Möglichkeit ein unabhängiger externer Auditor gefunden werden. Basierend auf den Ergebnissen des internen Audits sowie den erreichten Zielen wird das Management-Review durchgeführt. Darin nimmt das Management eine Risikoabschätzung vor, bewertet die allgemeine Wirksamkeit des ISMS und legt bei Bedarf weitere Maßnahmen fest.

Jetzt ist die Organisation für die erste Stufe der Zertifizierungsaudits bereit. Dazu kommt bei mittelgroßen Firmen in der Regel ein Auditor für ein bis zwei Tage. Auch der geforderte Fachexperte sollte an dem Stufe-1-Audit beteiligt sein. Werden in dieser ersten Stufe noch Probleme gefunden, so hat das Unternehmen noch bis zur zweiten Stufe Zeit, diese zu beheben. Zu diesem Termin kommen in der Regel zwei oder mehrere Auditoren und gegebenenfalls noch der Fachexperte, um die Norm-Konformität des ISMS zu beurteilen.

Nach dem erfolgreichen Abschluss der Zertifizierung in Stufe 2 gibt der Lead-Auditor seinen Bericht und eine Empfehlung an die Zertifizierungsstelle. Diese folgt in nahezu allen Fällen, gegebenenfalls nach Nachfragen, dessen Votum. Wurden in dem Audit wesentliche Abweichungen von den Normforderungen gefunden, so ist dies noch nicht das Ende. Vielmehr hat das Unternehmen bis zu 90 Tage Zeit, diese Abweichungen zu beheben. Die erfolgreiche Behebung wird dann anhand vorgelegter Dokumente oder eines Nachaudits geprüft.

Das Zertifikat gilt, wie ein normales ISO/IEC 27001-Zertifikat, drei Jahre, wobei in jährlichem Abstand Überwachungsaudits durchgeführt werden.

DR. STEFAN KREMPL

Jahrgang 1962

- 1982-1990 Studium der Physik, TU München
- 1997-98 Debis Systemhaus
- 1998-99 Giesecke & Devrient
- seit 2000 Mitgründer Utomi AG (heute netfiles.de und my-files.de)
- 2005-2015 GPP AG
- seit 2014 Vorstand, Süd IT AG

e|m|w

Energie. Markt. Wettbewerb.

energate gmbh
Norbertstraße 5
D-45131 Essen
Tel.: +49 (0) 201.1022.500
Fax: +49 (0) 201.1022.555
www.energate.de