IT-Security

Was ist die ISO 27001 auf Basis IT-Grundschutz wert?

Datum: 13.05.2014
Autor(en): Stanislav Wittmann

Zertifizierungen in der Informationssicherheit, besonders nach ISO 27001, kommen in Mode. Die Krönung stellt eine besondere Form dar - die ISO 27001 auf der Basis von IT-Grundschutz. Was steckt dahinter?

Der Weg zur Zertifizierung ist relativ strikt vorgegeben und überschneidet sich in einigen Teilen mit der herkömmlichen ISO 27001. Zunächst sind in einer **Sicherheitsleitlinie (Security Policy)**[1] die Kernpunkte der Sicherheitsstrategie festzuhalten. Die Leitlinie soll kein Roman sein, sondern vielmehr in prägnanter Form auf höchstens fünf bis zehn Seiten die Grundsätze zur Informationssicherheit vermitteln.

Die Policy enthält Compliance-Prinzipien wie das Bekenntnis der Geschäftsführung zur Informationssicherheit oder den Beitrag der Mitarbeiter, Sicherheitsvorfälle und Verletzungen der drei **Grundwerte**[2] zu melden. Dann beginnt die Dokumentation. Alle Räume, Systeme und die darauf laufenden Anwendungen sind tabellarisch zu protokollieren. Das heißt konkret, dass beispielsweise in einem Großraumbüro Computer derselben Anwendung zu protokollieren sind. Das können Rechner der Finanzabteilung, der IT oder der Geschäftsführung sein. Auch Faxgeräte, Multifunktionsdrucker und Server sind zu berücksichtigen. Nicht zu vergessen Smartphones, Tablets und selbst Computersysteme in Fahrzeugen. Neben der tabellarischen Auflistung soll ein **Netzplan**[3] helfen, die Vernetzung der Systeme eines Unternehmens zu durchschauen. Das alles erfolgt unter dem Oberbegriff "IT-Strukturanalyse".

Anschließend erfolgt die **Schutzbedarfsfeststellung**[4]. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt drei **Schutzbedarfskategorien**[5] vor: normal, hoch und sehr hoch. Mit der Einstufung "sehr hoch" sollten Unternehmen vorsichtig umgehen, weil diese einen oft unverhältnismäßig hohen Aufwand bedeutet und schnell viel Geld verschlingen kann.

Die Schutzbedarfsfeststellung erfolgt zunächst allgemein bezogen auf die drei Grundwerte der Informationssicherheit. Das kann in der Praxis folgendermaßen aussehen:

Grundwert Vertraulichkeit

Der Grundwert Vertraulichkeit hat das Ziel, dass Informationen (beispielsweise personenbezogene Daten) nicht in falsche Hände fallen dürfen. Es gibt folgende Abstufungen:

- **Schutzbedarf normal:** Bei Verstoß drohen allenfalls geringfügige juristische Konsequenzen.
- **Schutzbedarf hoch:** Verstöße beeinträchtigen das informationelle Selbstbestimmungsrecht und haben beträchtliche juristische Konsequenzen.
- **Schutzbedarf sehr hoch:** Verstöße würden zu existenzbedrohenden Konsequenzen des Unternehmens führen (beispielsweise öffentlicher Zugang von Patientendaten in einer Privatklinik).

Grundwert Integrität

Der Grundwert Integrität verfolgt das Ziel, dass Informationen nicht verfälscht werden dürfen (beispielsweise bei Angeboten oder Rechnungen). Es gibt folgende Abstufungen:

- **Schutzbedarf normal:** Bei Verfälschung ist der Schaden kleiner 5000 Euro
- **Schutzbedarf hoch:** Verfälschungen verursachen einen Schaden zwischen 5000 und 50.000 Euro.
- **Schutzbedarf sehr hoch:** Verfälschungen führen zu einem Schaden von über 50.000 Euro.

Grundwert Verfügbarkeit

Der Grundwert Verfügbarkeit verfolgt das Ziel, dass Informationen abrufbar sein müssen (was beispielsweise bei einem Server-Totalausfall nicht mehr der Fall ist). Es gibt folgende Abstufungen:

- **Schutzbedarf normal:** Eine Ausfallzeit über drei Tage ist tolerierbar und verursacht einen Schaden von maximal 5000 Euro.
- **Schutzbedarf hoch:** Eine Ausfallzeit über 24 Stunden verursacht einen Schaden von über 5000 Euro.
- **Schutzbedarf sehr hoch:** Bereits eine Stunde Ausfallzeit bedroht die Existenz des Unternehmens, bei einem Schaden von über 100.000 Euro.

Nach der allgemeinen Schutzbedarfsfeststellung gilt es, die Anwendungen, Systeme und schließlich die Räume zu klassifizieren. Hier ist es wichtig, logisch abzuleiten. Das heißt: Verwaltet ein Server eine hochverfügbare Datei, so sollten man nicht am Kühlsystem oder an der Dimensionierung des Servers sparen. Denn logischerweise ist auch der Server als hochverfügbar einzustufen.

[Hinweis auf Bildergalerie: **Vorbereitung des Zertifikats -**] [gal1]

Daraus lässt sich auch ableiten, dass der Server nicht in einer Besenkammer stehen darf. Also sollte ein hierfür vorgesehener Serverraum über mindestens dieselben Anforderungen wie der Server selbst oder die darauf laufende Anwendung verfügen. Das BSI verwendet hierfür den Begriff des "Maximierungsprinzips". **Weitere Prinzipien**[6] zur Festlegung des Schutzbedarfs lassen sich beim BSI nachlesen.

Modellierung und Basis-Sicherheitscheck

Das BSI verfügt über **drei Grundschutzkataloge (GS-Kataloge)**[7]: "Bausteine", "Gefährdungen" und "Maßnahmen". Nachdem alles klassifiziert ist, erfolgt die so genannte Modellierung mit den Bausteinen, die bereits in fünf Schichten sortiert sind.

Konkret kann die Modellierung folgendermaßen ablaufen: Da Datenverluste existenzbedrohend für Unternehmen sein können, sollen Datensicherungen vorgenommen werden - auf Basis des **Bausteins B. 1.4 - Datensicherungskonzept**[8]. Zielobjekt wären alle Datenträger, bei denen das Unternehmen im Falle eines Datenverlustes in die Röhre schaut. Verfügt die Firma weiterhin über einen Serverraum, so wird hierfür der **Baustein B 2.4**[9] auf diesen angewendet. Aus diese Weise lassen sich Bausteine aller fünf Schichten auf Anwendungsbedarf prüfen.

Im Anschluss folgt ein zeitintensiver Part, der Soll-Ist-Vergleich - im Fachjargon auch als **Basis-Sicherheitscheck**[10] bezeichnet. Dabei wird jeder Baustein auseinander genommen und die darin enthaltenen Maßnahmen auf deren Umsetzungsgrad geprüft. Bleiben wir an dieser Stelle beim Baustein B. 2.4 Serverraum. Jeder Baustein enthält neben potenziellen Gefahren auch Schutzmaßnahmen. So enthält der Baustein Serverraum neben Gefahren wie Feuer, Sabotage oder Ausfall der Stromversorgung auch Gegenmaßnahmen, welche das Risiko der Gefahren mindern sollen.

Beim Serverraum beispielsweise gibt es 16 Maßnahmen. Einige davon, wie ein Rauchverbot oder die angepasste Aufteilung der Stromkreise, sollten obligatorisch sein. Jede Maßnahme der ausgewählten Bausteine wird auf ihren Umsetzungsgrad hin geprüft. Wichtig für die Zertifizierung: Den Maßnahmen sind so genannte **Siegelstufen**[11] in Form von Buchstaben zugeteilt - A, B, C, W oder Z. Für die Zertifizierung sind grundsätzlich Maßnahmen der Stufen A, B und C erforderlich. Prinzipiell lässt sich sagen: Je früher der Buchstabe im Alphabet, desto elementarer die Maßnahme. So stellt ein Rauchverbot im Serverraum die Siegelstufe A dar, während Redundanzen der technischen Infrastruktur als Z-Maßnahme eingestuft und nicht zwingend für eine Zertifizierung erforderlich sind.

Für die Zertifizierung sind vom BSI 82 Prozent an erfüllten Maßnahmen als Richtwert vorgegeben. Dabei steht die Sinnhaftigkeit der Maßnahmen im Vordergrund - nicht die relative Prozentangabe. Es gilt: Wer schreibt, bleibt. Das Unternehmen ist nicht verpflichtet, alle Maßnahmen umzusetzen, wenn es plausible Begründungen vorlegen kann. Eine produktive Kommunikation mit dem **Auditor**[12] kann erhebliche Ressourcen sparen.

Wie Andreas Teuscher, Vorstandsmitglied der **ISACA Germany Chapter e.V.**[13] und ISO 27001 Lead Auditor zu bedenken gibt, sollten die Auditees zwei Punkte nicht aus den Augen verlieren: "Zum einen muss das BSI-Auditierungsschema, also das besondere Vorgehen, beachtet werden. Zum anderen sollten das Risikomanagement und vor allem die Restrisikoübernahmen Berücksichtigung finden." Dies sei besonders vor dem Hintergrund wichtig, dass das BSI bis vor kurzen keine Restrisikoübernahmen gekannt habe.

Realisierung und Schwierigkeiten

Nach dem Soll-Ist-Vergleich erfolgt eine **Realisierungsplanung**[14] für die noch benötigten Maßnahmen. Dafür wird der Aufwand der Maßnahme als Geldbetrag und Stundenaufwand kalkuliert und terminiert.

Schwierigkeiten kann noch die sogenannte **ergänzende Sicherheitsanalyse**[15] und Risikoanalyse machen. In diesem Abschnitt erfolgt eine Art Gefährdungsbeurteilung samt Risikomanagement für Zielobjekte mit folgenden Kriterien:

- Der Schutzbedarf ist in mindestens einem der drei Grundwerte hoch oder sehr hoch.
- Für das zu behandelnde Zielobjekt gibt es keinen Baustein (wie derzeit beispielsweise für das Betriebssystem **Windows 8**[16]).
- Der vorhandene Baustein des BSI reicht vom Umfang oder der Qualität her nicht aus.

Die Zertifizierung

Die **Zertifizierung**[17] selbst ist mit der herkömmlichen ISO 27001 vergleichbar, wobei die Zertifizierungsstelle in diesem Fall das BSI selbst ist, das auch an den Prüfer respektive Auditor einige Anforderungen stellt. Diese müssen unter anderem nachweisen, dass sie ihrer Tätigkeit stets nachkommen. Das wird mit eine Art Punkteverfahren sichergestellt. So hat ein lizensierter BSI-Auditor die Aufgabe, eine bestimmte Anzahl an Tätigkeiten innerhalb von drei Jahren nachzuweisen. Das können Audits, der Besuch von Fachmessen oder Weiterbildungskurse sein. Das Verfahren soll die Kompetenz der Auditoren sicherstellen. Schaffen Auditoren nicht die geforderte Punktzahl, kann das BSI dem Auditor die **Re-Zertifizierung**[18] verwehren.

Vor der eigentlichen Zertifizierung müssen Auditortestate erlangt werden, die zwei Jahre lang gültig und nicht wiederholbar sind. Im Rahmen der Testierung soll eine zunehmende Zahl geforderter Maßnahmen umgesetzt werden. Beim ersten Testat, der Einstiegsstufe, sind rund 55 Prozent der Maßnahmen erforderlich. Das zweite Testat, die Aufbaustufe, verlangt bereits 72 Prozent. Ist der Zertifizierungsprozess mit 82 Prozent der Maßnahmen überstanden, ist das ISO 27001-Zertifikat drei Jahre lang gültig.

Teuscher dazu: "Wie alle Zertifizierungsstellen unterliegt auch das BSI mit seiner Zertifizierungsstelle der ISO-17021-Norm. Teil dieser Norm ist unter anderem auch die Qualifikation der Leitenden Auditoren. Diese müssen in der Berufungszeit mindestens drei Zertifizierungsaudits durchlaufen sowie am jährlichen Erfahrungsaustausch und noch an weiteren Maßnahmen zur Weiterentwicklung

teilgenommen haben." Das Ziel dieses Vorgangs sei es, nicht praktizierende Auditoren, die beispielsweise nur beraten, den Titel abzuerkennen. In der Praxis stelle es sich laut Teuscher aber wesentlich schwieriger dar, als man annehmen könne: "Es gibt das berühmte Henne-Ei-Problem. In den meisten meisten Beratungsprojekten wird ausdrücklich nach leitenden Auditoren gefragt, die ihren Fokus wiederum auf die Auditierung und nicht auf die Beratung legen sollten." Dieses Dilemma könne man wohl nur durch weitere Aufklärung in den Behörden entschärfen.

[Hinweis auf Bildergalerie: **12 Tipps für eine schlanke ISO 27001-Einführung -**] gal2

Mit Re-Zertifizierungsaudits kann die Zertifizierung anschließend aufrechterhalten werden. Ein jährliches Überwachungsaudit umschließt den Wartungsprozess. Überwachungsaudits sind nicht zu unterschätzen. Erfolgen nämlich "wesentliche Änderungen am zertifizierten Unternehmen", sind diese der Zertifizierungsstelle des BSI schriftlich mitzuteilen. Wechselndes outgesourctes Personal würde beispielsweise darunter fallen.

Die Geschäftsleitung soll sich auch die Frage stellen, welche Unternehmensphilosophie sie vorgibt. Denn eine ISO 27001 auf der Basis von IT-Grundschutz verschlingt nicht unerhebliche Ressourcen. Es empfiehlt sich, nicht gleich aufgrund von Minimalunterschieden im Stunden- oder Tagessatz den Dienstleister zu wechseln. Überhaupt steht das eindeutig erhöhte Sicherheitsrisiko durch wechselndes Personal in keinem Verhältnis zu den Instandhaltungskosten der Zertifizierung, zumal allein die Einarbeitungszeit bereits für sich spricht.

Wolfgang Berger, Leiter des **Business Reframing Instituts**[19] in Karlsruhe, meint dazu: "Wechselndes Personal ist ein Kostenrisiko. Die Kosten der Neubesetzung und der Einarbeitungszeit stehen in keinem Verhältnis zu den Instandhaltungskosten der Zertifizierung. Wechselndes Personal ist aber vor allem auch ein Sicherheitsrisiko. Wer sich in eine ihm nicht vertraute Unternehmenskultur nicht einlebt, reagiert seinen Frust manchmal durch Verrat ab."

Vor- und Nachteile gegenüber der ISO 27001

Was nun? Auf der Basis von IT-Grundschutz oder doch die "einfache" ISO 27001? Es ist eine Abwägungssache. Natürlich ist die "BSI-Zertifizierung" mit der ISO 27001 vollständig kompatibel. Auch berücksichtigt diese Empfehlungen der kürzlich neu überarbeiteten **ISO 27002**[20]. Das Verfahren ähnelt einer Bedienungsanleitung - versteht man es erst einmal, lässt es sich im Regelfall ohne größere Hürden umsetzen.

Auf der anderen Seite stehen neben dem enormen Dokumentationsaufwand kaum Freiheiten gegenüber einem Verfahren, dass zwar kaum Schwächen besitzt, gleichwohl aber aktuell zu halten ist. Denn die Abhängigkeit vom GS-Katalog kann durchaus zum Verhängnis werden. Sollte das BSI nicht seiner Pflicht nachkommen können, Gefahren, Maßnahmen oder Bausteine rechtzeitig zu aktualisieren, können Risiken für bestimmte Gefahren beträchtlich steigen. Gerade die IT-Branche ist ein schnelllebiges Geschäft. So sollte beispielsweise der Baustein Windows 8 möglichst vor der Vorstellung des nächsten Betriebssystems erscheinen.

Fazit

Ob nun ISO 27001 oder ISO 27001 auf der Basis von IT-Grundschutz: Unternehmen sollten die Zertifizierung nicht rein aus juristischen Exkulpationsabsichten, sondern vielmehr aus sicherheitsbewusstem Eigeninteresse anstreben. Dann wird vermutlich jede Form einer ISO 27001 - Zertifizierung ihren Zweck erfüllen

Letztlich ist es eine Frage der Abwägung. Möchte ein Unternehmen mehr Freiheiten und eine individuelleres Konzept mit dem Mut zur Lücke, ist die wohl die "herkömmliche" Version der ISO 27001 die richtige Lösung.

Entscheidet es sich hingegen für eine strikte, dafür umfassende und höchst wahrscheinlich aufwändigere Lösung, kann die ISO 27001 auf der Basis von IT-Grundschutz eine Option sein. Hinzu kommt eine gewisse Abhängigkeit vom BSI, da dieser die Entwicklungen der Sicherheitstechnik verfolgen muss, um den GS-Katalog aktuell zu halten.

Eine Norm ist und bleibt auch eine Norm. Vom Gesetzgeber gefordert ist sie nicht. Die ISO 27001 hat keinen öffentlich-rechtlichen Charakter, gleichwohl reflektieren Normen den Stand der Technik. Es besteht ja auch die Möglichkeit, die ISO 27001 als Vorlage für ein Sicherheitskonzept zu verwenden, jedoch keine Zertifizierung zu beabsichtigen. Eine weitere Möglichkeit wäre, einzelne Teile der Norm oder des GS-Kataloges für sein Unternehmen zu verwenden. Das BSI stellt immerhin die GS-Kataloge und sehr umfangreiches weiterführendes Material **kostenlos zum Download**[21] zur Verfügung. (sh)

Links im Artikel:

[1] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Sicherheitsmanagement/Sicherheitsleitlinie/siche**
[2] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html**
[3] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/strukturanalyse/Netzplan/netzplan_node.html**
[4] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Schutzbedarfsfeststellung/schutzbedarfsfeststell**
[5] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Schutzbedarfsfeststellung/Schutzbedarfskategori**
[6] **https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile**
[7] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html**
[8] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01004.html**
[9] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b02/b02004.html**
[10] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/BasisSicherheitscheck/basissicherheitscheck_noc**
[11] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Modellierung/Bausteine/bausteine_node.html**
[12] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/Veroeffentlichungen/ISO27001Auditoren/auditoren27001.html**
[13] **http://www.isaca.de/**
[14] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Realisierungsplan/Beispiel/beispiel_node.html**

[15] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursGSTOOL47/02_Anwendung/06_ITGrundschutzPruefen/08_Ergaenz**
[16] **http://www.computerwoche.de/k/windows-8%2C3464**
[17] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Zertifizierung/Zertifizierungsprozess/zertifizieru**
[18] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/Veroeffentlichungen/Antraege/antraege_node.html**
[19] **http://www.business-reframing.de/**
[20] **http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533**
[21] **https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html**
