SCHWERPUNKT INFORMATIONSSICHERHEIT FÜR SICHERHEITSTECHNIK

RZ-ZERTIFIZIERUNG

ISO 27001 klassisch oder auf Basis von IT-Grundschutz?

Konkurrenz der Optionen

Zertifizierungen für Rechenzentren (RZ) sind mittlerweile weit verbreitet und werden von Nutzern, Kunden und je nach Branche auch von Prüforganisationen gefordert. Dabei „konkurrieren" am Markt verschiedene Zertifizierungen. Neben einer klassischen Infrastrukturzertifizierung, die eine Aussage über die Sicherheit und Verfügbarkeit eines Rechenzentrums trifft, kann man sein Rechenzentrum auch hinsichtlich der Betriebsführung, der Energieeffizienz, einer Kombination aus vorgenannten oder eben auch unter Gesichtspunkten des Informationssicherheitsmanagements zertifizieren. Die internationale Norm ISO/IEC 27001 IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation.

Mehrwert der Sonderoption?

Eine besondere Form stellt dabei die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz dar. Die Frage ist, wo liegen die Unterschiede und gibt es sogar einen „Mehrwert" gegenüber einer klassischen ISO 27001 Zertifizierung?

Große Schnittmenge

Um es vorwegzunehmen, die Zertifizierung auf Basis des IT-Grundschutzes deckt die ISO 27001 komplett ab. Und die weitere gute Nachricht ist, dass dieser Weg zur Zertifizierung sich in weiten Teilen mit der ISO 27001 überschneidet. Allerdings ist das Verfahren sehr strikt vorgegeben und weitaus arbeitsintensiver als eine klassische ISO 27001 Zertifizierung. Dies gilt insbesondere dann, wenn die in vielen Betrieben geführte Dokumentation über die IT schlecht strukturiert, lückenhaft oder gar nicht vorhanden ist.

Grundsätze der Informationssicherheit

Wie bei der ISO 27001 sind in einer Sicherheitsleitlinie (sog. Security Policy) zunächst die Kernpunkte der Sicherheitsstrategie festzuhalten. Diese Kernpunkte sollen die Grundsätze zur Informationssicherheit vermitteln können. Und diese behandeln letztlich immer die Grundwerte in der Informationssicherheit:

- Vertraulichkeit,
- Integrität und
- Verfügbarkeit.

Diese müssen in ausreichender Qualität vorhanden sein, damit das System „IT" notwendige Informationen zu jeder Zeit, unverfälscht und an den berechtigten Adressaten bereitstellt.

Anspruchsvolle Dokumentation

Doch mit einer Sicherheitsleitlinie oder Policy ist das Ziel noch nicht erreicht. Der schwierigste Teil auf dem Weg zu einer erfolgreichen Zertifizierung ist die Erfüllung der oftmals ungeliebten Dokumentationsanforderungen. Auf ein Rechenzentrum bezogen ergeben sich eine Vielzahl an zu beachtenden Punkten aus dem Baukasten des IT-Grundschutzes des BSI (Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de). Es gilt, einen Informationsverbund zu modellieren, der in Bezug auf ein Rechenzentrum die

Bausteine für den Standort und dessen Risiken, für das Gebäude an sich, die Räume, die Server, die verbindenden Netze sowie für die Anwendungen und Daten in Relation zueinander bringt. Diese Informationen sind tabellarisch zu protokollieren und darüber hinaus soll die Vernetzung der vorhandenen Systeme über einen Netzplan visualisiert werden.

„GSTOOL" und Alternativen

Diesen sicherlich aufwendigsten Teil auf dem Weg zur Zertifizierung fasst man unter dem Oberbegriff „IT-Strukturanalyse" zusammen. Früher hat das BSI dafür ein Softwaretool bereitgestellt (das sog. GSTOOL) – allerdings nur bis Ende 2014. Neben dem offiziellen GSTOOL des BSI gab es bereits seit mehreren Jahren von verschiedenen Drittanbietern entwickelte Tools, welche ebenfalls die BSI-Standards umsetzen konnten. Heute stellt das BSI daher nur noch eine aktuelle Übersicht an Tools zur Verfügung, mit denen man seinen Informationsverbund BSI-konform modellieren kann (Kurzlink: https://bit.ly/2DvZypi).

Drei Schutzbedarfskategorien

Der nächste Schritt beinhaltet die sogenannte Schutzbedarfsfeststellung. Das BSI gibt drei Schutzbedarfskategorien vor: normal, hoch und sehr hoch. Mit der Einstufung „sehr hoch" sollte man sehr bewusst und eher sparsam umgehen, weil diese Einstufung einen oft unverhältnismäßig hohen operativen Aufwand bedeuten kann und dann zwangsläufig auch zu einem hohen finanziellen Aufwand führt. Das hängt u. a. damit zusammen, dass z. B. nicht nur der Server in die Schutzbedarfskategorie „sehr hoch" eingestuft wird, sondern dann auch der Raum, das Gebäude, das Netz etc. zwangsläufig und nach dem Grundsatz der Gleichwertigkeit als „sehr hoch" einzustufen sind. Das BSI verwendet hierfür den Begriff des „Maximierungsprinzips". Doch was soll man sich eigentlich im Rahmen der Schutzbedarfsfeststellung unter „sehr hoch" vorstellen? Nun, die Schutzbedarfsfeststellung erfolgt zunächst allgemein bezogen auf die drei eingangs erwähnten Grundwerte der Informationssicherheit. Das kann in der Praxis bedeuten, dass ein IT-Sicherheitsvorfall zu existenzbedrohenden Konsequenzen des Unternehmens führen kann oder mindestens zu einem beträchtlichen finanziellen Schaden, der so hoch ist, dass man diesen im Boxsportjargon als „Wirkungstreffer" bezeichnen würde.

Basis-Sicherheitscheck

Ist die Modellierung und Schutzbedarfsfeststellung abgeschlossen, erfolgt ein weiterer, ebenfalls zeitaufwendiger Arbeitsschritt auf dem Weg zur Zertifizierung: ein Soll-Ist-Abgleich (auch als Basis-Sicherheitscheck bezeichnet). Dabei wird jeder Baustein des IT-Grundschutzes berücksichtigt und die damit verbundenen Maßnahmen werden auf deren Umsetzungsgrad geprüft. So beinhaltet der Baustein „INF.2 – Infrastruktur Rechenzentrum/ Serverraum" insgesamt 28 Basisanforderungen. Jede Maßnahme der ausgewählten Bausteine wird auf den Umsetzungsgrad hin überprüft.

Richtwerte für Maßnahmen

Für die Zertifizierung sind vom BSI 82 Prozent an erfüllten Maßnahmen als Richtwert vorgegeben. Dabei steht die Sinnhaftigkeit der Maßnahmen im Vordergrund. Das Unternehmen ist nicht verpflichtet, alle Maßnahmen umzusetzen, wenn es plausible Begründungen und Kompensationen vorlegen kann. Hier hilft wie bei jeder Zertifizierung eine offene Kommunikation mit dem verantwortlichen Auditor. Die Zertifizierung selbst ist mit der herkömmlichen ISO 27001 vergleichbar, wobei die Zertifizierungsstelle in diesem Fall das BSI selbst ist, das auch an den Prüfer (Auditor) einige Anforderungen stellt.

Auditorentestate

Vor der eigentlichen Zertifizierung müssen Auditorentestate erlangt werden, die zwei Jahre lang gültig und nicht wiederholbar sind. Beim ersten Testat ist eine Erfüllung von rund 55 Prozent der Maßnahmen erforderlich. Beim zweiten bereits 72 Prozent, bis schließlich zu den bereits erwähnten bzw. geforderten 82 Prozent. Das Zertifikat gilt dann für drei Jahre.

Auf Sicherheitsaspekt fokussieren

Fazit:
Mit Re-Zertifizierungsaudits kann die Zertifizierung anschließend aufrechterhalten werden. Doch für welche Variante soll man sich entscheiden? Für den RZ-Bereich ist es letzt-

lich eine Kosten-Nutzen Rechnung, denn eine ISO 27001 auf der Basis von IT-Grundschutz verschlingt nicht unerhebliche Ressourcen. Natürlich ist die „BSI-Zertifizierung“ mit der ISO 27001 vollständig kompatibel. Ob nun aber ISO 27001 oder ISO 27001 auf der Basis von IT-Grundschutz: Unternehmen sollten die Zertifizierung immer aus sicherheitsbewusstem Eigeninteresse anstreben. Exkulpation (Entlastung vom Vorwurf des Verschuldens) oder positive Marketingaspekte sollten nur als „Beifang “betrachtet werden.

Der Autor Uwe Hoffmeister
Bachelor of Science in Computer Science

Sicherheitsberater, Redaktionsmitglied beim Sicherheits-Berater (seit 2004) mit den Spezialgebieten Sicherheitskonzeption und Beratung im Umfeld höchstverfügbarer Rechenzentren, Schwachstellenanalysen, IT- und Sicherheitsaudits sowie Rechenzentrumszertifizierungen

SCHWERPUNKT INFORMATIONSSICHERHEIT FÜR SICHERHEITSTECHNIK

ITIL

Unverzichtbare IT-Betriebsprozesse

Security-LAN

Wenn IT abseits der IT betrieben wird, ist das möglicherweise eine gewollte Sicherheitsmaßnahme. Es ist zum Beispiel durchaus üblich, für den Betrieb der Sicherheitstechnik ein eigenes IT-Netz ohne Anbindung an die normale „Office-IT“ vorzusehen. In diesem „Security-LAN“ wird eine Mischung aus Standardkomponenten, wie Windows-PC und einige Standard-Server und aufgabenspezifische IT, wie Steuergeräte der Zutrittskontrolle, Videokameras und dergleichen, betrieben.

Standardwerk für IT-Prozesse

Das Betreiben auch solch untypischer IT sollte dabei dringend die Erkenntnisse zum IT-Betrieb berücksichtigen, die die normale IT in den letzten 20 Jahren gewonnen hat. Das Standardwerk zu diesem Thema ist ITIL (IT Infrastructure Library). ITIL ist im Grunde eine Sammlung von Empfehlungen und beschreibt die Prozesse, die nötig sind oder sein könnten, um die Leistung IT wunsch- und anforderungsgemäß für den Kunden bereitzustellen. Es ist gewiss ein Unterschied, ob hier zig maßgeschneiderte Prozesse für einen Weltkonzern oder einige IT-gestützte Leistungen für einige dutzend Anwender bereitgestellt und unterstützt werden müssen. Entsprechend ist es mehr als ratsam, aus dem Füllhorn der ITIL Prozesse auch nur die „best practices“ herauszusuchen und auf den eigenen Bedarf zu adaptieren, die im konkreten Einsatzfall nützlich sein werden.

Maßnahmen:

Banal, aber realistisch

Es ist allgemein anerkannt, dass mindestens drei essentielle Unterstützungsprozesse für IT-Services etabliert sein sollten, die ganz banale Erkenntnisse umsetzen:

1. IT ist kompliziert. Alles, was ich heute gemacht habe, habe ich nach etwa einer Woche vergessen.
2. „Eben mal“ sind die schlimmsten beiden Worte in der IT. Unzureichend durchdachte und geplante Änderungen führen gerne ins Chaos.
3. Probleme kann man nur lösen, wenn man sie bemerkt.