REVISION DER INFORMATIONSSICHERHEIT

Quelle: Information des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Informationssicherheitsrevision (IS-Revision) ist ein Bestandteil eines jeden erfolgreichen Informationssicherheitsmanagements. Nur durch die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheits-Prozesses können Aussagen über deren wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit und damit über den aktuellen Zustand der Informationssicherheit getroffen werden. Die IS-Revision ist somit ein Werkzeug zum Feststellen, Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus in einer Institution.

Die Hauptaufgabe der IS-Revision ist es, das Management, das IS-Management-Team und insbesondere den IT-Sicherheitsbeauftragten bei der Umsetzung und Optimierung der Informationssicherheit zu unterstützen und zu begleiten. Die Prüfungstätigkeit zielt darauf ab, die Informationssicherheit zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Wirtschaftlichkeit der Sicherheitsmaßnahmen und der Sicherheitsprozesse zu optimieren.

Hierzu hat das BSI ein Verfahren entwickelt, das sowohl die Bundesverwaltung, als auch andere Behörden, Banken, Versicherungen, Institutionen der freien Wirtschaft und Dienstleister nutzen können, um den Status der Informationssicherheit in einer Institution festzustellen und Schwachstellen identifizieren zu können.

Das BSI qualifiziert ausschließlich BSI-zertifizierte ISO 27001 Auditteamleiter im Rahmen eines speziellen Prüfungsprozederes zu Information Security Revisoren (IS-Revisor), die für Bundesbehörden sowie andere Behörden, Banken und Versicherungen die Dienstleistung "IS-Revision" anbieten. Der Qualifikationsnachweis ist die ISO 27001 Auditorzertifizierung auf der Basis von IT-Grundschutz zusammen mit der IS-Revisor-Bestätigungsurkunde des BSI.

1. Die IS-Kurzrevision

Die IS-Kurzrevision ist ein Verfahren zur Einschätzung des Informationssicherheitsstatus und -prozesses in einer Institution. Ziel der IS-Kurzrevision ist es, der Leitungsebene mit relativ wenig Aufwand einen Überblick über den Sicherheitsstatus und die bestehenden sicherheitskritischen Themenbereiche in der eigenen Institution zu verschaffen. Bei einer IS-Kurzrevision werden Maßnahmen aus dem IT-Grundschutz betrachtet, die eine wesentliche Grundlage für Informationssicherheit bilden und sich darüber hinaus aufgrund von Erfahrungswerten als problembehaftet erwiesen haben.

Der zeitliche Aufwand für eine IS-Kurzrevision beschränkt sich auf ungefähr 8 bis 10 Personentage.

Um eine IS-Kurzrevision durchführen zu lassen, bestehen keine Voraussetzungen hinsichtlich der Umsetzung von IT-Grundschutz. Dokumentationen, wie zum Beispiel das Sicherheitskonzept, müssen noch nicht vorhanden sein.

2. Die IS-Revision im IS-Managementprozess

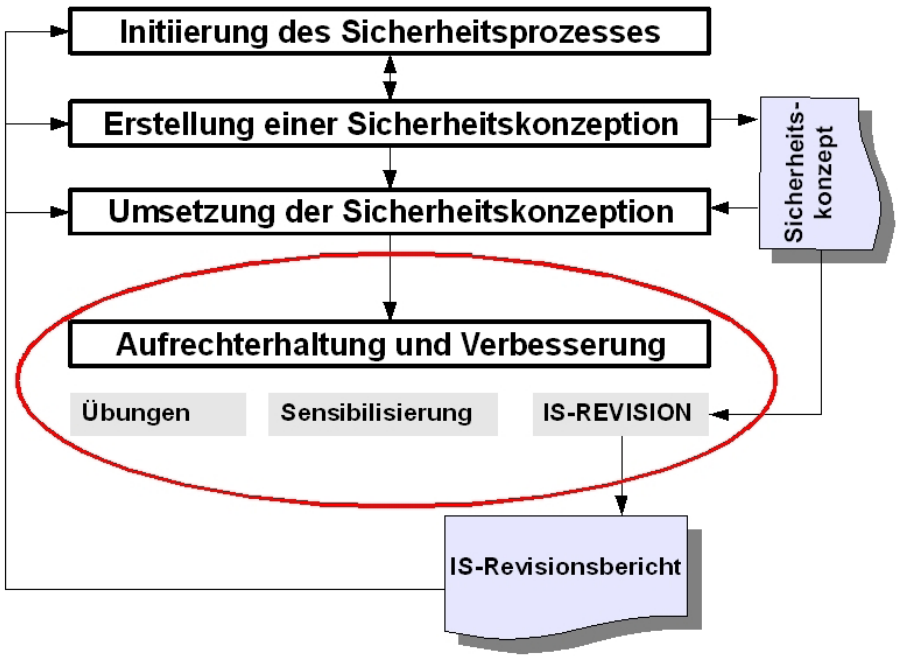
Die Praxis zeigt, dass eine umfassende, unternehmens- bzw. behördenweite Informationssicherheit, die auf dauerhafte Erfüllung der Anforderungen und nachhaltige Begrenzung der Risiken ausgerichtet ist, nur durch ein Informationssicherheitsmanagement erreicht werden kann. Der BSI-Standard 100-1 „Managementsysteme für Informationssicherheit (ISMS)“ (siehe [BSI1]) beschreibt den Informationssicherheitsprozess. Innerhalb des ISMS ist die IS-Revision Teil des Informationssicherheitsprozesses und fügt sich in die „Check“-Phase nach dem PDCA-Modell von Deming ein.

Der Informationssicherheitsprozess wird von der Leitungsebene initiiert und beginnt mit der „Plan“-Phase. In dieser Phase wird die Sicherheitsorganisation aufgebaut.

In der anschließenden „Do“-Phase werden das Sicherheitskonzept erstellt und die erforderlichen Maßnahmen umgesetzt.

Die folgende „Check“-Phase dient der Überprüfung der IT-Sicherheitsstrategie, der IT-Sicherheitsorganisation, des Sicherheitskonzepts und der Maßnahmenumsetzung. Grundlage für die Erfolgskontrollen in der „Check“-Phase ist immer das Sicherheitskonzept. Eine mögliche Methode der Erfolgskontrolle ist die IS-Revision.

Das Ergebnis der „Check“-Phase, z. B. der IS-Revisionsbericht, wird gemäß dem Informationssicherheitsprozess in der darauf folgenden „Act“-Phase ausgewertet und weiterverarbeitet. Das bedeutet, dass die Geschäftsprozesse optimiert und Sicherheitslücken bei der Maßnahmenumset-zung geschlossen werden.



Integration der IS-Revision im Informationssicherheits-Managementprozess

3. Unterschiedliche Arten einer IS-Revision

Es existieren unterschiedliche Ausprägungen der IS-Revision, wobei zwischen IS-Kurzrevision, IS-Querschnittsrevision, und IS-Partialrevision unterschieden wird.

3.1. IS-Kurzrevision □das Einstiegsverfahren

Die IS-Kurzrevision verschafft dem IS-Management mit relativ wenig Aufwand einen Überblick über den Sicherheitsstatus in der Institution (siehe Abschnitt 1).

3.2. IS-Querschnittsrevision □das IS-Revisionsverfahren gemäß UP Bund

Ist der Sicherheitsprozess weiter fortgeschritten und ein Großteil der IT-Grundschutz-Maßnahmen umgesetzt, ist eine IS-Querschnittsrevision durchzuführen. Eine IS-Querschnittsrevision hat einen ganzheitlichem Ansatz und ein breites Prüfspektrum. Bei einer IS-Querschnittsrevision werden alle Schichten des IT-Grundschutzes anhand von Stichproben geprüft.
Prüfgegenstand bei der IS-Querschnittsrevision ist immer die gesamte Institution. Sie hat das Ziel, einen umfassenden Eindruck von dem Informationssicherheitsstatus der Institution zu geben. Die IS-Querschnittsrevision ist die IS-Revision, die für Bundesbehörden gemäß UP Bund verpflichtend durchzuführen ist. Für andere Behörden, Banken und Versicherungen führt sie zu einem aussagekräftigen Ergebnis hinsichtlich der Einhaltung und Umsetzung der Vorgaben, Regeln und Maßnahmen des Informationssicherheits-Managementprozesses.

3.3. IS-Partialrevision □die IS-Revision für Spezialfälle

Eine IS-Partialrevision beschränkt sich auf einen speziellen Ausschnitt der Institution und wird bei Bedarf z. B. durch das IS-Management-Teamangestoßen. Die Prüftiefe ist wesentlich größer als bei der IS-Querschnittsrevision.
Die IS-Partialrevision ist eine anlassbezogene IS-Revision, die z. B. nach größeren Umstrukturierungen, Sicherheitsvorfällen oder bei Einführung neuer Geschäftsprozesse bzw. neuer Technologien durchgeführt wird. Sie ist prädestiniert für die IS-Revision von kritischen Geschäftsprozessen. Da sich eine IS-Partialrevision auf bestimmte Geschäftsprozesse oder IT-Verfahren beschränkt, werden auch nur die damit verbundenen Systeme und die hierfür anzuwendenden Bausteine des IT-Grundschutzes betrachtet. Dadurch kann die Prüftiefe deutlich erhöht werden. Abhängig vom definierten Prüfumfang kann bei einer IS-Partialrevision eine stichprobenbasierte Prüfung oder eine vollständige Prüfung aller zutreffenden Maßnahmen sinnvoll sein. Darüber hinaus gelten die gleichen Regelungen und Abläufe wie bei der IS-Querschnittsrevision.

4. Grundsätze der IS-Revision

Das IS-Revisionsteamist unabhängig und objektiv. Es unterstützt die Institution bei der Erreichung ihrer Ziele, indem das Team mit einem systematischen und zielgerichteten Ansatz die Effektivität des Sicherheitsprozesses bewertet und diesen zu verbessern hilft.
Grundvoraussetzung für jede Revision, somit auch für die IS-Revision, ist ein uneingeschränktes Informations- und Einsichtnahme recht. Dies bedeutet, dass dem IS-Revisionsteam keine Informationen vorenthalten werden dürfen. Dies beinhaltet auch die Einsichtnahme in sensible oder amtlich geheim gehaltene Informationen, die das Informationssicherheitsmanagement und den IT-Betrieb betreffen, sofern das IS-Revisionsteameinen entsprechenden Bedarf glaubhaft machen kann.
Das Referenzwerk für IS-Revisionen sind die IT-Grundschutz Kataloge (siehe [GSK]) und die BSI-Standards (siehe [BSI]). Insoweit diese Werke zu den eingesetzten Techniken keine Aussage treffen, sind andere einschlägige Vorschriften, Gesetze, Standards oder Vorgaben durch Hersteller zu verwenden. Die Nutzung dieser Regelwerke ist zu dokumentieren und zu begründen.
Jedes IS-Revisionsteam sollte zur Gewährleistung der Unabhängigkeit und Objektivität aus.

Weiterführende Informationen:

Accuris AG
Informationssicherheit & Datenschutz
Münchner Technologiezentrum
Agnes-Pockels-Bogen 1
80995 München
Tel. 089-9034000
www.accuris.de
office@accuris.de