Sicherheitskonzept
nach ISO 27001 auf der Basis von IT-Grundschutz

Dr.-Ing. Christian Scharff/BSI-zertifizierter ISO 27001Lead Auditor

Ein Informationssicherheitskonzept dient der Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Aus diesem Grund muss ein Sicherheitskonzept sorgfältig geplant und umgesetzt sowie regelmäßig überprüft werden.

Vor allem bei großen Behörden und Unternehmen kann es mehrere Sicherheitskonzepte geben, die verschiedene Organisationsbereiche abdecken. Komplexe Geschäftsprozesse oder Anwendungen können in eigenen Sicherheitskonzepten behandelt werden.

Das Sicherheitskonzept wird in den folgenden Phasen erstellt.

Phase 1: Festlegung des Geltungsbereichs/Informationsverbunds

Der festgelegte Geltungsbereich wird im Weiteren als Informationsverbund (früher: IT-Verbund) bezeichnet und stellt detailliert den Bereich dar, für den das Sicherheitskonzept umgesetzt werden soll. Ein Informationsverbund kann sich somit auf Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten beziehen. Er umfasst alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in diesem Anwendungsbereich der Informationsverarbeitung dienen.

Der Informationsverbund muss so festgelegt sein, dass die betrachteten Geschäftsprozesse und Informationen diesem Bereich vollständig zugeordnet werden können. Die Abhängigkeiten aller sicherheitsrelevanten Prozesse sind zu berücksichtigen. Die Schnittstellen zu den anderen Bereichen müssen klar definiert werden, so dass der Informationsverbund im Gesamtunternehmen eine sinnvolle Mindestgröße einnimmt.

Phase 2: IT-Strukturanalyse

Die IT-Strukturanalyse stellt eine Analyse des Ist-Zustands des Informationsverbunds dar. Dabei wird der Informationsverbund strukturiert erfasst. Die Ergebnisse dieser Analyse sollten enthalten:

- Beschreibung der Geschäftsprozesse sowie der darin verarbeiteten Informationen,
- im Informationsverbund betriebene Anwendungen mit Bezug auf die dadurch gestützten Geschäftsprozesse,
- im Informationsverbund eingesetzte vernetzte und nicht-vernetzte IT-Systeme,
- die Kommunikationsverbindungen zwischen den IT-Systemen und nach außen
- die IT-Räumlichkeiten (Serverräume und Rechenzentrum sowie andere IT-Räume)
- Beschreibung der Sicherheits-Infrastruktur

Phase: 3: Schutzbedarfsfeststellung

Für die zu schützenden Informationen und Geschäftsprozesse ist von dem jeweiligen Verantwortlichen (Informationseigentümer) zusammen mit dem Sicherheitsmanagement der Schutzbedarf festzulegen. Der Schutzbedarf wird dabei mit Hilfe von Schutzbedarfskategorien festgelegt. Die Bewertung des Schutzbedarfs der jeweiligen

Datenart erfolgt anhand einer qualitativen Abschätzung des Schadens und dessen Einordnung in eine der drei Kategorien:

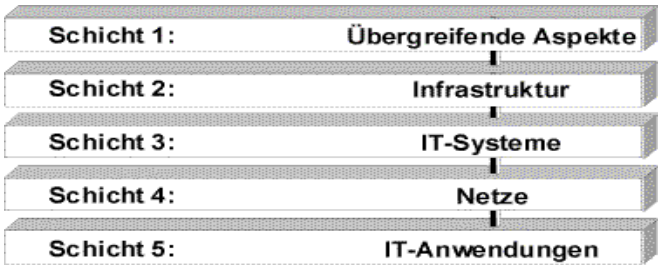
- Normal (die Schadensauswirkungen sind begrenzt und überschaubar),
- Hoch (die Schadensauswirkungen können beträchtlich sein),
- Sehr Hoch (die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen).

In der Schutzbedarfsfeststellung sind folgende Schritte enthalten:

- Es wird analysiert, welche Gefährdungen bzw. Risiken für die Institution als Folge unzureichender Informationssicherheit bestehen.
- Mögliche Schäden durch Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit werden identifiziert.
- Die potentiellen Auswirkungen auf die Geschäftstätigkeit oder die Aufgabenerfüllung durch Sicherheitsvorfälle und andere Sicherheitsrisiken werden analysiert und bewertet.

Phase 4: Modellierung

Bei der Modellierung erfolgt die Nachbildung des realen Informationsverbunds mit Hilfe der Bausteine der IT-Grundschutz-Kataloge auf Basis des nachfolgend dargestellten Schichtenmodells.



Der Informationsverbund wird dabei in fünf Schichten unterteilt. Jeder Schicht ist eine Reihe von Bausteinen zugeordnet. Als Ergebnis steht das IT-Grundschutz-Modell des realen Informationsverbunds, das aus verschiedenen Bausteinen besteht und eine Korrelation zwischen den Grundschutz-Bausteinen und den Gegebenheiten des Informationsverbunds beinhaltet. Über die verwendeten Grundschutz-Bausteine werden die relevanten Standard-Sicherheitsmaßnahmen identifiziert.

Phase 5: Basis-Sicherheitscheck

Das als Ergebnis der Modellierung spezifische Paket von Sicherheitsmaßnahmen stellt die Soll-Vorgabe der erforderlichen Maßnahmen dar. Um zu ermitteln, welche der Sicherheitsmaßnahmen bereits umgesetzt und an welchen Stellen noch Lücken sind, wird ein Basis-Sicherheitscheck durchgeführt.

Der Basis-Sicherheitscheck stellt die Aufnahme des tatsächlichen festgestellten Umsetzungsstatus der gemäß Modellierung identifizierten Sicherheitsmaßnahmen zum Prüfzeitpunkt dar. Dabei wird für jede Maßnahme, die in den für die Modellierung herangezogenen Bausteinen enthalten ist, der Umsetzungsstatus dokumentiert. Der Umsetzungsstatus kann wie folgt dokumentiert sein:

"entbehrlich" bedeutet, dass diese Maßnahme im De-Mail-Verbund nicht erforderlich/nicht relevant ist

"ja" bedeutet, dass diese Maßnahme vollständig umgesetzt ist

"teilweise" bedeutet, dass diese Maßnahme nur bisher nur teilweise umgesetzt ist
"nein" bedeutet, dass diese Maßnahme noch nicht umgesetzt ist, diese aber erforderlich ist

Sofern eine Maßnahme als "entbehrlich" angesehen wird, ist dies nachvollziehbar zu begründen.

Phase 6: Ergänzende Sicherheitsanalyse

Eine ergänzende Sicherheitsanalyse ist erforderlich für Elemente des Informationsverbunds, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen der IT-Grundschutz-Kataloge nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (z. B. in Umgebungen oder mit Anwendungen) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

In der Vorgehensweise nach IT-Grundschutz wird implizit eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt. In bestimmten Fällen, beispielsweise wenn der betrachtete Informationsverbund Komponenten mit hohem oder sehr hohem Schutzbedarf enthält, muss jedoch eine ergänzende Sicherheitsanalyse in Form einer expliziten Risikoanalyse oder/und Penetrationstest durchgeführt werden. Die hierfür notwendigen Arbeitsschritte sind in den BSI-Standards 100-2 und 100-3 erläutert.

Phase 7: Konsolidierung des Sicherheitskonzepts

Vor der Fertigstellung eines Sicherheitskonzeptes müssen die in der Risikoanalyse zusätzlich identifizierten Maßnahmen mit den IT-Grundschutz-Maßnahmen konsolidiert werden. Dabei ist für alle neu ermittelten Sicherheitsmaßnahmen zu überprüfen, ob sie die vorhandenen Maßnahmen ersetzen, ergänzen oder in ihrer Wirkung beeinträchtigen.

Bei der Konsolidierung des Sicherheitskonzepts werden

1. ungeeignete Sicherheitsmaßnahmen verworfen und nach eingehender Analyse durch wirksame Maßnahmen ersetzt.
2. Widersprüche oder Inkonsistenzen bei den Sicherheitsmaßnahmen werden aufgelöst und durch einheitliche und aufeinander abgestimmte Mechanismen ersetzt.
3. praktikable Lösungen erarbeitet, die die Benutzer möglichst wenig einschränken oder behindern. Sicherheitsmaßnahmen, die von den Benutzern nicht akzeptiert werden, sind wirkungslos.
4. zu aufwendige oder zu teure Sicherheitsmaßnahmen überarbeitet oder verworfen und durch angemessene Schutzmaßnahmen ersetzt.

Phase 8: Ergänzender Basis-Sicherheitscheck

Durch die ergänzende Sicherheitsanalyse/Risikoanalyse ergeben sich in der Regel Änderungen am Sicherheitskonzept (Konsolidierung). Daher ist anschließend noch der Umsetzungsstatus der neu hinzugekommenen oder geänderten Maßnahmen zu prüfen. Dies geschieht, indem die Ergebnisse des Basis-Sicherheitschecks vervollständigt und auf den neuesten Stand gebracht werden.

Umsetzung des Sicherheitskonzepts

Ein Sicherheitskonzept ist nur wirksam, wenn die darin vorgesehenen Maßnahmen auch zeitnah in die Praxis umgesetzt werden. Dies muss geplant und kontrolliert werden.

Quellen:

BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise

IT-Grundschutzkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI), M 2.195 Erstellung eines Sicherheitskonzepts