Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 100-3
Risikoanalyse auf der Basis von IT-Grundschutz
Version 2.0

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

1.1 Versionshistorie

Februar 2004	Version 1.0
Dezember 2005	Version 2.0

1.2 Zielsetzung

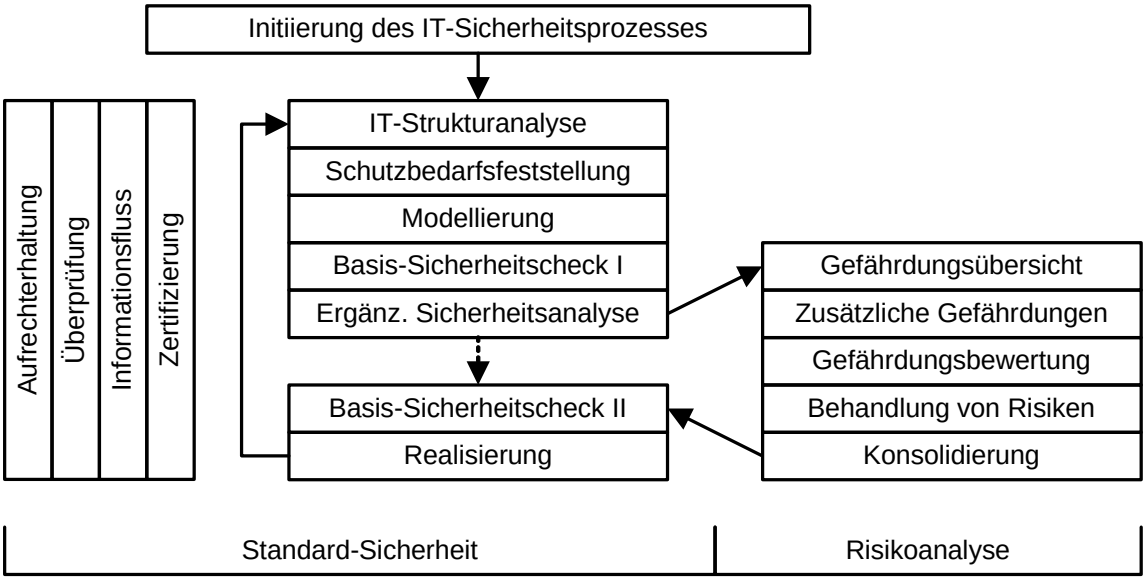
Nachfolgend wird eine Methodik erläutert, wie mit Hilfe der in den IT-Grundschutz-Katalogen [GS-KAT] aufgeführten Gefährdungen eine vereinfachte Analyse von IT-Risiken durchgeführt werden kann. Potentielle Anwendungsgebiete einer solchen Analyse in Behörden und Unternehmen sind beispielsweise IT-Komponenten oder IT-Bereiche, die

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

In diesen Fällen stellen sich folgende Fragen:

- Welchen Gefährdungen für die Informationsverarbeitung ist durch die Umsetzung der relevanten IT-Grundschutz-Bausteine noch nicht ausreichend oder sogar noch gar nicht Rechnung getragen?
- Müssen eventuell zusätzliche IT-Sicherheitsmaßnahmen, die über das IT-Grundschutz-Modell hinausgehen, eingeplant und umgesetzt werden?

Das vorliegende Dokument beschreibt eine Methodik, wie mit möglichst geringem Aufwand für bestimmte Zielobjekte festgestellt werden kann, ob und in welcher Hinsicht über den IT-Grundschutz hinaus Handlungsbedarf zur Begrenzung von IT-Risiken besteht.



Im IT-Sicherheitshandbuch [SHB] und in einigen anderen Vorgehensweisen zur Risiko- und Sicherheitsanalyse werden unter anderem auch *Eintrittswahrscheinlichkeiten* von Schadensereignissen betrachtet, um Entscheidungen zum Umgang mit Risiken zu treffen. Es hat sich jedoch gezeigt, dass die Abschätzung dieser Wahrscheinlichkeiten in der Praxis oft schwierig ist, da keine Grundlagen für verlässliche Schätzungen vorhanden sind. Auch die Interpretation der Wahrscheinlichkeiten ist in vielen Fällen fraglich. In der hier beschriebenen Methodik werden deshalb Eintrittswahrscheinlichkeiten nicht explizit, sondern lediglich implizit im Rahmen der Ermittlung und Bewertung von Gefährdungen betrachtet.

1.3 Adressatenkreis

Dieses Dokument richtet sich an IT-Sicherheitsverantwortliche, -beauftragte, -experten, -berater und alle Interessierte, die mit dem Management von IT-Sicherheit oder mit der Durchführung von IT-Risikoanalysen betraut sind.

Anwender der in diesem Dokument beschriebenen Methodik sollten mit der IT-Grundschutz-Vorgehensweise [GS-VOR] vertraut sein.

1.4 Anwendungsweise

Dieses Dokument beschreibt eine Methodik zur Durchführung von IT-Risikoanalysen, die ein bestehendes IT-Grundschutz-Sicherheitskonzept ergänzen. Dabei werden die in den IT-Grundschutz-Katalogen beschriebenen Gefährdungen als Hilfsmittel verwendet.

Es wird empfohlen, die in den Kapiteln 2 bis 8 dargestellte Methodik Schritt für Schritt durchzuarbeiten.

1.5 Literaturverzeichnis

[GS-KAT] IT-Grundschutz-Kataloge, BSI, *http://www.bsi.bund.de/gshb*

[GS-VOR] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, *http://www.bsi.bund.de/gshb*

[SHB] IT-Sicherheitshandbuch - Handbuch für die sichere Anwendung der Informationstechnik, BSI, Version 1.0 - März 1992, Bundesdruckerei

2 Vorarbeiten

Bevor die eigentliche Risikoanalyse beginnt, sollten folgende Vorarbeiten abgeschlossen sein, die in der IT-Grundschutz-Vorgehensweise des BSI beschrieben sind:

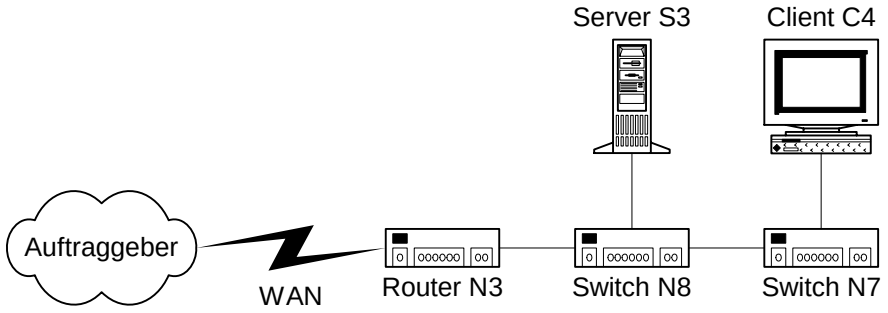
- Es sollte ein systematischer *IT-Sicherheitsprozess initiiert* worden sein. Dies dient dazu, die Aktivitäten im Bereich der IT-Sicherheit in geordnete Bahnen zu lenken. Beispielsweise müssen geeignete Rollen und Aufgaben definiert werden. Weitere Informationen zur Initiierung des IT-Sicherheitsprozesses finden sich in Kapitel 3 der IT-Grundschutz-Vorgehensweise.
- Für den IT-Verbund muss eine *IT-Strukturanalyse* gemäß Kapitel 4.1 der IT-Grundschutz-Vorgehensweise durchgeführt worden sein. Dadurch werden die wichtigsten Informationen über den IT-Verbund ermittelt, zum Beispiel der bereinigte Netzplan sowie eine Liste der wichtigsten IT-Anwendungen mit Abhängigkeit von den IT-Systemen.
- Anschließend muss eine *Schutzbedarfsfeststellung* gemäß Kapitel 4.2 der IT-Grundschutz-Vorgehensweise durchgeführt worden sein. Als Ergebnis liegt der Schutzbedarf der IT-Anwendungen, der IT-Systeme, der IT-genutzten Räume sowie eine Liste der kritischen Kommunikationsverbindungen vor. Der Schutzbedarf bezieht sich jeweils auf die Grundwerte *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* und wird in den drei Stufen *normal*, *hoch* und *sehr hoch* festgelegt.
- Es muss eine *Modellierung* gemäß Kapitel 4.3 der IT-Grundschutz-Vorgehensweise und Kapitel 2 der IT-Grundschutz-Kataloge durchgeführt worden sein. Dabei wird für jeden Baustein der IT-Grundschutz-Kataloge festgestellt, auf welche Zielobjekte im realen IT-Verbund er anzuwenden ist. Die in den einzelnen Bausteinen genannten Standard-Sicherheitsmaßnahmen bilden die Basis für das IT-Grundschutz-Sicherheitskonzept des betrachteten IT-Verbunds.
- Es muss vor der Risikoanalyse ein *Basis-Sicherheitscheck* gemäß Kapitel 4.4 der IT-Grundschutz-Vorgehensweise durchgeführt werden. Dadurch wird festgestellt, welche Standard-Sicherheitsmaßnahmen für den vorliegenden IT-Verbund bereits umgesetzt sind und wo noch Defizite bestehen.
- Es muss eine *ergänzende Sicherheitsanalyse* gemäß Kapitel 4.5 der IT-Grundschutz-Vorgehensweise durchgeführt worden sein. Bei der ergänzenden Sicherheitsanalyse wird entschieden, für welche Zielobjekte eine Risikoanalyse durchgeführt werden soll und für welche Zielobjekte dies dagegen entbehrlich ist.

Die Zielobjekte, für die im Rahmen der ergänzenden Sicherheitsanalyse entschieden wurde, dass für sie eine Risikoanalyse durchzuführen ist, werden im Folgenden als *betrachtete Zielobjekte* oder als *betrachtete Komponenten* bezeichnet.

Beispiel:

Ein Zulieferunternehmen unterhält eine Kommunikationsverbindung zum Hauptauftraggeber. Über diese Verbindung meldet der Auftraggeber ständig den aktuellen Bedarf an Zulieferprodukten in den jeweiligen Farben, Größen und Sorten. Um das Datenvolumen zu minimieren, werden jeweils nur die Änderungen gegenüber dem zuvor gemeldeten Bedarf übertragen. Diese Bedarfsmeldungen verwendet das Zulieferunternehmen als Grundlage für den Einsatz der Produktionskapazitäten. Auf diese Weise ist gewährleistet, dass das Zulieferunternehmen möglichst genau die jeweils benötigten Stückzahlen in den einzelnen Farben, Größen und Sorten produziert und liefert.

Technisch ist die Kommunikationsverbindung durch eine gemietete Standleitung zum Hauptauftraggeber realisiert. Bereits ein Ausfall von zwei Stunden kann zu erheblichen Überproduktionen oder Lieferengpässen und somit zu hohen Kosten für das Unternehmen führen. Folgender Teilbereich des gesamten IT-Verbunds weist somit einen hohen Schutzbedarf in Bezug auf Verfügbarkeit auf:



Die betroffenen Komponenten befinden sich in den Räumen M.723 (Serverraum), M.811 (Technikraum) und E.5 (Leitstand im Fertigungsbereich). Im Rahmen der ergänzenden Sicherheitsanalyse wurde entschieden, dass für alle anderen Komponenten mit hohem Schutzbedarf keine Risikoanalyse erforderlich ist.

3 Erstellung der Gefährdungsübersicht

Als Ausgangspunkt für die Risikoanalyse bieten sich die in den IT-Grundschutz-Katalogen aufgeführten, für die betrachteten Zielobjekte relevanten Gefährdungen an. Anders als im IT-Sicherheitshandbuch werden Bedrohungen, Schwachstellen und Risiken hierbei nicht separat untersucht.

Ziel der folgenden Arbeitsschritte ist es, eine Übersicht über die Gefährdungen zu erstellen, die auf die betrachteten Zielobjekte des IT-Verbunds wirken. Hierfür ist es zweckmäßig, den IT-Verbund zunächst auf die betrachteten Komponenten zu reduzieren.

1. Aus der Modellierung des IT-Verbunds werden als erstes alle Zielobjekte oder Gruppen von Zielobjekten gestrichen, für die laut ergänzender Sicherheitsanalyse kein Bedarf für eine Risikoanalyse besteht. Das heißt, es werden alle nicht-betrachteten Zielobjekte aus der Modellierung gestrichen. Hierbei können in der Regel nur in den Schichten 2 bis 5 Streichungen vorgenommen werden, da die Bausteine in Schicht 1 in der Regel alle oder zumindest viele Zielobjekte betreffen.

   Beispiel: (Auszug)

Nr.	Titel des Bausteins	Zielobjekt	
B 2.3	Büroraum	~~Raum M.501~~	streichen
B 2.4	Serverraum	Raum M.723	
B 2.6	Raum für technische Infrastruktur	Raum M.811	
B 3.101	Allgemeiner Server	~~S2~~	streichen
B 3.101	Allgemeiner Server	S3	
B 3.105	Server unter Novell Netware 4.x	~~S2~~	streichen
B 3.105	Server unter Novell Netware 4.x	S3	
B 3.205	Client unter Windows NT	~~C2~~	streichen
B 3.207	Client unter Windows 2000	C4	
B 3.301	Sicherheitsgateway (Firewall)	N3	

2. Anschließend werden aus der verbleibenden Tabelle alle Bausteine gestrichen, für die kein Zielobjekt und keine Gruppe von Zielobjekten mehr übrig ist. Diese Bausteine sind offenbar für die betrachteten Zielobjekte nicht relevant.

   In einigen Fällen können auch aus Schicht 1 Bausteine gestrichen werden, wenn offensichtlich ist, dass das im Baustein behandelte Thema für die jeweilige Risikoanalyse irrelevant ist.

   Beispiele:

   - Auf die Bausteine B 1.3 *Notfallvorsorge-Konzept* und B 1.8 *Behandlung von Sicherheitsvorfällen* kann meist verzichtet werden, wenn in der Risikoanalyse nur Teilbereiche behandelt werden, die einen normalen Schutzbedarf in Bezug auf Verfügbarkeit haben.
   - Auf den Baustein B 1.7 *Kryptokonzept* kann meist verzichtet werden, wenn in der Risikoanalyse nur Teilbereiche behandelt werden, die einen normalen Schutzbedarf in Bezug auf Vertraulichkeit und Integrität haben.

Als Ergebnis dieser Schritte liegt eine Tabelle vor, in der die Bausteine aufgeführt sind, die für die betrachteten Zielobjekte relevant sind. Die Bausteine der Schicht 1 sind dabei für alle oder für viele Zielobjekte wichtig, die Bausteine in den übrigen vier Schichten beziehen sich dagegen auf spezielle Zielobjekte oder Gruppen von Zielobjekten.

Beispiel: (Auszug)

Nr.	Titel des Bausteins	Zielobjekt
B 2.4	Serverraum	Raum M.723
B 2.6	Raum für technische Infrastruktur	Raum M.811
B 3.101	Allgemeiner Server	S3
B 3.105	Server unter Novell Netware 4.x	S3
B 3.207	Client unter Windows 2000	C4
B 3.301	Sicherheitsgateway (Firewall)	N3

3. Jeder Baustein aus den IT-Grundschutz-Katalogen verweist auf eine Liste von Gefährdungen. Für jedes Zielobjekt in der Tabelle werden Nummer und Titel dieser Gefährdungen aus den Bausteinen zusammen getragen und dem jeweiligen Zielobjekt zugeordnet.
4. Als Ergebnis liegt eine Tabelle vor, die jedem Zielobjekt eine Liste mit relevanten Gefährdungen zuordnet. Aus dieser Tabelle sollten pro Zielobjekt alle doppelten oder mehrfach genannten Gefährdungen entfernt werden.
5. Anschließend sollten die Gefährdungen in der Tabelle pro Zielobjekt thematisch sortiert werden. Einige Gefährdungen in den IT-Grundschutz-Katalogen behandeln ähnliche Sicherheitsprobleme oder unterschiedliche Ausprägungen der gleichen Bedrohung (z. B. G 1.2 *Ausfall des IT-Systems* und G 4.31 *Ausfall oder Störung von Netzkomponenten*).
6. Um die nachfolgende Analyse zu erleichtern, sollte in der Tabelle für jedes Zielobjekt der Schutzbedarf vermerkt werden, der im Rahmen der Schutzbedarfsfeststellung in den drei Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit ermittelt wurde. Für das übergeordnete Zielobjekt *gesamter IT-Verbund* kann diese Zuordnung entfallen.

Diese Tabelle stellt eine *Gefährdungsübersicht* für die betrachteten Zielobjekte dar. Sie dient als Ausgangspunkt für die nachfolgende *Ermittlung zusätzlicher Gefährdungen*.

Beispiel: (Auszug)

Kommunikationsserver S3	
Vertraulichkeit:	normal
Integrität:	hoch
Verfügbarkeit:	hoch
G 1.2	*Ausfall des IT-Systems*
G 3.2	*Fahrlässige Zerstörung von Gerät oder Daten*
G 4.1	*Ausfall der Stromversorgung*
G 5.57	*Netzanalyse-Tools*
G 5.85	*Integritätsverlust schützenswerter Informationen*
usw.	

Raum M.811	
Vertraulichkeit:	normal
Integrität:	normal
Verfügbarkeit:	hoch
G 1.4	*Feuer*
G 1.5	*Wasser*
G 2.6	*Unbefugter Zutritt zu schutzbedürftigen Räumen*
G 5.3	*Unbefugtes Eindringen in ein Gebäude*
G 5.5	*Vandalismus*
usw.	

4 Ermittlung zusätzlicher Gefährdungen

Für die betrachteten Zielobjekte gibt es unter Umständen einzelne zusätzliche Gefährdungen, die über die im IT-Grundschutz-Modell vorgesehenen Gefährdungen hinausgehen. Diese müssen ebenfalls berücksichtigt werden. In den IT-Grundschutz-Katalogen sind in der Regel nur solche Gefährdungen *nicht* aufgeführt, die

- durch eine besondere Technologie, ein spezielles Produkt oder einen besonderen Anwendungsfall bedingt sind oder
- in üblichen Einsatzszenarien nur unter sehr speziellen Voraussetzungen zu einem Schaden führen oder
- sehr gute Fachkenntnisse, Gelegenheiten und Mittel eines Angreifers voraussetzen.

Beispiele hierfür sind die vorsätzliche Ausschaltung eines gesamten Standortes mit Waffengewalt oder ein technisch komplizierter Angriff unter aktiver Mithilfe eines internen Administrators.

Für die IT-Sicherheit *relevante Gefährdungen* sind solche,

- die zu einem nennenswerten Schaden führen können und
- die im vorliegenden Anwendungsfall und Einsatzumfeld realistisch sind.

Bei der Ermittlung zusätzlicher relevanter Gefährdungen sollte der Schutzbedarf des jeweiligen Zielobjekts in Bezug auf die drei *Grundwerte* der IT-Sicherheit - *Vertraulichkeit, Integrität* und *Verfügbarkeit* - berücksichtigt werden:

1. Hat das Zielobjekt in einem bestimmten Grundwert den Schutzbedarf *sehr hoch*, sollten vorrangig solche Gefährdungen gesucht werden, die diesen Grundwert beeinträchtigen. Bei dieser Schutzbedarfskategorie ist davon auszugehen, dass es relevante Gefährdungen gibt, die nicht in den IT-Grundschutz-Katalogen enthalten sind.
2. Auch wenn das Zielobjekt in einem bestimmten Grundwert den Schutzbedarf *hoch* hat, sollten solche Gefährdungen gesucht werden, die diesen Grundwert beeinträchtigen. Bei dieser Schutzbedarfskategorie gibt es unter Umständen relevante Gefährdungen, die nicht in den IT-Grundschutz-Katalogen enthalten sind.
3. Hat das Zielobjekt in einem bestimmten Grundwert den Schutzbedarf *normal*, sind die in den IT-Grundschutz-Katalogen aufgeführten Gefährdungen - und somit auch die empfohlenen Sicherheitsmaßnahmen - für diesen Grundwert in der Regel ausreichend.

Unabhängig vom Schutzbedarf des betrachteten Zielobjekts ist die Ermittlung zusätzlicher relevanter Gefährdungen besonders wichtig, wenn es in den IT-Grundschutz-Katalogen keinen geeigneten Baustein für das Zielobjekt gibt oder wenn das Zielobjekt in einem Einsatzszenario (Umgebung, Anwendung) betrieben wird, das in den IT-Grundschutz-Katalogen nicht vorgesehen ist.

Die folgenden Fragestellungen sind bei der Ermittlung zusätzlicher Gefährdungen zu berücksichtigen:

- Von welchen möglichen Ereignissen aus dem Bereich *höhere Gewalt* droht besondere Gefahr für den IT-Verbund?
- Welche *organisatorischen Mängel* müssen auf jeden Fall vermieden werden, um die IT-Sicherheit zu gewährleisten?
- Welche *menschlichen Fehlhandlungen* können den sicheren IT-Betrieb besonders beeinträchtigen?
- Welche speziellen Sicherheitsprobleme können beim jeweils betrachteten Zielobjekt durch *technisches Versagen* entstehen?

- Welche besondere Gefahr droht durch vorsätzliche Angriffe von *Außentätern*? Damit sind Personen gemeint, die nicht der eigenen Institution angehören und auch nicht durch besondere Vereinbarungen Zugang zu oder Zugriff auf interne Ressourcen haben.
- Auf welche Weise können *Innentäter* durch vorsätzliche Handlungen den ordnungsgemäßen und sicheren Betrieb des jeweiligen Zielobjekts beeinträchtigen? Durch vorhandene Zugangs- und Zugriffsberechtigungen sowie durch Insider-Wissen droht hier oft besondere Gefahr.

Für jedes betrachtete Zielobjekt wird als erstes geprüft, ob weitere Gefährdungen berücksichtigt werden müssen. Quellen für diese speziellen Gefährdungen sind beispielsweise

- die Dokumentation des Herstellers,
- Schwachstellenpublikationen im Internet und
- eigene Bedrohungsanalysen.

Außerdem kann es durchaus zielführend sein, bei der Ermittlung zusätzlicher Gefährdungen erneut die IT-Grundschutz-Gefährdungskataloge G 1 bis G 5 als Quellen heranzuziehen. Möglicherweise sind dort weitere relevante Gefährdungen aufgeführt, die jedoch bislang nicht berücksichtigt wurden, weil beispielsweise die entsprechenden Bausteine nicht in der Modellierung enthalten sind.

In der Praxis ist es oft so, dass zusätzliche Gefährdungen gleich mehrere Zielobjekte betreffen. Die identifizierten zusätzlichen Gefährdungen werden in der Gefährdungsübersicht ergänzt.

Wichtig: Wenn relevante Gefährdungen nicht berücksichtigt werden, kann dies zu Lücken im resultierenden IT-Sicherheitskonzept führen. Im Zweifelsfall sollte daher sorgfältig analysiert werden, ob und - wenn ja - welche Gefährdungen noch fehlen. Hierbei ist es oft ratsam, auf externe Beratungsdienstleistungen zurück zu greifen.

In der Praxis hat es sich bewährt, zur Ermittlung zusätzlicher Gefährdungen ein gemeinsames Brainstorming mit allen beteiligten Mitarbeitern durchzuführen. Es sollten IT-Sicherheitsbeauftragte, Projektleiter, Administratoren und Benutzer des jeweils betrachteten Zielobjekts, ggf. auch externe Sachverständige beteiligt werden. Der Arbeitsauftrag an die Teilnehmer sollte klar formuliert sein und die Zeit für das Brainstorming begrenzt werden. Die Erfahrung zeigt, dass ein Zeitraum von 2 Stunden eine sinnvolle Obergrenze ist. Ein IT-Sicherheitsexperte sollte das Brainstorming moderieren.

Beispiel: (Auszug)

Im Rahmen eines Brainstormings identifiziert das Unternehmen unter anderem folgende zusätzliche Gefährdungen:

gesamter IT-Verbund	
G 2.B1	*Unzureichende Synchronisierung von Wirk- und Backup-System*
	Aufgrund der hohen Verfügbarkeitsanforderungen werden Komponenten des Kommunikationssystems zum Auftraggeber doppelt vorgehalten. Wenn die Backup-Komponenten nicht auf dem aktuellen Stand sind, besteht die Gefahr, dass keine funktionierende Verbindung zum Auftraggeber aufgebaut werden kann.
G 5.70	*Manipulation durch Familienangehörige und Besucher*
	Diese Gefährdung ist in den IT-Grundschutz-Katalogen enthalten und wird von Baustein B 2.8 *Häuslicher Arbeitsplatz* referenziert. Dieser Baustein ist jedoch nicht in der Modellierung des vorliegenden IT-Verbunds enthalten. Dennoch muss die Gefährdung G 5.70 berücksichtigt werden, weil regelmäßig Besucher durch die Räumlichkeiten der Firma geführt werden. G 5.70 wird deshalb zusätzlich in die Risikobetrachtung einbezogen.
usw.	

Switch N7	
Vertraulichkeit:	normal
Integrität:	normal
Verfügbarkeit:	hoch
G 2.B2	*Beschädigung von Informationstechnik im Fertigungsbereich*
	Der Client C4 und der Switch N7 werden im Fertigungsbereich des Unternehmens betrieben und sind deshalb besonderen physischen Gefahren ausgesetzt. Die Geräte können beschädigt, zerstört oder deren Lebensdauer reduziert werden.
usw.	

Client C4	
Vertraulichkeit:	normal
Integrität:	hoch
Verfügbarkeit:	hoch
G 2.B2	*Beschädigung von Informationstechnik im Fertigungsbereich*
	siehe Switch N7
G 4.B1	*Inkompatibilitäten zwischen Fertigungs- und Kommunikations-Software*
	Der Client C4 wird nicht nur zur Kommunikation mit dem Auftraggeber benutzt, sondern es werden weitere Programme zur Unterstützung der Fertigung darauf betrieben. Durch Inkompatibilitäten zwischen diesen Programmen kann es zu Abstürzen und somit zum Verlust der Verfügbarkeit kommen.
usw.	

5 Gefährdungsbewertung

Im nächsten Schritt wird die Gefährdungsübersicht systematisch abgearbeitet und für jedes Zielobjekt und jede Gefährdung geprüft, ob die bereits umgesetzten oder zumindest im IT-Sicherheitskonzept vorgesehenen IT-Sicherheitsmaßnahmen einen ausreichenden Schutz bieten. In der Regel wird es sich hierbei um Standard-Sicherheitsmaßnahmen aus den IT-Grundschutz-Katalogen handeln. Die Prüfung erfolgt anhand des IT-Sicherheitskonzepts und anhand folgender Prüfkriterien:

- Vollständigkeit

  Bieten die Standard-Sicherheitsmaßnahmen Schutz gegen alle Aspekte der jeweiligen Gefährdung? (Beispiel: Wurde auch an die Hintertür zum Gebäude gedacht?)

- Mechanismenstärke

  Wirken die in den Standard-Sicherheitsmaßnahmen empfohlenen Schutzmechanismen der jeweiligen Gefährdung ausreichend stark entgegen? (Beispiel: Sind die Vorgaben zur Mindest-Schlüssellänge ausreichend?)

- Zuverlässigkeit

  Können die vorgesehenen Sicherheitsmechanismen nicht zu leicht umgangen werden? (Beispiel: Wie leicht können sich Benutzer Zutritt zum Serverraum verschaffen und dadurch die Zugriffskontrolle auf Dateien umgehen?)

Das Ergebnis der Prüfung wird in der Gefährdungsübersicht für jede Gefährdung einzeln in der Spalte *OK* vermerkt (*J/N*).

OK=J bedeutet, dass die bereits umgesetzten oder zumindest im IT-Sicherheitskonzept vorgesehenen IT-Sicherheitsmaßnahmen einen *ausreichenden Schutz* vor der jeweiligen Gefährdung bieten oder die jeweilige Gefährdung für die vorliegende Risikoanalyse ohnehin *nicht relevant* ist (beispielsweise weil ein anderer Grundwert betroffen ist).

OK=N bedeutet, dass die bereits umgesetzten oder zumindest im IT-Sicherheitskonzept vorgesehenen IT-Sicherheitsmaßnahmen *keinen ausreichenden Schutz* vor der jeweiligen Gefährdung bieten.

Hinweis: Im Rahmen der Gefährdungsbewertung kommen oftmals erste Ideen zur Sprache, mit welchen IT-Sicherheitsmaßnahmen den Gefährdungen begegnet werden kann. Diese Vorschläge sind für die nachfolgenden Arbeitsschritte nützlich und sollten deshalb notiert werden.

Die Gefährdungsbewertung liefert eine Übersicht, welchen Gefährdungen für die betrachteten Zielobjekte durch die Maßnahmen der IT-Grundschutz-Kataloge ausreichend Rechnung getragen ist (*OK=J*), und wo gegebenenfalls noch Risiken bestehen (*OK=N*). Die Behandlung dieser Risiken ist Gegenstand des nächsten Abschnitts.

Beispiel: (Auszug)

Im Zulieferunternehmen wurde anhand der ergänzten Gefährdungsübersicht eine Gefährdungsbewertung durchgeführt. Das Ergebnis ist, dass unter anderem für folgende Gefährdungen die IT-Grundschutzmaßnahmen nicht ausreichen (*OK=N*):

Kommunikationsserver S3		
Vertraulichkeit:	normal	
Integrität:	hoch	
Verfügbarkeit:	hoch	
G 1.2	*Ausfall des IT-Systems*	*OK=N*
	Dem Ausfall des Servers S3 muss zuverlässig vorgebeugt werden. Die Maßnahmen der IT-Grundschutz-Kataloge reichen nicht aus.	
G 5.85	*Integritätsverlust schützenswerter Informationen*	*OK=N*
	Die vom Auftraggeber gesendeten Bedarfsinformationen dürfen nicht verfälscht werden. Anderenfalls können erhebliche Überproduktionen oder Lieferengpässe und somit hohe Kosten für das Unternehmen entstehen.	
usw.		

Client C4		
Vertraulichkeit:	normal	
Integrität:	hoch	
Verfügbarkeit:	hoch	
G 1.2	*Ausfall des IT-Systems*	*OK=N*
	Zur Kommunikation mit dem Auftraggeber wird auf dem Client C4 spezielle Software verwendet, deren Installation aufwendig und zeitraubend ist.	
G 2.B2	*Beschädigung von Informationstechnik im Fertigungsbereich*	*OK=N*
	Der Betrieb von IT in maschinellen Fertigungsbereichen wird in den IT-Grundschutz-Katalogen nur am Rande behandelt.	
usw.		

6 Behandlung von Risiken

In der Praxis ergeben sich im Rahmen der Gefährdungsbewertung meist mehrere Gefährdungen, denen die Maßnahmen aus den IT-Grundschutz-Katalogen nicht ausreichend entgegenwirken. Aus diesen *verbleibenden Gefährdungen* können sich *Risiken* für den Betrieb des IT-Verbundes ergeben.

Es muss deshalb entschieden werden, wie mit den verbleibenden Gefährdungen umgegangen wird. Bei dieser Entscheidung muss auf jeden Fall die Leitungsebene beteiligt werden, da sich daraus u. U. erhebliche Risiken ergeben oder zusätzliche Kosten entstehen können. Für jede Gefährdung in der vervollständigten Gefährdungsübersicht mit *OK=N* gibt es folgende Alternativen:

A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen: Die verbleibende Gefährdung wird beseitigt, indem ein oder mehrere zusätzliche IT-Sicherheitsmaßnahmen erarbeitet und umgesetzt werden, die der Gefährdung hinreichend entgegenwirken. Als Informationsquellen über zusätzliche IT-Sicherheitsmaßnahmen kommen beispielsweise in Frage:

- die Dokumentation und der Service des Herstellers, wenn es sich bei dem betroffenen Zielobjekt um ein Produkt handelt,
- Standards und "Best Practices", wie sie beispielsweise von Gremien im Bereich IT-Sicherheit erarbeitet werden,
- andere Veröffentlichungen und Dienstleistungen, die beispielsweise im Internet oder von spezialisierten Unternehmen angeboten werden,
- Erfahrungen, die innerhalb der eigenen Institution oder bei Kooperationspartnern gewonnen wurden.

B. Risiko-Reduktion durch Umstrukturierung: Die verbleibende Gefährdung wird beseitigt, indem der Geschäftsprozess oder der IT-Verbund umstrukturiert wird. Gründe für diese Entscheidung können beispielsweise sein:

- Alle wirksamen Gegenmaßnahmen sind sehr teuer, die verbleibende Gefährdung kann aber trotzdem nicht hingenommen werden.
- Die Umstrukturierung bietet sich ohnehin aus anderen Gründen an, zum Beispiel zur Kostensenkung.
- Alle wirksamen Gegenmaßnahmen würden erhebliche Einschränkungen für die Funktion oder den Komfort des Systems mit sich bringen.

C. Risiko-Übernahme: Die verbleibende Gefährdung und damit auch das daraus resultierende Risiko wird akzeptiert. Gründe für diese Entscheidung können beispielsweise sein:

- Die Gefährdung führt nur unter ganz speziellen Voraussetzungen zu einem Schaden.
- Gegen die jeweilige Gefährdung sind derzeit keine wirksamen Gegenmaßnahmen bekannt und sie lässt sich in der Praxis auch kaum vermeiden.
- Aufwand und Kosten für wirksame Gegenmaßnahmen überschreiten den zu schützenden Wert.

D. Risiko-Transfer: Das Risiko, das sich durch die verbleibende Gefährdung ergibt, wird an eine andere Institution übertragen, zum Beispiel durch Abschluss eines Versicherungsvertrags oder durch Outsourcing. Gründe für diese Entscheidung können beispielsweise sein:

- Die möglichen Schäden sind rein finanzieller Art.
- Es ist ohnehin aus anderen Gründen geplant, Teile des IT-Betriebs auszulagern.
- Der Vertragspartner ist aus wirtschaftlichen oder technischen Gründen besser in der Lage, mit dem Risiko umzugehen.

Zur Vorbereitung einer fundierten Entscheidung, welche der vier Alternativen zur Behandlung des jeweiligen Risikos gewählt wird, sollte ein Brainstorming darüber durchgeführt werden, welche zusätzlichen IT-Sicherheitsmaßnahmen (Alternative A) grundsätzlich in Frage kommen. Dabei sollten die o. g. Informationsquellen herangezogen werden.

Hinweis: In einigen Fällen lassen sich nur gegen bestimmte - aber nicht alle - Teilaspekte einer Gefährdung IT-Sicherheitsmaßnahmen identifizieren. Hier stellt sich dann die Frage, wie mit der Gefährdung umgegangen wird (Alternative A oder C/D). Die jeweilige Gefährdung sollten in diesem Fall in zwei Gefährdungen aufgeteilt werden, die dann getrennt mit Alternative A bzw. C/D behandelt werden.

Es sollte auch berücksichtigt werden, welche IT-Sicherheitsmechanismen für das jeweilige Zielobjekt bereits vorhanden sind. Hierbei kann auf die Ergebnisse des Basis-Sicherheitschecks (siehe Kapitel 4.4 der IT-Grundschutz-Vorgehensweise) zurückgegriffen werden.

Der hypothetische Aufwand und Kosten für ggf. erforderliche IT-Sicherheitsmaßnahmen und Informationen über bereits vorhandene IT-Sicherheitsmechanismen sind wichtige Entscheidungshilfen.

- Bei Alternative A werden die zusätzlichen IT-Sicherheitsmaßnahmen im IT-Sicherheitskonzept ergänzt. Es genügt ein eindeutiger Verweis auf die entsprechende detaillierte Beschreibung der Maßnahmen. Falls die zusätzlichen IT-Sicherheitsmaßnahmen der betroffenen Gefährdung ausreichend entgegen wirken, wird der jeweilige *OK*-Status in der Gefährdungsübersicht von *N* auf *J* korrigiert.
- Alternative B führt in der Regel dazu, dass für die betroffenen Teile des IT-Verbunds auch der IT-Sicherheitsprozess neu gestartet werden muss. Dies beginnt meist bei der IT-Strukturanalyse. Selbstverständlich kann dabei aber auf die bisher erarbeiteten Informationen und Dokumente zurückgegriffen werden.
- Bei Alternative C muss auf jeden Fall das sich daraus ergebende Risiko transparent gemacht werden. Die Entscheidung wird von der Leitungsebene getroffen und nachvollziehbar dokumentiert.
- Bei Alternative D ist die sachgerechte Vertragsgestaltung einer der wichtigsten Aspekte. Besonders bei Outsourcing-Vorhaben sollte hierzu auf fundierten juristischen Sachverstand zurückgegriffen werden. Die Entscheidung wird von der Leitungsebene getroffen und nachvollziehbar dokumentiert.

Wichtig: Der Umgang mit Gefährdungen, gegen die in den IT-Grundschutz-Katalogen keine ausreichend wirksamen Gegenmaßnahmen beschrieben werden, kann entscheidend für das Gesamtrisiko des IT-Betriebs sein. Es sollte überlegt werden, hierzu auf externe Beratungsdienstleistungen zurückzugreifen.

Nachdem für jede verbleibende Gefährdung in der Gefährdungsübersicht eine Entscheidung getroffen wurde, welche der beschriebenen Handlungsoptionen gewählt wird, kann das IT-Sicherheitskonzept für den betrachteten IT-Verbund fertig gestellt werden.

Beispiel: (Auszug)

Für die in Kapitel 0 mit *OK=N* identifizierten Gefährdungen wurden folgende Entscheidungen getroffen:

Kommunikationsserver S3	
Vertraulichkeit:	normal
Integrität:	hoch
Verfügbarkeit:	hoch
G 1.2	*Ausfall des IT-Systems*
"A"	Zusätzliche IT-Sicherheitsmaßnahme:
M 6.B1	*Bereithalten eines vollständigen Ersatzsystems zur Kommunikation mit dem Auftraggeber* Es wird ein vollständiges Ersatzsystem zur Kommunikation mit dem Auftraggeber bereit gehalten. Dies umfasst alle technischen Komponenten einschließlich Kommunikationsverbindungen. Das Ersatzsystem wird in Raum E.3 gelagert. Es wird sichergestellt, dass das Ersatzsystem jederzeit die gleiche Konfiguration wie das Produktionssystem aufweist und innerhalb von 30 Minuten einsatzbereit ist. Die Kommunikation mit dem Auftraggeber erfolgt über eine Wählverbindung. Das gesamte Ersatzsystem einschließlich Wählverbindung wird mindestens einmal pro Quartal und bei jeder Konfigurationsänderung getestet.
G 5.85	*Integritätsverlust schützenswerter Informationen*
"C"	Risiko-Übernahme: Das Risiko wird durch die in den Übertragungs- und IT-Systemen eingebauten Sicherheitsmechanismen zwar etwas reduziert, jedoch sind weiterhin Sicherheitsvorfälle denkbar, die zu verfälschten Bedarfsinformationen und somit zu hohen Kosten für das Unternehmen führen können. Dieses Restrisiko wird von der Geschäftsführung akzeptiert und verantwortet, da alle wirksamen Gegenmaßnahmen unwirtschaftlich sind.
usw.	

Client C4	
Vertraulichkeit:	normal
Integrität:	hoch
Verfügbarkeit:	hoch
G 1.2	*Ausfall des IT-Systems*
"A"	Zusätzliche IT-Sicherheitsmaßnahme:
M 6.B1	*Bereithalten eines vollständigen Ersatzsystems zur Kommunikation mit dem Auftraggeber* Hinweis: siehe Kommunikationsserver S3
G 2.B2	*Beschädigung von Informationstechnik im Fertigungsbereich*
"A"	Zusätzliche IT-Sicherheitsmaßnahme:
M 1.B1	*Einsatz eines besonders geschützten Industrie-PCs im Fertigungsbereich* Die größten Gefahren für den Client C4 im Fertigungsbereich gehen von Luftverunreinigungen, Spritzwasser und Vibrationen aus. Anstelle eines handelsüblichen PCs wird deshalb ein Industrie-PC eingesetzt, der besonders gegen physische Gefahren geschützt ist. Der Industrie-PC muss folgende Anforderungen erfüllen: - geeignet für den Einbau in Standard-19-Zoll-Schränke - integriertes oder ausklappbares Display - leicht auswechselbarer Luftfilter - Schutz gegen Spritzwasser gemäß Schutzart IP 54 - Schutz gegen Vibration mindestens 0,2 g bei 0-500 Hz
usw.	

7 Konsolidierung des IT-Sicherheitskonzepts

Falls bei der Behandlung von verbleibenden Gefährdungen zusätzliche Maßnahmen zu den Standard-Sicherheitsmaßnahmen hinzugefügt wurden, muss das IT-Sicherheitskonzept anschließend konsolidiert werden. Konkret bedeutet dies, dass die IT-Sicherheitsmaßnahmen für jedes Zielobjekt anhand folgender Kriterien überprüft werden:

Eignung der IT-Sicherheitsmaßnahmen zur Abwehr der Gefährdungen

- Werden alle Aspekte der relevanten Gefährdungen vollständig abgedeckt?
- Sind die getroffenen Gegenmaßnahmen in Einklang mit den Sicherheitszielen?

Zusammenwirken der IT-Sicherheitsmaßnahmen

- Unterstützen sich die Maßnahmen bei der Abwehr der relevanten Gefährdungen?
- Ergibt sich durch das Zusammenwirken der Maßnahmen ein wirksames Ganzes?
- Stehen die Maßnahmen nicht im Widerspruch zueinander?

Benutzerfreundlichkeit der IT-Sicherheitsmaßnahmen

- Sind die getroffenen Maßnahmen tolerant gegenüber Bedienungs- und Betriebsfehlern?
- Sind die getroffenen Maßnahmen für die Benutzer transparent?
- Ist für die Benutzer ersichtlich, wenn eine Maßnahme ausfällt?
- Können die Benutzer die Maßnahme nicht zu leicht umgehen?

Angemessenheit der IT-Sicherheitsmaßnahme

- Sind die getroffenen Maßnahmen für die jeweiligen Gefährdungen angemessen?
- Stehen die Kosten und der Aufwand für die Umsetzung in einem sachgerechten Verhältnis zum Schutzbedarf der betroffenen Zielobjekte?

Auf dieser Grundlage sollte das IT-Sicherheitskonzept bereinigt und konsolidiert werden:

1. Ungeeignete IT-Sicherheitsmaßnahmen sollten verworfen und nach eingehender Analyse durch wirksame Maßnahmen ersetzt werden.
2. Widersprüche oder Inkonsistenzen bei den IT-Sicherheitsmaßnahmen sollten aufgelöst und durch einheitliche und aufeinander abgestimmte Mechanismen ersetzt werden.
3. IT-Sicherheitsmaßnahmen, die von den Benutzern nicht akzeptiert werden, sind wirkungslos. Es sollten praktikable Lösungen erarbeitet werden, die die Benutzer möglichst wenig einschränken oder behindern.
4. Zu aufwendige oder zu teure IT-Sicherheitsmaßnahmen sollten überarbeitet oder verworfen und durch angemessenen Schutzmaßnahmen ersetzt werden. Auf der anderen Seite gefährden zu schwache Maßnahmen die IT-Sicherheit. Auch sie sollten überarbeitet oder ersetzt werden.

Es kann durchaus zweckmäßig sein, neben der Risikoanalyse weitere Verfahren zur Verbesserung der IT-Sicherheit heranzuziehen, zum Beispiel Penetrationstests. Dabei wird versucht, das Angriffsverhalten eines vorsätzlichen Innen- oder Außentäters zu simulieren. Die Ergebnisse können wiederum Änderungen im IT-Sicherheitskonzept nach sich ziehen.

Beispiel: (Auszug)

Bei der Konsolidierung des IT-Sicherheitskonzepts für das Zulieferunternehmen wurde unter anderem Folgendes festgestellt:

- Auch für das in Maßnahme M 6.B1 geforderte Ersatzsystem müssen die relevanten Maßnahmen der IT-Grundschutz-Kataloge umgesetzt werden. Unterschiede zum Produktivsystem bestehen nur hinsichtlich des Aufstellungsortes und der WAN-Verbindung. Das Ersatzsystem ist somit in die IT-Grundschutz-Modellierung zu integrieren.
- Die aufgrund des IT-Grundschutzes vorgesehene Maßnahme M 6.53 *Redundante Auslegung der Netzkomponenten* wird für den Switch N7 durch die Maßnahme M 6.B1 konkretisiert. Nach Umsetzung von M 6.B1 ist auch M 6.53 für das Zielobjekt N7 umgesetzt. Maßnahme M 6.53 kann deshalb für den Switch N7 aus dem IT-Sicherheitskonzept gestrichen werden.
- Vor zwei Jahren wurde entschieden, dass die Maßnahme M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation* entbehrlich ist. Eine gemeinsame Projektgruppe mit dem Auftraggeber ist zu dem Ergebnis gekommen, dass diese Entscheidung nicht mehr dem Stand der Technik entspricht. Die Vorgaben zur Konfiguration der Router werden deshalb kurzfristig überarbeitet.
- Die zusätzliche IT-Sicherheitsmaßnahme M 1.B1 trägt den besonderen infrastrukturellen Rahmenbedingungen des Clients C4 Rechnung. Im Fertigungsbereich wird außer diesem Client weitere Informationstechnik betrieben, die zwar nicht Gegenstand der Risikoanalyse ist, die aber dennoch angemessen geschützt werden muss. Das Unternehmen nimmt die Umsetzung der Maßnahme M 1.B1 zum Anlass, eine Richtlinie für den sicheren Betrieb von Informationstechnik im Fertigungsbereich zu erarbeiten.
- usw.

8 Rückführung in den IT-Sicherheitsprozess

Nach der Konsolidierung des IT-Sicherheitskonzepts kann der Sicherheitsprozess, wie er in der IT-Grundschutz-Vorgehensweise beschrieben ist, fortgesetzt werden. Das ergänzte IT-Sicherheitskonzept dient somit als Basis für folgende Arbeitsschritte:

- *Basis-Sicherheitscheck* (Kapitel 4.4 der IT-Grundschutz-Vorgehensweise). Im Rahmen der Vorarbeiten wurde bereits ein Basis-Sicherheitscheck für die laut IT-Grundschutz-Modell vorgesehenen Maßnahmen durchgeführt. Da sich bei der Risikoanalyse in der Regel Änderungen am IT-Sicherheitskonzept ergeben, ist anschließend noch der Umsetzungsstatus der neu hinzugekommenen oder geänderten Maßnahmen zu prüfen. Gegebenenfalls veraltete Ergebnisse sollten auf den neuesten Stand gebracht werden.
- *Realisierung von IT-Sicherheitsmaßnahmen* (Kapitel 4.6 der IT-Grundschutz-Vorgehensweise). Die im IT-Sicherheitskonzept für die einzelnen Zielobjekte vorgesehenen IT-Sicherheitsmaßnahmen müssen in die Praxis umgesetzt werden, damit sie wirksam werden können. Dies umfasst unter anderem eine Kosten- und Aufwandsschätzung sowie die Festlegung der Umsetzungsreihenfolge.
- *Aufrechterhaltung der IT-Sicherheit und kontinuierliche Verbesserung* (Kapitel 5 der IT-Grundschutz-Vorgehensweise). Um den IT-Sicherheitsprozess aufrecht zu erhalten und kontinuierlich verbessern zu können, müssen nicht nur angemessene IT-Sicherheitsmaßnahmen implementiert und Dokumente fortlaufend aktualisiert werden, sondern auch der IT-Sicherheitsprozess muss auch regelmäßig auf seine Effektivität und Effizienz hin überprüft werden.
- *Überprüfung des IT-Sicherheitsprozesses in allen Ebenen* (Kapitel 5.1 der IT-Grundschutz-Vorgehensweise). Regelmäßig überprüft werden müssen unter anderem die Umsetzung des Realisierungsplans, die Eignung der IT-Sicherheitsstrategie, die Aktualität der IT-Sicherheitsziele und die Wirtschaftlichkeit des IT-Sicherheitsprozesses. Die Ergebnisse der Überprüfungen fließen in die Fortschreibung des IT-Sicherheitsprozesses ein.
- *Informationsfluss im IT-Sicherheitsprozess* (Kapitel 5.2 der IT-Grundschutz-Vorgehensweise). Die Leitungsebene muss von der IT-Sicherheitsorganisation regelmäßig in angemessener Form über Ergebnisse von Überprüfungen, IT-Sicherheitsvorfälle, den Status des IT-Sicherheitsprozesses und gegebenenfalls über weitere Aspekte der IT-Sicherheit informiert werden. Dabei sollten Probleme, Erfolge und Verbesserungsmöglichkeiten aufgezeigt werden.
- *IT-Grundschutz-Zertifizierung* (Kapitel 5.3 der IT-Grundschutz-Vorgehensweise). In vielen Fällen ist es wünschenswert, den Stellenwert der IT-Sicherheit und die erfolgreiche Umsetzung des IT-Grundschutzes in einer Behörde bzw. einem Unternehmen nach innen und außen transparent zu machen. Hierfür hat das BSI mit dem IT-Grundschutz-Testat und der "Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz" geeignete Mechanismen geschaffen.
- *Übernahme in das GSTOOL* (siehe *http://www.bsi.bund.de/gstool*). Falls das IT-Sicherheitsmanagement durch das GSTOOL oder eine andere Software unterstützt wird, sollten die Arbeitsergebnisse der Risikoanalyse - soweit möglich - dort eingearbeitet werden. Beim GSTOOL gilt dies insbesondere für neue oder geänderte IT-Sicherheitsmaßnahmen, die in dieser Form nicht in den IT-Grundschutz-Katalogen enthalten sind.