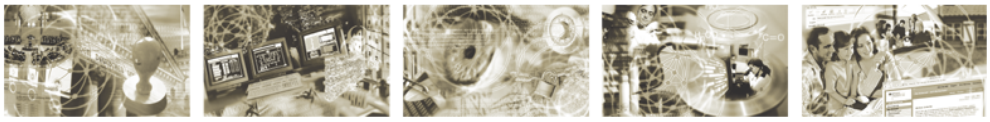
Bundesamt
für Sicherheit in der
Informationstechnik



Ergänzung zum BSI-Standard 100-3, Version 2.5

Verwendung der elementaren Gefährdungen aus den IT-Grundschutz-Katalogen zur Durchführung von Risikoanalysen

Stand: 03. August 2011

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5369
E-Mail: grundschutz@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

Der BSI-Standard 100-3 [BSI3] beschreibt eine Methodik, wie mit Hilfe der in den IT-Grundschutz-Katalogen [GSK] aufgeführten Gefährdungen eine vereinfachte Analyse von Risiken für die Informationsverarbeitung durchgeführt werden kann. Dabei stehen folgende Fragen im Vordergrund:

- 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 ergänzende Sicherheitsmaßnahmen, die über das IT-Grundschutz-Modell hinausgehen, eingeplant und umgesetzt werden?

Als Ausgangspunkt für die in [BSI3] beschriebene Methodik dienen die Gefährdungen in den Katalogen G 1 bis G 5 aus [GSK]. Mittlerweile umfassen diese fünf Gefährdungskataloge circa 450 Einzelgefährdungen. Dies erschwert die Betrachtung und Bewertung sämtlicher Gefährdungen bei Risikoanalysen. Daher hat das BSI aus den teilweise sehr spezifischen Einzelgefährdungen die generellen Aspekte herausgearbeitet und 46 generische Gefährdungen erarbeitet. Diese sogenannten *elementaren Gefährdungen* wurden im Zuge der 12. Ergänzungslieferung in den IT-Grundschutz-Katalogen im Gefährdungskatalog G 0 veröffentlicht.

Zielsetzung des vorliegenden Dokuments ist es, aufbauend auf dem BSI-Standard 100-3 aufzuzeigen, wie die elementaren Gefährdungen für die Durchführung von Risikoanalysen genutzt werden können. Die hierzu notwendigen Anpassungen der in [BSI3] dargestellten Vorgehensweise werden beschrieben.

Bei der praktischen Umsetzung der BSI-Standards haben Anwender somit die Wahl, ob sie Risikoanalysen gemäß BSI-Standard 100-3 mittels der Einzelgefährdungen aus den Gefährdungskatalogen G 1 bis G 5 oder anhand der neuen elementaren Gefährdungen aus Gefährdungskatalog G 0 durchführen. Für die Durchführung neuer Risikoanalysen empfiehlt das BSI die Verwendung der elementaren Gefährdungen, da dies im Vergleich zur Nutzung der Einzelgefährdungen meist einen geringeren Aufwand mit sich bringt, ohne dass Abstriche beim erreichbaren Sicherheitsniveau in Kauf genommen werden müssen.

2 Übersicht über die elementaren Gefährdungen

Bei der Erstellung der elementaren Gefährdungen wurden die im Folgenden aufgeführten Ziele verfolgt. Elementare Gefährdungen sind

- für die Verwendung bei der Risikoanalyse optimiert,
- produktneutral (immer),
- technikneutral (möglichst – bestimmte Technologien prägen so stark den Markt, dass sie auch die abstrahierten Gefährdungen beeinflussen),
- kompatibel mit vergleichbaren internationalen Katalogen,
- nahtlos in den IT-Grundschutz-Ansatz integriert.

Da die elementaren Gefährdungen hauptsächlich die effiziente Durchführung von Risikoanalysen ermöglichen sollen, wurde der Fokus darauf gelegt, tatsächliche Gefahren zu benennen. Gefährdungen, die überwiegend die fehlende oder unzureichende Umsetzung von Sicherheitsmaßnahmen thematisieren und somit auf indirekte Gefahren verweisen, wurden bewusst vermieden.

Bei der Erarbeitung der elementaren Gefährdungen wurde mitbetrachtet, welcher Grundwert der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) durch die jeweilige Gefährdung beschädigt würde. Da diese Information bei verschiedenen Schritten der Sicherheitskonzeption von Interesse sein kann, werden sie in der folgenden Tabelle mitgelistet. Nicht alle Gefährdungen lassen sich auf genau einen Grundwert abbilden, sondern verschiedene Gefährdungen betreffen mehrere Grundwerte. Dabei ist dies so zu interpretieren, dass durch die jeweilige Gefährdung die dazu aufgeführten Grundwerte direkt beeinträchtigt werden. Bei vielen Gefährdungen lässt sich nämlich diskutieren, in wie weit alle drei Grundwerte betroffen sein könnten, weil sich auch indirekte Auswirkungen ableiten lassen. So wird z. B. zu G 0.1 Feuer als einziger betroffener Grundwert Verfügbarkeit genannt. Natürlich könnte ein Feuer auch dazu führen, dass Datenträger nur geringfügig beschädigt würden, so dass Dateien auf den ersten Blick vorhanden wären, aber es zu Integritätsverlusten gekommen ist. Ein anderes Szenario könnte sein, dass bei einem Brand vertrauliche Unterlagen durch Rettungsmaßnahmen auf einmal für Unbefugte zugänglich wären – beides wären aber indirekte Auswirkungen auf die Grundwerte Vertraulichkeit und Integrität, nur Verfügbarkeit ist unmittelbar beeinträchtigt.

In der folgenden Tabelle findet sich eine Übersicht über die elementaren Gefährdungen. Dabei steht A für Availability (Verfügbarkeit), C für Confidentiality (Vertraulichkeit) und I für Integrity (Integrität).

	Gefährdung	**Grundwert**
G 0.01	Feuer	I,A
G 0.02	Ungünstige klimatische Bedingungen	I,A
G 0.03	Wasser	I,A
G 0.04	Verschmutzung, Staub, Korrosion	I,A
G 0.05	Naturkatastrophen	A
G 0.06	Katastrophen im Umfeld	A

G 0.07	Großereignisse im Umfeld	C,I,A
G 0.08	Ausfall oder Störung der Stromversorgung	I,A
G 0.09	Ausfall oder Störung von Kommunikationsnetzen	I,A
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A
G 0.11	Ausfall oder Störung von Dienstleistern	C,I,A
G 0.12	Elektromagnetische Störstrahlung	I,A
G 0.13	Abfangen kompromittierender Strahlung	C
G 0.14	Ausspähen von Informationen / Spionage	C
G 0.15	Abhören	C
G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	C,A
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten	C,A
G 0.18	Fehlplanung oder fehlende Anpassung	C,I,A
G 0.19	Offenlegung schützenswerter Informationen	C
G 0.20	Informationen aus unzuverlässiger Quelle	C,I,A
G 0.21	Manipulation von Hard- und Software	C,I,A
G 0.22	Manipulation von Informationen	I
G 0.23	Unbefugtes Eindringen in IT-Systeme	C,I
G 0.24	Zerstörung von Geräten oder Datenträgern	A
G 0.25	Ausfall von Geräten oder Systemen	A
G 0.26	Fehlfunktion von Geräten oder Systemen	C,I,A
G 0.27	Ressourcenmangel	A
G 0.28	Software-Schwachstellen oder –Fehler	C,I,A
G 0.29	Verstoß gegen Gesetze oder Regelungen	C,I,A
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C,I,A
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C,I,A
G 0.32	Missbrauch von Berechtigungen	C,I,A
G 0.33	Personalausfall	A
G 0.34	Anschlag	C,I,A
G 0.35	Nötigung, Erpressung oder Korruption	C,I,A
G 0.36	Identitätsdiebstahl	C,I,A
G 0.37	Abstreiten von Handlungen	C,I
G 0.38	Missbrauch personenbezogener Daten	C
G 0.39	Schadprogramme	C,I,A
G 0.40	Verhinderung von Diensten (Denial of Service)	A
G 0.41	Sabotage	A
G 0.42	Social Engineering	C,I

G 0.43	Einspielen von Nachrichten	C,I
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C,I,A
G 0.45	Datenverlust	A
G 0.46	Integritätsverlust schützenswerter Informationen	I

3 Erstellung der Gefährdungsübersicht

Um die elementaren Gefährdungen bei der Durchführung von Risikoanalysen einzusetzen, kann die in [BSI3] beschriebene Methodik nahezu unverändert angewandt werden. Inhaltliche Anpassungen sind lediglich beim Arbeitsschritt *Erstellung der Gefährdungsübersicht* (siehe Kapitel 3 in [BSI3]) erforderlich. Im Folgenden wird beschrieben, wie mit Hilfe der elementaren Gefährdungen eine Gefährdungsübersicht für die betrachteten Zielobjekte erstellt werden kann.

Ausgangspunkt für die Erstellung der Gefährdungsübersicht ist die Liste der Zielobjekte und Zielobjektgruppen, die in der Risikoanalyse betrachtet werden sollen ("betrachtete Zielobjekte"). Diese Liste liegt als Ergebnis der ergänzenden Sicherheitsanalyse vor (siehe Kapitel 4.6 in [BSI2] und Kapitel 2 in [BSI3]). Ergänzt wird diese Liste um das übergeordnete Zielobjekt *gesamter Informationsverbund*, sofern dieses Zielobjekt nicht ohnehin bereits in der Liste enthalten ist.

Beispiel: (Auszug)

Nummer	***Kurzbeschreibung***
IV	gesamter Informationsverbund
M.723	Serverraum
M.811	Technikraum
S3	Kommunikationsserver
C4	Client
N3	Router
N7	Switch

Tabelle 1: Liste der betrachteten Zielobjekte (Auszug)

Im Gefährdungskatalog G 0 der IT-Grundschutz-Kataloge hat das BSI elementare Gefährdungen, die für die Verwendung im Rahmen einer Risikoanalyse optimiert sind, veröffentlicht. Anhand des Katalogs G 0 werden nun nacheinander jedem betrachteten Zielobjekt die elementaren Gefährdungen zugeordnet, die für das jeweilige Zielobjekt *prinzipiell* zu einem *nennenswerten Schaden* führen können. Dabei ist es unerheblich, wie hoch der mögliche Schaden genau ist. Dieser Aspekt wird in einem späteren Arbeitsschritt behandelt. Auch die für das jeweilige Zielobjekt geplanten oder bereits umgesetzten Sicherheitsmaßnahmen sollten bei der Zuordnung der elementaren Gefährdungen *nicht* berücksichtigt werden. Dieser Aspekt wird ebenfalls in einem späteren Arbeitsschritt behandelt.

Insgesamt wird die Zuordnung der elementaren Gefährdungen zu den betrachteten Zielobjekten also unter der Annahme getroffen, dass keine Sicherheitsmaßnahmen, beispielsweise aus den IT-Grundschutz-Katalogen oder aus anderen Quellen, in Kraft sind.

In der Praxis hat der Typ des jeweiligen Zielobjekts einen wesentlichen Einfluss darauf, welche elementaren Gefährdungen überhaupt darauf anwendbar sind. So wird die Gefährdung G 0.28 *Software-Schwachstellen oder -Fehler* nur selten für einen Büroraum relevant sein, sondern eher für

die darin betriebenen Clients. Gefährdungen, die sich nicht auf konkrete technische Komponenten beziehen, beispielsweise G 0.29 *Verstoß gegen Gesetze oder Regelungen*, eignen sich meist für Zielobjekte vom Typ *Anwendung*, *Geschäftsprozess* oder *gesamter Informationsverbund*.

Als Ergebnis liegt eine Tabelle vor, die jedem Zielobjekt eine Liste mit relevanten elementaren Gefährdungen zuordnet.

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 Informationsverbund* 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 0.8	*Ausfall oder Störung der Stromversorgung*
G 0.22	*Manipulation von Informationen*
G 0.23	*Unbefugtes Eindringen in IT-Systeme*
G 0.24	*Zerstörung von Geräten oder Datenträgern*
G 0.25	*Ausfall von Geräten oder Systemen*
usw.	

Tabelle 2: Gefährdungsübersicht für das Zielobjekt S3 (Auszug)

Raum M.811	
Vertraulichkeit:	normal
Integrität:	normal
Verfügbarkeit:	hoch
G 0.1	*Feuer*
G 0.3	*Wasser*
G 0.24	*Zerstörung von Geräten oder Datenträgern* (z. B. Klimaanlage)
G 0.41	*Sabotage*
G 0.44	*Unbefugtes Eindringen in Räumlichkeiten*
usw.	

Tabelle 3: Gefährdungsübersicht für das Zielobjekt M.811 (Auszug)

4 Erstellung benutzerdefinierter Bausteine

Häufig soll auf Basis der Risikoanalyse ein benutzerdefinierter Baustein erstellt werden, für einen Themenbereich, der bisher in den IT-Grundschutz-Katalogen noch nicht ausreichend abgedeckt war, um den betrachteten Informationsverbund modellieren zu können. Andererseits sind die IT-Grundschutz-Kataloge so umfassend, dass häufig zumindest für Teilbereiche vorhandene Bausteine der IT-Grundschutz-Kataloge als Grundlage für die Risikoanalyse mit herangezogen werden können. Hierbei sollte einerseits soweit wie möglich auf den vorhandenen Materialien aufgebaut werden, um unnötigen Aufwand zu vermeiden, aber andererseits möglichst offen potentielle neue oder erweiterte Gefährdungen diskutiert werden, um keine Risiken zu übersehen.

Für den betrachteten Bereich muss zunächst eine Gefährdungsanalyse durchgeführt werden.

Dafür sollten für den betrachteten Bereich die elementaren Gefährdungen aus Gefährdungskatalog G 0 unter die Lupe genommen werden und überlegt werden, ob diese für das jeweilige Zielobjekt relevant sind, also prinzipiell zu einem nennenswerten Schaden führen können. Dafür ist jede elementare Gefährdung daraufhin zu bewerten, ob diese direkt, indirekt oder gar nicht auf das Zielobjekt einwirken kann.

Wird beispielsweise ein spezifisches Server-Betriebssystem betrachtet, ist die elementare Gefährdung G 0.25 "Ausfall von Geräten und Systemen" eine relevante Gefährdung, gegen die spezifische Sicherheitsmaßnahmen zu ergreifen sind. Im ersten Moment könnte es außerdem naheliegend sein, die elementare Gefährdung G 0.1 Feuer als relevant für dieses Zielobjekt einzustufen, mit der Begründung "Ein Brand verursacht den Ausfall des Servers". Dabei ist aber der Server-Ausfall eine Folgeerscheinung des Feuers, also eine indirekte Einwirkung auf die Hardware. Wodurch der Ausfall verursacht wird, ist im Allgemeinen für die Auswahl der erforderlichen Sicherheitsmaßnahmen irrelevant. Ein Betriebssystem bietet keine spezifischen Schutzmaßnahmen gegen Feuer, es würden durch die Betrachtung von G 0.1 Feuer keine neuen Aspekte gegenüber G 0.25 "Ausfall von Geräten und Systemen" entstehen.

Gefährdung	Grundwerte	Wirkung & Relevanz	Kommentar
G 0.01 Feuer	**Verfügbarkeit, Integrität**	**Indirekte Wirkung / Nicht relevant**	Die Gefährdung für ein Betriebssystem durch *Feuer* ist indirekt, es würden durch die Betrachtung von G 0.1 Feuer keine neuen Aspekte gegenüber G 0.25 „Ausfall von Geräten und Systemen“ abgedeckt. Die indirekte Gefährdung durch *G 0.01 Feuer* wird u.a. mit *G 0.25 Ausfall von Geräten und Systemen abgedeckt.*
G 0.09 Ausfall oder Störung von Kommunikationsnetzen	**Verfügbarkeit, Integrität**	**Indirekte Wirkung / Nicht relevant**	Die Gefährdung für ein Betriebssystem durch Ausfall oder Störung von Kommunikationsnetzen ist indirekt, es würden durch die Betrachtung von G 0.9 keine neuen Aspekte gegenüber G 0.26 Fehlfunktionen von Geräten und Systemen entstehen.Ein Betriebssystem bietet keine spezifischen Schutzmaßnahmen gegen G 0.09, die Gefährdung ist somit hier nicht relevant. Es sind keine spezifischen Maßnahmen erforderlich.
G 0.25 Ausfall von Geräten und Systemen	**Verfügbarkeit**	**Direkte Wirkung / Relevant**	Die Gefährdung durch G 0.26 Fehlfunktionen von Geräten und Systemen wirkt direkt auf ein Betriebssystem. Daher sind Maßnahmen gehen G 0.26 Fehlfunktionen von Geräten und Systemen zu prüfen.
G 0.26 Fehlfunktion von Geräten und Systemen	**Verttaulichkeit, Verfügbarkeit, Integrität**	**Direkte Wirkung / Relevant**	Die Gefährdung durch G 0.25 Ausfall von Geräten und Systemen wirkt direkt auf ein Betriebssystem. Daher sind Maßnahmen gehen G 0.25 Ausfall von Geräten und Systemen zu prüfen.

Tabelle: Beispiel zur Ermittlung zusätzlicher elementarer Gefährdungen

Anschließend sollte diskutiert werden, ob damit alle relevanten Gefährdungen identifiziert worden sind, also eine Vollständigkeitsprüfung durchgeführt werden, wie im BSI-Standard 100-3 in Kapitel 4 "Ermittlung zusätzlicher Gefährdungen" beschrieben. Dafür ist es hilfreich, einschlägige Informationen über den betrachteten Bereich zusammenzutragen, z. B. aus dem Internet. Lohnenswert ist es auch, in den IT-Grundschutz-Katalogen nachzuschlagen, welche existierenden Bausteine ähnliche Themen oder Vorgehensweisen abdecken, wie sie für den zu erstellenden Baustein benötigt werden. Außerdem sollten die Hilfsmittel auf den IT-Grundschutz-Webseiten gesichtet werden, ob ähnliche Aspekte durch Materialien dort behandelt werden. Darauf aufbauend sollten die in den relevanten vorhandenen Bausteinen beschriebenen Gefährdungen gesichtet werden.

Anschließend müssen die als relevant identifizierten elementaren Gefährdungen mit den Gefährdungen aus ähnlichen Bausteinen oder anderen Informationsquellen konsolidiert werden und zu einer möglichst passgenauen, übersichtlichen Gefährdungsliste zusammengefasst werden.

5 Weitere Arbeitsschritte

Gemäß [BSI3] schließen sich an den Arbeitsschritt *Erstellung der Gefährdungsübersicht* folgende weitere Arbeitsschritte an:

- *Ermittlung zusätzlicher Gefährdungen*
- *Gefährdungsbewertung*
- *Behandlung von Risiken*
- *Konsolidierung des Sicherheitskonzepts*
- *Rückführung in den Sicherheitsprozess*

Zur Nutzung der elementaren Gefährdungen sind an diesen Arbeitsschritten keine methodischen Änderungen erforderlich. Beim Abarbeiten dieser Arbeitsschritte treten die elementaren Gefährdungen an die Stelle der spezifischen Einzelgefährdungen. Die in [BSI3] bisher aufgeführten Beispiele sind auf die Nutzung der spezifischen Einzelgefährdungen zugeschnitten, diese können aber einfach durch elementare Gefährdungen ersetzt werden.

Literaturverzeichnis

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.5, Mai 2008, https://www.bsi.bund.de/grundschutz/standards

[BSI2] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Mai 2008, https://www.bsi.bund.de/grundschutz/standards

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.5, Mai 2008, https://www.bsi.bund.de/grundschutz/standards

[GSK] IT-Grundschutz-Kataloge – Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, https://www.bsi.bund.de/grundschutz/kataloge