Elementare Gefährdungen

Für effizientere Risikoanalysen hat das BSI als Ergänzung der bestehenden Gefährdungskataloge zur IT-Grundschutz-Vorgehensweise nunmehr „elementare Gefährdungen" definiert.

Isabel Münch, BSI

Die in den IT-Grundschutz-Katalogen enthaltenen Gefährdungskataloge bilden ein wichtiges Fundament für die Anwendung der IT-Grundschutz-Vorgehensweise [2] und der Risikoanalyse auf der Basis von IT-Grundschutz [3]. Die fünf Gefährdungskataloge enthalten zusammen eine Vielzahl von Einzelgefährdungen – davon sind einige so allgemeingültig, dass sie in fast jedem Baustein zitiert werden, andere aber wiederum so spezifisch, dass sie nur für einen Aspekt in einem einzelnen Baustein relevant sind. Dies erschwert die Behandlung und das Durcharbeiten sämtlicher Gefährdungen bei Risikoanalysen. Daher hat das BSI aus diesen Gefährdungen die generellen Aspekte herausgearbeitet und 46 elementare Gefährdungen erarbeitet.

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. Die elementaren Gefährdungen sollen die vorhandenen Gefährdungskataloge G 1 bis G 5 nicht ersetzen und werden daher in einem separaten Gefährdungskatalog G 0 zur Verfügung gestellt.

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, inwieweit alle drei Grundwerte betroffen sein könnten, weil sich auch indirekte Auswirkungen ableiten lassen.

So wird zum Beispiel zu „G 0.1 Feuer" als einziger betroffener Grundwert Verfügbarkeit genannt. Natürlich könnte ein Feuer auch dazu führen, dass Datenträger nur geringfügig beschädigt würden, sodass 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.

Elementare Gefährdungen und 100-3

Der BSI-Standard 100-3 [3] beschreibt eine Methodik, wie mithilfe der in den IT-Grundschutz-Katalogen [5] aufgeführten Gefährdungen eine vereinfachte Analyse von Risiken für die Informationsverarbeitung durchgeführt werden kann. Zunächst muss für eine Risikoanalyse eine Gefährdungsanalyse durchgeführt werden – Ausgangspunkt für eine Risikoanalyse basierend auf IT-Grundschutz sind dabei die relevanten Gefährdungen aus den IT-Grundschutz-Katalogen.

Bisher wurden dafür über die jeweils relevanten Bausteine aus den IT-Grundschutz-Katalogen die Gefährdungen aus den Katalogen G 1 bis G 5, die in den Bausteinen zitiert werden, in einer Liste zusammengetragen, die die Grundlage für die Ermittlung zusätzlicher Gefährdungen gebildet hat. Da die Gefährdungskataloge G 1 bis G 5 bereits jetzt umfangreich sind und mit der Erstellung neuer IT-Grundschutz-Bausteine weiter wachsen werden, gibt es bei dieser Vorgehensweise sehr viele verschiedene Gefährdungen, die in die Risikoanalyse eingehen. Mit den elementaren Gefährdungen aus dem neuen Katalog G 0 können nun nacheinander jedem betrachteten Zielobjekt die elementaren Gefährdungen zugeordnet werden, die für das jeweilige Zielobjekt prinzipiell zu einem nennenswerten Schaden führen können.

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, son-

Elementare Gefährdungen

Für effizientere Risikoanalysen hat das BSI als Ergänzung der bestehenden Gefährdungskataloge zur IT-Grundschutz-Vorgehensweise nunmehr „elementare Gefährdungen" definiert.

Isabel Münch, BSI

Die in den IT-Grundschutz-Katalogen enthaltenen Gefährdungskataloge bilden ein wichtiges Fundament für die Anwendung der IT-Grundschutz-Vorgehensweise [2] und der Risikoanalyse auf der Basis von IT-Grundschutz [3]. Die fünf Gefährdungskataloge enthalten zusammen eine Vielzahl von Einzelgefährdungen – davon sind einige so allgemeingültig, dass sie in fast jedem Baustein zitiert werden, andere aber wiederum so spezifisch, dass sie nur für einen Aspekt in einem einzelnen Baustein relevant sind. Dies erschwert die Behandlung und das Durcharbeiten sämtlicher Gefährdungen bei Risikoanalysen. Daher hat das BSI aus diesen Gefährdungen die generellen Aspekte herausgearbeitet und 46 elementare Gefährdungen erarbeitet.

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. Die elementaren Gefährdungen sollen die vorhandenen Gefährdungskataloge G 1 bis G 5 nicht ersetzen und werden daher in einem separaten Gefährdungskatalog G 0 zur Verfügung gestellt.

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, inwieweit alle drei Grundwerte betroffen sein könnten, weil sich auch indirekte Auswirkungen ableiten lassen.

So wird zum Beispiel zu „G 0.1 Feuer" als einziger betroffener Grundwert Verfügbarkeit genannt. Natürlich könnte ein Feuer auch dazu führen, dass Datenträger nur geringfügig beschädigt würden, sodass 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.

Elementare Gefährdungen und 100-3

Der BSI-Standard 100-3 [3] beschreibt eine Methodik, wie mithilfe der in den IT-Grundschutz-Katalogen [5] aufgeführten Gefährdungen eine vereinfachte Analyse von Risiken für die Informationsverarbeitung durchgeführt werden kann. Zunächst muss für eine Risikoanalyse eine Gefährdungsanalyse durchgeführt werden – Ausgangspunkt für eine Risikoanalyse basierend auf IT-Grundschutz sind dabei die relevanten Gefährdungen aus den IT-Grundschutz-Katalogen.

Bisher wurden dafür über die jeweils relevanten Bausteine aus den IT-Grundschutz-Katalogen die Gefährdungen aus den Katalogen G 1 bis G 5, die in den Bausteinen zitiert werden, in einer Liste zusammengetragen, die die Grundlage für die Ermittlung zusätzlicher Gefährdungen gebildet hat. Da die Gefährdungskataloge G 1 bis G 5 bereits jetzt umfangreich sind und mit der Erstellung neuer IT-Grundschutz-Bausteine weiter wachsen werden, gibt es bei dieser Vorgehensweise sehr viele verschiedene Gefährdungen, die in die Risikoanalyse eingehen. Mit den elementaren Gefährdungen aus dem neuen Katalog G 0 können nun nacheinander jedem betrachteten Zielobjekt die elementaren Gefährdungen zugeordnet werden, die für das jeweilige Zielobjekt prinzipiell zu einem nennenswerten Schaden führen können.

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, son-

dern 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". Das Ergebnis ist dann eine Tabelle, in der jedem Zielobjekt eine Liste mit relevanten elementaren Gefährdungen zugeordnet ist.

Tabelle 1: Übersicht über die elementaren Gefährdungen mit Zuordnung zu betroffenen Grundwerten der Informationssicherheit – 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 oder Produkte 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 und 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 oder Erpressung	C,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 (DoS)	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

Erstellung und Auswahl

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

- für die Verwendung bei der Risikoanalyse optimiert,
- grundsätzlich produktneutral,
- möglichst technikneutral (dabei ist zu berücksichtigen, dass bestimmte Technologie den Markt so stark prägt, dass sie auch die abstrahierten Gefährdungen beeinflusst),
- kompatibel mit vergleichbaren internationalen Katalogen,
- nahtlos in den IT-Grundschutz-Ansatz integriert.

Dabei sollte die Menge der elementaren Gefährdungen überschaubar bleiben, nach vielen Diskussionen mit internen und externen Experten hat sich die Anzahl der Gefährdungen bei 46 eingependelt. Dies ist eine Größenordnung, die einerseits die notwendige Differenzierung zwischen den unterschiedlichen Bedrohungen erlaubt und andererseits bei den Analysen überschaubar und beherrschbar bleibt.

Die Reduktion der Gefährdungen auf eine überschaubare Anzahl der wichtigsten Gefährdungen – so genannte elementare Gefährdungen – erfolgte unter Berücksichtigung internationaler Standards zur Risikoanalyse wie „Expression des Besoins et Identification des Objectifs de Sécurité" (EBIOS, [1]), dem Standard ISO/IEC 27005 zum Risikomanagement [7] und der

Information Risk Analysis Methodology" (IRAM) der nternationalen Vereinigung Information Security Forum ISF) [6].

Diese Standards wurden im BSI daraufhin gesich- et, inwieweit sie als Grundlage für die Risikoanalyse auf Basis von IT-Grundschutz genutzt werden könnten. Leider erfüllt keines dieser Werke alle Anforderungen, die zur Einbettung in die IT-Grundschutz-Vorgehensweise und vor allem die Risikoanalyse auf Basis von BSI-Standard 100-3 formuliert wurden. Dies erklärt sich natürlich auch dadurch, dass jede der betrachteten Gefährdungssammlungen für eine andere Form der Risikoanalyse und auch für ein anderes Zielpublikum entwickelt wurde.

Daher hat das BSI die Liste der bestehenden Gefährdungen aus den IT-Grundschutz-Katalogen analysiert und kategorisiert. Abschließend wurden die daraus resultierenden Gefährdungen mit denen der oben genannten internationalen Standards abgeglichen und auf Vollständigkeit geprüft.

Die Zwischenergebnisse waren eine Vielzahl von Tabellen zur Ein- und Zuordnung der IT-Grundschutz-Gefährdungen mit EBIOS, IRAM, ISO 27005 sowie zu den drei Grundwerten der Informationssicherheit, das heißt Vertraulichkeit, Integrität und Verfügbarkeit. Anschließend wurden basierend hierauf die vorhandenen Gefährdungen in ihrer Anzahl reduziert, verallgemeinert und angepasst. Schließlich wurde eine Liste von elementaren Gefährdungen erarbeitet, die einen neuen Gefährdungskatalog mit den 46 elementaren Gefährdungen G 0.1 bis G 0.46 ergeben.

Hintergründe und Erläuterungen

Bei den bereits geführten Diskussionen hat sich gezeigt, dass einige Aspekte rund um die Auswahl der elementaren Gefährdungen erläuterungsbedürftig sind. Dazu gehören beispielsweise die im Folgenden diskutierten Punkte.

Auch in dem jetzt vorliegenden reduzierten Gefährdungskatalog der elementaren Gefährdungen ist trotz aller Kürze eine gewisse Redundanz vorhanden. Eine völlige Redundanzfreiheit ist aus Sicht des BSI nicht zu erreichen, es sei denn, man würde sich auf die elementarsten Gefährdungen beschränken, also auf den Verlust der drei Grundwerte der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit. Dazu hat sich bei den verschiedenen Entwürfen auch gezeigt, dass weitere Reduktionen der Gefährdungen dazu führen, dass diese zu abstrakt werden und zu wenig substanziell und greifbar sind für Risikobewertungen und für Sensibilisierungsmaßnahmen.

Anwender haben häufig die Frage gestellt, warum bei den elementaren Gefährdungen aus ihrer Sicht bestimmte Aspekte fehlen. Tatsächlich waren mehrere Iterationsrunden notwendig, um den jetzt vorliegenden, abgerundeten Katalog elementarer Gefährdung zu konsolidieren. Die meisten der vermissten Aspekte fanden sich aber in anderen der elementaren Gefährdungen. Durch die Reduktion der elementaren Gefährdungen auf die wesentlichen Gefährdungen wurden natürlich auch die jeweiligen Beispiele und Details stark gekürzt.

Sicherheitsexperten haben die unterschiedlichsten Schwerpunkte und suchen typischerweise zunächst die in ihrem Bereich derzeit populären Gefährdungen. Die Diskussionen mit Experten mit unterschiedlichen Ausrichtungen haben gezeigt, dass die formulierten elementaren Gefährdungen eine angemessene und in typischen Szenarien vollständige Grundlage für Risikoanalysen bieten.

„Abwesenheit von Maßnahmen" als Gefährdung

Gefragt wurde bei Diskussionen aber auch immer wieder nach Gefährdungen, bei denen die Abwesenheit einer Sicherheitsmaßnahme im Vordergrund stand. Die bestehenden (bausteinspezifischen) Gefährdungen des IT-Grundschutzes dienen dazu, dem Leser einen Überblick über die typischen Sicherheitsprobleme, die sich im Kontext des jeweiligen Bausteins häufig ergeben, zu vermitteln. Entsprechend dem „Best Practice"-Ansatz des IT-Grundschutzes umfasst dies auch Gefährdungen, die zumindest vom Titel her keine tatsächliche Bedrohung darstellen, sondern die „Abwesenheit" einer gängigen Sicherheitsmaßnahme. Beispiele hierfür sind:

- G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung,
- G 2.49 Fehlende oder unzureichende Schulung der Telearbeiter,
- G 2.121 Unzureichende Kontrolle von WLANs,
- G 2.144 Unzureichende Notfall-Planung bei einem Samba-Server.

Keine dieser Überschriften beschreibt eine tatsächliche Bedrohung der Informationen, sondern in allen Fällen hebt die Überschrift auf die mangelhafte Umsetzung einer gängigen Sicherheitsmaßnahme ab. Für sich gesehen ist diese mangelhafte Umsetzung zunächst einmal kein Problem. Die Erfahrung zeigt jedoch, dass daraus in vielen Fällen tatsächliche Bedrohungen resultieren. Für die genannten Beispiele könnten die tatsächlichen Bedrohungen etwa wie folgt formuliert werden:

_____ Kompromittierung kryptografischer Schlüssel,

_____ Fehlbedienung oder Verstoß gegen Sicherheitsregelungen im Rahmen der Telearbeit,

_____ Sicherheitsmängel in der Konfiguration oder Nutzung von WLANs,

_____ Ausfall von File-Services.

Hier wird erneut deutlich, dass eine Maßnahme im Allgemeinen gegen mehrere Bedrohungen wirkt und dass umgekehrt eine Bedrohung in der Regel durch mehrere Maßnahmen adressiert werden muss. Um Gefährdungen nicht nur für die Motivation von Maßnahmen, sondern auch für Risikoanalysen nutzbar zu machen, ist es wichtig, dass die konkrete Gefahr, die sich für eine Institution ergibt, deutlich wird, möglichst schon in der Überschrift steht.

Literatur

[1] Agence nationale de la sécurité des systèmes d'information (ANSSI), EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité, Juli 2009, www.ssi.gouv.fr/site_article45.html

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

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

[4] BSI, Ergänzung zum BSI-Standard 100-3, Verwendung der elementaren Gefährdungen aus den IT-Grundschutz-Katalogen zur Durchführung von Risikoanalysen, www.bsi.bund.de/grundschutz/standards

[5] BSI, IT-Grundschutz-Kataloge, Stand 12. Ergänzungslieferung, www.bsi.bund.de/grundschutz/kataloge

[6] Information Security Forum (ISF), Information Risk Analysis Methodology, www.securityforum.org/services/publictools/publiciram/

[7] ISO/IEC 27005:2008, Information technology – Security techniques – Information security risk management, ISO/IEC JTC1/SC27, erhältlich über www.iso.org/iso/

Eine wesentliche Zielsetzung der elementaren Gefährdungen ist die effiziente Nutzbarkeit für Risikoanalysen. Im Rahmen der elementaren Gefährdungen sollen deshalb möglichst keine „Abwesenheiten von Maßnahmen", sondern nur tatsächliche Bedrohungen oder Schwachstellen aufgeführt werden – dies ist ein wesentlicher Unterschied zu den bestehenden (bausteinspezifischen) Gefährdungen.

Eine gewisse Ausnahme bildet allerdings „G 0.35 Imageschaden", deren Überschrift nahe legt, dass es sich hierbei nicht um eine Gefährdung, sondern um eine Schadensfolge handelt. In den Diskussionen hierzu hat sich die pragmatische Auffassung durchgesetzt, dass der mögliche Imageschaden für Risikoanalysen ein so wichtiger Aspekt ist, dass der kleine Schönheitsfehler in Kauf genommen werden kann.

Strukturierung des Gefährdungskataloges

In den Diskussionen wurde auch immer wieder überlegt, ob der Katalog mit den elementaren Gefährdungen durch Zwischenüberschriften untergliedert werden sollte. Dies hätte natürlich den Vorteil, schneller diejenigen Gefährdungen finden zu können, die für eine Risikobetrachtung als relevant herangezogen werden sollten. Andererseits ließen sich keine Gliederungskriterien finden, auf die sich alle Gefährdungen nahtlos hätten abbilden lassen.

In den Gefährdungslisten in den oben erwähnten Standards sind die Gefährdungen nach verschiedenen Kategorien gruppiert. Beispielsweise sind das bei IRAM „Externe Angriffe", „Interner Missbrauch", „Diebstahl", „Systemstörung", „Ausfall/Unterbrechung von Diensten", „Menschliche Fehler", „Unvorhergesehene Effekte von Änderungen". Etliche dieser Kategorien sind aber in sich nicht ausreichend trennscharf. Ist beispielsweise „R41 – System overload" eine Systemstörung, eine Dienst-Unterbrechung, ein menschlicher Fehler oder sogar ein Angriff (z. B. ein Denial-of-Service-Angriff)?

Bei ISO 27005 sind die Gefährdungen wie folgt kategorisiert: „Physical damage", „Natural events", „Loss of essential services", „Disturbance due to radiation", „Compromise of information", „Technical failures", „Unauthorised actions", „Compromise of functions", „Human Threats" – bei diesem Ansatz gehen allerdings Schadensquellen, Schadensursachen und Schadensarten durcheinander.

Bei der Erstellung der Gefährdungen hat sich das BSI an pragmatischen Schadensszenarien orientiert, nicht an den Schadensquellen, wie beispielsweise „Na-

Angriff". Auch eine durchgängige Orientierung an Schadensursachen oder Schadensarten ließ sich nicht umsetzen, wie zum Beispiel „Zerstörung von Komponenten", „Systemausfälle" oder „wirtschaftliche Verluste". Daher kommen Schadensquellen als Gliederungsstruktur nicht infrage (so wie beispielsweise bei EBIOS) und ebenso wenig Schadensursachen oder Schadensarten.

Ein anderer Ansatz wäre gewesen, zu hinterfragen, welcher Grundwert der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) durch die jeweilige Gefährdung beschädigt würde. Es lassen sich aber nicht alle Gefährdungen auf genau einen Grundwert abbilden, sondern verschiedene Gefährdungen betreffen mehrere Grundwerte. Daher wäre auch diese Vorgehensweise nicht sinnvoll gewesen.

Da sich trotz verschiedener Ansätze keine sinnvollen Gliederungskriterien identifizieren ließen, ist der neue Gefährdungskatalog G 0 der elementaren Gefährdungen wie auch die wesentlichen umfangreicheren Gefährdungskataloge G 1 bis G 5 *nicht* durch Zwischenüberschriften untergliedert. Eine flache Struktur erscheint sinnvoll und ist aus Sicht des BSI auch unproblematisch, da der Gefährdungskatalog G 0 nur 46 Gefährdungen enthält.

Fazit

In der 12. Ergänzungslieferung der IT-Grundschutz-Kataloge wird zusätzlich zu den Katalogen G 1 „Höhere Gewalt", G 2 „Organisatorische Mängel", G 3 „Menschliche Fehlhandlungen", G 4 „Technisches Versagen" und G 5 „Vorsätzliche Handlungen" ein weiterer Gefährdungskatalog G 0 „Elementare Gefährdungen" eingeführt. Außerdem wird zum BSI-Standard 100-3 eine Ergänzung zur Verwendung der elementaren Gefährdungen zur Durchführung von Risikoanalysen veröffentlicht.

Da die IT-Grundschutz-Gefährdungen in erster Linie als Motivation für die in den jeweiligen Bausteinen empfohlenen Sicherheitsmaßnahmen dienen, werden in den Bausteinen auch weiterhin die spezifischen Gefährdungen aus den Katalogen G 1 bis G 5 referenziert werden.

Kommentare zu Struktur und Inhalten der elementaren Gefährdungen sind ausdrücklich erwünscht, um die Praktikabilität und Anwendbarkeit dieses neuen Gefährdungskatalogs mit IT-Grundschutz-Anwendern diskutieren zu können (gerne auch per E-Mail an grundschutz@bsi.bund.de) ■

kurz notiert

Überblickspapier Smartphones

Das BSI hat Anfang September das „Überblickspapier Smartphones" veröffentlicht. Dieses erste IT-Grundschutz-Überblickspapier befasst sich mit typischen Gefährdungen der Informationssicherheit bei Smartphones sowie möglichen Gegenmaßnahmen. Mit den Überblickspapieren bietet das BSI ab sofort in loser Folge Lösungsansätze zu aktuellen Themen der Informationssicherheit, die zu einem späteren Zeitpunkt auch in den IT-Grundschutz eingearbeitet werden.

„An das BSI werden häufig Wünsche für IT-Grundschutz-Bausteine herangetragen, die aus verschiedenen Gründen nicht zeitnah realisierbar sind", erklärt Isabel Münch, Referatsleiterin für Grundlagen der Informationssicherheit und IT-Grundschutz im BSI. „Mit den Überblickspapieren bieten wir nun spezifische Sicherheitsempfehlungen zu aktuellen neuen Vorgehensweisen, Technologie oder Anwendungen, mit denen auf IT-Grundschutz basierende Sicherheitskonzepte schnell und flexibel erweitert werden können."

Zur Ermittlung der momentan in der Wirtschaft relevanten Themen hat das BSI im April 2011 eine Umfrage unter IT-Grundschutz-Anwendern durchgeführt – das mit Abstand wichtigste in der Umfrage genannte Thema war der sichere Umgang mit Smartphones.

Die verbreitete Nutzung macht Smartphones auch für Angreifer attraktiv und für das Informationssicherheitsmanagement zu einer Herausforderung – das neue Überblickspapier adressiert diese Herausforderungen und bietet konkrete Hilfestellungen für die sichere Nutzung von Smartphones im geschäftlichen und privaten Umfeld an.

Das Überblickspapier sowie weitere Informationen sind über www.bsi.bund.de/DE/Themen/ITGrundschutz/Ueberblickspapiere/Ueberblickspapiere_node.html abrufbar. Die nächsten IT-Grundschutz-Überblickspapiere werden sich voraussichtlich mit Netzzugangskontrollen, Skype sowie der Nutzung privater IT-Geräte im dienstlichen Umfeld beschäftigen. ■