M. Meier, D. Reinhardt, S. Wendzel (Hrsg.): Sicherheit 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 161

IT-Grundschutz in großen Institutionen – Herausforderungen und Lösungsstrategien

Timo Brecher[1], Sabine Kammerhofer[2], Severin Rast[3]

Abstract: Große Institutionen sind einerseits auf eine standardisierte Vorgehensweise für das Informationssicherheitsmanagement angewiesen, haben andererseits aber stets besondere Anforderungen, die vom Standard abweichen. Dies führt regelmäßig zu Herausforderungen bei der Anwendung des IT-Grundschutzes: Es gibt einen vielfältigen methodischen Kontext; der Informationsverbund ist sehr komplex; Projekte haben sehr lange Laufzeiten; es bestehen besondere betriebliche Anforderungen und oft die Notwendigkeit eigene Bausteine zu definieren. Dieser Artikel betrachtet diese Herausforderungen und stellt geeignete Lösungsansätze vor.

Keywords: Modellierung und Verifikation von Sicherheit, Sicherheitsmanagement, IT-Grundschutz, IT-Sicherheitskonzeption

1 Einleitung

Große Behörden und Unternehmen haben besondere Anforderungen an Planung, Realisierung und Betrieb zeitgemäßer und wirtschaftlicher IT-Systeme. Sicherheit ist hierbei ein wesentlicher Aspekt, der jedoch nie allein, sondern stets eingebettet in die Gesamtheit der Prozesse und Aktivitäten der Institution zu betrachten ist. Der IT-Grundschutz bietet hierzu eine bewährte Methodik und solide Maßnahmenkataloge, bringt jedoch in Anwendungsfällen abseits des idealen Informationsverbundes seine eigenen Herausforderungen mit.

2 Herausforderungen bei der Anwendung des IT-Grundschutzes in großen Institutionen

Im Rahmen der Anwendung der IT-Grundschutz-Methodik in verschiedenen großen Institutionen ließ sich eine Reihe von Problemstellungen identifizieren, die regelmäßig zu bewältigen sind. In den nachfolgenden Abschnitten werden fünf wesentliche Herausforderungen näher betrachtet.

[1] Infodas GmbH, IT Security, Rhonestr. 2, 50765 Köln, t.brecher@infodas.de
[2] Infodas GmbH, IT Security, Rhonestr. 2, 50765 Köln, s.kammerhofer@infodas.de
[3] Infodas GmbH, IT Security, Rhonestr. 2, 50765 Köln, s.rast@infodas.de

2.1 IT-Grundschutz im Kontext der IT-Governance

Der mit der IT-Grundschutz-Vorgehensweise beschriebene Anwendungsansatz für die Etablierung und Aufrechterhaltung eines Managementsystems für Informationssicherheit und Erstellung von IT-Sicherheitskonzepten ist vollständig kompatibel zum internationalen Standard ISO/IEC 27001 und ist gut auf den Einsatz in Behörden und Unternehmen ausgerichtet. Die IT-Grundschutz-Kataloge sind seit Jahren praxiserprobt und ermöglichen eine effiziente Auswahl der relevanten IT-Sicherheitsmaßnahmen. In großen Institutionen entstehen bei der Einführung des IT-Grundschutzes allerdings stets Wechselwirkungen mit anderen Standards und Vorschriften. Neben internen Vorschriften zur IT-Sicherheit[4], können dies zum einen interne und externe Anforderungen und Standards aus den Bereichen Datenschutz[5], Geheimschutz[6], Risikomanagement[7] sein; zum anderen spielen Architekturmodelle[8] und Best Practise Frameworks[9] in der modernen IT-Governance eine immer größere Rolle. Dies führt zu einer Vielfalt an unterschiedlichen Betrachtungsweisen für die in einer Institution eingesetzte IT, die jeweils mit eigenen Begriffsdefinitionen und analytischen Strukturen einhergehen. Für ein funktionierendes ISMS und ein wirksames IT-Sicherheitskonzept ist ein einheitliches institutionsübergreifendes Verständnis des Informationsverbundes und der zu seiner Realisierung genutzten IT jedoch eine wesentliche Voraussetzung. Im Rahmen einer transparenten IT-Sicherheitskonzeption müssen daher die für eine Institution relevanten Betrachtungsweisen für alle Zielgruppen nachvollziehbar miteinander in Beziehung gesetzt werden.

2.2 IT-Sicherheitskonzeption für komplexe Informationsverbünde

Die in der Keynote zum BSI-Kongress präsentierte Bestandsaufnahme zeigt, dass die IT der unmittelbaren Bundesverwaltung Ende 2013 mit ihren knapp 200 Behörden auf über 1.300 Rechenzentren und Serverräume an unzähligen Standorten verteilt ist [MAIZ]. Bei großen Bundesbehörden besteht somit häufig das Problem, dass der zu betrachtende Anwendungsbereich bzw. Informationsverbund zu umfangreich und zu komplex ist, um diesen über ein einzelnes IT-Sicherheitskonzept adäquat abdecken zu können. Dies führt zu einer Unterteilung des Informationsverbundes in einzelne Teilbereiche. Die wesentlichen Herausforderungen stellen hier die unterschiedlichen Modellierungsmöglichkeiten sowie der Umgang mit Redundanzen (z.B. gleiche Maßnahmen in gleichen Bausteinen unterschiedlicher Teilbereiche), die in weiterer Folge zu Konsistenzproblemen führen können.

Der Maßnahmenkatalog des IT-Grundschutzes wurde mit der Zielsetzung erstellt,

[4] Z.B. [ZDv 54/100]
[5] Z.B. [BDSG] oder [EU Rl]
[6] Z.B. [VSA] oder [GSH]
[7] Z.B. [MaRisk] oder [ISO31000]
[8] Z.B. [IETF] oder [SOA]
[9] Z.B. [ITIL] oder [COBIT]

Informationsverbünde von Unternehmen und Behörden als Ganzes zuverlässig zu schützen. Dabei werden die organisatorischen, technischen, personellen und infrastrukturellen Aspekte untersucht.

Beispiel: Mit Einführung des IT-Grundschutzes als Methodik für die Erstellung von IT-Sicherheitskonzepten in der Bundeswehr muss die Verzahnung von projektbezogenen IT-Sicherheitskonzepten und dienststellenbezogenen IT-Sicherheitskonzepten[10] grundlegend neu überdacht werden. Eine Unterscheidung zwischen Maßnahmen, die in der Verantwortung einer Dienststelle und Maßnahmen, die in Verantwortung des Projekts liegen, ist nicht vorgesehen. Diese Unterscheidung muss der Ersteller eines bundeswehrspezifischen IT-Sicherheitskonzepts vornehmen.

2.3 Besonderheiten bei langen Projektlaufzeiten

Ein weiteres Problem bei der Anwendung des IT-Grundschutzes auf Projekte in großen Institutionen stellt die oftmals lange Projektlaufzeit dar. Bei einer Projektlaufzeit von mehreren Jahren sind Dienstpostenwechsel, z.B. beim IT-Sicherheitsbeauftragten, keine Seltenheit, so dass im Anschluss eine Einarbeitungs- und Übergabezeit stattfinden muss, um einen gänzlichen Knowhow-Verlust zu vermeiden.

Lange Projektzeiten sind auch ein Problem, wenn sich in diesem Zeitraum Vorschriften- und Weisungslagen ändern. Wenn die Vertragsgestaltung diesen Aspekt nicht berücksichtigt, ergeben sich erhebliche Probleme bei der Zusammenarbeit mit den Herstellern/Dienstleistern. Falls durch die Änderung der Vorschriften- und Weisungslagen Mehraufwände entstehen, sind die Hersteller/Dienstleister in der Regel nicht in der Lage die IT-Sicherheitsmaßnahmen gemäß IT-Sicherheitskonzept kostenneutral umzusetzen, so dass vertragliche Änderungen notwendig werden, die zeitaufwendiges Änderungsmanagement und zusätzliche Nachweisführung erfordern.

Beispiel: Durch eine behördenspezifische Vorschriftenänderung kann ein System nur mit einem vorschriftenkonformen Patchmanagement abgenommen werden. Diese Anforderung wurde zwar von der Behörde im Lastenheft dokumentiert, ohne jedoch die zum Zeitpunkt des Vertragsschlusses noch nicht vorliegenden behördenspezifischen Anforderungen zu berücksichtigen. Eine Abnahme kann in diesem Fall nur erfolgen, wenn der Vertrag entsprechend angepasst wird, was oft zu erheblichen Mehrkosten führt.

2.4 Besondere betriebliche Anforderungen

Der IT-Grundschutz ist für die Anwendbarkeit sowohl auf Büro- als auch auf Rechenzentrumsumgebungen ausgelegt. Falls von der Institution an ein IT-System

[10] Im dienstellenbezogenen IT-Sicherheitskonzept wird der gesamte Informationsverbund der Dienststelle mit den darin genutzten bzw. betriebenen Projekten betrachtet.

besondere betriebliche Anforderungen gestellt werden, führt diese Pauschalisierung des IT-Grundschutzes zu Problemen, wenn die Umsetzung von IT-Sicherheitsmaßnahmen den besonderen betrieblichen Anforderungen widerspricht. Eine Entbehrlichkeit der IT-Sicherheitsmaßnahme kann nicht begründet werden. Damit ist eine Risikobewertung erforderlich.

Beispiel: Ein für den operativen Betrieb wichtiges Computersystem in der Brückenkonsole an Bord eines Schiffes soll die IT-Grundschutzmaßnahme M 4.2 – Bildschirmsperre [GSK] umsetzen. In dieser Maßnahme wird gefordert, dass der Zeitraum, nach dem sich eine Bildschirmsperre wegen fehlender Benutzereingaben aktiviert, gewisse Grenzen weder unter- noch überschreiten sollte. Die Umsetzung dieser Maßnahme ist jedoch in dieser spezifischen Einsatzumgebung nicht möglich, da der Blick auf die Konsolenanzeige niemals versperrt sein darf, um kurzfristig auf navigatorische Anweisungen reagieren zu können.

2.5 Erweiterung des IT-Grundschutzes durch zusätzliche Bausteine

„Die IT-Grundschutz-Kataloge enthalten die Gefährdungslage und die Maßnahmenempfehlungen für verschiedene Komponenten, Vorgehensweisen und IT-Systeme, die jeweils in einem Baustein zusammengefasst werden“ [100-2, S. 60]. Der Fortschritt der technischen Entwicklung einerseits und die besonderen Anforderungen großer Behörden und Unternehmen an ihre IT andererseits führen dazu, dass nicht für alle eingesetzten Hard- und Softwarekomponenten oder übergreifende Aspekte passende Bausteine in den IT-Grundschutz-Katalogen vorliegen. Insbesondere in den Bereichen von Appliances und Embedded Systems, neuen Softwareversionen mit deutlich erweitertem Funktionsumfang[11] oder auch besonderem Schutzbedarf ist die Erstellung neuer Bausteine notwendig[12]. Dies führt zu einer Erhöhung des Aufwands für die Erstellung des IT-Sicherheitskonzepts und zu Unsicherheiten in der Planung des IT-Sicherheitsmanagements, etwa bei Ergänzungslieferungen des IT-Grundschutzes, in denen offizielle Bausteine eingeführt werden, die selbst erstellte ersetzen. Ein strategisch und langfristig ausgerichtetes ISMS braucht daher Prozesse zur effizienten Erstellung und zum Management selbsterstellter Bausteine.

3 Lösungsstrategien

Zu den im vorherigen Abschnitt beschriebenen Herausforderungen werden nachfolgend Lösungsstrategien vorgestellt, die basierend auf praktischen Erfahrungen eine universelle Anwendung finden können.

[11] Z.B. beim Umstieg von Windows 7 auf Windows 8/8.1

[12] Eine Vorgehensweise hierzu ist in der unveröffentlichten BSI-Richtlinie "Erstellung eines Bausteins für die IT Grundschutz Kataloge" beschrieben.

3.1 Abbildung des IT-Grundschutzes auf weitere Frameworks und Modelle

Gültige Vorschriftenlage, Governance-Frameworks und der IT-Grundschutz betrachten den Informationsverbund aus sehr unterschiedlichen Perspektiven. Diese transparent aufeinander abzubilden bzw. miteinander in Beziehung zu setzen und ein einheitliches Verständnis dieser Beziehungen über den gesamten ISMS-Prozess zu gewährleisten, ist ein Schlüssel für die institutionsübergreifende Wirksamkeit eines ISMS. Hierzu hat es sich bewährt, frühzeitig ein institutionsspezifisches Modell zu entwickeln und dieses in der gesamten IT-Sicherheitsdokumentation konsistent anzuwenden. Die folgende Abbildung stellt ein vereinfachtes Beispiel für ein solches Modell dar.

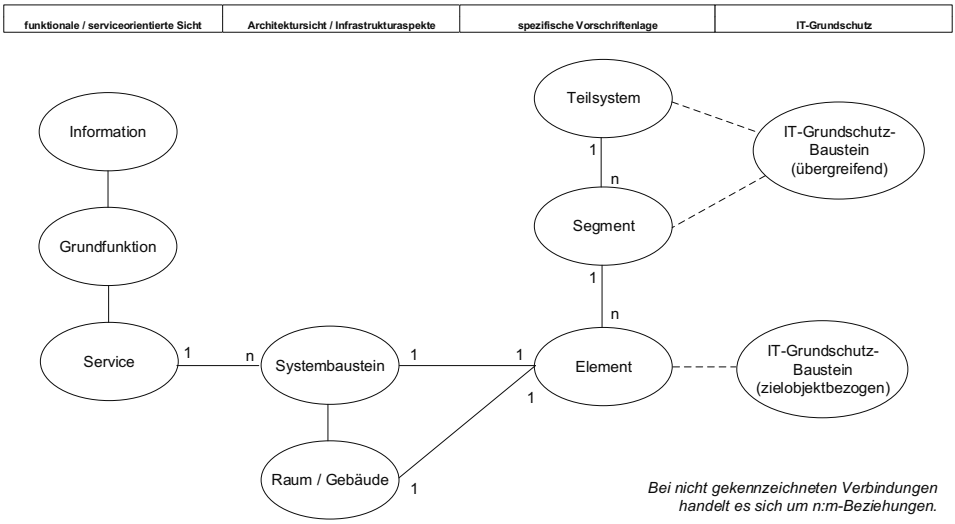

Abbildung 1: Abbildung unterschiedlicher Sichten auf den IT-Grundschutz

In der funktionalen Sicht eines serviceorientierten Frameworks werden die Services als grundlegende Elemente der Betrachtung identifiziert. Diese lassen sich Systembausteinen einer Architektursicht zuordnen, die wiederum als Elemente gemäß der spezifischen Vorschriftenlage der Institution[13] betrachtet werden. Diese Elemente werden als Zielobjekte mit IT-Grundschutz-Bausteinen der Schichten zwei bis fünf im IT-Sicherheitskonzept modelliert, während übergeordneten Struktureinheiten (Teilsysteme und Segmente) die IT-Grundschutz-Bausteine der Schicht eins zugeordnet werden.

[13] In diesem Beispiel [ZDv]

3.2 Modularisierung einer IT-Sicherheitskonzeption

Bei sehr umfangreichen und komplexen Institutionen hat sich im Rahmen der IT-Sicherheitskonzepterstellung ein modularer und schichtenorientierter Aufbau bewährt. Ziel der Modularisierung ist die redundanzfreie Zusammenfassung typischer Zielobjekte und ihrer korrespondierenden IT-Grundschutz-Bausteine bzw. sonstiger institutionsspezifischer Bausteine zu wiederverwendbaren, standardisierten Modulen des übergreifenden IT-Sicherheitskonzepts. Diese können bei der Erstellung von IT-Sicherheitskonzepten für konkrete Teilbereiche nach Bedarf genutzt werden.

Im Rahmen der Erstellung der übergeordneten IT-Sicherheitskonzeption werden neben den Modulen auch die organisatorischen Aspekte (insbesondere Schicht 1 und 2 der IT-Grundschutz-Kataloge des BSI) beschrieben. Untergeordnet werden verfahrens- und systembezogene IT-Sicherheitskonzepte erstellt, welche sich im Wesentlichen auf die Bausteine der Schichten 3 bis 5 beziehen und die bereits im übergreifenden IT-Sicherheitskonzept behandelten Themen größtenteils durch Verweise abdecken können.

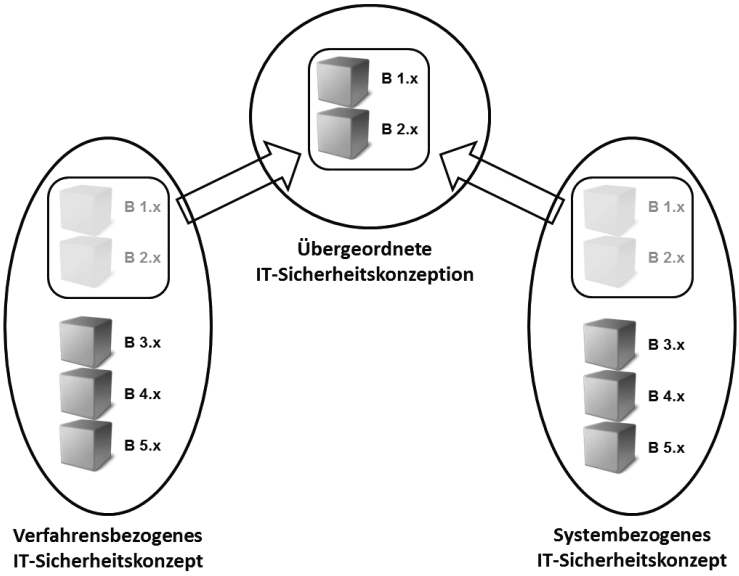

Abbildung 2: Referenzen von Modulen auf eine übergeordnete IT-Sicherheitskonzeption

Der modulare Aufbau der IT-Sicherheitskonzeption bietet die folgenden Vorteile:

- Wenn sowohl die Systemarchitektur als auch die IT-Sicherheitskonzepte modular strukturiert sind, können die System-Komponenten und -Bausteine auf einfache Weise den Modulen der IT-Sicherheitskonzepte zugeordnet werden (siehe auch Abschnitt 3.1).

- Bei neuen IT-Verfahren ist eine erneute Sicherheitsanalyse der schon bekannten und untersuchten Systemanteile in der Regel entbehrlich. Damit ist es ausreichend, nur noch die neu hinzukommenden Zielobjekte sicherheitstechnisch zu betrachten.

- Aufgrund des modularen Aufbaus der IT-Sicherheitskonzeption können Redundanzen in davon abgeleiteten Richtlinien und Anweisungen vermieden werden. So wird nicht nur die Erstellung der IT-Sicherheitskonzepte erleichtert, sondern insbesondere auch deren Fortschreibung vereinfacht, da Änderungen nur zentral notwendig sind und folglich auch Inkonsistenzen vorgebeugt wird.

- Durch den modularen Aufbau wird außerdem die Handhabbarkeit der IT-Sicherheitskonzepte wesentlich verbessert, da immer nur die jeweils relevanten Module der IT-Sicherheitskonzepte betrachtet werden müssen. Die hiermit verbundene klare Abgrenzung der Einzelaspekte erleichtert nicht nur die Abgrenzung von Zuständigkeiten bei der Bearbeitung, sondern auch die Durchführung von IT-Sicherheitsaudits.

3.3 Berücksichtigung von personellen und vertraglichen Änderungen

Bei langen Projektlaufzeiten ist ein funktionierendes Wissensmanagement bei Dienstpostenwechseln vorzusehen. Hierzu sind, neben dem Führen einer vollständigen Dokumentation, Stellvertreter von Schlüsselpersonal der IT-Sicherheit zu ernennen und von Beginn an in die Projektarbeit einzubinden, so dass bei Ausfall oder Wechsel von Personal die Aufgaben ohne eine lange Einarbeitungszeit übernommen werden können.

Bei der Planung von komplexen Realisierungsprojekten, bei denen Umsetzung von IT-Sicherheitsmaßnahmen gefordert ist, ist darauf zu achten, bereits bei Kalkulation und Vertragsgestaltung zukünftige Änderungen der Vorschriften- und Weisungslage zu berücksichtigen. Dafür hat sich eine den Baufortschritt begleitende und idealerweise vom realisierenden Auftragnehmer bzw. der realisierenden Stelle unabhängige Beratung durch Fachpersonal bewährt, die bereits in der Planungsphase beginnt. So können zukünftige Änderungen der Vorschriften- und Weisungslage, die Auswirkungen auf Anforderungen der IT-Sicherheit haben, kurzfristig berücksichtigt werden, um einen zeitgerechten Abschluss des Projektes nicht zu gefährden.

3.4 Strukturiertes Vorgehen bei Zielobjekten mit besonderen betrieblichen Anforderungen

Einen bewährten Ansatz stellt die Kombination aus standardisierter Risikoanalyse und -behandlung sowie bedarfsgerechter Erstellung zusätzlicher Maßnahmen bzw. Bausteine dar.

Wenn bei einem betrachteten Zielobjekt besondere betriebliche Anforderungen bestehen, ist das Zusammenspiel von technischen, infrastrukturellen, personellen und organisatorischen IT-Sicherheitsmaßnahmen neu zu bewerten. Diese Bewertung wird im Rahmen einer standardisierten Risikoanalyse dokumentiert und kann bei Betrachtung von gleichartigen Zielobjekten oder Szenarien wiederverwendet werden.

Führt das Ergebnis der Risikoanalyse dazu, dass die Gefährdungen nicht ausreichend durch die vorliegende Kombination von IT-Sicherheitsmaßnahmen abgedeckt sind, müssen zusätzliche Maßnahmen bzw. Bausteine erstellt werden. Gleiches gilt für Zielobjekte, bei denen besondere betriebliche Anforderungen dazu führen, dass sie nicht mit Standard-Bausteinen des IT-Grundschutzes modelliert werden können.

3.5 Managementkonzept für zusätzliche IT-Grundschutz-Bausteine

Die Entwicklung von zusätzlichen IT-Grundschutz-Bausteinen ist oft der einzige Weg, um spezifische Systeme des Informationsverbunds in der Modellierung abzubilden und relevante IT-Sicherheitsmaßnahmen zu identifizieren. Um den dabei entstehenden Aufwand nachhaltig zu reduzieren, hat sich die frühzeitige Entwicklung und Anwendung eines Managementkonzepts für die eigene Institution bewährt. Ein solches Konzept sollte folgende Aspekte betrachten und entsprechende verbindliche Vorgaben für die Umsetzung innerhalb der IT-Sicherheitskonzeption der Institution vorgeben:

- Zu berücksichtigende Vorschriftenlage
- Begründende Ausgangslage für die Modifikation bestehender Bausteine oder die Neuentwicklung von Bausteinen
- Vorgaben zur Anwendung den IT-Grundschutz-Katalogen vorliegender IT-Sicherheitsmaßnahmen
- Begründende Ausgangslage für die Modifikation oder Neuentwicklung von IT-Sicherheitsmaßnahmen
- Prüfverfahren und Qualitätssicherung
- Richtlinien zur Dokumentation und Veröffentlichung neuer Bausteine innerhalb der eigenen Institution
- Pflege und kontinuierliche Verbesserung der Bausteine über den gesamten Lebenszyklus

Diese Aufzählung deckt die notwendigen Mindestinhalte eines Managementkonzeptes zur Entwicklung von Bausteinen ab und ist institutionsspezifisch anzupassen.

4 Zusammenfassung und Ausblick

Um den Herausforderungen bei der zeitgemäßen Anwendung des IT-Grundschutzes in großen Institutionen zu begegnen, hat sich eine Vielzahl unterschiedlicher Lösungsansätze bewährt. Oft ist es nicht nur eine, sondern eine Kombination mehrerer Herausforderungen, die durch das ISMS einer großen Institution bewältigt werden muss. Daher ist eine enge Verzahnung dieser Lösungsansätze Grundlage für effizientes IT-Sicherheitsmanagement.

Die Abbildung des IT-Grundschutzes auf weitere Frameworks und Modelle kann eine solide Grundlage bilden, um die IT-Grundschutz-Methodik in die komplexen Prozesse und Betrachtungsweisen einer großen Institution einzubinden. Hierauf aufbauend fördern modulare Ansätze die Effizienz und Flexibilität der IT-Sicherheitskonzeption und die kontinuierliche Aufrechterhaltung des IT-Sicherheitsprozesses. Sind lange Projektlaufzeiten abzusehen, insbesondere bei der Planung und Realisierung neuer Systemanteile, sind Maßnahmen zum Erhalt von Wissen bei beteiligtem Personal und vertraglicher Anpassungsbedarf bei Änderungen in der Vorschriftenlage frühzeitig einzuplanen. Werden Zielobjekte mit besonderen betrieblichen Anforderungen identifiziert, bietet eine wiederverwendbare Risikoanalyse die Möglichkeit, Besonderheiten des Systems gezielt zu betrachten und effizient in eine modulare IT-Sicherheitskonzeption zu überführen. Besteht die Notwendigkeit für einzelne Zielobjekte zusätzliche Bausteine zu entwickeln, sollte das entsprechende Vorgehen einem Managementkonzept folgen, um Redundanzen zu vermeiden und Wiederverwendbarkeit zu optimieren. Ein solches Managementkonzept kann dann in den übergreifenden Anteil der IT-Sicherheitskonzeption der Institution aufgenommen werden.

In Zukunft wird der modulare Ansatz durch die Modernisierung des IT-Grundschutzes, insbesondere durch die Auswahl der Vorgehensweise, noch weiter unterstützt. Der modernisierte IT-Grundschutz wird verschiedene Methodiken anbieten, die sich an unterschiedliche Anwendergruppen richten und unterschiedliche Ziele verfolgen. „Beispielsweise kann sich eine Institution als Ziel setzen, zunächst möglichst flächendeckend alle Basis-Anforderungen umzusetzen ("Basisabsicherung"), um schnellstmöglich die größten Risiken zu senken, bevor die tatsächlichen Sicherheitsanforderungen im Detail analysiert werden. Ein anderer denkbarer Ansatz ist, sich zunächst auf den Schutz der essenziellen Werte der Institution („Kernabsicherung“) zu konzentrieren“ [MOD GS]. Für die IT-Sicherheitskonzepterstellung in komplexen Institutionen bietet sich somit eine Mischform aus diesen neuen Vorgehensweisen an. Die institutionsweite Basisabsicherung wird durch das übergreifende IT-Sicherheitskonzept gewährleistet und die verfahrensbezogenen oder systembezogenen IT-Sicherheitskonzepte stellen die Kernabsicherung des Informationsverbundes sicher.

Einen weiteren Vorteil für die IT-Sicherheitskonzeption in komplexen Institutionen bietet die Modernisierung des IT-Grundschutzes im Bereich der IT-Grundschutz-Profile. „Die modernisierten IT-Grundschutz-Profile sind als Schablonen zu verstehen, mit

denen verschiedene Anwender(-gruppen) selbstständig den IT-Grundschutz auf ihre Bedürfnisse anpassen können“ [MOD GS]. Hier ist denkbar, dass komplexe Behörden oder Unternehmen zentral definieren, welche Profile in welchem Teil des Informationsverbundes bzw. Modul der IT-Sicherheitskonzeption zur Anwendung kommen.

Literaturverzeichnis

[100-2] BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise, Version 2.0. BSI, 2008.

[BDSG] Bundesdatenschutzgesetz. Juris, 25.2.2015.

[COBIT] COBIT 5, Framework for IT Governance, Risk, Security and Auditing. ISACA, 2013.

[EU Rl] EU Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation). 2002.

[GSH] Geheimschutzhandbuch. 08.09.2014, BMWi.

[GSK] IT-Grundschutz-Kataloge des BSI, 14. Ergänzungslieferung. BSI, 2014.

[IETF] B. Khasnabish; e.a. IETF Cloud Reference Framework. 2011.

[ISO31000] ISO/IEC 31000 Standard, Risk Management. International Organization for Standardization, 2009.

[ITIL] IT Infrastructure Library. Axelos, 2013.

[MAIZ] Dr. Thomas de Maizière. Keynote zum BSI-Kongress 2015. www.bmi.bund.de/SharedDocs/Reden/DE/2015/05/ministerrede-bsi-kongress.html. BMI, 2015.

[MaRisk] Mindestanforderungen an das Risikomanagement, Rundschreiben 10/2012 (BA). BaFin, 2012.

[MOD GS] www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/Kernpunkte/itgrundschutz_kernpunkte_node.html. BSI, 2015

[SOA] Ali Arsanjani; e.a. The SOA Manifesto. soa-manifesto.org/. 2013.

[VSA] Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung). GBMI, 26.04.2010.

[ZDv] Zentrale Dienstvorschrift (ZDv) 54/100, IT-Sicherheit in der Bundeswehr. Bundeswehr, April 2013.