Besonderheiten bei der Anwendung der IT-Grundschutz Methodik bei einem Telekommunikationsdienstleister

Wolfgang Böhmer[1] · Thomas Milde[2]

[1]Technische Universität Darmstadt
wboehmer@cdc.informatik.tu-darmstadt.de

[2]T-Systems International GmbH – TC Division
thomas.milde@telekom.de

Zusammenfassung

Im Bereich der Unternehmensabsicherung (Enterprise Security) haben sich Management Systeme gemäß dem Deming Zyklus (PDCA-Zyklus) etabliert. Zu nennen sind das ISMS (Information Security Management System) der ISO/IEC 27001:year [SC213]. Allerdings hat sich in Deutschland im öffentlichen Sektor der BSI Standard 100-2 bzw. die Zertifizierung nach *ISO 27001 auf Basis von IT-Grundschutz* des BSI (Bonn) durchgesetzt. Die Grundschutz Methodik, die in dem BSI Standard 100-2 [fSidIB08a] beschrieben ist, geht immer von einer Institution oder Behörde aus, die für sich genommen eine Einheit bildet. Diese Situation liegt bei einem Telekommunikationsdienstleister oder einer anderen großen Institution in Deutschland allerdings nicht vor. Zudem betreiben letztere, aus dem Zwang zum wirtschaftlichen, erfolgreichen Handeln, üblicherweise ihr ISMS prozessorientiert entlang der Wertschöpfungsketten und deutlich seltener technologiebezogen. Somit stellt sich die Frage, wie die Abgrenzung des Informationsverbundes (IV) in diesem Fall vorzunehmen ist. Anhand eines Beispiels für einen Informationsverbund, der seit 2015 zertifiziert ist, wird in diesem Beitrag eine praxisbewährte und zertifizierungskonforme Lösung vorgestellt, die für große Institutionen richtungsweisend sein kann.

1 Einführung

Im öffentlichen Sektor, beispielsweise in den Körperschaften des öffentlichen Rechts, hat sich die BSI Norm *ISO 27001 auf Basis von IT-Grundschutz* in den letzten Dekaden durchgesetzt. Dabei zeichnen sich die ISO/IEC 27001:year[1] (nativ) und die *ISO 27001 auf Basis von IT-Grundschutz* durch eine enge Verwandtschaft aus. Gleichermaßen gibt es gravierende Unterschiede[2] auf die in diesem Beitrag nicht eingegangen wird.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert im BSI Standard 100-

[1] Korrekt wird die ISO/IEC 27001 immer mit einer Jahres Bezeichnung angegeben. Die Fassung aus dem Jahr 2005, also ISO/IEC 2700:2005 [SC205], läuft in wenigen Monaten aus und aktuell ist die Fassung ISO/IEC 27001:2013. Um hier auf die internationale Norm ISO/IEC 27001 hinzuweisen, wird hier das Kürzel :year angehängt.

[2] Eine der herausragenden Unterschiede liegt in der Art und Weise wie eine Risikoanalyse durchgeführt wird. Denn es wird auf die Betrachtung der Eintrittswahrscheinlichkeit eines Risikoszenarios (vgl. BSI 100-3, [fSidIB08b]) verzichtet und mit Gefährdungen gearbeitet.

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 276-287.

2 [fSidIB08a] die Definition und Abgrenzung eines Informationsverbundes (IV). Definition und Abgrenzung eines IV sind bei einer Zertifizierung nach *ISO 27001 auf der Basis von IT-Grundschutz* eine zwingende Voraussetzung für die Antragstellung zur Zertifizierung. Ein IV definiert mit seiner Abgrenzung den Geltungsbereich (Scope) für den Untersuchungsgegenstand der Zertifizierung und gibt u.a. den Rahmen für die Sicherheitskonzeption und insbesondere die zu betrachtenden Zielobjekte, so z.B. für die IT Strukturanalyse, Modellierung, Basissicherheitscheck etc. vor. Graphisch wird ein IV durch den bereinigten Netzplan dargestellt.

Gemäß der Begriffsdefinition der IT-Grundschutzkataloge des BSI ist ein IV mit folgenden Eigenschaften definiert:
Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.
Ein Informationsverbund kann die gesamte Informationsverarbeitung einer Institution oder auch einzelne Bereiche umfassen. (vgl. [fSidIB08a] Kapitel 4.1, Seite 38). Demzufolge muss die Abgrenzung eines IV durch die oben aufgeführten Eigenschaften definiert werden und ebenso die Schnittstellen zu diesen aufgeführten Eigenschaften, wenn es sich um Bereiche einer Institution handelt.

In diesem Beitrag wird untersucht, wie die Anforderungen an einen Informationsverbund (IV) gemäß BSI Standard 100-2 in einem Großkonzern (Telekommunikationsdienstleister) für einen einzelnen Bereich erfüllt werden können. Gleichwohl werden typische Zielobjekte, wie z.B. eMail bzw. Exchange Server, TK-Anlage, Patch-Server, Personalverwaltung, Gebäudeverwaltung etc. nicht dem Informationsverbund zugeordnet, obwohl sie – nach Auslegung des Standards – zugeordnet werden müssten.

Die Schwierigkeit für den Telekommunikationsdienstleister liegt darin begründet, dass z.B. nicht nur ein Exchange Server verwendet wird, sondern eine Anzahl > 50 über das ganze Land (Europa) verteilt sind. Würden diese Exchange Server mit in den Informationsverbund hineingenommen werden, wie der BSI Standard 100-2 und die auf die IT-Strukturanalyse aufbauende Modellierung nahe legt, wäre durch dieses Konstrukt ein Großteil der gesamten Infrastruktur und Technik des Telekommunikationsdienstleisters mit in dem IV hinzugezogen worden. Somit stellt sich die Frage, in wieweit und nach welchem Prinzip in einem solchen Fall ein sinnvoll abgegrenzter IV, der konform zum BSI Standard 100-2 ist, definiert werden kann. Die BSI Standards 100-1/2/3/4 liefern zu dieser Fragestellung keine Antwort.

Dieser Beitrag ist in sechs Abschnitte unterteilt. Im zweiten Abschnitt wird ein kurzer Überblick über die relevante Literatur gegeben und im Anschluss, im Abschnitt drei, der einen Schwerpunkt des Artikels darstellt wird die Forschungsfrage diskutiert und eine Lösung gemäß dem Prinzip der Beherrschung präsentiert. Das Beherrschungsprinzip ist der Regelsatz nach dem eine Sortierung bzw. Unterscheidung vorgenommen wird. Der Abschnitt vier stellt den zweiten Schwerpunkt des Artikels dar, in dem die risikoorientierte Schnittstellenbetrachtung auf Grund der Schnittmengen diskutiert wird. Insbesondere werden die Schnittstellen diskutiert, die sich zwischen dem Konzern, den Kunden und dem Informationsverbund ergeben. Im Abschnitt fünf wird auf die richtungsweisende Betrachtung eines solchen Informationsverbundes für Großkonzerne eingegangen und im letzten Abschnitt folgt eine kurze Zusammenfassung der wesentlichen Ergebnisse. Mit einem Ausblick auf weiterführende Untersuchungen schließt der Beitrag.

2 Literaturüberblick

Management Systeme deren Bedeutung und gerade Informations-Sicherheitsmanagement-Systeme (ISMS) sind in der Literatur unter vielfältigen Aspekten diskutiert worden. Angefangen von praktischen Aspekten einer Implementierung [Bea11] bis hin zu theoretischen Aspekten und Überlegungen ob ein ISMS z.B. einer Zielfunktion folgt, wie in dem Artikel von [Boe10b] untersucht wird. Ein weiterer Aspekt sind Fragestellungen zur Wirkung bzw. Arbeitsweise von Management Systemen, die nach dem Artikel von [Boe10a] wie ein Balance-System zwischen den Phasen Plan/Do und Check/Act agieren oder mittels Schlüsselindikator die Effektivität bestimmen [Rum16]. Dagegen gibt es wenige Artikel, die sich mit dem Geltungsbereich seiner Bedeutung und dessen Abgrenzung bezogen auf ein ISMS bzw. einen Informationsverbund mit Blick auf die Risiken beschäftigen. Zwar stellt das BSI auf seiner Webpage unter der Rubrik Hilfsmittel sogenannte Beispiele für Profile für kleine Institutionen, für den Mittelstand und einer großen Institution bereit; doch auch in dem zuletzt genannten Profil ist im Kapitel 3 zum Thema Definition und Abgrenzung des IT-Verbundes kein Hinweis zu der vorliegenden Fragestellung zu finden [fSidIB04].

3 IV Abgrenzung durch Beherrschung

Ein Informationsverbund kann die gesamte Informationsverarbeitung einer Institution oder auch einzelner Bereiche umfassen, vgl. [fSidIB08a] Kapitel 4.1, Seite 38. Diese Aussage gilt ebenso für die ISO/IEC 27001:year (nativ), wie z.B. bei [Bea11, SC213] zu entnehmen ist.

Um für den Begriff ”einzelner Bereiche” eine Regelung zu treffen, wird die Abgrenzung für den IV mittels des Beherrschungsprinzips vorgenommen.

Der Begriff ”Beherrschung” bedeutet in diesem Zusammenhang zum einen, dass die umzusetzenden Maßnahmen aus der Anwendung der *ISO 27001 auf Basis von IT-Grundschutz* uneingeschränkt von der Organisation des Informationsverbundes umgesetzt werden können, und zum anderen, dass von Dritten bezogene Leistungen ausgeschlossen sind. Der Regelsatz der Beherrschung kann für einen IV wie folgt verwendet werden.

Alle folgenden im Informationsverbund vorhandenen Elemente:

- Prozesse sowie die dafür erforderlichen,
- Rollen und Berechtigungen,
- Technologie (Netztechnik, IT),
- Infrastruktur (inkl. Gebäude, Räume, Haustechnik),
- Informationen und Daten

müssen vom Informations-Sicherheitsmanagement-System (ISMS) des IV dirigiert (beherrscht) werden können. Damit ist eine genaue Abgrenzung von Zuständigkeiten, Lokationen, Prozessen, Infrastruktur und Verantwortungen im Sinne des BSI, 100-2, Kapitel 4.1 gegeben. Weiterhin muss die Forderung zur Modellierung entsprechend dem Schichtenmodell des BSI erfüllt werden.

Der vorliegende Fall besteht aus einem Kundennetz (Auftraggeber, AG), das durch den Telekommunikationsdienstleister (Auftragnehmer, AN) zur Verfügung gestellt wird. Dieses Netz wird für den Kunden (AG) vom AN in einem Netzwerkmanagementcenter (NMC) überwacht, gewartet und es werden bei Bedarf Entstörungen vorgenommen.

Die Abbildung 1 illustriert die wesentlichen Aspekte. Auf der rechten Seite der Abbildung sind der IV mit seinen vier Hauptprozessen (HP-1, HP-2, HP-3, HP-4) und das Netz in dem NMC zur Verwaltung und Betreuung des Netzes für die AG skizziert. Im unteren Bereich sind die Hauptprozesse dargestellt. Dabei kommt dem Prozess HP-2 eine herausragende Rolle zu. Der Prozess HP-2 ist auf der linken Seite der Grafik detaillierter illustriert. In diesem Prozess findet der Überwachungsvorgang des Kundennetzes sowie des Netzes des NMC selbst statt.

Falls Anomalien oder Störungen erkannt wurden, wird der Entstörungsprozess angestoßen. Je nach Art der Störung wird entsprechend gehandelt. Der Prozess HP-4 führt eine geordnete Änderung in den ursprünglichen (sicheren) Zustand der Systeme zurück. Die tatsächliche Anpassung der Änderung im NMC bzw. im Netz wird dann vom Prozess HP-1 vorgenommen.

Die Hauptprozesse haben jedoch Wechselwirkungen mit den Prozessen des Telekommunikationsdienstleisters. Zu nennen sind z.B. alle Personalprozesse, um Mitarbeiter des NMC einzustellen oder zu entlassen. Aus dem Blickwinkel des IV und dem ISMS werden an dieser Schnittstelle besondere Bedingungen an die Auswahl und Fähigkeiten gestellt, und bei Überführung der Mitarbeiter in den IV werden diese geprüft.

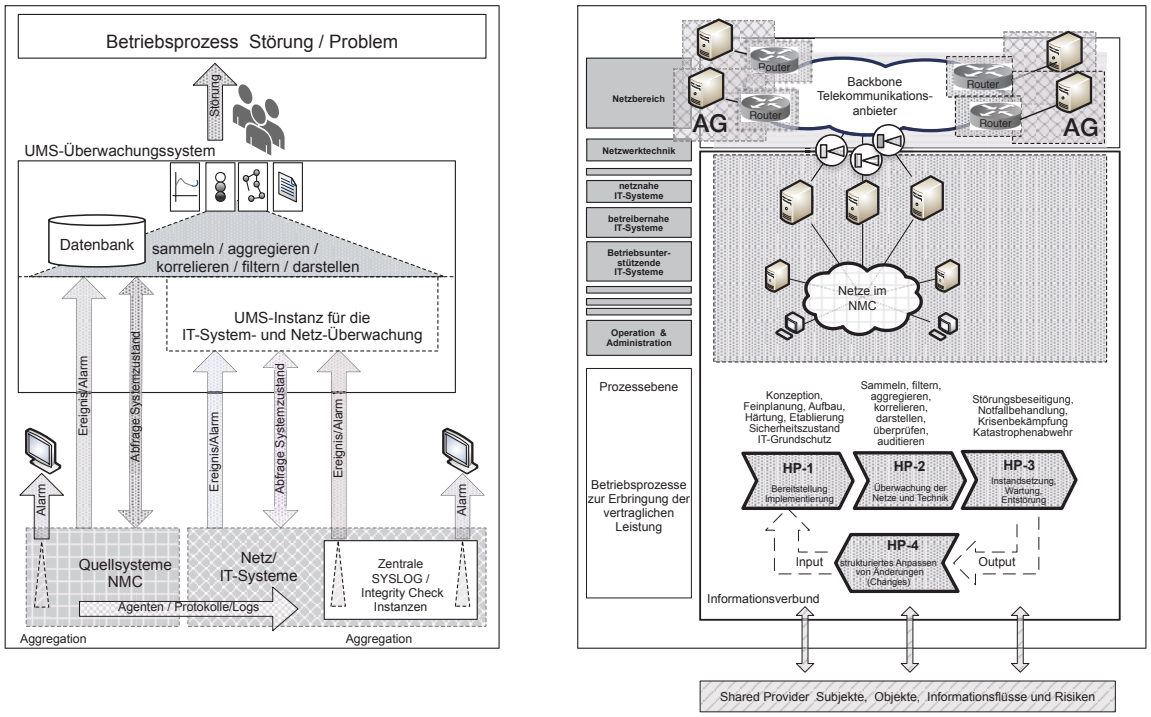

Abb. 1: Fachaufgaben, Prozesse und Netzdarstellung des IV

Zum erklärten Geschäftsmodell des Telekommunikationsdienstleisters gehört, dass es weder dedizierte Netze, noch eine dedizierte Netzüberwachung allein für einen Kunden vorgesehen sind. Gerade in der Bereitstellung von Netzen für viele Kunden liegt das Geschäftsmodell begründet. Daraus ergeben sich für die Abgrenzung des Informationsverbundes bestimmte Herausforderungen.

Die Abbildung 2 illustriert den Geltungsbereich (Scope) in einer mengentheoretischen Darstellung für ein Netzwerk Management Center (NMC). Die beiden Mengen "A" (Auftraggeber, AG) und "B" (Auftragnehmer, AN) sind zwei voneinander getrennte Firmen.

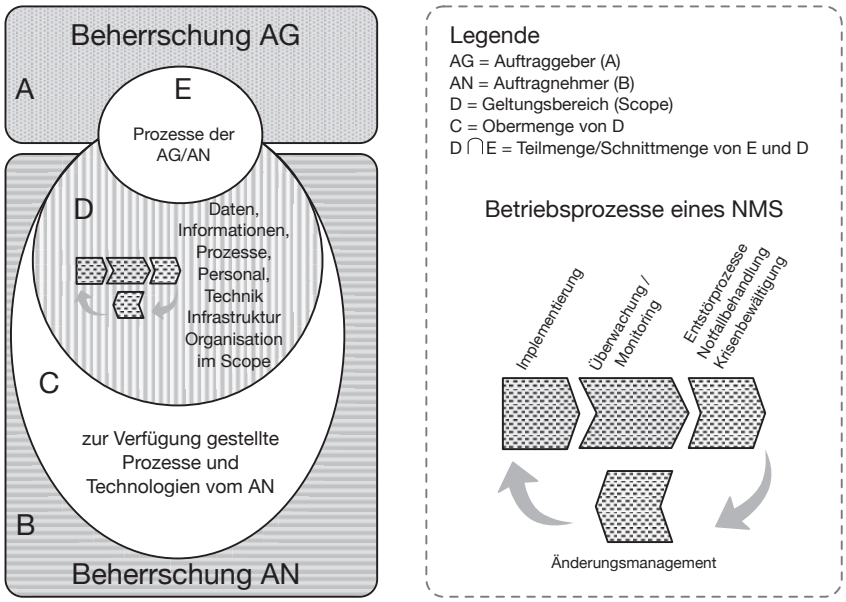

Abb. 2: Abstrakte Darstellung des IV

Eine mengentheoretische Darstellung bietet sich gerade hier an, da die einzelnen Elemente der o.g. fünf Punkte (Daten/Informationen, Infrastrukturen, Organisation, Personen und Technik) zunächst nicht näher für die Abgrenzung benannt werden sollen. Ziel dieser mengentheoretischen Darstellung ist es, die Schnittmengen abstrakt zu erfassen, um dann konkret alle sich ergebenden Schnittstellen zu identifizieren, die dann in dem nachfolgenden Abschnitt detaillierter diskutiert werden.

Bei der Überschneidung der Menge "E" und der Menge "D" entsteht eine gemeinsame Schnittmenge. Hier ist der Grundsatz der Beherrschung verletzt und es können Policies bzw. Richtlinien nur in gemeinsamer Abstimmung verabschiedet werden. Der Grundsatz der Beherrschung besagt, dass in dieser Teilmenge nicht uneingeschränkt die Vorgaben, die durch das ISMS vorgegeben werden, umgesetzt werden können.

Ist der Grundsatz der Beherrschung nicht gegeben, wird ein kooperatives Verhalten zwischen der AG und der AN in der Schnittmenge von "E" und "D" erwartet. Die Menge "C" stellt eine Obermenge der Menge "D" dar. Anders ausgedrückt, kann auch von einem eingebetteten Informationsverbund gesprochen werden. Die Menge "C" beinhaltet alle Elemente des Telekommunikationsdienstleisters und die Menge "D" nur diejenigen Zielobjekte, die auch in dem Informationsverbund enthalten sind und von dem ISMS beherrscht werden.

Ziel und Zweck eines Informations-Sicherheitsmanagement Systems ist es, den Zustand, den das IT/Inf.-Sicherheitskonzept nach der Maßnahme M 2.195 für die Zielobjekte im Geltungsbereiche für die Schutzziele vorgibt, über eine Zeitspanne, z.B. einen Zertifizierungszyklus, auf dem vordefinierten Niveau zu halten. Dies gelingt nur in dem IV wenn der Regelsatz der Beherrschung durch das ISMS ausgeübt werden kann.

4 Risikoorientierte Schnittstellenbetrachtung des IV

In diesem Abschnitt werden Risiken bzw. Gefährdungen diskutiert, die auf den IV über die Schnittstellen einwirken können oder im IV selber entstehen. Die Schnittstellen können gemäß

der Definition zur Abgrenzung eines Informationsverbundes von infrastruktureller, organisatorischer, personeller oder technischer Natur (Charakter) sein. Durch die Schnittstellen der Schnittmenge "D" wird der abgegrenzte Informationsverbund gebildet.

Die Menge "C", die eine Obermenge von der Menge "D" darstellt, unterliegt einer Überwachung durch einen bei der DAKKS akkreditierten Zertifizierungsanbieter mit einem ISO/IEC 27001:2013 (nativ) Zertifikat.

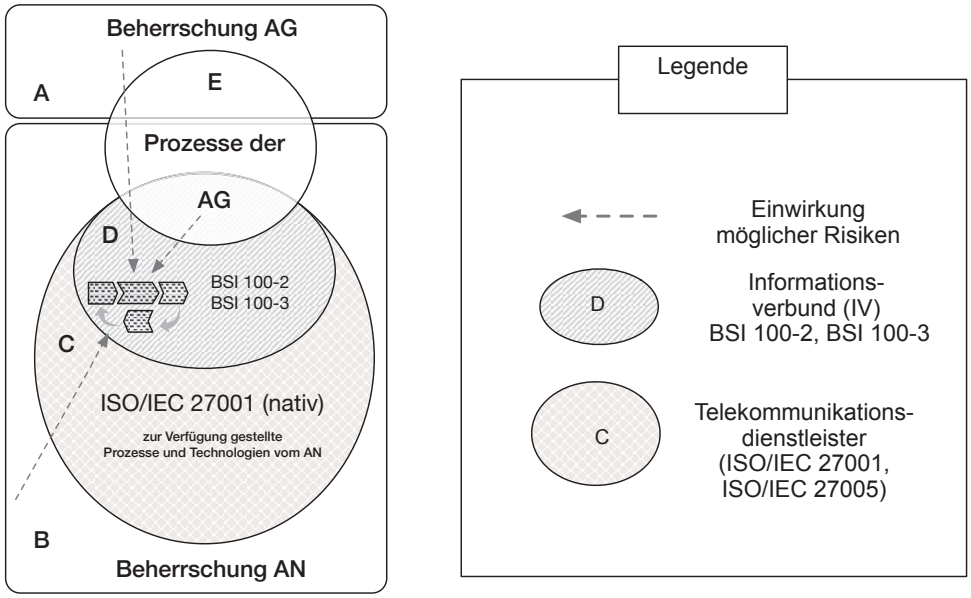

Abb. 3: Risiko- bzw. Gefährdungsbetrachtung im und auf den IV

Über die Schnittstellen, hervorgerufen durch die Schnittmengen, können Subjekte, Objekte oder auch Informationsflüsse je nach Charakter der Schnittstelle ausgetauscht werden. Dabei kann eine Schnittstelle unidirektional oder auch bidirektional sein. Diese Informationsflüsse können durchaus mit Risiken einhergehen. Somit sind Risikoanalysen bei einem Schnittstellenübergang von der Menge "C" zur Menge "D" vorzunehmen. Die Abbildung 3 illustriert durch die gestrichelten Pfeile die möglichen Risiken, die auf die Menge "D" einwirken können.

Für die Vorgehensweise zur Ermittlung der Risiken, bzw. Gefährdungen im Informationsverbund, also innerhalb der Menge "D", werden die BSI Standards 100-2 und 100-3 verwendet (vgl. Abbildung 3). Dabei stellen die Bausteine eine pauschalisierte Gefährdungsbetrachtung mit entsprechenden Maßnahmen dar (vgl. Abbildung 4). Diese pauschalisierte Betrachtung nimmt dem Anwender die Arbeit ab immer wieder für bestimmte typische Gefährdungen, für ein Zielobjekt bei einem neuen IV, immer wieder zu wiederholen. In der Abbildung 4 ist dies durch die Illustration der Bausteine im unteren Bereich der Abbildung zu sehen.

Grundsätzlich ist ein Baustein wie in Gleichung 1, bzw. als Abbildung 4 dargestellt, als kartesisches Produkt aufgebaut. D.h. Gefährdungen g und Maßnahmen m sind durch das kartesische Produkt mit einer rechtseindeutigen Relation f verbunden und es gilt $f(g) = m$. Da die Mengen der Gefährdungen und die Mengen der Maßnahmen abzählbar sind, werden die Mengen mit ihrer Mächtigkeit | | dargestellt. Die Gleichung 1 bezeichnet einen beliebigen Baustein B als formalen Ausdruck

$$B = |G| \times |M| \quad \text{mit} \quad \{g, m\} \,|\, g \in G \wedge m \in M\}. \tag{1}$$

Die endliche Menge G mit der Kardinalität $|G|$ enthält verschiedene Gefährdungen, die mit g bezeichnet werden. Die endliche Menge M mit der Kardinalität $|M|$ enthält unterschiedliche Maßnahmen, die mit m bezeichnet werden. Dabei ist $l, k \in \mathbb{N}$ eine Indexmenge. Es gilt

$$G = \{g \mid g_1 \leq g \leq g_l\} \wedge l \in \mathbb{N} \text{ und } M = \{m \mid m_1 \leq m \leq m_k\} \wedge k \in \mathbb{N}. \quad (2)$$

Oftmals wird in den Standards 100-2, und 100-3 der Begriff der Kreuzreferenztabellen als Ausdruck für das kartesische Produkt der Gleichung 1 verwendet. Dies ist in der Abbildung 4 illustriert. Dabei folgt die Grafik im unteren Bereich den pauschalisierten Gefährdungs- und Maßnahmenbetrachtungen mittels Bausteinen einer Ergänzungslieferung und der obere Bereich zeigt die individuelle Gefährdungs- und Maßnahmenbetrachtung.

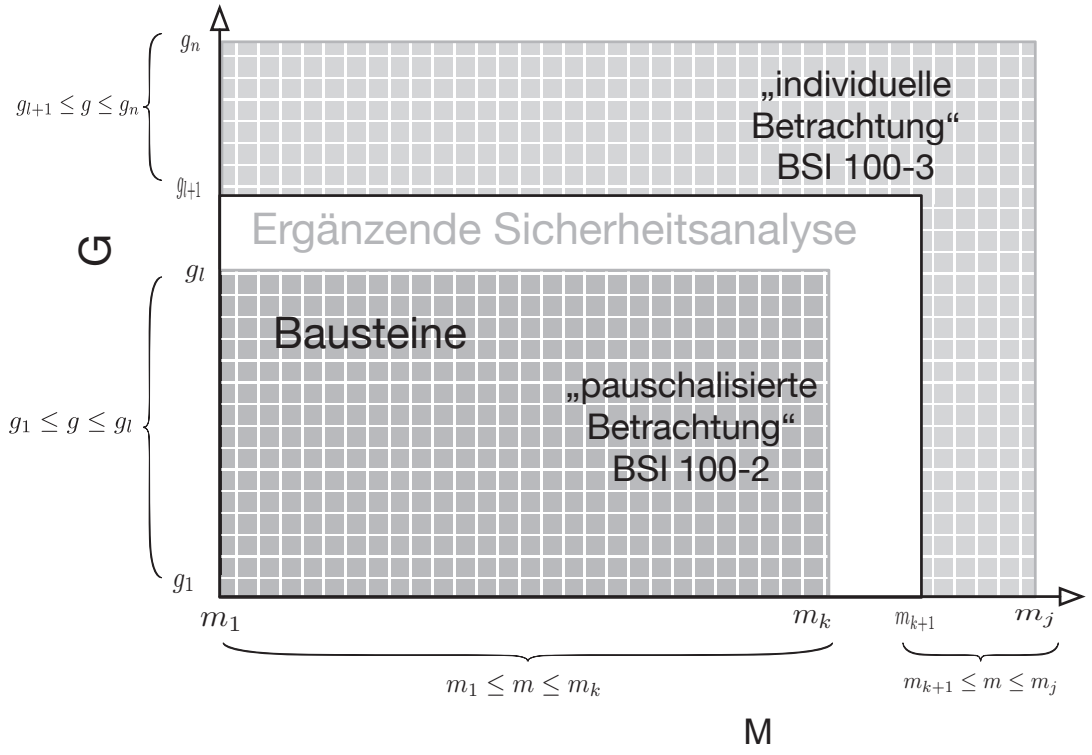

Abb. 4: Kartesisches Produkt aus der Menge der Gefährdungen G und Maßnahmen M

Die ergänzende Sicherheitsanalyse stellt eine Art Filter für den Übergang der pauschalisierten zur individuellen Betrachtungsweise in der Abbildung 4 dar.

Für den Baustein 3.204 der Grundschutzkataloge bedeutet dies, dass die pauschalisierte Betrachtung des kartesischen Produktes der endlichen Menge G mit der Mächtigkeit 28 und der endlichen Menge M mit der Mächtigkeit 29 mit der Gleichung 3

$$B_{3.204} = \left\{ G = \{g \mid g_1 \leq g \leq g_{28}\} \times M = \{m \mid m_1 \leq m \leq m_{29}\} \right\} \quad (3)$$

dargestellt werden kann. Da es sich bei dem vorliegenden Informationsverbund im Wesentlichen um ein Netzwerkmanagementcenter (NMC) handelt und die Grundschutzkataloge in erster

Linie für eine Bürokommunikation ausgelegt sind, ist es in diesem besonderen Umfeld notwendig, eine ergänzende Sicherheitsanalyse und eine Risiko- bzw. Gefährdungsanalyse vorzunehmen, wie es vom BSI Standard 100-3, Kapitel 1.2 auf Seite 4 gefordert wird [fSidIB08b].

Folglich wird die Menge der zusätzlichen Gefährdungen zG und die Menge der benutzerdefinierten Gefährdungen bG und die Mengen der korrespondierenden Maßnahmen zM, bM in der individuellen Gefährdungsanalyse identifiziert.

$$zG \wedge bG = \{g \mid g_{l+1} \leq g \leq g_n\} \wedge l, n \in \mathbb{N} \wedge l + 1 < n \tag{4}$$

$$zM \wedge bM = \{m \mid m_{k+1} \leq m \leq m_j\} \wedge k, j \in \mathbb{N} \wedge k + 1 < j \tag{5}$$

Diese sind in der Abbildung 4 in dem oberen Bereich dargestellt und als individuelle Betrachtung ausgewiesen. In der Praxis wird dann oftmals daraus ein benutzerdefinierter Baustein bB entwickelt. Es ist leicht einzusehen, dass der benutzerdefinierter Baustein bB dem formalen Ausdruck der Gleichung 1 entsprechen[3] muss.

Die Schnittstellen (Interface, IF) zwischen den Mengen "E", "C" und "D" werden bezogen auf die infrastrukturellen, organisatorischen, personellen und technischen Zielobjekte in Risikoszenarien R_{szn} gemäß der ISO/IEC 27005:2011 entwickelt.

Die Gleichung 6 illustriert die Szenarien ($R_{sz(IF)}$) an den Schnittstellen ($IF_{1,\ldots,n}$) für die infrastrukturellen, organisatorischen, personellen und technischen Zielobjekte, die in den Informationsverbund wechseln oder diesen verlassen. Dabei steht E_p für die Ereigniswahrscheinlichkeit, die einer Wahrscheinlichkeitsverteilung unterliegt. Das Kürzel b steht für eine Bedrohung und das Kürzel S für eine Schwachstelle. Die linearen Gleichungen 6 beschreiben jeweils ein Risikoszenario für eine Schnittstelle bzw. für den bidirektionalen Informationsübergang in den IV.

Das Risikoszenario ($R_{sz(IF)}$) kann jedoch nur unter der Bedingung, dass eine Bedrohung genau die dazu passende Schwachstelle findet zur negativen Auswirkung gelangen. Wir folgen hier dem Gedanken der Bayes Theorie und der bedingten Wahrscheinlichkeit, wie in der Dissertation von [AP05] angeregt wird, oder auch [Ale00, DVG08] für operationelle Risiken favorisiert.

$$\begin{aligned}
R_{sz(IF1)}\,[€] &= E_{p1}\,(b_1 \mid S_1) \cdot I_1\,[€] \\
R_{sz(IS2)}\,[€] &= E_{p2}\,(b_2 \mid S_2) \cdot I_2\,[€] \\
R_{sz(IF3)}\,[€] &= E_{p3}\,(b_3 \mid S_3) \cdot I_3\,[€] \\
&\vdots \\
R_{sz(IFn)}\,[€] &= E_{pn}\,(b_n \mid S_n) \cdot I_n\,[€]
\end{aligned} \tag{6}$$

Die negativen Auswirkungen in der Gleichung 6 werden mit (I) wie Impakt bezeichnet. Der Begriff Impakt deutet auf den möglichen Schaden hin, der in € bemessen wird. Da die Bedrohung und die Schwachstelle dimensionslos sind und keine Einheit haben, erhält auch das Risikoszenario die Einheit €. Die Risikobehandlung (vermindern, vermeiden, übertragen, akzeptieren, eliminieren) folgt der ISO/IEC 27005 [SC211].

[3] Bedauerlicher Weise sind einige Werkzeuge (Grundschutz Tools, z.B. Verinice bis zur Version 1.11) so aufgebaut, dass bei der Erstellung eines benutzerdefinierten Bausteines nur Maßnahmen eingebracht werden können.

Die Abbildung 5 illustriert den Wahrscheinlichkeitsraum Pr_E, in dem sich die Menge der Bedrohungen und die der Schwachstellen durch die Schnittmenge $b \cap S$ als Risikoszenario gemäß der Gleichung 6 ergibt.

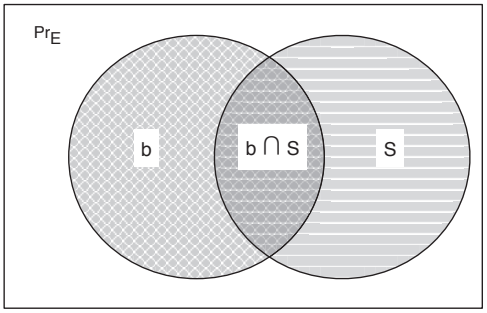

Abb. 5: Bedrohungen und Schwachstellen in einem Wahrscheinlichkeitsraum

Die Abbildung 6 illustriert das Zusammenspiel zwischen Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Risiken. Die Abbildung 6 kann weitergehend als Bayesian Netzwerk (BN) oder auch als Angriffsbaum (attack tree) verstanden werden. Denn E_p stellt in der Grafik (vgl. Gl. 6) die Wahrscheinlichkeit des Übergangs von einem Knoten zu dem nächsten durch eine mögliche Kante dar.

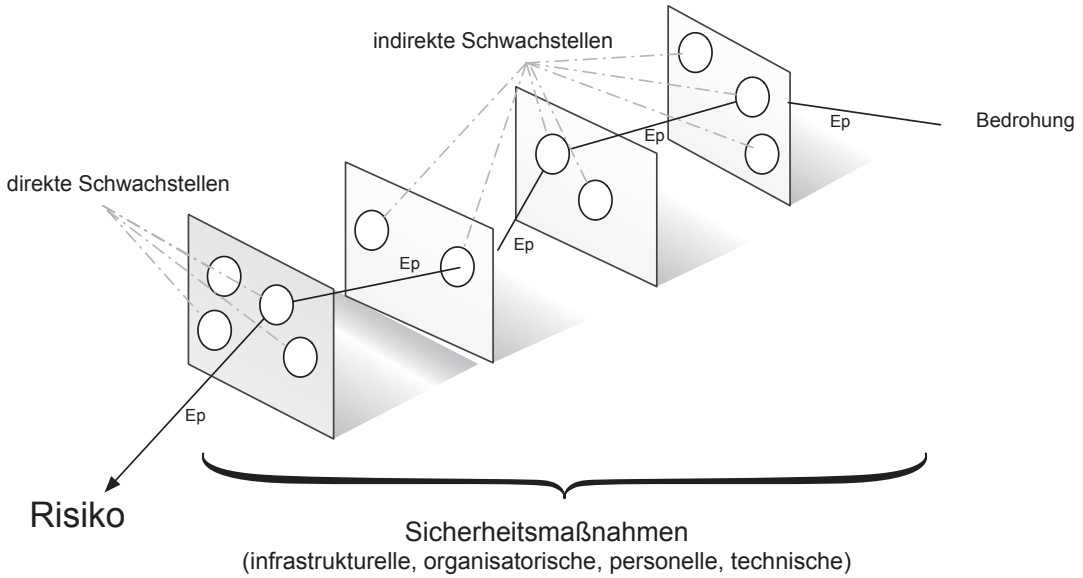

Abb. 6: Illustration bedingter Wahrscheinlichkeiten und bedingter Risiken gemäß der Bayes Theorie

Weiterführend kann diese Art der Betrachtung als Grundlage für die Untersuchung von nachhaltig andauernden Bedrohungen (Advanced Persistent Threats, APT) verwendet werden, wie in einer Analyse des Value ad Risk (VaR) in einer empirischen Untersuchung für eine Voice-Over-IP-Telefonie von [Boe13] vorgeschlagen wurde. Eine Erweiterung derartiger Analysen mit genetischen Algorithmen und einer Gewichtsfunktion (crime function) wurden von dem Autor ebenfalls vorgeschlagen [Boe14].

Als Beispiel kann der oben erwähnte Patch-Server betrachtet werden. Dieser ist außerhalb des IV und gehört zu den Elementen der Menge "C". Dort werden Patches z.B. für das erwähnte

Unix/Linux-System vom Hersteller, z.B. Oracle-Linux, bezogen. Beim Übergang in den IV wird eine Risikoanalyse bezogen auf die technische Schnittstelle ($R_{sz(IF)}$) durchgeführt und als Maßnahmen unter anderem ein Virusscan und ein Integritätsabgleich mit einer Hashfunktion vorgenommen.

Abschließend kann ausgeführt werden, dass in dem Zusammenspiel der Mengen "C" und "D" innerhalb der Menge "D" die Anwendungen des BSI Standard 100-2 und 100-3 erfolgen. Risikoanalysen werden an den Schnittstellen der Schnittmenge Menge "C"∩"D" (vgl. Abbildung 5) vorgenommen. Bei sorgfältiger Durchführung gemäß Gleichung 6 ist eine hinreichende Absicherung gegeben, die jährlich auf Änderung wiederholt werden muss.

Die präzise und eindeutige Beschreibung von Informationsübergabepunkten (Datenfluss an dedizierten Schnittstellen) im Zuge der Abgrenzung des IV, hat auch hinsichtlich des Datenschutzes wesentliche Vorteile. So bspw. bei der zweifelsfreien Erkennung, ob bzw. Bestätigung, dass Funktionsübertragung oder Auftragsdatenverarbeitung vorliegt. Des Weiteren hilft das Modell bei der Erstellung und Pflege des Verfahrensverzeichnisses.

Im Kontext Geheimschutz (Umgang mit Verschlusssachen des Bundes/der Länder in Unternehmen[4]) nützt das Modell bei der Erstellung notwendiger Kontroll- und Sperrzonenanweisungen sowie bei der Erstellung von Informationstechnik-Geheimschutzanweisung (ITGA). Darüber hinaus hilft es auch bei der Einstufung von Verschlusssachen (Informationen) durch den TK-Anbieter nach Maßgabe des VS-Auftraggebers (Teilmenge der öffentlichen Hand; Grundlage bildet die Verschlusssachenanweisung des Bundes/der Länder[5]).

Anzumerken ist, dass durch die beschriebene Vorgehensweise des eingebetteten IV, auch die Forderungen aus dem Baustein B1.11 (Outsourcing) inklusive der dort genannten Gefährdungen aus Sicht der Autoren für den vorliegenden Fall obsolet sind. Die oben beschriebene Vorgehensweise des eingebetteten IV trägt – konsequent angewendet – zu einer deutlich höheren Risikotransparenz im IV bei, und damit zu einer verkürzten Reaktionszeit auf sich entwickelnde Risiken. Ferner wirkt sich dies auf eine bessere Planung von Investitionen aus und beides wirkt sich als Vorteil für den Erhalt des Sicherheitsniveaus des IV aus.

Abschließend sei in diesem Abschnitt nochmal auf die auf der Hand liegenden Vorteile hingewiesen, denn bei einer (externen) Erweiterung durch Einbinden/Ändern weiterer Leistungserbringer außerhalb des IV über Schnittstellen ist das Einbinden/Ändern deutlich einfacher durchzuführen, als eine Neudefinition und damit Abgrenzung des IV mit allen sich daraus ergebenden möglichen Konsequenzen z.B. für die Zertifizierung.

5 IV Aspekte für einen Großkonzern

Alle großen Firmen, Unternehmen und Telekommunikationsdienstleister haben eine ähnliche Herausforderung zu meistern, wenn es gilt nur einen Bereich des Unternehmens als einen Informationsverbund zu definieren und zu zertifizieren. Die hier vorgeschlagene Lösung kann in einfacher Weise auch auf andere Situationen übertragen werden. Für die Definition eines Be-

[4] Geheimschutzhandbuch für die Wirtschaft, vgl. Kapitel 6, https://bmwi-sicherheitsforum.de/ handbuch/text/fk_menu=11

[5] Allgemeine Verwaltungsvorschrift des Bundesministeriums des Inneren zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA) vom 31. März 2006, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/SicherheitAllgemein/VSA.pdf?_blob=publicationFile

reiches geben die Standards des BSI 100-1/2/3/4 wenig Auskunft und so ist diese Lösung als Vorlage für große Unternehmen zu verwenden. Dass diese Lösung so vom BSI akzeptiert worden ist, zeigt die erfolgreiche Zertifizierung und das inzwischen erfolgreich absolvierte erste Überwachungsaudit.

6 Zusammenfassung und Ausblick

In diesem Beitrag wurde gezeigt wie ein den Standards des BSI konformer Informationsverbund definiert werden kann, der nur Teilbereiche eines Unternehmens abdeckt. Im Falle eines großen Telekommunikationsdienstleisters, der für seine Kunden u.a. Netze zur Verfügung stellt, stellt sich die Frage nach einer geeigneten Abgrenzung des IV. Weiterhin war die Forderung nach einer Zertifizierung des IV von dem Telekommunikationsdienstleister zu erfüllen. Eine besondere Herausforderung stellen die Schnittstellen aufgrund der Schnittmengen dar (vgl. Abbildung 3). Die Abgrenzung folgt dem Regelsatz der Beherrschung. Damit wird innerhalb des Informationsverbundes (IV) gemäß des Standards 100-3 die Risiko- bzw. Gefährdungsanalyse durchgeführt. An den Schnittstellen für infrastrukturelle, organisatorische, personelle und technische Zielobjekte, an denen Informationsflüsse bidirektional in und aus den IV wechseln, wird die ISO/IEC 27005:2011 [SC211] verwendet. Hierbei ist es sehr hilfreich, dass Telekommunikationsdienstleister bei der Anwendung von Methoden, Verfahren und Werkzeugen der ISO/IEC 27001:year (native) zumeist langjährige Erfahrungen haben.

In einer nächsten Untersuchung wird analysiert wie z.B. in der Schnittmenge $D \cap E$ (vgl. Abbildung 3) in der das Beherrschungsprinzip nicht gilt und nur ein kooperatives Verhalten zielführend ist, das Thema Notfallmanagement kooperativ behandelt werden kann.

Literatur

[Ale00] C. Alexander: Bayesian methods for measuring operational risk. *Discussion Papers in Finance*, 2000.

[AP05] K. Adusei-Poku: *Operational Risk management Implementing a Bayesian Network for Foreign Exchange and Money Market Settlement*. PhD thesis, Universität Göttingen, 2005.

[Bea11] M. Brenner and et al: *Praxisbuch ISO/IEC 27001*. Hanser Verlag, München, Erste Auflage, edition, 2011.

[Boe10a] W. Böhmer: Managementsysteme sind Balance-Systeme – Diskussion relevanter Kennzahlen eines ISMS gemäß ISO/IEC 27001:2005. In *Multikonferenz Wirtschaftsinformatik, Göttingen (MKWI2010)*, 2010.

[Boe10b] W. Böhmer: Toward a target function of an Information Security Management System. *The Third IEEE International Symposium on Trust, Security and Privacy for Emerging Applications (TSP-10), Bradford, UK*, June 29 - July 1, 2010.

[Boe13] W. Böhmer: How to estimate a technical var with the conditional probability and attack trees. *ARES Conference, The International Dependability Conference, IEEE Computer Society, University of Regensburg, Germany September 2nd - 6th, proceedings*, 2013.

[Boe14] W. Böhmer: Towards to analyze sophisticated attacks, with conditional probability, genetic algorithm and a crime function. Lecture Notes in Computer Science

(LNCS), Volume 8708, Proccedings of ARES 2014 Conference, University of Fribourg, Switzerland, September 8th – 12th, 2014, 09, 2014.

[DVG08] L. Dalla Valle, P. Giudici: A bayesian approach to estimate the marginal loss distributions in operational risk management. *Comput. Stat. Data Anal.*, 52(6):3107–3127, 2008.

[fSidIB04] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ein IT-Grundschutzprofil für eine große Institution. www.bsi.bund.de/gshb, Godesberger Allee 185-189, 53175 Bonn, 11, 2004.

[fSidIB08a] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise. www.bsi.bund.de/gshb, Godesberger Allee 185-189, 53175 Bonn, Version 2.0, 2008.

[fSidIB08b] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz. www.bsi.bund.de/gshb, Godesberger Allee 185-189, 53175 Bonn, Version 2.5, 2008.

[Rum16] R. Rumpel: Messen und Bewerten der Wirksamkeit von Informationssicherheits-Managementsystemen. IT Governance, Fachzeitschrift der ISACA Germany Chapter, Heft 23, März 2016.

[SC205] SC27: ISO/IEC 27001:2005, Information technology - Security techniques – Information security management systems – Requirements. Beuth-Verlag, Berlin, 10, 2005.

[SC211] SC27: ISO/IEC 27005:2011, Information technology - Security techniques – Information security risk management (2nd. edt.). Beuth-Verlag, Berlin, 07, 2011.

[SC213] SC27: ISO/IEC 27001:2013, Information technology - Security techniques – Information security management systems – Requirements. Beuth-Verlag, Berlin, Burggrafenstraße 6, 10787 Berlin, 10-1, 2013.