Auszug aus <kes> – Die Zeitschrift für Informations-Sicherheit,
Ausgabe 2017 #2, www.kes.info

Wirtschaftsgrundschutz

Die Vervollständigung der Grundschutzkataloge durch Sicherheitsaspekte jenseits der IT auf Basis des IT-Grundschutz-Gedankens

Der Wirtschaftsgrundschutz greift auf Basis der bekannten IT-Grundschutzstruktur Sicherheitsthemen außerhalb der klassischen IT-Angriffsfelder auf. Es ist ein Leitfaden entstanden, der allen Verantwortlichen für Unternehmenssicherheit sowohl in der freien Wirtschaft als auch im behördlichen Umfeld als Blaupause für Aufbau und Ablauf der Sicherheitsorganisation dienen kann.

Von Timo Kob, Berlin/Wien, und Björn Schmelter, Berlin

Cybersicherheit ist heute präsenter denn je und bildet sich auch in der Novellierung des IT-Grundschutzes ab. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstreicht mit seinem neu gestalteten Leitbild ebenfalls die Bedeutung aller erdenklicher Cybersicherheitsszenarien.

Der Cyber-Hype bedeutet jedoch nicht, dass andere Themenkomplexe, wie physische oder personelle Sicherheit, an Bedeutung verlieren. Ganz im Gegenteil bilden Angriffe in den klassischen Sicherheitsdisziplinen meist einen Startpunkt für komplexe Angriffe im Cyberraum. Und gerade mit der zunehmenden Verbreitung von IT außerhalb klassischer IT-Systeme – wie wir sie heute vor allem unter den Schlagwörtern „Internet of Things“ oder „Industrie 4.0“ wahrnehmen – steigt auch die Bedeutung weiterer Sicherheitsaspekte, da die Interdependenzen immer größer werden.

Ein besonders kritischer Aspekt ist die Sammlung von sicherheitsrelevanten Informationen, um zum Beispiel das Erraten von Passwörtern oder die gezielte Ansprache im Spearphishing zu ermöglichen. Hierauf zielen Maßnahmen der personellen Sicherheit (z. B. in Form von Sensibilisierungskampagnen oder der Einstellung geeigneter Mitarbeiter) und der physischen Sicherheit (z. B. durch Zutrittsbeschränkungen und das Wegschließen sensibler Informationen).

Nun ist dieser Ansatz sicherlich nicht neu: Bereits seit Jahrzehnten existieren sowohl die klassischen Sicherheitsthemen – auch außerhalb der IT – sowie Cyber- beziehungsweise IT-Sicherheitsthemen. Eine Herausforderung, der sich aber alle stellen müssen, ist die Integration all dieser Sicherheitsaspekte und die Vermeidung redundanter Aufgaben. Das Schlüsselwort dabei lautet „einheitliches Sicherheitsniveau“, damit jedes Themenfeld der Unternehmenssicherheit die gleiche Strategie fährt. Andernfalls entsteht hier schnell an einem spezifischen Punkt das „schwächste Glied in der Kette“ und damit ein mögliches Einfallstor für Angriffe.

Mit dem IT-Grundschutz gibt es bereits einen Standard, der sich vor allem mit den IT-Sicherheitsaspekten auseinandersetzt. Praktische Ansätze, die zudem leicht zugänglich sind und auf einem breiten Konsens basieren, gab es bisher für die weiteren Security-Themen aber kaum: Übergreifende, ganzheitliche Sicherheitskonzepte von IT- bis personeller Sicherheit, von physischer Safety und Security bis hin zum Krisenmanagement waren und sind die Ausnahme.

Offener Standard

Um hier Abhilfe zu schaffen, wurde von 2014 bis 2016 von der HiSolutions AG und dem ASW Bundesverband unter Einbindung der FH Campus Wien als akademischem Partner ein Forschungsprojekt unter Schirmherrschaft des Bundesamts für Verfassungsschutz (BfV) und des BSI durchgeführt. Die Ergebnisse dieses Projekts werden seit November 2016 sukzessive als „Wirtschaftsgrundschutz“ veröffentlicht – alle zugehörigen Inhalte sind kostenfrei auf www.wirtschaftsschutz.info abrufbar.

Kernidee des Wirtschaftsgrundschutzes ist es, die Philosophie und Methodik des IT-Grundschutzes

als profundes und anerkanntes Werkzeug für Gefährdungen in der (oder besser durch die) IT um ein Werk für die klassischen Sicherheitsaspekte zu ergänzen. Eine sprachliche Nähe der beiden Werke ist dabei Absicht, um auch hier den anschließenden Charakter hervorzuheben.

Dabei meint „Wirtschaftsschutz" weder, dass der IT-Grundschutz nicht ebenso für die Wirtschaft relevant ist, noch, dass er nur für die Wirtschaft geeignet wäre: Der Name soll vielmehr die ergänzende Bedeutung des Wirtschaftsgrundschutzes für einen ganzheitlichen Wirtschaftsschutz verdeutlichen.

Der Wirtschaftsgrundschutz ist ebenso wie der IT-Grundschutz als offener, lebender und konsensorientierter Standard zu verstehen. Alle Bausteine und Inhalte werden durch so genannte Expertenkreise begleitet und schlussendlich bewertet: So werden unterschiedlichste Branchenerkenntnisse in dem im Wirtschaftsgrundschutz beschriebenen Sicherheitsmanagement festgehalten und manifestiert. Neue Themen können – gesteuert durch den ASW Bundesverband – von allen Experten frei initiiert werden. Um sich für eine Mitarbeit zu melden, genügt eine Mail an info@asw-bundesverband.de.

Basis

Die grundlegende Idee des Wirtschaftsgrundschutzes beruht auf einem ganzheitlichen Schutzmodell, das nicht nur sämtliche Werte einer Institution abdeckt, sondern für deren Schutz auch alle erforderlichen Funktionen und Bereiche unter einer zentralen Funktion zusammenfasst und steuert. Dies stellt die unabdingbare Voraussetzung für ein einheitliches Sicherheitsniveau und eine effiziente Gestaltung des Sicherheitsmanagementsystems unter Berücksichtigung potenzieller Synergien dar.

Der Wirtschaftsgrundschutz verfolgt die Idee einer integrierten Unternehmenssicherheit und unterscheidet die zu betrachtenden sicherheitsrelevanten Themenfelder der Sicherheitsorganisation in Kernthemen und übergreifende Themen: Die Kernthemen werden im Wirtschaftsgrundschutz durch einzelne Schichten dargestellt. Diese werden in der Regel innerhalb einer Institution durch die Aufbauorganisation strukturiert und dedizierten Bereichen oder Gruppen zugeordnet.

Jedes Kernthema fokussiert dabei bestimmte Schutzwerte oder -ziele der Institution, die zur Erreichung eines einheitlichen und ganzheitlichen Sicherheitsniveaus erforderlich sind. In der Praxis sind diese Kernthemen dann beispielsweise durch Begriffe wie „physische Sicherheit", „personelle Sicherheit" oder auch „Informationssicherheit" und „Business-Continuity- & Crisis-Management" besetzt. Die Schichten innerhalb des Wirtschaftsgrundschutzes orientieren sich an denen des IT-Grundschutzes und lauten:

- Übergreifende Aspekte
- Infrastruktur
- Mitarbeiter
- Produkte und Dienstleistungen
- Externe Parteien

Die Übersicht in Abbildung 1 verdeutlicht, wie das Sicherheitsmanagementsystem im Wirtschaftsgrundschutz mit anderen Geschäftsbereichen einer Institution zusammenarbeitet.

Neben den Kernthemen wird in der Praxis die Notwendigkeit einer Verzahnung von Themen immer deutlicher – vermeintlich klassische Kernthemen werden so zu Treibern für eine neue Struktur der Unternehmenssicherheit. Dieser Gedanke macht im Wirtschaftsgrundschutz die Idee der themenübergreifenden Prozesse erforderlich: Diese umfassen sicherheitsrelevante Koordinationsthemen, die mittels einer geeigneten Ablauforganisation themen- und gegebenenfalls auch fachbereichsübergreifend behandelt werden. Die Prozesse wirken sich daher sowohl in mehreren Themengebieten des Sicherheitsmanagementsystems als auch in anderen Geschäftsbereichen aus. Im Wirtschaftsgrundschutz werden die folgenden themenübergreifenden Prozesse abgebildet, die nachfolgend kurz vorgestellt werden:

- Sicherheitsrisikomanagement
- Berechtigungsmanagement
- Sicherheitsvorfallmanagement

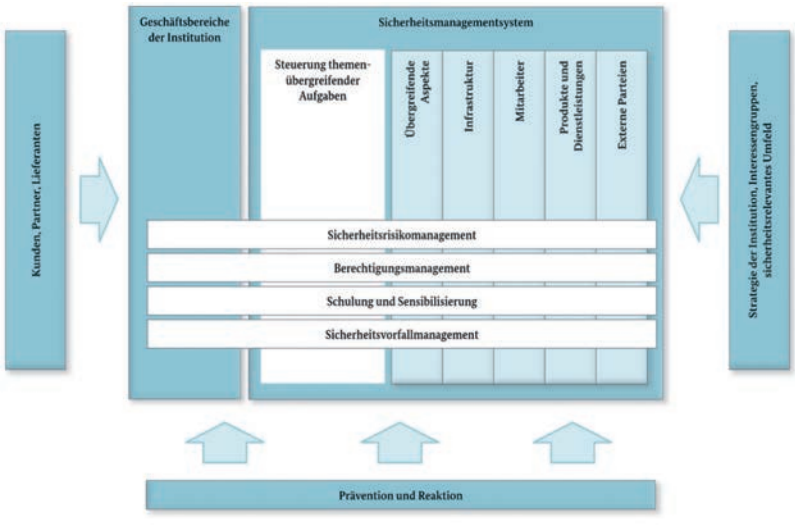

Abbildung 1: Sicherheitsmanagementsystem im Überblick

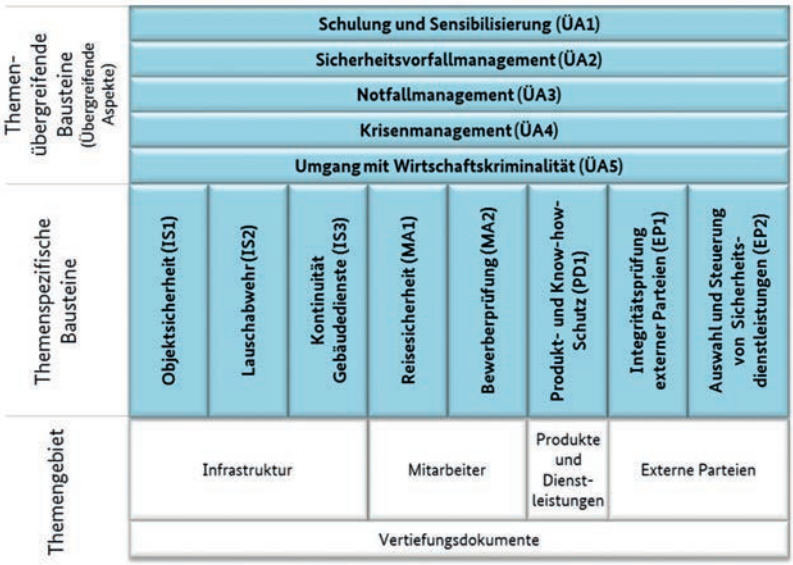

Abbildung 2: Bausteinstruktur des Wirtschaftsgrundschutzes

_____ Schulung und Sensibilisierung

Sicherheitsrisikomanagement

Innerhalb des Sicherheitsmanagementsystems werden Sicherheitsrisiken identifiziert und bewertet und gegebenenfalls ihre Behandlung initiiert. Unter dem Begriff Sicherheitsrisikomanagement wird hierbei die Identifikation und Bewertung von Gefährdungen verstanden, die sich nachteilig auf die definierten Sicherheitsziele für Personen, Prozesse, Informationen, Vermögenswerte, Dienstleister und Infrastruktur auswirken können.

Dabei steht eine einheitliche Herangehensweise im Vordergrund der Betrachtung: Ziel ist eine Vergleichbarkeit von Sichtweise und Wertung der analysierten Gefährdungen innerhalb der Kernthemen. Dazu beschreibt der Wirtschaftsgrundschutz eine zentral definierte Vorgehensweise und Methodik, die in den einzelnen Disziplinen je nach Erforderlichkeit fachspezifisch ergänzt wird. Ergänzend sind analog zum IT-Grundschutz je Baustein innerhalb eines Themenfelds relevante Bedrohungen und Gefährdungen aufgelistet. Gemeinsam mit dem IT-Grundschutz entsteht damit ein allumfassender Gefährdungskatalog.

Berechtigungsmanagement

Im Rahmen des Berechtigungsmanagements definiert eine Institution einen übergreifenden Prozess, der sicherstellt, dass erteilte Berechtigungen für Mitarbeiter oder Externe

_____ nach Bedarf und auf Antrag erteilt werden,

_____ nach Wegfall des Bedarfs wieder entzogen werden,

_____ zwischen Zugriffsberechtigungen für technische Systeme und

Initiative Wirtschaftsschutz

Aufgrund der zunehmenden Sicherheitsanforderungen im Bereich der Wirtschaftsspionage, Sabotage und Konkurrenzausspähung wurde 2016 die Initiative Wirtschaftsschutz als Schulterschluss zwischen Wirtschaft und Staat unter der Koordination des Bundesministeriums des Innern (BMI) gegründet. Mit ihr werden Expertise und Entwicklung eines umfassenden Schutzkonzepts, bestehend aus Maßnahmen und Projekten für einen verbesserten Wirtschaftsschutz, gebündelt.

Die Hauptakteure der Initiative Wirtschaftsschutz sind:

_____ Allianz für Sicherheit in der Wirtschaft (ASW Bundesverband)

_____ Bundesverband der Deutschen Industrie (BDI)

_____ Bundesverband der Sicherheitswirtschaft (BDSW)

_____ Deutscher Industrie- und Handelskammertag (DIHK)

_____ Bundesamt für Sicherheit in der Informationstechnik (BSI)

_____ Bundesamt für Verfassungsschutz (BfV)

_____ Bundeskriminalamt (BKA)

_____ Bundesministerium des Innern (BMI)

_____ Bundesnachrichtendienst (BND)

Als eines der ersten Werke neben dem Handbuch Wirtschaftsgrundschutz hat die Initiative den „Leitfaden Wirtschaftsschutz“ veröffentlicht, der ein Produkt von der Wirtschaft für die Wirtschaft darstellt. Anhand eines Blicks auf alle unternehmensinternen Prozesse liefert er einen Überblick zur Identifikation schutzbedürftiger Bereiche.

Zusätzlich wird eine Zwei-Tages-Schulung unter dem Titel „Geschäftsdaten schützen – für den Ernstfall rüsten!“ angeboten; sowie in Partnerschaft mit dem Bitkom ein Live-Online-Seminar.

Alle Informationen sind gemäß dem Motto der Initiative Wirtschaftsschutz „neutral – kostenfrei – vertraulich“ auf www.wirtschaftsschutz.info zu finden.

den physischen Zutrittsberechtigungen abgestimmt sowie

_____ jederzeit dokumentiert und nachvollziehbar sind.

Zielsetzung ist auch hier die Integration aller am Berechtigungsprozess beteiligten Akteure: Die Bereiche Personalwesen und Informationsverarbeitung sowie das Gebäudemanagement müssen letztlich an einem Strang ziehen – Medienbrüche zwischen „Zettelwirtschaft", „Zutrittskartensystem" und „Active Directory" werden durch intelligente organisatorische und technische Lösungen vermieden. Die Unternehmenssicherheit wird so mit dem Wirtschaftsgrundschutz zum Treiber und verhindert Sicherheitslücken.

Sicherheitsvorfallmanagement

Das Sicherheitsvorfallmanagement verfolgt das Ziel, eine zentrale Instanz zu schaffen, der auftretende Incidents gemeldet werden, die diese qualifiziert und dann die notwendigen Maßnahmen zu deren Bewältigung einleitet.

Schulung und Sensibilisierung

Der Aufbau eines integrierten Ansatzes innerhalb der Unternehmenssicherheit bedeutet in erster Linie einen massiven „Change" für die Organisation und die Beteiligten. Ein zentrales Management von Schulungs- und Sensibilisierungsmaßnahmen ermöglicht die Darstellung der erforderlichen Mitwirkung des Personals über die einzelnen Disziplinen hinaus. Dadurch lässt sich der Grundgedanke eines integrierten Ansatzes in einer effizienten Form vermitteln – vor allem Schnittstellen und gegenseitige Wechselwirkungen können durch diese gesamtheitliche Sicht besonders gut dargestellt werden.

Tabelle 1: Ausbaustufen von Maßnahmen im Wirtschaftsgrundschutz

Kategorie	Beschreibung	Bestimmung
A – Basismaßnahmen	• grundlegende Mechanismen als Fundament für den Einstieg in das Themengebiet • müssen grundsätzlich von allen Institutionen implementiert werden • essenziell für die Gewährleistung eines basalen Sicherheitsniveaus innerhalb des betrachteten Bausteins	• Basisschutz • geringe bis mittlere Risikoexposition
B – Standardmaßnahmen	• erste Aufbaustufe • relevant zur Erzielung eines höheren Reifegrads in einem Themengebiet • erforderlich, wenn Basismaßnahmen die identifizierten Gefährdungen nicht ausreichend abdecken	• erhöhter Schutz • mittlere bis hohe Risikoexposition • besondere Einsatzszenarien
C – Erweiterte Maßnahmen	• wichtig für die ganzheitliche Betrachtung eines Themengebiets • notwendige Ergänzung der aus einem erhöhten Schutzbedarf resultierenden höheren Sicherheitsanforderungen	• erweiterter Schutz • sehr hohe Risikoexposition

Bausteine

Wie im IT-Grundschutz werden anschließend mithilfe von Bausteinen die Kern- und Querschnittsthemen in Subthemen untergliedert und fachlich vertieft. Auf Basis des Forschungsantrags sind derzeit die in der Abbildung 2 dargestellten Bausteine geplant oder bereits erstellt und werden nun sukzessive veröffentlicht. Jeder Baustein wird dazu in drei wesentliche Kapitel unterteilt:

_____ Relevanzentscheidung: Dem Anwender oder Interessierten eines Bausteins wird im Vorfeld anhand von Fragen die Ermittlung der Relevanz des Bausteins für ihn ermöglicht. So kann hierbei herauskommen, dass ein Baustein für die Institution gar nicht anwendbar ist oder vielleicht nur Teile, etwa Basismaßnahmen, notwendig sind.

_____ Gefährdungsübersicht: stellt die Risikoszenarien dar, die mithilfe der Maßnahmen in diesem Baustein berücksichtigt worden sind. So erkennt der Leser auch, ob eventuell noch weitere Maßnahmen notwendig sind oder welche Ausbaustufe der Maßnahmen für ihn relevant ist.

_____ Maßnahmenbeschreibung: Zu guter Letzt erfolgt die Auflistung der Maßnahmen zum vertieften Thema. Diese werden, ebenfalls analog zum IT-Grundschutz, in drei Ausbaustufen unterteilt (siehe Tabelle 1).

Fazit

Der Wirtschaftsgrundschutz schließt nahtlos an den IT-Grund-

schutz an und kann ab sofort sowohl beim Aufbau einer übergreifenden Unternehmenssicherheit als Leitfaden herangezogen werden als auch bei der Ausgestaltung einzelner spezifischer Sicherheitsaspekte helfen. Dabei lässt er sich flexibel als führender Leitfaden oder als mögliche Ausbaustufe einer BSI IT-Grundschutzzertifizierung nutzen.

Neben der Bedeutung als Leitfaden für Lenker und Gestalter innerhalb der Unternehmenssicherheit stellt der Wirtschaftsgrundschutz perpektivisch auch einen Compliancebaustein dar: Denn mit der im Frühjahr 2016 vom EU-Parlament verabschiedeten Richtlinie zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (sog. Trade-Secret-Directive) wurde ein weiterer Meilenstein zur Etablierung europaweiter Mindeststandards für den Schutz von Betriebs- und Geschäftsgeheimnissen erreicht.

Auch wenn die Richtlinie erst noch in nationales Recht übernommen werden muss, wird eine Stärkung des Schutzes der Betriebs- und Geschäftsgeheimnisse für deutsche Unternehmen durch die verbesserten Anspruchsgrundlagen und Rechtsfolgen erwartet, die Opfer von Know-how-Diebstahl geltend machen können. Im Umkehrschluss bedingen die dadurch gestiegenen Anforderungen an Geschäftsgeheimnisse, dass hier ausreichende beziehungsweise angemessene Geheimhaltungsmaßnahmen ergriffen werden. Wenn man die Angemessenheit der Maßnahmen nicht nachweisen kann, sind Informationen nicht länger als Geschäftsgeheimnis geschützt.

Auch wenn bisher noch keine konkreten Vorschläge oder Vorhaben für die Umsetzung bestehen, sollten Institutionen auch bisher ergriffene Maßnahmen anhand der Mindeststandards der Richtlinie überprüfen und gegebenenfalls anpassen. Da der Richtlinie die genauen Voraussetzungen für die Angemessenheit nicht zu entnehmen sind, kann der Wirtschaftsgrundschutz auch hier eine wichtige Orientierungshilfe bei Planung, Implementierung, Überprüfung und Nachweis darstellen. ■

Prof. Dipl.-Inform. Timo Kob ist Professor für Wirtschaftsschutz und Compliance an der FH Campus Wien und Vorstand der HiSolutions AG. Björn Schmelter ist Product Manager für Wirtschaftsgrundschutz und Sicherheitsrisikomanagement bei der HiSolutions AG.

Informations-Sicherheit im Abonnement

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

<kes>

— strategisches Know-how

— Trends und Neuentwicklungen

— Hilfen zum Risikomanagement

— einschlägige Gesetze im Umfeld der IT und TK

— wichtige Messen und Kongresse

— Anwenderberichte

— BSI-Forum

— IT-Grundschutz

Fax-Rückantwort an +49 89 2183-7620

Ich/Wir abonniere(n) die Zeitschrift <kes> ab Ausgabe _____

Das Abonnement umfasst das Recht zur Nutzung des Abo-Bereichs auf www.kes.info mit allen aktuellen Beiträgen und dem **<kes>-Archiv** sowie den Bezug des <kes>/SecuPedia-Newsletters.

Jahresbezugspreis (sechs Ausgaben) € 135,00 inkl. MwSt. und Versandkosten (Ausland € 159,30).
Der Bezugszeitraum beträgt ein Jahr. Sie können das Abonnement jederzeit, spätestens jedoch acht Wochen vor Ende des Bezugsjahres kündigen. Sonst verlängert sich das Abo automatisch um ein weiteres Jahr.

Datenschutzhinweis: Ihre persönlichen Angaben werden von der DATAKONTEXT GmbH ausschließlich zur Vertragserfüllung einschließlich Zusendung des Newsletters, evtl. unter Einbeziehung von Dienstleistern, verwendet. Darüber hinaus erfolgt die Weitergabe an Dritte nur zur Vertragserfüllung oder wenn wir gesetzlich dazu verpflichtet sind. Falls Sie keine weiteren Informationen von DATAKONTEXT mehr erhalten wollen, können Sie uns dies jederzeit mit Wirkung in die Zukunft an die DATAKONTEXT GmbH, Augustinusstr. 9d, 50226 Frechen, per Fax an +49 2234 98949-44 oder per E-Mail an werbewiderspruch@datakontext.com mitteilen.

* erforderlich zur Zusendung des Secupedia-Newsletters – zusätzlich erhalten Sie Informationen zu eigenen ähnlichen Produkten per E-Mail. Sie können dieser Ansprache jederzeit widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

QR-Code für Bestellung per E-Mail

Firma _____ Abteilung _____

Name/Vorname _____

E-Mail* _____

Telefon (Geschäftl.) _____ Fax (freiwillige Angabe) _____

Straße/Nr. _____

PLZ/Ort _____

Datum/Unterschrift _____