SECFIRM Security Consultants

Unternehmensberatung | Sicherheitsunternehmen | Begutachtung

Nachvollziehbarkeit und System in der Planung von Objektschutzmaßnahmen

mgr Mario Trutzenberger EMBA

Sandro M. Trutzenberger B.Sc

Inhalt

Einleitung

Regelmäßig sind als „Physisches Sicherheitskonzept“, „Sicherheitskonzept“ oder „Objektschutzkonzept“ titulierte Schriftstücke zu sehen, die quasi aus dem Nichts Planungen von Einbruchmeldeanlagen, Zutrittskontrollanlagen und/oder Videoüberwachungsanlagen – oftmals in einer Art Anbotsform – hinwerfen, manchmal sogar noch verbrämt durch Empfehlungen wie ein Grundstück einzuzäunen und auf Fenster und Türen zu achten. Der „Planer“ legt dem Kunden praktisch „ex cathedra“ vor, was für ihn gut ist und mit Sicherheit seine Sicherheitsansprüche und -notwendigkeiten erfüllt. Sein Wissen ist de facto unbestritten, weshalb er auch nicht herleiten muss, wie er auf die zu Papier gebrachten Ideen gekommen ist. Schließlich ist er der Fachmann!

Vorweg: einerseits ist das unseriös für den Kunden, andererseits ein Wahnsinn zu auditieren und nicht zuletzt ein Irrsinn zu überprüfen und ggf. sachverständig (in allfälligen Schadensfällen) zu bewerten …

… und zeugt oftmals von mangelndem Sachverstand oder Überschätzung bzw. Überforderung des Erstellers bzw. Planers …

Stellt sich also die Frage, was ein Objektschutzkonzept genau ist und wie man es aufbauen kann, um den Regeln der Wissenschaft, Kunst, Technik und Normen … und was alles man sonst noch erfüllen möchte, zu genügen.

Dieses Paper soll einen kurzen Einblick in Möglichkeiten bieten, wobei es sich unter Aussparung wissenschaftlicher Modelle und Herleitungen auf normative Grundlagen beschränkt.

Die ÖNORM-Serie S 2412 ff

Eine probate Möglichkeit, ein Objektschutzkonzept systematisch aufzusetzen, bietet die ÖNORM-Serie S 2412 ff:

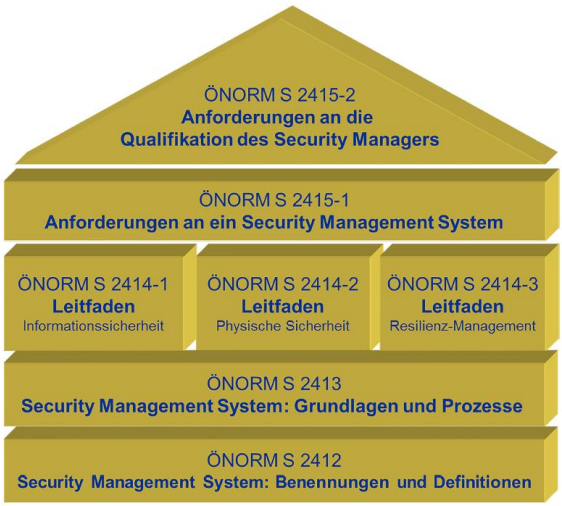

Abbildung 1 Quelle: ÖNORM S 2412:2017

Die **ÖNORM S 2412** bietet – bis auf wenige spezielle, in anderen Normen der Familie angeführte Definitionen den Grundkörper der Benennungen und Definitionen für die Normenserie.

Für das weitere Lesen und Verständnis der Normenfamilie ist es gut, den Aufbau zu verstehen, der der ÖNORM S 2413 und den Leitfäden zugrunde liegt:

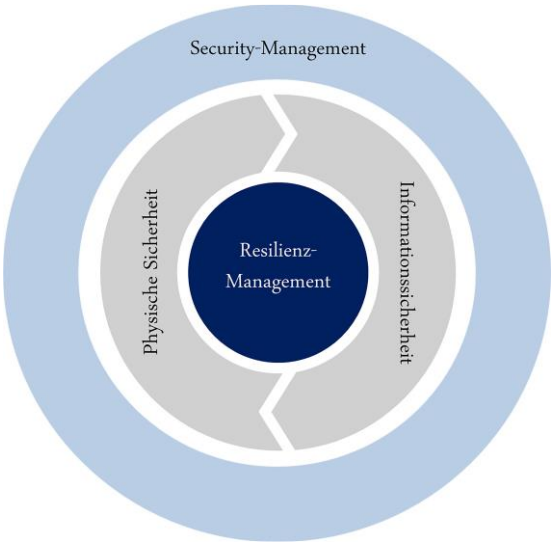

Abbildung 2 Quelle: ÖNORM S 2413:2017

Die Normenserie geht davon aus, dass das Security Management praktisch die organisatorische Basis und Klammer für das im Zentrum stehende Resilienz-Management und die Domänen Physische Sicherheit und Informationssicherheit darstellt. Angemerkt sei hier, dass dabei von einer typischen Konzernstruktur ausgegangen wurde; kleinere Organisationen, die natürlich ebenfalls Sicherheitsbedarf haben, wenden oftmals nur einzelne Domänen an und bringen den allenfalls noch erforderlichen Rest in diesem Konzept unter.

In der **ÖNORM S 2413** wird das Security-Management behandelt, insbesondere die Prozesse und die Dokumentation. Diese Norm definiert jedoch auch, welchen Domänen welche Teildisziplinen zugeordnet sind, beispielsweise sind der Domäne „Physische Sicherheit" insbesondere die Fachdisziplinen (a) persönliche Sicherheit inclusive der Reisesicherheit, (b) Veranstaltungsschutz, (c) Sabotageschutz sowie der (d) Schutz vor Wirtschafts- und Industriespionage zugeordnet, weshalb wir uns dann – es geht ja um Objektschutz – eingehender mit dieser Norm beschäftigen werden.

Die **ÖNORM S 2414** gliedert sich in 3 Leitfäden: (1) den Leitfaden für die Einbettung der Informationssicherheit in das Security Management System, (2) den Leitfaden für die Einbettung der physischen Sicherheit in das Security Management System und (3) den Leitfaden für die Einbettung von Resilienz-Management in das Security Management System.

Die **ÖNORM S 2415** bildet die Grundlage für Organisations- und Personszertifizierungen und definiert im Teil (1) die Anforderungen an ein Security-Managementsystem und im Teil (2) jene an den Security-Manager.

ÖNORM S 2414-2: Physische Sicherheit

An dieser Stelle sei noch einmal in Erinnerung gerufen, dass die Normenfamilie für große Organisationen das Modell anbietet, auf Basis eines Security-Management-System das Resilienzmanagement, das Physische Sicherheitsmanagement sowie die Informationssicherheit einzubetten (deshalb nennen sich die ÖNORMEN S 2414-1, -2 und -3 auch „Leitfäden zur Einbettung"). Wenn wir Security abseits großer Organisationen und Strukturen finden, finden wir in der Regel EINE vorherrschende oder ausgeprägte Domäne, in die bestenfalls wesentliche oder benötigte Elemente der anderen eingearbeitet sind. Um Beispiele zu nennen: wenn wir ein Bankinstitut mit einem Headquarter in Österreich, vielleicht 9 Landesdirektionen oder 3 Regionaldirektionen (z.B. Österreich West, Ost und Süd) und einem Netz mit 350 Filialen betrachten, wird sich dort ein strukturiertes Security-Management als integriertes Managementsystem finden (oder sollte es zumindest): im Optimalfall in Form einer Stabsstelle, die der Unternehmensleitung die benötigte Fachexpertise zur Verfügung stellt und das Managementsystem steuert. Betrachten wir jedoch einen Juwelier, der ja jedenfalls „Security" benötigt, alleine aus Gründen der Risikoabwälzung an einen Versicherer, der ja in seinen Bedingungen festlegt, unter welchen Voraussetzungen er welches Risiko bis zu welcher Höhe gegen welche Prämienzahlung übernimmt, werden wir i.d.R. ausschließlich Maßnahmen des Objektschutzes vorfinden und das entweder in jener Ausprägung, die der Inhaber der Security zumisst, hoffentlich aber auch in jener Ausprägung, die der Versicherer als Voraussetzung für die Deckungsübernahme im Schadenfall definiert. Ausgeprägte Maßnahmen der Informationssicherheit – wahrscheinlich bis auf

den Schutz von Kunden-, Lieferanten- und Buchhaltungsdaten werden sich beim Juwelier nicht finden. Sehen wir uns beispielsweise ein Unternehmen an, welches Software entwickelt oder eine Unternehmensberatung, werden hingegen vermutlich Maßnahmen der Informationssicherheit ausgeprägter sein und die Physische Sicherheit wird als Grundlage für die Informationssicherheit dienen.

Wir betrachten nun den Objektschutz isoliert, also ohne uns Gedanken über das „Security-Managemet" sowie das Resilienz-Management und die Informationssicherheit zu machen. Für das Verständnis der weiteren Ausführungen konzentrieren wir uns nur mehr auf die ÖNORM S 2414-2.

Security-Policy | Teilbereich Physische Sicherheit

Besteht im Rahmen eines Security-Managementsystems eine „allgemeine" Security-Policy, ergänzen wir sie nun um die Anforderungen unsere Domäne, ansonsten – wird z.B. Objektschutz singulär betrieben – wird hier die Policy erstellt: Einer spezifischen Analysephase folgt die Erstellung der Policy mit zumindest folgendem Inhalt: Festlegung des Anwendungsbereiches, Definition des Auftrags und Festlegung des Risikoappetits. Diese Policy ist durch die Oberste Leitung freizugeben.

Erstellung der Richtlinie „Physische Sicherheit"

Auf Basis der Security-Policy der Gesamtorganisation erfolgen hier die Definitionen der Methodik, der man bei der Erstellung des Objektschutzkonzeptes folgt, der Methodik des Security-Risk-Assessment, der Schutzziele und der Aufbau- und Ablauforganisation im Objektschutz sowie die Schnittstellen.

Security-Risiko-Analyse

Risiko = Eintrittswahrscheinlichkeit x Auswirkung. Grundsätzlich richtig. Neben den Kardinalfragen, wo man im Bereich des Objektschutzes halbwegs näherungsweise Eintrittswahrscheinlichkeiten herbekommt stellt sich die Frage, ob man mit dieser Basisformel auskommt. Vorweg: hält man ein „Objektschutzkonzept", „Sicherheitskonzept" oder wie immer ein derartiges Schriftstück genannt wird, in Händen, das entweder KEINE oder eine Risikoanalyse nach der Methode R = P x C beinhaltet, kann man davon ausgehen, dass der Ersteller entweder ein besonderes Verhältnis zu Allwissendheit oder die Fähigkeit zum Lesen aus Glaskugel oder Kaffeesatz hat oder es schlicht und einfach nicht besser kann. Die Norm geht davon aus, dass einer Security-Risiko-Analyse eine Zuordnung eines Assets zu einem Kritikalitätslevel, eine Kontextanalyse, die Identifikation der Schlüsselressourcen der Organisation sowie eine Bedrohungs- und Verwundbarkeitsanalyse vorausgehen. Als Grundlage für die Risikobehandlung dient das berechnete Security-Risiko auf Basis der spezifischen Eintrittswahrscheinlichkeit und der Bewertung des risikobasierten Schadensausmaßes.

Risikobehandlung

Hier folgt die Norm dem Grundsatz „prevent – delay – respond – recover": nach Planung von Maßnahmen und einer Kosten-Nutzen-Analyse erfolgt eine Neuberechnung des Security-Risikos mit den geplanten Maßnahmen und eine Gegenüberstellung des alten und des neuen Risikos und damit eine Überprüfung der Effizienz der angedachten Maßnahmen.

Zur Maßnahmenplanung können der Norm gemäß im Bereich der Objektsicherheit entweder (a) Wirtschaftsgrundschutz,

Baustein IS1 Objektsicherheit, oder die ÖNORM S 2420 herangezogen werden.

Umsetzung

Haben die Maßnahmen sich als effizient erwiesen, erfolgt die Maßnahmenumsetzung nach Prüfung etwaiger Synergiemöglichkeiten in der Organisation.

Überprüfung und Überwachung

Wie in jedem Managementsystem sind Maßnahmen der kontinuierlichen Verbesserung zu planen; die Werkzeuge dafür finden sich innerhalb der Normenfamilie in ÖNORM S 2413.

Exkurs Wirtschaftsgrundschutz, Baustein IS1 Objektsicherheit

Als eine der möglichen Methoden der Maßnahmenplanung im Rahmen der Risikobehandlung ist der Baustein IS 1 des Wirtschaftsgrundschutzes genannt.

Der Wirtschaftsgrundschutz (www.wirtschaftsgrundschutz.info) ist ein aus Deutschland stammendes ganzheitliches Schutzmodell für den Schutz von Unternehmenswerten und wird vom Bundesamt für Verfassungsschutz, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Allianz für Sicherheit in der Wirtschaft e.V. herausgegeben. An der Erarbeitung beteiligt sich die Wirtschaft gemeinsam mit Behörden wie Bundeskriminalamt und Bundesnachrichtendienst.

Der Baustein „Objektsicherheit“ unterscheidet nicht scharf zwischen intentionalen Bedrohungen und nicht intentionalen Gefahren, sondern führt bei „Gefährdungen im Zusammenhang mit Aspekten der Gebäudesicherheit“ neben intentionalen Bedrohungen auch Naturgefahren/Naturereignisse sowie ungeeignetes Personal … an.

Das scheint vordergründig egal zu sein (auch deutsche Autoren wir WENK[1] behandeln zum Thema Objektsicherheit intentionale Bedrohungen und verschiedene Arten anderer Risiken und Gefahren gemeinsam), wirft jedoch die Frage nach der Methodik der Risikoanalyse auf: zweifelsohne passt die Methode der Security-Risc-Analysis wie oben beschrieben nicht für die Risikoberechnung von Erdbeben, Hangrutschen, Muren- und Lawinen- sowie Hochwassergefahr …, weshalb die Vermischung der Risiken alleine aus dieser Überlegung problematisch scheint. Üblich sind derartige „gemeinsame“ Betrachtungen meist dann, wenn auf ein „klassisches Sicherheitskonzept“ verzichtet wird und die Objektschutzmaßnahmen lediglich darauf abzielen, Forderungen von Versicherungen zu erfüllen, um im Schadenfall umfängliche Deckung lukrieren zu können. Dabei handelt es sich aber um von Risikoabwälzung getriebene Maßnahmen, nicht von risikobasierten.

Der Wirtschaftsgrundschutz, Baustein Objektsicherheit beschreibt Maßnahmen, die sich in die Prozessblöcke „Führungsprozess“, „Betriebsprozess“ sowie „Berichts- und Kontrollprozess“ gliedern und einem Deming-Kreislauf folgen:

[1] Wenk, E. (1999). Objektschutzplanung für Führungskräfte im Sicherheitsbereich. Stuttgart, München, Hannover, Berlin, Weimar, Dresden: Richard Boorberg Verlag

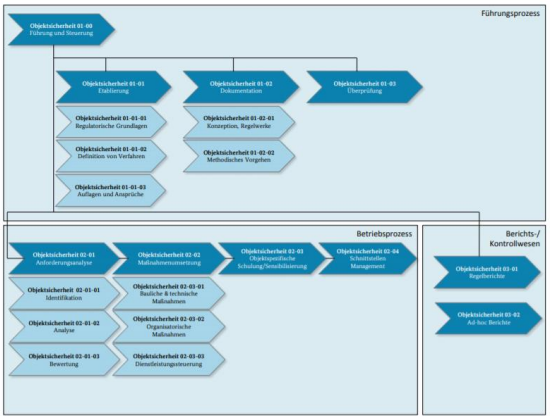

Abbildung 3 Quelle: Wirtschaftsgrundschutz, Baustein S1 Objektsicherheit

Die Maßnahmen werden in drei Kategorien gegliedert: A-Kategorie – Basismaßnahmen: unabdingbarer Wirtschaftsgrundschutz, B-Kategorie – Standardmaßnahmen: vollständiger Wirtschaftsgrundschutz und C-Kategorie – erweiterte Maßnahmen: erweiterter Schutz bei hohem Risikopotential:

A - Basismaßnahmen	B - Standardmaßnahmen	C - erweiterte Maßnahmen
M 1 Verantwortungsübernahme der Institution und Festlegen des erwarteten Sicherheitsniveaus	A +	A und B +
M 2 Ermitteln der Anforderungen aus der Geschäftstätigkeit	M 3 Erfassen der Sicherheitsbedürfnisse der Mitarbeiter und Nutzer	M 13 Überprüfen der Angemessenheit festgelegter Maßnahmen
M 4 Durchführen von Standort- und Umfeldanalysen	M 5 Durchführen objektbezogener Risikobewertungen	
M 6 Erstellen einer Sicherheitskonzeption	M 9 Definieren von Sicherheitszonen	
M 7 Schaffen der erforderlichen Regelwerke	M 10 Einbinden von Sicherheitsdienstleistungen in die Objektsicherheit	
M 8 Anforderungsgerechtes Umsetzen der definierten Sicherheitsmaßnahmen	M 11 Ausbildung, Schulung, Sensibilisierung	
	M 12 Kontrolle und Nachweisführung umgesetzter Maßnahmen	

Abbildung 4 Quelle: Wirtschaftsgrundschutz, Baustein S1 Objektsicherheit

Zusammengefasst entspricht der Ablauf der Planung folgenden, im Anhang dargestellten Schritten und enthält na. Maßnahmen:

Vorbereitung	Anforderungsaufnahme	Analyse
Verantwortungsübernahme für Objektsicherheit	Ermitteln von Anforderungen	Standort- und Umfeldanalyse
Festlegung Sicherheitsniveau	Erfassen der Sicherheitsbedürfnisse	Risikobewertung
Ableitung Sicherheitsstrategie		

Umsetzung	Überprüfung
Definieren von Sicherheitszonen	Kontrolle umgesetzter Maßnahmen
Erstellen Sicherheitskonzeption	Überprüfung der Wirksamkeit und Angemessenheit
Schaffen erforderlicher Regelwerke	
Umsetzen von Sicherheitsmaßnahmen	
Ausbildung, Schulung, Sensibilisierung	

Abbildung 5 4 Quelle: Wirtschaftsgrundschutz, Baustein S1 Objektsicherheit

Exkurs ÖNORM S 2420

Die ÖNORM nennt neben dem Wirtschaftsgrundschutz auch die ÖNORM S 2420 als probaten Ansatz der Maßnahmenplanung.

Grundsätzlich ist anzuführen, dass die Norm im Vorwort taxativ festlegt, für welche Art von Objekten sie gilt, beispielsweise für Kritische Infrastruktur, GROSSE Handelsunternehmen, Geld-, Kredit- und Versicherungsunternehmen, Großindustrie … und (interessanterweise auch für) Objekte für Großveranstaltungen. Der Juwelier, „normale Industrie- und Handwerksbetriebe“ und andere als große Handelsunternehmen sind demnach nicht adressiert.

Der prozessuale Ablauf zur Erstellung von Schutzkonzepten umfasst die Festlegung des Schutzzieles, die Feststellung des Ist-Zustandes, die Bewertung der intentionalen Gefahren und Priorisierung der Maßnahmensetzung, die Festlegung des akzeptierten Restrisikos und die Feststellung der erforderlichen Maßnahmen. Am Ende erfolgt die Erstellung eines Schutzkonzeptes.

Als Ziele der zu planenden Maßnahmen werden die Verringerung der Auswirkung und der Wahrscheinlichkeit des Schadeneintrittes genannt. Die Maßnahmen werden in mechanische, elektronische und organisatorische Maßnahmen gegliedert, wobei operative Sicherheitsdienstleistungen den organisatorischen Sicherheitsmaßnahmen zugeschlagen werden.

„Kochrezept"

Aus der Praxis der Planung sowie jener der Beurteilung haben wir einen Prozess entwickelt, der in mehreren Prozessebenen eine Schritt- für Schritt-Anleitung zur Planung, Umsetzung und Aufrechterhaltung von Maßnahmen des Objektschutzes anbietet. Der Prozess widerspricht keiner der angeführten normativen Forderungen und ist vielfältig anwendbar: er kann sowohl bei großen als auch kleinen Infrastrukturen abgearbeitet werden, egal, ob ein Security-Management-System besteht oder nicht, er funktioniert bei allen Kritikalitäten und kann ebenso bei speziellen Stakeholderanforderungen oder der Notwendigkeit zur Anwendung von leges speciales eingesetzt werden.

Sind Objektschutzkonzepte und -systeme zu beurteilen, bietet er einen Anhalt zur Qualifizierung von Herleitung, Inhalt und Zusammenwirken verschiedener Gewerke.

Im Hintergrund laufen sozusagen ua. die Planungsgrundsätze „deter – detect – delay – deny – respond", und das Zusammenwirken von baulichen, mechanischen, elektronischen, personellen und organisatorischen Maßnahmen sowie des sogenannten Zwiebelschalenprinzipes ... mit.

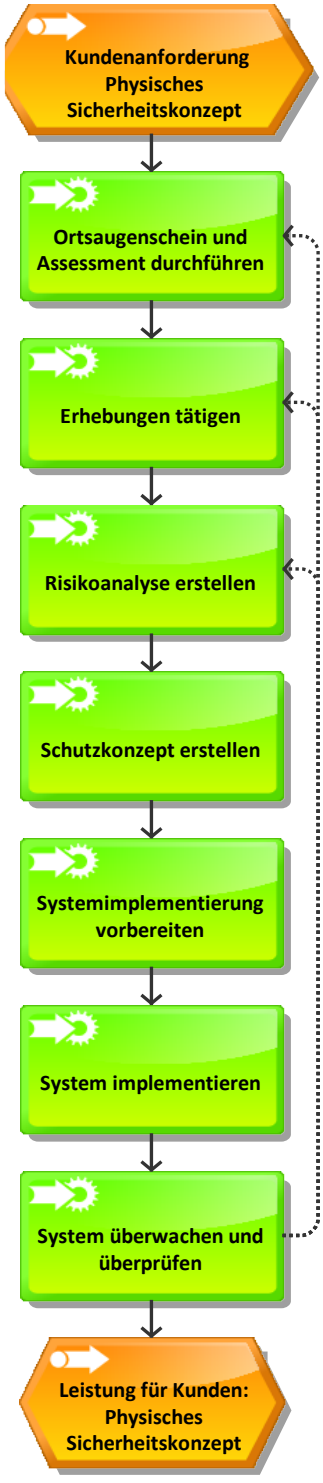

Abbildung 6 Quelle: Eigene Darstellung

Die erste Prozessebene

Ortsaugenschein und Assessment: Neben einer Besichtigung und Dokumentation

des Objektes erfolgt ua. die Dokumentation relevanter Abläufe, vorhandener Schutzmaßnahmen, interner und externer Schnittstellen, interner und externer Stakeholder und deren Forderungen, die Erarbeitung der zu schützenden Assets, des angestrebten Schutzstandards und des tolerierbaren Restrisikos sowie der zur Verfügung stehenden Ressourcen (temporär, pecuniär, personell ...).

Am Ende dieses Prozessschrittes sollte man das Objekt und die betreibende Organisation sowie Auftragsziel und Rahmen soweit kennen, dass man überblicken kann, ob der Auftrag für den Planer überhaupt ausführbar ist bzw. dass für die weiteren Schritte alle erforderlichen Informationen zur Verfügung stehen.

Erhebungen: Da auch Erhebungen zu tätigen sind, die nicht alle 1:1 in die Security-Risiko-Analyse einfließen, wurde dieser Schritt als eigener Prozessschritt etabliert. Hier erfolgt die Interventionszeitberechnung, die objektbezogene Auswertung von Statistiken, die Erhebungen und Beurteilungen bedrohungsbegünstigender und bedrohungsminimierender Faktoren, erste Überlegungen zu zu erwartenden Täterqualitäten und -fähigkeiten, möglichen modi operandi etc. Teile dieser Erhebungen fließen als Faktoren in die Security-Risiko-Analyse ein.

Risikoanalyse: In der Security-Risiko-Analyse erfolgt die Beurteilung und Qualifizierung aller möglicher Angriffe auf die definierten Assets. Teil der Risikoanalyse ist die Entwicklung von Maßnahmen zur Minimierung intolerabler Risiken in den tolerablen oder zumindestens ALARP-Bereich und die Überprüfung der Maßnahmenwirksamkeit im Rahmen der Risiko-Neuberechnung unter Einbeziehung der Maßnahmen.

Schutzkonzept: Jene Maßnahmen, die in der Risikoanalyse eine entsprechende Risikoreduktion bewirkt haben, werden nunmehr im Schutzkonzept ausgeführt und detailliert, wobei besonderer Wert auf - dem Prinzip der Abschreckung, Detektion, Verzögerung, Zurückweisung und Angriffsbeendigung folgend - das Zusammenwirken baulicher, mechanischer, elektronischer, personeller und organisatorischer Schutzmaßnahmen gelegt wird. Das Konzept muss sich dem Grundsatz „soviel als nötig, sowenig als möglich“ derart in die Organisation einfügen, dass alle Schnittstellen sauber bedient und alle Stakeholderforerungen umgesetzt – der Bedrohung entsprechend – betriebsinterne Abläufe so wenig als möglich gestört oder behindert werden und die Maßnahmenumsetzungen durch breite Akzeptanz und allgemeines Verständnis sichergestellt ist.

Vorbereitung der Implementierung: In diesem Prozessschritt zu erbringende Leistungen sind auftragsabhängig und können ua. die (funktionale) Ausschreibung der Gewerke und Dienstleistungen und die Anbotsbeurteilung sowie die Unterstützung des Auftraggebers bei der Auftragsvergabe ebenso umfassen wie die Planung des Projektmanagement für die Maßnahmenumsetzung und Gewerkeimplementierung.

Maßnahmenimplementierung: Auch in diesem Prozessschritt sind die zu erbringenden Leistungen variabel und auftragsabhängig. In der Praxis zeigt sich jedoch – insbesondere bei Projekten größeren Umfangs und erhöhter Komplexität – die Vorteilhaftigkeit der Begleitung der Maßnahmenumsetzung und -implementierung, da auftretende Schwierigkeiten und Probleme frühzeitig und im Rahmen des Gesamtkonzepts und ohne dies zu verändern

gelöst und das Abweichen von Vorgaben frühzeitig erkannt und korrigiert werden kann. Jedenfalls empfehlenswert ist eine Abnahme der Gewerke und Maßnahmen durch den Konzeptersteller vor Freigabe der Rechnungen.

Die Maßnahmenimplementierung endet mit der Verortung des Systems in der Organisation und sozusagen der Systemübergabe an die Organisation.

System überwachen und überprüfen: Die Systemimplementierung und Übergabe an die Organisation beendet jedoch keinesfalls die Tätigkeiten im Rahmen des Schutzsystems, auch wenn zumindest 9 von 10 Objektschutzsystemen an diesem Punkt ihr „Sterben" beginnen: Jahre nach der Implementierung (wenn der Planer vergessen hat, Maßnahmen der Systemaufrechterhaltung zu implementieren oder die Organisation die Maßnahmen nicht gelebt hat) sieht man – meist anlassbezogen, also wenn etwas passiert ist oder eine (geänderte) Stakeholderforderung zu einer Überprüfung führt – nicht gewartete, nicht gelebte, (teilweise) nicht funktionierende … Systeme und/oder Systeme, die entweder nicht mehr dem Stand der Technik oder den Regeln der Kunst oder aber auch nicht mehr den Anforderungen entsprechen.

Im Sinne eines Kreislaufes der ständigen Verbesserung sind hier insbesondere zwei Maßnahmenblöcke zu planen und implementieren: einerseits Maßnahmen der Überprüfung der Funktionalität, wozu auch Wartungen, Dokumentationen etc. gehören, andererseits die regelmäßige Überprüfung der Angemessenheit (geänderte Assets, geänderte Bedrohungen, geänderte Risikoabwälzung, geänderte Stakeholderforderungen …).

Neben Wartungs- und Instandhaltungsarbeiten sowie Evaluierungen sind hier regelmäßig wiederkehrende Audits ein probates Mittel, um Schutzsysteme in erforderlichem Umfang und angemessener Qualität aufrechtzuerhalten, wobei externe Audits unter dem Aspekt des Need-to-know abzuwägen sind.

Zusammenfassung

Neben dem Grundverständnis, dass Einzelkomponenten wie Sicherheitstüren oder Alarmanlagen noch lange keine „Sicherheits"- oder „Schutzkonzepte" sind und ebensowenig ein Objektschutzmanagementsystem darstellen oder ersetzen, sollte bei Auftraggebern und allen seriösen Anbietern von sicherheitsrelevanten Gewerken und/oder Dienstleistungen das Bewusstsein vorhanden sein, dass einem Objektschutzsystem einerseits Grundsätze hinterlegt sein müssen, die gleichsam den Ductus aller Maßnahmen vorgeben und andererseits die Maßnahmen nicht irgendwoher kommen können, sondern einem nachvollziehbarem Prozess folgend auf nachvollziehbaren Herleitungen basieren müssen.

Nur transparente, einem Ductus folgende und nachvollziehbare Systeme können (a) eine adäquate Antwort auf intentionale Bedrohungen sein, (b) richtig gelebt und aufrechterhalten sowie (c) der Effizienz und Güte nach beurteilt werden.

Die Autoren:

Mario Trutzenberger, ist selbstständiger Sicherheitsberater für Physical Security, Notfall- und Krisenmanagement und Materiellen Geheimschutz und modulverantwortlicher Lektor für Physische Sicherheit im Fachbereich Risiko- und Sicherheitsmanagement an der FH Campus Wien.

Sandro M. Trutzenberger ist Absolvent des Bachelorstudiums Integriertes Sicherheits-Management, Student im Masterstudium Public Management und Security-Consultant mit Schwerpunkten Security-Risc-Analysis und Physical Security.

Näheres unter https://secfirm.at.