SECFIRM Security Consultants

Unternehmensberatung | Sicherheitsunternehmen | Begutachtung

Die Machbarkeitsstudie in der Objektschutzplanung

mgr Mario Trutzenberger EMBA

Sandro M. Trutzenberger, B.Sc

© Mario & Sandro Trutzenberger 2020

Inhalt

Vorwort 3
Von der Idee bis zur Implementierung 3
Verortung 3
Literatur und Normung 4
Prozess 5
Fazit 7

© Mario & Sandro Trutzenberger 2020

Vorwort

Insbesondere wenn man in der Planung und Umsetzung starke Stakeholder, die hohe Anforderungen an ein Physisches Sicherheitssystem stellen, an Bord hat und/oder wenn von der Maßnahmenumsetzung hohe Kosten zu erwarten sind oder wenn die Unternehmensstrategie zumindest in Teilen von der Umsetzung bestimmter Schutzmaßnahmen abhängig ist, empfiehlt es sich, vor der Detailplanung eine Machbarkeitsstudie zu erstellen, um einerseits mit Stakeholdern abklären zu können, ob die Umsetzung von in der Machbarkeitsstudie geplanter Modelle zu einer Akzeptanz führen werden und einen ersten groben Überblick über benötigte Ressourcen und zeitliche Horizonte zu erhalten. Die Kosten einer solchen Studie sind vergleichsweise gering und amortisieren sich bei Umsetzung der Maßnahmen, weil dann bereits Gerüst und Ductus vorliegen.

Von der Idee bis zur Implementierung

Physische Sicherheit beginnt zuerst im Kopf des Bedarfsträgers. Entweder aus einer Sicherheitsüberlegung heraus, oder aber weil ein anderes Ansinnen z.B. aufgrund gesetzlicher Vorgaben oder sonstiger Stakeholderforderungen Maßnahmen der Physischen Sicherheit nach sich ziehen.

Hat man sich grundsätzlich geeinigt, dass ein Bedarf an Maßnahmen der Physischen Sicherheit besteht, sind schier unzählige Zugänge festzustellen: während eine Vielzahl von Unternehmen entsprechende Expertise in den Reihen der eigenen Mitarbeiter such, suchen andere einen passenden Berater.

Grundsätzlich hat sich in mehr als 15 Jahren einschlägiger Beratungserfahrung herausgestellt, dass in Unternehmen dann mit einer (Grund)expertise zu rechnen sein wird, wenn ein Security-Management-System implementiert ist, welches von einem /einer entsprechend ausgebildeten und erfahrenen Head of Security geleitet wird. Derartige leitende Mitarbeiter verfügen auch über eine realistische Sichtweise auf und Einschätzung ihrer Grenzen und können beurteilen, ab wann und wofür ggf. fachliche Spezialexpertise beizuziehen ist. I.d.R. mit nicht ausreichender Expertise im Haus ist erfahrungsgemäß dann zu rechnen, wenn (a) kein oder (b) kein einem anerkannten Regulativ oder einer normativen Grundlage zuordenbares Sicherheitssystem vorfindbar ist und natürlich, wenn (c) kein strukturiertes Sicherheitssystem vorliegt. „C“ findet man oft bei schnell gewachsenen Unternehmen oder Unternehmen, die aufgrund ihrer Geschäftsbereiche zwar doch ein gewisses Sicherheitsbewusstsein entwickelt haben oder entwickeln mussten, aber sich für die Befriedigung dieses Bewusstseins keiner interner oder externer Experten/Expertinnen bedient haben: oftmals wurden dann sicherheitsrelevante Rollen und Verantwortlichkeiten Mitarbeitern und Mitarbeiterinnen „umgehängt“, von denen man annimmt, sie könnten aufgrund ihrer Grundtätigkeit einen wie immer gearteten Zugang zu Security-Management -Themen haben.

Verortung

Bevor wir das Thema „Machbarkeitsstudie“ betrachten, versuchen wir das Thema zu verorten und zu definieren.

© Mario & Sandro Trutzenberger 2020

Während im anglikanischen Sprachraum von Security und Safety gesprochen wird, fasst die deutsche Sprache die Begriffe in einen einzigen, nämlich „Sicherheit" zusammen um Experten dann zu zwingen, die Anglizismen Security und Safety in ihren Sprachgebrauch zu übernehmen, um deutlich zu machen, wovon überhaupt die Rede ist. Safety bedeutet den Schutz vor nicht intentionalen Gefahren, z.B. Arbeitnehmerschutz, Brandschutz ..., während Security vor intentionalen, also gewollten, kriminellen, Angriffen schützt. Die Zusammenfassung in den Begriff „Sicherheit" resultiert vermutlich daraus, dass einerseits jede der beiden „Sicherheiten" wesentliche und zwingend zu bedienende Schnittstellen für die jeweils andere Sicherheit definiert und irgendwie immer die Möglichkeit besteht, dass die eine Sicherheit die andere braucht. Ein Beispiel: betrachtet man den intentionalen Angriff „Sabotage", so kann ein möglicher modus operandi Brandstiftung sein. In diesem Fall bedient sich die Security der Brandmeldeanlage (die grundsätzlich der Safety zugeordnet ist) sozusagen als 1st oder 3rd line of defence: wenn schon (bezogen auf die 3rd line of defence) erste bauliche und/oder mechanische Hürden überwunden worden sind und die Detektion durch die Einbruchmeldeanlage erfolgt ist, wodurch Interventionskräfte zur Unterbindung des rechtswidrigen Angriffes alarmiert worden sind, wird nun durch die Brandmeldeanlage nun auch die Feuerwehr und somit ebenfalls Sicherheitskräfte zur Beendigung des rechtswidrigen Angriffes alarmiert.

Diese Sichtweise manifestiert sich auch in der akademischen Ausbildung im Themenbereich „Sicherheit": während im anglikanischen Raum auch im Ausbildungsbereich i.d.R. eine strikte Trennung der Themen zumindest in der Lehre vorgenommen wird, werden die beiden Themenbereiche insbesondere im D-A-CH-Raum integriert: vor einer allfälligen Spezialisierung insbesondere in der Security kommt man i.d.R. nicht über eine zusätzliche Ausbildung im Safety-Bereich umher: die meisten Security-Manager sind hier auch ausgebildete Sicherheitsfachkräfte, Brandschutzbeauftragte ...

Literatur und Normung

Wir bleiben im Schwerpunktbereich Security. Und selbst der ist wieder breit gefächert: Begriffe wie Corporate Security-Management, Security-Management, Resilienzmanagement ... lassen wir hier genauso außen vor wie Informationssicherheit und akzeptieren „Physische Sicherheit" gem. ÖNORM S 2413 als Teil des Gesamtsystems.

Abbildung 1 Quelle: ÖNORM S 2413:2017

Die Definitionennorm S 2412 der Normungsfamilie S 241X definiert (ÖNORM S 2412, Pkt. 2.36) Physische Sicherheit als >Erhaltung von Verfügbarkeit, Vertraulichkeit und Integrität von Assets durch die Nutzung von ganzheitlichen Maßnahmen<, ÖNORM S 2413 normiert, dass ua. folgende Themengebiete der Disziplin „Physische Sicherheit" zuzuordnen sind:

© Mario & Sandro Trutzenberger 2020

Objektschutz, persönliche Sicherheit inklusive Reisesicherheit, Veranstaltungsschutz, Sabotageschutz, Schutz vor Wirtschafts- und Industriespionage.

In der Literatur finden sich verschiedene Grundsätze zur Planung physischer Sicherheitsmaßnahmen, von denen ich hier das Printip >deter – detect – delay – deny – respond< kurz betrachten möchte, es interpretiert nämlich auch das vielleicht landläufig bekanntere Zwiebelschalenprinzip. Demnach ist ein Objektschutzsystem mehrschichtig aufzubauen: eine Vielzahl von Barrieren müssen von (internen und/oder externen Tätern) überwunden werden, um zum „in der Mitte etablierten" Asset zu gelangen. Zu Beginn steht die Abschreckung, wird diese ignoriert, muss bereits die Detektion, die die Einleitung von Interventionsmaßnahmen nach sich zieht, erfolgen. Nun gilt es, das Vordringen des Täters zum Schutzgut so lange zu verzögern, bis qualifizierte Interventionskräfte den rechtswidrigen Angriff unterbinden können. Unter der vorletzten Barriere, dem „delay" wird zusätzlich zum Verzögern noch das Zurückweisen definiert, das beispielsweise durch ein Wertschutzbehältnis verwirklicht werden kann.

Als weiteres Credo im Objektschutz gilt die zwingende Kombination von baulichen, technischen, elektronischen, personellen und organisatorischen Maßnahmen. Bauliche Maßnahmen samt gleichwertigen technischen Maßnahmen, mit welchen Hüllen in der Perimeter- bzw. Objekthülle öffenbar geschlossen werden, sollen den Täter davon abhalten, auf das Gelände/in das Objekt einzudringen. Erfolgt der Versuch der Überwindung, erfolgt die Detektion und der Nachweis durch elektronische Maßnahmen. Eine elektronische Maßnahme ist auch die der Zutrittskontrolle. Durch personelle Maßnahmen sind Empfang, interne Sicherheits- und Interventionskräfte, Kontroll- und externe Interventionskräfte abgedeckt und die organisatorischen Maßnahmen legen Rollen, Verantwortlichkeiten und Prozeduren fest.

Ausgehend von dieser Basis werden durch Spezifikationen in der Physischen Sicherheit, also auch im Objektschutz, spezielle Bedürfnisse bedient, beispielsweise die Forderungen des Transportgewerbes (TAPA), des Materiellen Geheimschutzes etc.

Wir sprechen also von einem kompletten Managementsystem, zumal JEDEM Sicherheitssystem zwingend ein PDCA-Kreislauf inhärent sein muss. Insbesondere in großen Unternehmen wird dieses Managementsystem in das Security-Management System eingebunden, in kleineren Unternehmen ohne ausgeprägtes Security Management müssen teilweise wesentliche Elemente wie die Inhalte einer klassischen Security Policy odgl. vom Physischen Sicherheitssystem getragen werden.

Prozess

Objektschutzkonzepte können nach mehreren Prozessen abgearbeitet werden: beispielshaft zu nennen sind der Baustein IS 1 des deutschen Wirtschaftsgrundschutzes, der (zu überarbeitenden und ins Gesamtsystem der ÖNORM S 241x einzufügende ÖNORM S 2420, der Normenfamilie S 241x, insbesondere e S 2414-2 ... wobei in Spezialfällen Ausprägungen anderer Normen oder Forderungen zu beachten sind. SECFIRM hat im Laufe der Beraterpraxis einen Prozess entwickelt, der im Grunde alle der genannten Forderungen wiedergibt und einerseits in der Planung

© Mario & Sandro Trutzenberger 2020

als „Kochrezept“ bis in die 4. Prozessebene abgearbeitet werden kann, andererseits im Bereich der Begutachtung als Leitfaden für die Bedienung aller geforderten Elemente dient.

Zu Beginn stehen Ortsaugenschein und Assessment: hier erfolgen Klärungen des Warum und Wieso, hier wird konkretisiert, wird das Objekt in Augenschein genommen, alle vorhandenen Sicherheitseinrichtungen für (eine spätere) Beurteilung dokumentiert und Schwachstellen aufgespürt.

In Kenntnis von Auftragsumfang und -umständen stehen nun Erhebungen an, die einerseits in die Risikoanalyse einfließen, andererseits direkt in die Planung, beispielsweise die Interventionszeitberechnung, die Täterqualitäten, zu erwartende modi operandi, die Qualifizierung makro- und mikrogeographischer Gegebenheiten, Attraktivitäten, statistische Wahrscheinlichkeiten etc.

Die darauf folgende **Security Risiko-Analyse** stellt eine Spezialform der Berechnungsmethode Risiko = Eintrittswahrscheinlichkeit x Auswirkung dar und berücksichtigt eine Vielzahl von Parametern.

Im Normalfall hat man jetzt ausreichend Erkenntnisse, um mit der Planung des Systems zu beginnen. Im hier behandelten speziellen Fall wird jedoch an dieser Stelle die Machbarkeitsstudie eingezogen:

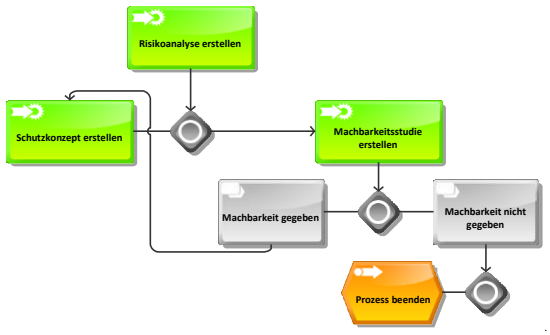

Abbildung 2 Ausschnitt Planungsprozess. Quelle: Mario Trutzenberger 2021

Anstatt in die Detailplanung zu gehen, werden die baulichen, mechanischen, elektronischen, personellen und organisatorischen Maßnahmen in jener Tiefe und jenem Detailierungsgrad dargelegt, dass es (a) einerseits möglich ist, zu überprüfen, ob mit den skizzierten Maßnahmen die Möglichkeit der Erfüllungen der Forderungen besteht und (b) eine Prognose der benötigten Ressourcen sowie (c) eines zeitlichen Horizontes ermöglicht wird.

Die vorgenannten Schritte sind für diese Machbarkeitsstudie unabdingbar.

Sie kann in 3 Ergebnissen münden:

(1) im besten Fall können die Forderungen mit den skizzierten Maßnahmen im angedachten Zeitrahmen erfüllt und die entsprechenden Ressourcen bereitgestellt werden.

(2) Kann eines der Kriterien Anforderungserfüllung, Ressourcen und Zeit nicht zufriedenstellend erfüllt werden, kann man an der Auftragsdefinition schrauben und mit geänderten Anforderungen den Prozess neu starten.

(3) Ist eine oder sind mehrere der Kriterien nicht erfüllbar, führt das zum Objektabbruch. Der Vorteil dieses frühzeitigen Abbruches liegt in einer wesentlichen Kostenersparnis im Vergleich zur „normalen“ Prozessfortführung, wo man beispielsweise erst bei der Endabnahme feststellen würde, dass die Anforderungen (z.B. von Stakeholdern) nicht erfüllt werden konnten.

Geht man von der Machbarkeit aus, erfolgt nun die Ausschreibung an erforderliche Gewerkeerrichter, die Anbotsbewertung samt Auftragsvergabe, die Gewerkeimplementierung, der Aufbau der Organisation, die Planung von Maßnahmen der Messung, Überwachung und

© Mario & Sandro Trutzenberger 2020

Aufrechterhaltung und die Implementierung des Systems in die Organisation samt Endabnahme.

Fazit

Je komplexer die Anforderungen, je stärker die Stakeholder, je umfangreicher Systeme ..., desto mehr empfiehlt sich das Einziehen einer Machbarkeitsstudie zwischen Risikoanalyse und Detailplanung, um ressourcenschonend zu überprüfen, ob und wie die gestellten Anforderungen erfüllt werden können und welcher Ressourcen und Zeitdauer die Umsetzungen bedürfen wird.

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.

Seit 16 Jahren beurteilt er im Auftrag von Versicherungen Maßnahmen des Einbruch- und Beraubungsschutzes in Objekten von Versicherungsnehmern sowohl in der Prävention als auch im Schadenfall.

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

Näheres unter https://secfirm.at

© Mario & Sandro Trutzenberger 2020