SECFIRM Security Consultants

Unternehmensberatung | Sicherheitsunternehmen | Begutachtung

Die (verkürzte) Sicht der ISO 2700X auf die Physische Sicherheit

mgr Mario Trutzenberger EMBA

Sandro M. Trutzenberger, B.Sc

Inhalt

Vorwort

Immer wieder stoßen wir in der Beratung auf die Behauptung, Maßnahmen der Physischen Sicherheit seien und gehörten gem. ISO 2700X geplant und umgesetzt, würden nach dieser Norm auditiert und der Ansprechpartner im Unternehmen bzgl. Physischer Sicherheit sei selbstverständlich der Chief Information Security Officer (CISO). Eben so oft stoßen wir auf Reaktionen von Unverständnis bis Ablehnung, wenn wir ins Treffen führen, dass die ISO 2700X die Informationssicherheit behandle, die Physische Sicherheit nur unter dem Aspekt der Informationssicherheit sehe und die Betrachtungsweise und Bedeutung entsprechend verkürze.

Interessanterweise werden von Klienten auch Sicherheitskonzepte ehemaliger Sicherheitsberater vorgelegt, die Objektschutzmaßnahmen ausschließlich unter dem Blickwinkel der ISO 2700X geplant und verkauft haben, obwohl nicht nur Informationen, sondern Gebäude, technische Anlagen, Güter... teils hoher Kritikalität auftragsgemäß zu schützen waren.

Welche Normen also heranziehen zur Planung und Beurteilung Physischer Schutzmaßnahmen bzw. von Maßnahmen des Schutzes von Objekten gegen intentionale Bedrohungen? Deckt die ISO 2700X alle Bedürfnisse pcto. Objektschutzmaßnahmen ab? Wie und unter welchem Blickwinkel sieht sie die Physische Sicherheit? Oder gibt es probatere Normen?

Was ist eigentlich „Physische Sicherheit", was ist „Objektschutz"?

Bereits hier scheiden sich Geister, Kulturen und Definitionen. Während im deutschen Sprachgebrauch „Security" und „Safety" in einem Begriff, der „Sicherheit" zusammengefasst werden, meint der englische Begriff „Security" die Sicherheit/den Schutz vor intentionalen, also de facto „kriminellen" Angriffen, „Safety" die Sicherheit in Bezug nicht intentionalen Gefahren, also beispielsweise vor Naturgefahren, Umweltgefahren, Gefahren, die von technischen Anlagen und Maschinen ausgehen etc. Während also der englische Begriff „Physical Security" (in der Literatur meist auf den Punkt gebracht als „Physical Protection" bezeichnet) physische Schutzmaßnahmen vor intentionalen/kriminellen Bedrohungen meint, finden sich im deutschen Sprachgebrauch unter der Überschrift „Physische Sicherheit" auch Schutzmaßnahmen gegen beispielsweise Hochwasser, Lawinen, Muren und sonstige Umweltgefahren. Selbiges gilt für den Begriff „Objektschutz": im Englischen als „Physical Protection" aber auch „Property Protection" oder „Site Protection" bezeichnet sind klar Schutzmaßnahmen gegen intentionelle Bedrohungen gemeint, während im deutschen Sprachgebrauch auch Schutzmaßnahmen von Objekten gegen Umweltgefahren umfasst sind.

Wenn wir im Deutschen also konkretisieren wollen, sind wir auf die englischen Substantiva „Security" und „Safety" angewiesen, um klar zu trennen.

Recht viel klarer wird es auch nicht, wenn wir in die **Normung** blicken: Die ÖNORM S 2413 normiert, dass die „Physischen Sicherheit" zumindest die Domänen, Objektschutz, persönliche Sicherheit incl. Reisesicherheit, Veranstaltungsschutz, Sabotageschutz sowie der Schutz vor Wirtschafts- und Industriespionage" umfass und gem. ÖNORM S 2412 als Erhaltung der Verfügbarkeit, Vertraulichkeit und Integrität von Assets (Anm.: unter Assets sind materielle

und immaterielle Ressourcen gemeint, die einen Wert für eine Organisation haben, also nicht nur Informationen) durch Nutzung von ganzheitlichen Maßnahmen definiert ist. Vorausgeschickt ist bereits das Verständnis, dass wir uns im Begriffsfeld „Security" und nicht „Safety" befinden.

Während also der Begriff der „Informationssicherheit" vergleichsweise klar definiert ist und zusammengefasst den Schutz von Informationen – egal in welcher Form sie vorliegen oder bestehen – umfasst, scheint in die „Physische Sicherheit" all das hineingepackt zu sein, was anderen Disziplinen der Security schwer zuordenbar ist.

Objektschutz (in der Norm konkretisiert als „gem. ÖNORM S 2420") ist der angesprochenen Norm zufolge die Gesamtheit aller technischen, organisatorischen und personellen Maßnahmen, die erforderlich sind, um ein Objekt mit den darin befindlichen körperlichen Sachen zu schützen, wobei der Schutz von Personen in diesen Objekten miteinbezogen wird.

Persönliche Sicherheit incl. Reisesicherheit scheint die Begriffe „Personenschutz" und den Personenschutz auf Reisen, gemeinhin „Travel Security" genannt, abzudecken. Beides eigenständige Disziplinen, die hohe Spezialisierung und einschlägiges Know-how, sowohl in der strategischen Planung als auch der operativen Durchführung voraussetzen.

Veranstaltungsschutz beschreibt die in Zusammenhang mit Veranstaltungen stehenden Sicherheitsmaßnahmen, also den Schutz der Veranstaltungsstätte (also Objektschutz) sowie der beteiligten Personen wie Künstler, Personal und Besucher (also Personenschutz) und den Schutz der Veranstaltung selbst, also die Sicherstellung des ungestörten und sicheren Ablaufs. Erneut eine hochspezialisierte Disziplin mit vielen Facetten, die wiederum enormes Know-how sowohl in der Planung als auch der operativen Umsetzung verlangt.

Sabotageschutz wird in den Begriffsbestimmungen der ÖNORM S 2412 eben so wenig definiert wie „Veranstaltungsschutz". Die Encyclopedia Britannica definiert „Sabotage" als „vorsätzliche Zerstörung von Eigentum oder Verlangsamung der Arbeit mit der Absicht, ein Unternehmen oder Wirtschaftssystem zu schädigen oder eine Regierung oder Nation in einer Zeit des nationalen Notstands zu schwächen". Im Duden ist Sabotage als „absichtliche [planmäßige] Beeinträchtigung der Leistungsfähigkeit politischer, militärischer oder wirtschaftlicher Einrichtungen durch [passiven] Widerstand, Störung des Arbeitsablaufs oder Beschädigung und Zerstörung von Anlagen, Maschinen o. Ä." definiert, das Österreichische StGB kennt den Begriff der Sabotage nur im § 260-Wehrmittelsabotage. Auf die Wirtschaft umgelegt ist also davon auszugehen, dass unter „Sabotage" aktives oder passives Tun mit dem Ziel verstanden wird, um einer Organisation Schaden zuzufügen. Anbetrachts der beiden zuvor zitierten Definitionen kann der Schaden also durch organisatorisches Tun oder Unterlassen (beispielsweise Arbeitsverlangsamung, Arbeitsverweigerung, bewusst fehlerhafte Arbeitsleistung) oder durch die Schädigung von Arbeitsmitteln wie beispielsweise Maschinen) herbeigeführt werden. Erneut eine hochkomplexe Materie, der mit Sicherheit nicht nur durch physische Schutzmaßnahmen zu begegnen ist, sondern ua. durch Aufklärung eines potentiellen Gegenüber, Pre-Employment-Screening, Maßnahmensetzung im Bereich der Mitarbeiterzufriedenheit ... aber auch in der physischen Verhinderung einer Schadenverwirklichung.

Und zuletzt der **Schutz vor Wirtschafts- und Industriespionage**, also das Auskundschaften von Geschäfts- und Betriebsgeheimnissen durch Mitbewerber oder Gegner oder Nachrichtendienste. Auch hier wird sofort klar, dass das nicht nur durch Maßnahmen der klassischen „Physischen Sicherheit" verhindert werden kann, sondern einen in hoher Fachkenntnis und Expertise verbundenen Mix aus Informationssicherheit in all ihren Ausprägungen, Sensibilisierungs- und Awarenessmaßnahmen, Aufklärungs- und Abwehrmaßnahmen und auch Maßnahmen der Physischen Sicherheit bedingt.

Also mit der Norm können wir die Frage nicht (zufriedenstellend) beantworten.

Versuchen wir es mit anderen Quellen:

Die US Army definiert „Physical Security" als Beschreibung von Sicherheitsmaßnahmen, die darauf ausgelegt sind, unbefugten Zugang zu Einrichtungen, Geräten und Ressourcen zu verweigern/verhindern und Personal und Eigentum vor Schäden oder Beeinträchtigungen (z. B. Spionage, Diebstahl oder terroristische Angriffe) zu schützen und den Einsatz mehrerer Schichten voneinander unabhängiger Systeme wie CCTV-Überwachung, Wachpersonal, Schutzbarrieren, Schlösser, Zugangskontrolle, Einbrucherkennung, Abschreckungssysteme, Brandschutz und andere Systeme zum Schutz von Personen und Eigentum umfassen kann[1]. PeidaXu ua. definieren ein Physical Protection System" als Integration von Menschen, Verfahren und Ausrüstung zum Schutz von Vermögenswerten oder Einrichtungen gegen Diebstahl Sabotage oder andere böswillige Angriffe durch Eindringlinge[2].

In der Praxis verstehen wir unter „Physischer Sicherheit" oder profaner gesagt „Maßnahmen des Objektschutzes" Maßnahmen zum Schutz von Objekten und Freigeländen samt darin befindlichen Menschen, beweglichen und unbeweglichen Sachen sowie materiellen und immateriellen Werten vor intentionalen Bedrohungen, wobei dies durch ein koordiniertes Zusammenwirken von technischen, organisatorischen und personellen Maßnahmen erreicht wird und im Wesentlichen dem Prinzip „deter – detect – delay – deny – respond" im Rahmen eines Mehrschichtmodelles folgt. Durch die erforderliche Gesamtausprägung samt PDCA kann Physische Sicherheit als eigenständiges Managementsystem in eine Organisation eingebettet oder in ein Security-Managementsystem integriert werden.

Managementnormen – Technische Normen - Gesetze

Während die Managementnormen die Fragen beantworten, wie Managementsysteme im Bereich der (Physical) Security aufzubauen, einzubetten und zu betreiben sind und wie speziell zugeschnitten auf den Bereich intentionaler Bedrohungen Risiken zu bewerten sind, gibt eine Vielzahl technischer Normen Möglichkeiten der Umsetzung konkreter Maßnahmen vor. Nur beispielhaft zu nennen sind hier Normen bzgl. des Widerstandswertes von Perimeterumfriedungen und Gebäudehüllen sowie von Verschlüssen in diesen Hüllen wie Toren, Türen, Fenstern ..., Normen bzgl. der Anforderungen an elektronische

[1] Headquarters, Department of the Army,Washington, DC, 8 January 2001, Field Manual No. 3-19.30 – Physical Security

[2] Safe Science, Volume 65, June 2014, Pages 125-137

Zutrittssysteme, Perimeterdetektionssysteme, Einbruch- und Überfallmeldeanlagen und Videoüberwachungssysteme zu Sicherheitszwecken, Normen für (Wert)schutzbehältnisse, gesetzliche und normative Vorgaben für personelle Sicherheitsdienstleistungen etc. Oftmals wirken sich Techniknormen auch auf die organisatorische Sicherheit aus, beispielsweise durch Vorgaben von Wartungen, Kontrollen, Instandhaltungsmaßnahmen udgl.

Gesetze begegnen uns als spezielle Stakeholderforderungen (ein Gesetzgeber fordert die Einhaltung von Vorschriften im Rahmen der Umsetzung von Sicherheitsmaßnahmen) und können die (Physische) Security vielfältig beeinflussen, beispielsweise als Forderungen des Arbeitnehmerschutzes (Offenhalten von Fluchtwegen, Gewährleistung von Tageslicht am Arbeitsplatz …), des Brandschutzes (Rücksichtnahme auf vorbeugenden und abwehrenden Brandschutz), des Datenschutzes (Umgang mit Daten beispielsweise in den Bereichen Videoüberwachung, Zutrittskontrolle, Besuchermanagement etc.), des Denkmalschutzes, Umweltschutzes, der Bauordnung etc. Gesetze und völkerrechtliche Vereinbarungen können aber auch dezidiert vorgeben, WIE wir Maßnahmen der Physischen Sicherheit zu planen haben, um ein angestrebtes Ziel zu erreichen, beispielsweise im Bereich des Schutzes staatlich oder völkerrechtlich klassifizierter Informationen.

Planung Physischer Sicherheit „nach dem Lehrbuch"

Nach allen Regeln der Kunst und normativen Vorgaben basiert ein Physisches Sicherheitssystem im Wesentlichen auf dem Ergebnis einer mit geeigneter Methode erstellten Risikoanalyse und gibt quasi Antwort auf die ermittelten und bewerteten Risiken zum Zweck der Senkung derselben. „Klassisch" werden die Assets ermittelt, danach in einer geeigneten Analysemethode die Risiken dargestellt und bewertet, nach Festlegung des Risikoappetits Maßnahmen zur Risikosenkung geplant und diese in einer neuerlichen Risikoanalyse bewertet, letztlich die Vorher- und Nachher-Bewertungen gegenübergestellt und die wirksamen und akzeptierten Maßnahmen im Detail geplant und so ein entsprechendes System designt. Finden diese Tätigkeiten und Planungen im Rahmen eines bestehenden Security-Management im Unternehmen statt, wird das System in dieses integriert, es kann aber auch als Stand-alone-Lösung geplant und umgesetzt werden – je nach Organisationsgröße und -bedarf (wobei sich in diesem Fall Elemente des Security-Management finden sollten/werden).

Ausschließliche Risikoabwälzung

Oftmals findet man Systeme, die de facto nichts von alledem enthalten, sondern Maßnahmen auflisten, die (lediglich) Antworten auf Stakeholderforderungen geben. Hauptsächlich ist dies dann der Fall, wenn ein Unternehmen sich nicht eigene Gedanken bzgl. des Schutzes unternehmenskritischer Werte macht bzw. den Weg der Beurteilung und Bearbeitung von Risiken geht, sondern lediglich auf Risikoabwälzung bedacht ist. In diesem Fall wendet man sich i.d.R. an einen Versicherer. Dieser hat aufgrund eigener Statistiken mögliche Risiken von Standardgewerben/Standardobjekten bewertet (und damit diese Bewertung dem Versicherungsnehmer abgenommen) und Maßnahmen festgelegt, der der Versicherungsnehmer einhalten muss, um gegen Bezahlung einer festgelegten Prämie im Schadenfall Entschädigung lukrieren zu können.

Diese Form der Risikoabwälzung wird von Versicherern i.d.R. in Bezug auf minderkritische Gewerbe/Sites bzw. geringe Deckungssummen angeboten. In Bezug auf komplexe Gewerbebetriebe/SItes, Gewerbe/SItes mit hohen Risiken oder hohen zu versichernden Werten wird meist der Weg der Individualbeurteilung gewählt: meist ermittelt ein Sachverständiger im Auftrag des Versicherers Risiken und maximale Schadenwerte und bewertet bestehende Sicherheitsmaßnahmen. Der Versicherer richtet dann Prämie und Deckungssumme nach der Qualität der bestehenden Sicherheitsmaßnahmen oder fordert risikoangemessene Sicherheitsmaßnahmen, um einen Vertrag einzugehen.

Leges speciales in der Physischen Sicherheit

Möchte eine Organisation beispielsweise staatlich klassifizierte Informationen in einem ihr gehörenden Objekt bearbeiten oder lagern, sind gesetzliche (z.B. InfoSiG, InfoSiV, Ressortvorschriften ...) oder bi- bzw. multilaterale Vorgaben (EU-Vorschriften, NATO-Vorschriften ...) umzusetzen, je nachdem, welche Informationen in welcher Klassifizierungsstufe in welcher Form gelagert und verarbeitet werden sollen. Auch in diesem Bereich müssen Stakeholderforderungen umgesetzt werden und sind der Freiheit in der Risikobehandlung gewisse Grenzen durch den Stakeholder gesetzt. Derartige Forderungen sind jedoch i.d.R. von hoher Güte und setzen (zumindest teilweise) die Anwendung von anerkannten Methoden (z.B. in Bezug auf die Risikoanalyse und die Risikobehandlung) und die Umsetzung von Maßnahmen anhand anerkannter Normen voraus, da ein hohes Maß an Überprüfbarkeit, Nachvollziehbarkeit und Auditierbarkeit gefordert ist. Aus diesem Grund kann man derartige Systeme durchaus „Mischsysteme“ nennen: ein oder mehrere Stakeholder geben vor, welche Methoden der Risikoidentifikation und -behandlung sie akzeptieren; dies bedingt vom Designer des Systems profunde Kenntnis der einschlägigen Literatur, Normung, Methodik und Technik sowie der spezialgesetzlichen Grundlagen.

Anzuwendende Managementnormen in der Physischen Sicherheit

Seit 2013 steht die ÖNORM S 2420 zur Planung Physischer Sicherheitsmaßnahmen zur Verfügung, seit 2017/2018 gibt die ÖNORM-Serie S 2412 ff den Stand der Wissenschaft wider. Vor 2013 standen neben ausländischen, z.B. deutschen, Normen insbesondere die Risikomanagementnormen zur Verfügung, um daraus Ableitungen für die Physische Sicherheit treffen zu können.

Anzuwendende technische Normen in der Physischen Sicherheit

Seit den 1980er Jahren bestehen in Österreich und Deutschland eine Vielzahl von Normen im Bereich der Sicherheitstechnik. Neben Vorgaben von Vereinen wie dem Österreichischen VSÖ – Verband der Sicherheitsunternehmen oder Verbänden wie dem Deutschen VdS - Verband der Sachversicherer standen ÖNORMEN und DIN-Normen, später dann Europanormen zur Verfügung. Technisch ist de facto jedes sicherheitsrelevante Gewerk normativ geregelt, beispielsweise Widerstandswerte von Verglasung, Fenstern, Türen ... gegen manuelle Einbruchversuche, Angriffe mit Schusswaffen und Sprengmitteln, Schlösser und Beschläge, Schutzbehältnisse und -räume, Zäune, bauliche Hüllen etc. Im elektronischen Bereich bestehen detaillierte Regelungen für die Planung und den Betrieb von Einbruch- und

Überfallmeldeanlagen, Videoüberwachungsanlagen, Zutrittskontrollanlagen … und das alles entweder als Vorgaben von Vereinen (VSÖ, siehe oben) oder Verbänden (VdS, siehe oben), der nationalen Normung sowie der Europäischen Normung … In Österreich bedient man sich bei der Planung von Zutrittskontrollanlagen, Videoüberwachungsanlagen und Einbruch- sowie Überfallmeldeanlagen hauptsächlich der VSÖ-Richtlinien (VSÖ – Österreichischer Verband für Elektrotechnik) R2 (Einbruch- und Überfallmeldeanlagen), R9 (Zutrittskontrollanlagen) und R10 (Zutrittskontrollanlagen). Diese Richtlinien beziehen sich auf die einschlägige Europanormierung und geben deren Forderungen wider.

Insbesondere die OVE-Richtlinien R2, R9 und R10 fordern neben detaillierter Planungsvorgaben und Definition von Risikoklassen (bzw. Szenarien in Bezug auf die Videoüberwachung), dass jede Sicherheitsanlage auf einem Schutzkonzept basieren muss und ein Zusammenwirken mechanischer und elektronischer Schutzmaßnahmen zu planen ist. Zudem ist gefordert, dass das Schutzkonzept neben den elektronischen auch bauliche/mechanische und organisatorische Sicherheitsmaßnahmen zu umfassen hat.

Die ISO 2700X und die Physische Sicherheit

Wie anfangs erwähnt werden in nicht wenigen auch großen Unternehmen Spezialdisziplinen wie Corporate Security, Security Management, Business Continuity, Physische Sicherheit … durch den CISO betrieben und im Rahmen der ISO 2700X „abgearbeitet".

Die ISO 2700X führt den Titel „Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme". Die ISO 27000 definiert „Informationssicherheit" als die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Informationen sind gem. zit. Norm Werte, die wie andere wichtige Wirtschaftsgüter für den Geschäftsbetrieb einer Organisation entscheidend sind und infolgedessen angemessen zu schützen sind und können in digitaler, materieller und nicht-materieller Form vorliegen.

Die ISO 2700X-Familie ist also für den Schutz von Informationen „zuständig".

Betrachtet man den Schutz von Informationen aus Sicht des umfassenden Security-Management, werden die bisher autark betriebenen Teilbereiche Informationssicherheit, Physische Sicherheit und Resilienzmanagement zu einem Security-Managementsystem vereint (ÖNORM S 2413). Die Informationssicherheit umfasst dabei die Themenbereiche Informationsschutz gem. ISO 27001, Know-how-Schutz, IKT/Cyber Security und die IT-Produktsicherheit.

Abbildung 1 Quelle: ÖNORM S 2413

Sowohl durch die Definitionen in der ISO 27000 als auch der ÖNORM S 2413 belegen also deutlich, dass die ISO 2700X-Famile den Schutz von Informationen adressiert, und bei weitem nicht das gesamte Feld der Security abdeckt.

Die ISO 27001 definiert Anforderungen an den Informationsschutz und bietet im Anhang A Maßnahmen und Maßnahmenziele, die bei der Informationssicherheitsrisikobehandlung zu berücksichtigen sind. Darunter finden sich unter A.11. Maßnahmen zur physischen und umgebungsbezogenen Sicherheit, wobei hier Maßnahmen gegen intentionale Bedrohungen mit Maßnahmen gegen Umweltgefahren sowie der Sicherstellung der Energieversorgung und Sicherheit der Verkabelung in kurzen Schlagworten erwähnt werden. Da eine Legaldefinition für den Begriff der Physischen Sicherheit in der ISO 27000 fehlt, ist nunmehr davon auszugehen, dass die „Physische Sicherheit" in der Normenfamilie durch die unter A.11. zusammengefassten Maßnahmen definiert ist.

In der ISO 27002, dem „Leitfaden für Informationssicherheitsmaßnahmen" widmet sich Kap. 11 der physischen und umgebungsbezogenen Sicherheit. Als Ziele werden

- die Verhinderung unbefugten Zutritts sowie der Beschädigung und Beeinträchtigung von Informationen und informationsverarbeitenden Einrichtungen der Organisation und
- die Unterbindung von Verlust, Beschädigung, Diebstahl oder Gefährdung von Werten und die Unterbrechung der Organisationstätigkeiten

genannt. Umgesetzt werden diese Ziele durch

- Physische Sicherheitsperimeter
- Physische Zutrittssteuerung
- Sicherung von Büros, Räumen und Einrichtungen
- Schutz vor externen umweltbedingten Einflüssen
- Schutz bei Arbeiten in Sicherheitsbereichen
- Maßnahmen bei Anlieferungs- und Ladebereichen
- die geeignete Platzierung und der Schutz von Geräten und Betriebsmitteln
- Schutz von Geräten und Betriebsmittels vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden
- Sicherheit der Verkabelung
- Instandhaltung von Geräten und Betriebsmitteln
- Schutz vor Entfernung von Geräten, Betriebsmitteln, Informationen oder Software vom Betriebsgelände
- Schutz von Einrichtungen zur Speicherung und Verarbeitung von Informationen außerhalb von Betriebsgebäuden
- Sichere Entsorgung oder Wiederverwertung von Geräten und Betriebsmitteln die Speichermedien enthalten
- Schutz von unbeaufsichtigten Benutzergeräten
- Richtlinien für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern...

Der oft verwendete Begriff „Betriebsmittel" ist in der ISO 27000 nicht definiert, aus dem Text geht jedoch hervor, dass es

sich um Ressourcen handelt, die der Informationsverarbeitung dienen. Demnach handelt es sich nicht pauschal um „grundsätzlich alle Unternehmensressourcen".

Kann mit der ISO 2700X-Familie der gesamte Security-Bedarf einer Organisation abgedeckt werden?

Unternehmen, die ihren gesamten Securitybedarf nach der ISO 2700X-Familie „abdecken", jedoch neben Informationen auch andere schützenswerte Güter haben (das ist zumindest die Facility, meist zudem Maschinen, Anlagen, Betriebsmittel, Werte und selbstverständlich auch Menschen) argumentieren oftmals, dass das, was zum Schutz von Informationen gut genug ist, auch für den Schutz aller anderen Unternehmenswerte gut genug sein muss. Diese Argumentation scheint mehrere Ursachen zu haben:

1. Informationen werden gegenüber anderen schützenswerten Unternehmenswerten überbewertet
2. Die ISO 2700X-Familie wird fälschlicherweise als Kochrezept für den Schutz von nicht nur Informationen, sondern „eh Allem" interpretiert
3. Es besteht Unkenntnis über methodisches Security-Management
4. Man hat mit der Informationssicherheit ohnehin schon eine „Sicherheits"funktion im Unternehmen: wer für eine Sicherheit zuständig ist, kann „eh alles" schützen
5. Die Informationssicherheit gem. ISO 2700X ist extrem auditgetrieben; mit jedem Audit kann man „was vorlegen/herzeigen". Und schließlich kommen in den Audits auch Bewertungen von Termini wie Business Continuity und Physische Sicherheit vor.
6. ...

Wo aber liegen mögliche Schwierigkeiten und Unzulänglichkeiten, wenn die gesamte Unternehmenssecurity versucht wird nach ISO 2700X abzuarbeiten? Eine der Antworten darauf geben uns die verschiedenen Personenzertifizierungen für ISMS-Manager & -Auditor nach ISO 27001, aber auch die ÖNORM S 2415-2: Anforderungen an die Qualifikation eines Security-Managers. Während die Zertifizierung nach ISO 27001 logisch auf Informationssicherheit abzielt und beschränkt ist, werden vom Security-Manager neben Prozess- und Integrationskenntnissen des gesamten Security-Management die Kenntnisse der Spezifika der Security-Risikobeurteilungen und Business-Impact-Analyse sowie die Methoden der Security-Risikobehandlung, Ereignisbewältigung und Maßnahmensteuerung in allen 3 großen Domänen nachgewiesen: Informationssicherheit + Resilienzmanagement + Physical Security!

Auch das Personenzertifizierungsschema (und das Organisationszertifizierungsschema gem. ÖNORM S 2415-1) zeigt deutlich, dass die Informationssicherheit lediglich EIN Bestandteil der Unternehmenssicherheit (-security) ist, nicht der EINZIGE.

Die (verkürzte) Sicht der ISO 2700X auf die Physische Sicherheit. Fazit

Maßnahmen, die geeignet sind, Informationen und Ressourcen für Informationen zu schützen, sind nicht zwingend geeignet, andere Unternehmenswerte in geeigneter Weise mit der gebotenen Effizienz zu schützen. Maßnahmen der Risikoanalyse, -bewertung und -behandlung, die für Informationsrisiken probat sind, sind nicht zwingend geeignet für alle anderen Security-Risiken.

Wie jede der Security-Disziplinen fordern sowohl die Informationssicherheit als auch die Physische Sicherheit ein breites Spektrum an spezifischer Fachkenntnis. Neben den jeweiligen Spezifika der einzelnen Managementsysteme sind die Spezifika der Risikoanalysen und -behandlungen zu nennen, zudem jeweils umfangreiche Kenntnisse des eigenen normativen und gesetzlichen Umfeldes.

Die Physische Sicherheit ist mit eine der Basen für ua. den Aufbau der Informationssicherheit: meist befinden sich Informationen (in welcher Form auch immer) in Objekten. Während die ISO 27001 und 27002 entsprechende Schutzmaßnahmen zu Recht fordern, weiß die Physische Sicherheit, wie diese Maßnahmen lege artis zu gestalten sind, hat die Methode für Planung, Gestaltung, Implementierung und Aufrechterhaltung der physischen Sicherheitsmaßnahmen und zur Messung der Effizienz. Zusätzlich kann die Physische Sicherheit auch andere Unternehmenswerte adäquat schützen, nicht nur Informationen. Anders gesagt und auf die Beziehung der Informationssicherheit zur Physischen Sicherheit bezogen: die Informationssicherheit fordert ua. Perimeterschutzmaßnahmen, Maßnahmen der Zutrittskontrolle und -beschränkung etc., die Physische Sicherheit weiß, wie diese Maßnahmen zu gestalten sind.

Meint man also, die Physische Sicherheit sei durch die ISO 2700X (ausreichend) bedient, so ist festzustellen, dass die ISO 27001 und 27002 Forderungen an die Physische Sicherheit stellen, die die Informationssicherheit und nicht mehr betreffen. Will man die Forderungen lege artis umsetzen und ggf. noch andere Unternehmenswerte als nur Informationen schützen, bedarf es der Expertise der Physischen Sicherheit.

Das eigentliche Fazit: wenn jede Funktion in der Security sich richtig ein- (und nicht über-) schätzt und jede ihre Expertise beisteuert … erst dann wird's gut.

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 ua. im Auftrag von Versicherungen Maßnahmen der Physischen Sicherheit sowohl in der Prävention als auch im Schadenfall.

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

Näheres unter https://secfirm.at