SECFIRM Security Consultants

Unternehmensberatung | Sicherheitsunternehmen | Begutachtung

Das Need-to-know in der (Physischen) Sicherheit

mgr Mario Trutzenberger EMBA

Sandro M. Trutzenberger, B.Sc

Inhalt

Vorwort

Wer muss was wissen? Wer muss wieviel wissen? Wer muss alles wissen? Welches Wissen/welche Informationen ist überhaupt sicherheitsrelevant? Wie ist der Zugang zu diesem Wissen geregelt? Wird unterschieden, wer Zugang zu welchen Daten haben muss und wenn ja nach welchen Kriterien?

Diese Fragen könnte man fortsetzen. Sicher noch eine Zeit lang. Und bei jeder Beratung, in jedem zu beurteilenden Sicherheitssystem stellen sich diese Fragen, teils unter anderen, spezifischen Aspekten.

Dieses Papier will sich nicht damit auseinandersetzen, zu welchen schützenswerten Unternehmensinformationen, zu welchen Assets der Zugang aus Sicherheitsgründen zu beschränken ist – das muss nämlich in den Sicherheitskonzepten entsprechend geregelt sein und wird i.d.R. im Einvernehmen mit der InfoSec gestaltet. Hier stellen wir uns vielmehr die Frage, welche Teile der Sicherheitskonzepte, insbesondere des Physischen Sicherheitskonzeptes, schützenswert sind und deshalb zugangsrestriktiv zu behandeln sind. Es geht also um den Schutz der Sicherheitsmaßnahen selbst.

Dieses Papier will auch nicht die Informationssicherheit neu erfinden oder interpretieren, sondern lediglich aus der Erfahrung darauf hinweisen, dass die Sicherheit von Sicherheitskonzepten oftmals zu sorglos gehandhabt wird und Physical-Security-Verantwortliche und -Planer, die nicht gleichzeitig auch Informationsschützer sind darauf hinweisen, was bedacht werden könnte …

Das Physische Sicherheitskonzept

Für die weitere Betrachtung wird davon ausgegangen, dass Security-Konzepte grundsätzlich – auf den kleinsten gemeinsamen Nenner gebracht – adäquate Antworten auf erkannte und bewertete Risiken unter Einbeziehung von Stakeholderforderungen zum Schutz definierter Assets in einem dem Risikoappetit angemessenen Ausmaß geben sollen. Physische Sicherheitskonzepte bedürfen der Transparenz in der Herleitung und im Design, anderenfalls die Maßnahmen nicht (ausreichend) mess- und bewertbar, überprüf- und auditierbar und i.S.e. PDCA aufrechtzuerhalten sind.

Um Physische Sicherheitskonzepte entsprechend transparent und nachvollziehbar, lege artis, zu gestalten, können diverse Normen herangezogen werden.

Das Need-to-know-Prinzip

Die Geheischutzvorschrift des BMLV definiert das Need-to-know-Prinzip in der Art, dass Personen neben anderen Voraussetzungen Zugang zu klassifizierten Informationen nur gewährt werden darf, wenn und solange das für die Erfüllung ihrer dienstlichen Aufgaben erforderlich ist[1]. Die Grundlage für diese Definition findet sich in § 3 InfoSiG bzw. § 5 InfoSiV.

Die Informationssicherheit kennt das Least-Privilege-Prinzip (PoLP): Demnach sollte jedes Programm und jeder Benutzer eines IT-Systems mit der geringsten Menge an Privilegien arbeiten, die zur Ausführung der Aufgabe erforderlich sind, wobei die militärische Sicherheitsregel des

[1] BMLV, S90619/1-SI/2011, RN 10

"Need-to-know" als Beispiel für dieses Prinzip genannt wird[2].

Die RICHTLINIE (EU) 2016/943 des Europäischen Parlamentes und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung normiert für das Handling von Geschäftsgeheimnissen durch Gerichte, dass der Zugang zu von Parteien oder Dritten vorgelegten Dokumenten, die Geschäftsgeheimnisse oder angebliche Geschäftsgeheimnisse enthalten, ganz oder teilweise auf eine begrenzte Anzahl von Personen zu beschränken ist (Art. 8).

Zusammengefasst bedeutet das Need-to-know-Prinzip, dass (sensible) Informationen nur dann und insoweit zugänglich gemacht werden sollen, wenn (a) die Kenntnis derselben für eine Aufgabenerfüllung notwendig ist und (b) solange dies notwendig ist.

Der Staat verbindet das Need-to-know-Prinzip in Bezug auf den Zugang zu klassifizierten Informationen mit weiteren Und-Verknüpfungen wie entsprechende Verlässlichkeits- oder Sicherheitsüberprüfungen der in Frage kommenden Personen sowie Unterweisungen und hinterlegt das Prinzip mit Klassifizierungsschemata, Regeln für die Lagerung, die Erstellung, Einsichtnahme, Bearbeitung, Vervielfältigung, Vernichtung, Weitergabe und den Transport derartiger zugangsbeschränkter Informationen.

Auf den Bereich der (Physical) Security (in Bezug auf Sicherheitskonzepte und -maßnahmen) umgelegt bedeutet das, dass vorerst einmal zu definieren sein wird, (a) welche Informationen genau sensibel und einer Zugangsbeschränkung zu unterwerfen sind (b) welche Personen auf einzelne (möglichst kleinteilig gesplittete) Informationen Zugang haben müssen, wie lange dieser Zugang für die notwendige Aufgabenerfüllung gewährt werden muss und (c) wie diese Informationen zu handlen und verwahren sind, um den derart restriktiven Zugang auch zu gewährleisten.

Schützenswerte Informationen im Sicherheitskonzept

An dieser Stelle sei nochmals darauf hingewiesen, dass hier die Rede vom Schutz der Schutzmaßnahmen ist, also die Schutz- und Sicherheitsmaßnahmen selbst als Asset gesehen werden. Da das Schutzkonzept und die Schutzmaßnahmen definierte Unternehmenswerte schützen sollen, wird der konzipierte Schutzstandard in seiner Wirksamkeit minimiert oder nivelliert, wenn die Schutzmaßnahmen teilweise oder ganz kompromittiert werden. Mit jedem Mehr an Wissen über die Maßnahmen zum Schutz von Assets steigt die Gefahr der Angreifbarkeit, des Wirkungs- oder Totalverlustes dieses wertvollen Wissens.

Wir verwenden im Unternehmen zur Planung und Beurteilung von Physischen Schutzsystemen einen selbst entwickelten Prozess, der allen einschlägigen Normforderungen gerecht wird, der Systemplanungslogik folgt und ohne Unterschied in Bezug auf Organisationsgröße und Assetkritikalität anwendbar ist. Anhand dieses Prozesses werden wir die

[2] Saltzer, J. H. & Schroeder, M. D. "The Protection of Information in Computer Systems," 1278-1308. Proceedings of the IEEE 63, 9 (September 1975)

Schutzwürdigkeit einzelner Informationen im Sicherheitssystem diskutieren.

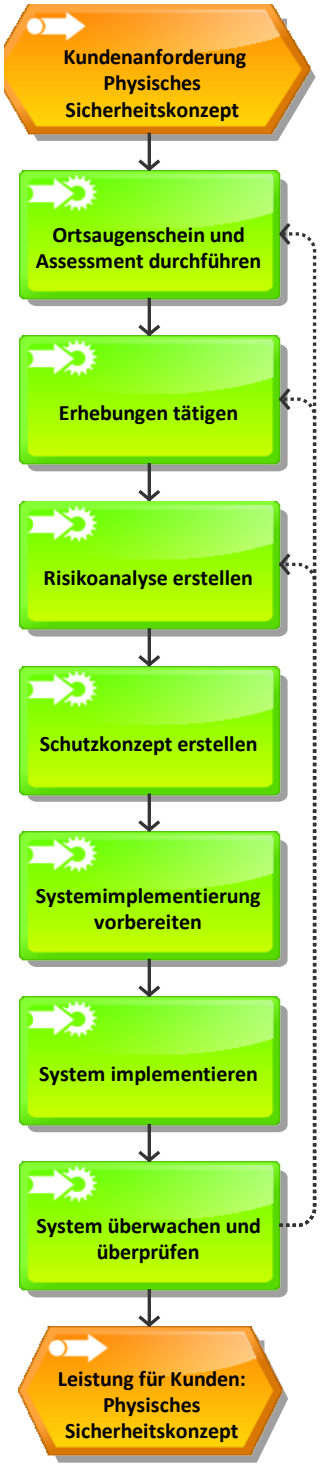

Abbildung 1 Eigene Darstellung

Ortsaugenschein und Assessment

Im Ortsaugenschein wird eine Site an sich inclusive all ihrer Sicherheitseinrichtungen aber auch Sicherheitslücken dokumentiert, im Assessment wird alles erfasst, was zum Verstehen der Organisation, zum Funktionieren der Site und zum Verstehen der Abläufe und Assets dient. Am Ende dieses Prozessschrittes steht eine umfassende und penible Dokumentation des Unternehmens bzw. des Standortes, die als Basis für die gesamte weitere Planung dient. Diese Dokumentation des status quo offenbart somit in strukturierter Form alle Sicherheitseinrichtungen samt deren Effizienz oder Nicht-Effizienz und legt für die Sicherheit wesentliche Abläufe und wesentliches Organisationswissen offen. Selbstredend ist dieses Dokument vor unbefugter Einsicht- und Kenntnisnahme zu schützen und der Kreis der Zugangsberechtigten auf das Notwendigste zu beschränken. In Frage für ein Need-to-know kommen neben der den Ortsaugenschein und das Assessment durchführenden/leitenden Person allenfalls unternehmensinterne Personen, die in Security- und Facilitymanagement entsprechende Aufgaben und Verantwortungen haben.

Erhebungen tätigen

In diesem Schritt erheben wir Faktoren, die später z.T. in die Security-Risikoanalyse einfließen, aus denen die Interventionszeit berechnet wird, die Schlüsse auf das potenzielle Gegenüber, dessen Fähigkeiten, mögliche modi operandi … zulassen. Diese Datensammlung enthält ua. Bewertungen von allgemein zugänglichen Informationen. Klar ist, dass die aus allgemein zugänglichen Quellen stammenden Informationen alleine keine Zugangsbeschränkung rechtfertigen. Sensibel ist jedoch die Interventionszeitanalyse, in der eine zeitliche

Näherung für die Dauer der Heranführung qualifizierter Interventionskräfte dargelegt wird, wobei dieser Zeitfaktor sich unmittelbar auf die Qualität baulicher und mechanischer Widerstandswerte im Perimeter, der Objektaußenhülle und allfälliger Zonenhüllen auswirkt und die Interaktion mit insbesondere elektronischen Maßnahmen bedingt. Diese Interventionszeitanalyse ist daher als sensibles Wissen einer Zugangsrestriktion zu unterwerfen. Beinhaltet dieser Prozessschritt auch die Darlegung spezifischen Wissens, beispielsweise mögliche spezifische modi operandi betreffend, die öffentlich (noch) nicht (voll)umfänglich zugänglich sind, sind auch die diese Informationen enthaltenden Schriftstücke einer Zugangsbeschränkung zu unterwerfen, da diese Informationen ggf. auch anleitenden Charakter haben könnten.

Risikoanalyse erstellen

Eine mit angemessener Methode durchgeführte Security-Risikoanalyse beinhaltet alle zu schützenden Assets, stellt Täterqualitäten und -fähigkeiten sowie mögliche Angriffsszenarien dar, bewertet mögliche Auswirkungen von Angriffen auf die Organisation unter dem Aspekt des status quo der Schutzmaßnahmen und beinhaltet eine Risiko-Neubewertung unter Betrachtung der Implementierung spezifischer Maßnahmen.

Da diese Analyse (a) alle Verwundbarkeiten im status quo, (b) alle denkbaren Angriffsszenarien, (c) die Auswirkung von Angriffen auf Assets auf die Organisation, (d) die zur Implementierung angedachten Maßnahmen sowie (e) die Neubewertung der Risiken nach Maßnahmenimplementierung darlegt, ist die Security-Risikoanalyse als sensibel zu qualifizieren und jedenfalls zugangszubeschränken. Für ein Need-to-know kommt neben der erstellenden Person maximal die in der Organisation securityverantwortliche Person, die zu implementierende Maßnahmen verantworten und deren Finanzierung sicherstellen muss, in Frage. Teileinheiten wie Facilitymanagement etc. werden kein Need-to-know haben alle Details zu kennen. Besteht der Bedarf, die identifizierten Risiken und die angedachten Maßnahmen zur Risikosenkung mehreren Personen vorzustellen, um beispielsweise eine Freigabe für die Maßnahmenumsetzung und Bereitstellung benötigter Ressourcen, oder auch nur Awareness zu erreichen, wird zu überlegen sein, was von der Risikoanalyse man in welchem Detaillierungsgrad offenlegen muss, um das angestrebte Ziel zu erreichen.

Schutzkonzept erstellen

Im Schutzkonzept werden nun alle in der Security-Risikoanalyse behandelten Maßnahmen, die aufgrund einer entsprechenden Fähigkeit zur Risikominimierung umgesetzt werden, detailliert. Dargelegt werden die baulichen, mechanischen, elektronischen, personellen und organisatorischen Sicherheitsmaßnahmen und deren Abstimmung und Zusammenwirken, dargelegt wird, wie beispielsweise anerkannte Prinzipien wie > deter – detect – delay – deny – respond < oder Mehrschalenprinzipien umgesetzt werden, festgelegt werden Rollen und Verantwortlichkeiten, die Implementierung des Systems in die Organisation sowie Maßnahmen der Effizienzmessung, der Aufrechterhaltung von Funktionalität und Angemessenheit sowie der ständigen Verbesserung.

Selbstverständlich ist dieses Konvolut an sensiblen Informationen vor unbefugter Kenntnis zu schützen. Hier sind aber entsprechende Unterscheidungen zu treffen.

Zum einen stellt sich die Frage, wer das Gesamtkonzept kennen muss, da dies in hohem Detaillierungsgrad die Einzelmaßnahmen und die Maßnahmenabstimmung preisgibt. Weiters stellt sich die Frage, wer in welcher Tiefe Kenntnis haben muss. Zudem wird zu klären sein, wer welchen Teil des Gesamtkonzepts in welcher Tiefe kennen muss, um seine Aufgaben erfüllen zu können. All diese Fragen bzw. viele von ihnen sind jeweils organisationsspezifisch zu sehen und zu beantworten. Vieles kann im Konzept selbst über Rollen und Verantwortlichkeiten gesteuert werden.

Das vollumfängliche Gesamtkonzept sollte neben der erstellenden Person wieder nur die im Unternehmen sicherheitsverantwortliche Peron kennen. Für jede Funktion/Person, die (Teil)kenntnis des Konzepts haben muss, ist festzulegen, welche Information diese Person/Funktion zur jeweiligen Aufgabenerfüllung benötigt und in welcher Tiefe sie es benötigt. Dadurch kann das Erfordernis bestehen, das im Gesamtkonzept enthaltene Know-how (a) entsprechend zu splitten und (b) hinsichtlich der Tiefe anzupassen. Wird beispielsweise ein Konzept Personen in Governance-Funktion vorgestellt mit dem Ziel der Entscheidung, die Maßnahmen umzusetzen und dafür Ressourcen bereitzustellen, besteht nicht die Notwendigkeit, alle Maßnahmen samt Herleitung in hohem Detaillierungsgrad zu präsentieren, d.h., das gesamte System in vollumfänglicher Planungs- und Gestaltungstiefe darzulegen, sondern wird es reichen eine Tiefe zu finden, die nicht alle Herleitungen und Details offenlegt, aber zur Entscheidungsfindung erforderlich ist. Zudem ist zu überprüfen, wer alles für eine entsprechende Entscheidungsfindung erforderlich ist und sicherzustellen, dass die Personen sich der Sensibilität der Informationen bewusst sind und die erhaltenen Informationen sensibilitätsangemessen handhaben. Hier gilt es jedenfalls sowohl im Splitting als auch der Tiefengestaltung das notwendige Maß der Reduktion zu finden und umzusetzen und diese Maßnahmen auch begründen und rechtfertigen zu können.

Systemimplementierung vorbereiten

Wurde übereingekommen, das Konzept umzusetzen, folgt die Suche nach passenden Gewerkeerrichtern und Dlenstleistern, die Festlegung von Zielen und Zwischenzielen auch zeitlicher Natur und letztendlich die Ausschreibung der erforderlichen Fremdleistungen, die Anbotsbewertung und die Beauftragung.

In diesem Bereich manifestiert sich das Need-to-know vorerst einmal im Informationssplitting: das Bauunternehmen muss nur die von ihm zu erbringenden Leistungen kennen, keinesfalls Leistungen, die von anderen Unternehmen zu erbringen sind und i.d.R. nicht den Grund der umzusetzenden Maßnahmen. Anforderungen an die Baugewerke sind von anderen Gewerkeerrichtern bekanntzugeben und entsprechend umzusetzen. Der Alarmanlagenerrichter muss nicht die Maßnahmen der baulich/mechanischen Gewerkeerrichter kennen (ausgenommen jene, die ihn unmittelbar in seiner Aufgabenerfüllung treffen) und ebenso nicht Maßnahmen der organisatorischen und personellen Sicherheit und Funktionsweisen anderer elektronischen Gewerke (wiederum ausgenommen jene, die sie in ihrer Aufgabenerfüllung unmittelbar tangieren). Ebenso muss der personelle Sicherheitsdienstleister bauliche, mechanische, elektronische und organisatorische Sicherheitsmaßnahmen nur soweit kennen, als sie seine Aufgabenerfüllung unmittelbar beeinflussen.

Somit darf – will man ein vernünftiges Need-to-know wahren – keinesfalls (wie leider oft festgestellt) das gesamte Sicherheitskonzept der Einladung zur Anbotslegung beigelegt werden, denn 90% der enthaltenen Informationen werden den einzelnen Adressaten nicht berühren.

Da nun sensible Informationen den engsten Kreis (Planer und erforderliche Funktionen in der Organisation) verlassen, sind zudem Anforderungen in Bezug auf Verwahrung, Verschwiegenheit, Weitergabe, Vervielfältigung, Transport, Vernichtung … an jenen Personenkreis zu definieren, dem Informationen zur Anbotsgestaltung übergeben werden. Zudem wird es ratsam sein, vom Informationsempfänger ggf. entsprechende Sicherheitsüberprüfungen (kritikalitätsabhängig) und Aufzeichnungen zu fordern, wem in seiner Organisation die Unterlagen zugänglich sind. Gleichzeitig müssen die zur Anbotslegung übermittelten Informationen jedoch von derartiger Qualität sein, dass sie als Basis für die Erstellung belastbarer Anbote tauglich sind.

Je enger der Kreis der potentiellen Auftragnehmer wird, desto mehr an Informationspreisgabe (selbstverständlich nur das entsprechende Gewerk betreffend) wird erforderlich sein. Im Gegenzug wird es ratsam sein, ein jeweils entsprechendes Mehr an vertraglicher Sicherheit betreffend den Umgang mit den beigestellten Informationen zu fordern und die Vertragstreue auch überprüfen zu können. Wird also mit fortschreitendem Prozess mehr an Informationstiefe preisgegeben, bleibt das strikte Informationssplitting zwingend aufrecht.

System implementieren

Sind im Bieter- oder Auswahlverfahren die geeigneten Errichter/Dienstleister gefunden, werden diese alle final geforderten und definierten Anforderungen an Verschwiegenheit, persönliche und Unternehmenssicherheits- und clearingmaßnahmen, Anforderungen an Mitarbeiter, die an der Gewerkeerrichtung beteiligt sind, Anforderung an Lagerung und Handling sicherheitssensibler Informationen etc. überprüfbar auf hohem Level nachweisen müssen. Im Rahmen der Implementierung wird darauf zu achten sein, dass neben einem optimalen zeitlichen und organisatorischen Ablauf auch ein Ablauf gewählt und gestaltet wird, der die Aufrechterhaltung des strikten Need-to-know gewährleistet. So wird zu vermeiden sein, dass alle möglichen Gewerkeerrichter gleichzeitig um, an und in der Site tätig sind, sich die Mitarbeiter der einzelnen Unternehmen austauschen können und jeder sieht, was der Andere gerade macht … Ebenso ist darauf zu achten, dass die eigenen Mitarbeiter im Rahmen der Implementierung nur das sehen und mitbekommen, was im Rahmen des Need-to-know vernünftiger Weise definiert und vertretbar ist und der Informationsaustausch mit Mitarbeitern von Fremdfirmen bestmöglich unterbunden wird, um unnötige Informationstransfers zu unterbinden.

Dieser Prozessschritt endet im Prinzip mit der Abnahme der einzelnen Gewerke, einem positiv bestandenen Probebetrieb samt allfällig erforderlicher Feinjustierungen und der Beseitigung von Kinderkrankheiten, der „Scharfschaltung“ des Systems und der Implementierung in die Organisation, somit der Überführung in den Regelbetrieb.

System überwachen und überprüfen

Im Regelkreis der ständigen Verbesserung ist die Effizienz des Systems zu messen und sind die Aufrechterhaltung der Funktionalität sowie der Angemessenheit

der Maßnahmen/des Systems sicherzustellen.

Sowohl im Qualitätsmanagement als auch in der Informationssicherheit ist man gewöhnt, sowohl durch unternehmensinterne als aber auch -externe Organisationseinheiten prüfen und auditieren zu lassen. Wenn es um die Security geht, wird hier ein – kritikalitätsangemessen – strenger Maßstab anzulegen sein. Weist man die Qualitätskontrolle beispielsweise der organisationseigenen QM-Stabsstelle zu, muss man sich bewusst sein, dass man den Kreis jener, die ein Need-to-know haben, erweitert. Die Frage wird sich stellen, ob die Aufrechterhaltung des Systems im Regelkreis der ständigen Verbesserung nicht durch jene Personen gewährleistet werden kann, die ohnehin bereits ein Need-to-know haben und zu beurteilen wird sein, ob bzw. falls ja welchen Nachteil es in sich birgt, wenn immer nur mit dem eigenen Blick auf das System gesehen wird. Externe Audits sind im Security-Bereich noch kritischer zu überdenken: gibt man dabei doch die intimsten Sicherheitsdetails, aber auch -lücken, -fehler und -unzulänglichkeiten vollumfänglich an Organisationsfremde preis. Hier ist einerseits genau abzuwägen, welche Vorteile eine externe Sichtweise auf das System bringt und – falls man das möchte oder Umstände das anraten – welche Anforderungen man in Bezug auf jene Personen und Organisationen definiert, um ihnen Zugang zu derart sensiblen Informationen zu gewähren.

Überlegungen zur praktischen Umsetzung

Selbstverständlich bieten der Werkzeuge der Informationssicherheit ausreichend Mittel und Möglichkeiten, Informationen systematisch und effizient zu schützen. Hier soll – wie auch oben erwähnt – nicht die Informationssicherheit neu erfunden werden, sondern insbesondere Planern von Physischen Schutzsystemen, die nicht auch InfoSec-Profis sind einige Hinweise gegeben werden, welche Maßnahmen – selbstverständlich kritikalitätsangemessen – angedacht werden können, um das Sicherheitssystem an sich zu schützen.

Ein Klassifizierungssystem alleine wird nicht die Lösung sein; eine Klassifizierung eines Dokuments/einer Information die einer Gruppe von Menschen gegenübersteht, die aufgrund von Überprüfungen, Unterweisungen, Freigaben … die Berechtigung hat, eine gewisse Klassifizierungsstufe einzusehen, steuert das Need-to-know nur teilweise. Ein derartiges Klassifizierungssystem kann aber als einer von verschiedenen Bausteinen in der Umsetzung eines Need-to-know angesehen werden. Was sollte aber alles geregelt sein, um den Grundsatz „Kenntnis nur wenn nötig“ bestmöglich umzusetzen?

Überprüfungen

Personen, die zu sicherheitskritischen Informationen Zugang haben sollen, sollten entsprechend sicherheits- und verlässlichkeitsüberprüft sein. Wo derartige Überprüfungen nicht gesetzlich gefordert und staatlich durchgeführt werden, muss die Organisation ein System schaffen, die Verlässlichkeit von Mitarbeitern mit Zugang zu Sicherheitskritischem (a) vor dem ersten Zugang und (b) wiederkehrend zu überprüfen. Derartige Überprüfungen bedürfen i.d.R. der Einwilligung der Mitarbeiter sowie deren Mitwirkung. Zur Verfügung steht eine i.d.R. breite Palette öffentlich zugänglicher Informationen, die mit Angaben der Mitarbeiter und Wahrnehmungen abgeglichen werden und ein relativ aussagekräftiges Bild ergeben können.

Unterweisungen

Die Organisation, die sicherheitskritische Sicherheitsinformationen schützen möchte/muss, ist aufgerufen, im Kreis der zugangsberechtigten Personen entsprechende Awareness hinsichtlich Sicherheitsbedarfs einerseits und möglicher Angriffe durch Innen- und Außentäter schaffen. Derartige Unterweisungen, die auch den sicheren Umgang mit sicherheitskritischen Informationen beinhalten sollen, sollten vor dem ersten Zugriff auf derartige Informationen und periodisch wiederkehrend sichergestellt sein.

Feststellung des Need-to-know

Die Organisation sollte Sorge tragen, dass eine Instanz implementiert ist, die feststellt, ob jemand den Bedarf hat, sicherheitskritische Informationen zu erhalten. Damit ist auch verbunden zu definieren, auf genau welche Informationen Zugang gewährt werden soll, und wie lange dieser Zugang gewährt werden muss.

Lagerung

Wesentlicher Teil der Umsetzung des „Kenntnis- nur- wenn-nötig"-Prinzips ist die Lösung der Lagerung derartiger Informationen. Erfolgt die Informationsvorhaltung in physischer Form (z.B. ausgedrucktes Sicherheitskonzept") ist eine zugriffssichere Lagerung vorzusehen, eine Dokumentation, wer wann Einsicht genommen hat, ebenso eine überprüfbare Regelung pcto. Vervielfältigung, Überführung in elektronische Form etc. Erfolgt die Vorhaltung derartiger Informationen in elektronischer Form, sind Speicherort und Zugriffsrechte entsprechend zu definieren, Zugriffe zu protokollieren etc.

Know-how-Splitting

Die Dokumente sollten so gestaltet werden, dass das Gesamt-know-how so kleinteilig wie möglich gesplittet vorliegt, sodass gewährleistet ist, dass Zugriff auf tatsächlich nur jene Informationen gewährt werden kann, die für die jeweilige Aufgabenerfüllung erforderlich ist. Gleichzeitig wird zu überlegen sein, wie man die Informationen, auf die Zugriff gewährt wird, gestaltet sind, das heißt, die Informationstiefe ist dem Unserbedarf anzupassen.

Information in externen Händen

Haben Organisationsmitarbeiter einen gewissen Bonus einer besonderen Verbindung zur Organisation, die eine gewisse Sorgfalt und Treue als gegeben voraussetzen läßt du eine entsprechende Steuerung und Kontrolle ermöglicht, ist bei Weitergabe sicherheitskritischer Informationen an Außenstehende eine entsprechende vertragliche Gestaltung zu treffen. Mögliche Werkzeuge sind Erhebungen zum Unternehmen und den Unternehmensverantwortlichen, Anforderungen an Geheimhaltung, Umgang, Lagerung, Zugänglichmachung, Mitarbeiter, die Kenntnis erlangen ... Neben der Vertragsverpflichtung muss eine Überprüfbarkeit vereinbart werden: alle diesbzgl. Vertragsbedingungen müssen beim Externen vor Informationserteilung und wiederkehrend überprüfbar sein. Ist der Sicherheitsplaner organisationsextern, sind an diesen seitens der Organisation die strengsten Maßstäbe anzulegen; schließlich ist er am Ende des Tages jene Person, die alle Kritikalitäten, alle Sicherheitseinrichtungen und alle Schwachstellen kennt. Eigentlich ist er damit die sicherheitskritischte Person. Demnach sind an ihn die höchsten Anforderungen hinsichtlich Verschwiegenheit, Lagerung, Handling etc. zu stellen.

Fazit

Assets sind nicht nur gegen intentionale Bedrohungen zu schützende Unternehmenswerte, als zu schützendes Asset sind auch jene Maßnahmen zu qualifizieren, die die primären Assets schützen, also auch das (Physical) Security-Managementsystem samt all seiner Herleitungen und Maßnahmen.

In Bezug auf alle Assets, also sowohl die primären (zu schützende Unternehmenswerte) also auch die sekundären (das Securitykonzept zum Schutz der Primärassets) sind – selbstverständlich kritikalitätsangepasste - Maßnahmen betreffend den Informationsschutz i.S.d. Zugangs zu securityrelevanten Informationen zu treffen. In Bezug auf das Schutzkonzept wird erfahrungsgemäß oftmals auf das Need-to-know vergessen, also das Prinzip „Kenntnis nur wenn nötig" ganz oder teilweise gebrochen. Gerade das Leben dieses Prinzips gewährleistet aber neben der Aufrechterhaltung der Effizienz der Sicherheitsmaßnahmen auch den Schutz der Primärassets.

In Bezug auf Sicherheitskonzepte sollte (a) im Organisationsbereich darauf geachtet werden, dass Zugang zu den Informationen nur jenen Personen gewährt wird, die diese Informationen zur Erfüllung von Aufgaben benötigen, (b) externen Personen, die zur Implementierung oder Aufrechterhaltung sicherheitsrelevanter Systeme erforderlich sind, nur Zugang zu den sie betreffenden Teilen des Sicherheitssystems gewährt wird und (c) der Zugang nur für jene Dauer und in jener Tiefe/jenem Detaillierungsgrad und jenes Segment betreffend erfolgt, der zur unmittelbaren Aufgabenerfüllung erforderlich ist.

Die Steuerung und Gestaltung muss kritikalitätsangemessen erfolgen. Als Grundsatz sollte gelten, dass das Gesamtkonzept maximal der Designer und der Sicherheitsverantwortliche der Organisation kennen sollten, Informationen an andere Personen sollten hinsichtlich Umfang und Detaillierungsgrad im Einzelfall gestaltet werden: soviel als nötig, sowenig als möglich.

Die Autoren:

Mario Trutzenberger ist selbstständiger Sicherheitsberater für Physical Security, Notfall- und Krisenmanagement und Materiellen Geheimschutz und leitet das Modul 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