Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 619

Effiziente Risikoanalyse anhand praktischer Erfahrungsbeispiele

Manfred Holzbach[1]

Abstract: Risikomanagement in der Praxis kann heute nicht mehr vollflächig erfolgen, sondern muss sich auf die lebenswichtigen Assets einer Organisation fokussieren und deren Bestand auch in Krisenfällen sichern können. Das gilt ganz besonders für KMUs, die immerhin das Rückgrat der Wirtschaft und wohl auch der Gesellschaft in Europa bilden. Anhand von 3 Beispielen unterschiedlicher Zielsetzung, Gefahrenstruktur und Schlussfolgerungen daraus wird gezeigt, wie mit Hilfe geeigneter Prioritätensetzung effiziente Risikoanalysen durchgeführt wurden resp. werden.

Keywords: Risikoanalyse, Risikomanagement, Cyber-Sicherheits-Check, sensible Daten, Attacken

1 Einleitung

Risikomanagement gemäß ISO/IEC 31000:2009 [ISO09] zur Identifikation, Analyse und Bewertung von Risiken für ein Unternehmen oder eine Organisation ist heute unbestrittener Weise unabdingbar. Nicht nur für große Einheiten, sondern auch für KMUs, Start-Ups oder ausgelagerte öffentliche Einrichtungen. Abhängig von ihrer Tätigkeit können diese im Zuge der Aufgabenteilung und Vernetzung volkswirtschaftlich kritische Points-of-Failure darstellen. So können Zulieferer für den Wirtschaftsstandort wertvolles Know-how besitzen oder Subauftragsnehmer sensible oder begehrte Informationen verarbeiten, welche für ihre Auftraggeber oder Dritte wesentliche Bedeutung haben. Somit können sie sich selbst, aber auch andere Einheiten in existenzbedrohende Lagen bringen – besonders in rechtlicher und finanzieller Hinsicht aber auch was Vertrauen und Reputation betrifft.

Risikomanagement kann überall angewendet werden, wo Risiken auftreten können. Dabei besteht die Zielsetzung im rechtzeitigen Erkennen von und dem Umgang mit solchen Risiken, welche die Existenz der Organisation gefährden, Leib und Leben anvertrauter Menschen bedrohen oder wo große Schadenspotenziale schlagend werden können. Es reicht dabei nicht, die identifizierten Einzelrisiken abzuarbeiten, sondern auch die Risikopotenziale aus deren Kombinationen zu erkennen und zu beherrschen.

Der Anforderung nach maximaler Breite und Tiefe an Analyse und Beherrschung stehen die endlichen verfügbaren Ressourcen, Zeit und Know-how, aber auch die Mobilität und

[1] Zentrum für sichere Informationstechnologie – Austria (A-SIT), Seidlgasse 22/9, 1030 Wien, manfred.holzbach@a-sit.at.

Kreativität von Angreifern entgegen. Es besteht auch immer die Gefahr, dass bei rein methodischem Ansatz etwas übersehen wird.

Mit der fortschreitenden Digitalisierung ist es aufgrund der immer stark ansteigenden Durchdringung, Vernetzung und Komplexität der sie ausmachenden IT-Systeme, Komponenten, Netzwerke und Applikationen nicht mehr möglich, alle potenziellen Gefahren und damit Risiken flächendeckend einzuschätzen. Nicht in der gegebenen Vielfalt, denn es gibt immer weniger industriell gefertigte Produkte, welche keine Software enthalten. So bringt es ein Herzschrittmacher auf 80.000 Codezeilen [JM13], das Elektrofahrzeug Chevrolet Volt auf 10 Millionen Codezeilen [LD10] und zum Vergleich die Flugsoftware der Boeing 787 auf 14 Millionen [DL11]). Und auch nicht im zeitlichen Verlauf, denn in jeder Sekunde werden täglich 390.000 neue Schadprogramme (also 4-5 pro Sekunde) registriert [SZ16].

Da sich dieser Beitrag an Risikomanagement-Experten wendet, wird darin Kenntnis der Risikomanagement- und Risikoanalysemethoden weitgehend vorausgesetzt.

2 Aufgabenstellung

Es handelt sich dabei um eine sich aus den praktischen Erfahrungen manifestierte Entwicklung.

Im Prinzip wird das gleiche Verfahren angewendet, unbeschadet davon ob es sich um ein großes Unternehmen oder ein Start-Up handelt. Der wesentliche Unterschied liegt in den verfügbaren Ressourcen, die für Detailtiefe, Einsatz von Experten, Tools, Ausführen von Pen-Tests zur Verfügung stehen.

Risikoanalysen, welche einen Bottom-Up Absatz verfolgen oder den flächendeckenden Anspruch stellen, alles abdecken zu können, werden etwa im Bereich der kritischen Infrastrukturen durchgeführt und stellen sich als Großprojekte über Monate oder Jahre mit Experten der unterschiedlichsten Disziplinen dar (Beispiel über eine umfassende Bewertung von Stromausfällen in [EC14]). In Bereichen wie exponierter Daten oder Software können sie nur bedingte Aussagen leisten bzw. sind sie mit vertretbarem Ressourcenaufwand nicht mehr umsetzbar, schon gar nicht für KMUs. Diese verarbeiten aber oft gesamt- oder volkswirtschaftlich äußerst wertvolle Assets, beispielsweise als Zulieferer oder Subauftragsnehmer.

Risikoanalyse ist heute noch viel wichtiger als je zuvor. Da sie jenseits kritischer Infrastrukturen nicht alles abdecken kann, ist es essentiell eine Methode zu haben die auf das jeweilige Problem, Budget und die Organisation angepasst ist.

Die in der Praxis zu lösende Aufgabe besteht darin, ein gezieltes, effizientes Vorgehen so zu gestalten, dass die Zielsetzung des Risikomanagements auch bei reduzierter Breite und Tiefe zuverlässig erreicht wird. Dies wird durch ein Schalenmodell, beginnend bei den Top-Assets (den „Kronjuwelen“) erreicht; dies schon aufgrund der Tatsache, dass

am Schluss immer ein Restrisiko in Kauf zu nehmen ist. Im Kern geht es darum, dort zu investieren, wo die Prioritäten sind und sich nicht in Details zu verlieren, welche keine lebenswichtigen Funktionen betreffen.

Das Schalenmodell geht vom Verstehen der Geschäftsprozesse aus und modelliert dann Assets nach Priorität aus deren Kritikalität:

- Welche Geschäftsprozesse sind für die Existenz des Unternehmens oder der Organisation unabdingbar?
- Was ist jeweils der maximal mögliche Schaden für die eigene aber auch davon mit betroffene Organisationen pro identifiziertem Bereich?

Die Assets sind exponiert gegen Gefährdungsbereiche, für welche Gefahrenkataloge und Kontrollziele aufgestellt werden – zunächst in groben Kategorien z.B. Gefahren im Zusammenhang mit Verfügbarkeit, Gefahren im Sinne des IT-Systems, dann je nach konkreter Situation und Bedarf weiter ins Detail gehend. Durch ein solches Top-Down Modell findet man die hohen Prioritäten vergleichsweise schnell.

Tiefer in Details wird dort gegangen, wo es sich dann als notwendig erweist oder wenn Problemzonen erkannt werden. Dabei wird zuerst hinterfragt, ob der betroffene Prozess oder sämtliche exponierten Informationen notwendig sind resp. ob und welche Alternativen es gibt. Somit werden sukzessive Schalen entfernt und zum Kern des Problems vorgedrungen. Jeder Ast des Risikobaumes, den man aufgrund geringer Priorität oder auch bereits festgestellter ausreichender Sicherheit abschneiden kann, bzw. jede eliminierte Schale spart Ressourcen in Form von Zeit und Geld.

Erst dann wird weiter nach unten in Richtung als kritisch ausgemachter Prozesse (insbesondere IT-Prozesse) weiter vorgegangen. Details werden erst nach deren Analyse gezielt untersucht (z.B. mittels Penetrationstests).

Zu betrachten sind unbedingt auch der Einfluss des Change Managements sowie von Notfallmaßnahmen und nicht standardisierbarer, aber im Krisenfall oft notwendiger Improvisation auf das Risiko.

Dies ist unabhängig davon, ob ein genormter Ansatz wie etwa ein Vorgehen gemäß BSI Standard 100-3 „Risikoanalyse auf Basis des IT Grundschutz“ [BSI08] gewählt wird oder nicht. Ein solcher erfüllt eine notwendige aber nicht hinreichende Bedingung für eine realistische Risikoeinschätzung. Denn es kann etwas übersehen werden oder eine aktuelle Schwachstelle entzieht sich den standardisierten Verfahren („Hintertüren“).

Im Vergleich mit dem heutigen Straßenverkehr könnte man sagen: „Genormter Ansatz bietet die STVO und einen Airbag, das notwendige Fahrkönnen muss als individuelle menschliche Fertigkeit eingebracht werden“.

„Kreativität ist gerade dort notwendig wo es gefährlich wird“.

„Analog zur Kriegsführung erweisen sich menschliche Qualitäten als unabdingbar“.

3 Praxisbeispiele

Vor diesem Hintergrund wird anhand von 3 praktischen Beispielen dargestellt, wie Risikoanalysen im Bereich von KMUs mit jeweils situativ unterschiedlichem Ziel, Zweck und unterschiedlicher Motivation und Methode, aber dennoch effizient und aussagekräftig durchgeführt wurden resp. werden. Die Beispiele handeln von Risikoanalysen, die A-SIT bei Organisationen tatsächlich umgesetzt hat resp. zur Zeit umsetzt. Die jeweiligen Unternehmen werden hier nicht genannt und Findings nicht veröffentlicht, wohl aber die unterschiedlichen Vorgehensweisen dargestellt, begründet und Erkenntnisse, welche die Methode betreffen, diskutiert.

3.1 Cyber-Sicherheits-Check bei einem öffentlichen Förderungsgeber

Die Servicestelle des Landes Steiermark für Unternehmen vergibt unter anderem Förderungsmittel des Landes und der Europäischen Union an Unternehmen, welche durch Innovationsmaßnahmen zur Stärkung der eigenen Wirtschaftskraft und des Wirtschaftsstandortes beitragen. Die Förderungsmittel werden beantragt, wobei die Innovation durch geeignete Detail-Unterlagen nachzuweisen ist, welche einen erheblichen wenn nicht unersetzlichen Wert und damit die Top-Assets darstellen. Die Schadenspotenziale reichen von erheblichen Ersatzforderungen über Compliance-Verletzungen bis zu massiver Image-Beschädigung nicht nur für die Servicestelle, sondern auch das Land.

Die Risikoanalyse erfolgte mittels Cyber-Sicherheits-Check, einer vom BSI[2] im Rahmen der Allianz für Cyber-Sicherheit vorgeschlagenen Vorgehensweise [BSI14], wobei die Risikoanalyse gemäß der „Cyber-Sicherheits-Exposition“ [BSI12] abgearbeitet wird. Als Grundlage für die Bewertung der implementierten oder geplanten Maßnahmen auf Notwendigkeit, Angemessenheit und Wirtschaftlichkeit werden die einzelnen Elemente der Infrastruktur, gespeicherten und übertragenen Daten sowie Verarbeitungsprozesse einer ganzheitlichen Cyber-Bedrohungsanalyse unterzogen und die Erkenntnisse kompakt und plakativ dargestellt. Damit erreicht man zügige und interaktive Kommunikation zwecks gemeinsamer Sichtweisen mit dem Management. Bemerkenswert dabei ist, dass man sich auf „Cyber“- Bedrohungen beschränkt, also Perimeter- und Safety-Aspekte nicht unmittelbar berücksichtigt.

Zunächst erfolgten interaktiv Bewertungen zur Cyber-Sicherheits-Exposition auf Basis standardisierter Fragestellungen zu Wert der Daten und Prozesse, Attraktivität für Angreifer, Art der Angreifer, zu erwartender Zielgerichtetheit von Angriffen, erfolgten Angriffen in der Vergangenheit, zu erwartendem maximalem Bedrohungsgrad und Transparenz für Angreifer – jeweils unterschieden zwischen Vertraulichkeit, Verfügbarkeit und Integrität. Die Einzelergebnisse werden nach einem vorgegebenen Gewichtungsschlüssel bewertet und eine Gesamt-Exposition pro Bereich ermittelt. Die

[2] Bundesamt für Sicherheit in der Informationstechnik, Bonn;Website www.bsi.bund.de.

„Schalen“ werden hier durch die Auswahl der Einzelfragen und Gewichtung der Antworten gebildet.

Aufgrund der wertvollen zu schützenden Daten ergeben sich entsprechend hohe Expositionen bei „Vertraulichkeit“, wobei zielgerichtete Angriffe denkbar aber bei wirksamen Maßnahmen unwahrscheinlicher sind als beim Unternehmen selbst, dem die Informationen gehören. Für die Exposition bei „Verfügbarkeit“ ist unter anderem die Möglichkeit von DoS Attacken zu bewerten.

Im zweiten Teil erfolgte die Bewertung des „Cyber-Sicherheits-Status“, d.h. der implementierten bzw. geplanten Maßnahmen. Dabei wird einem vorgegebenen Katalog von Maßnahmenzielen gefolgt, allfällige Mängel aufgezeigt und die Wirksamkeit bewertet – sowohl tabellarisch mit Ampel-Indikatoren als auch verbal ausgeführt. In dieser Bewertung liegt die Priorisierung ausgehend von der Exposition und damit das Schalenmodell.

Parallel wurden auf Wunsch der Organisation zusätzliche Schwachstellen Scans mit einem Tool bei einem Outsourcing-Dienstleister durchgeführt. Das ist zwar kein zwingender Bestandteil des Cyber-Sicherheits-Checks, die Erkenntnisse sind allerdings in die Gesamtbewertung eingeflossen und erwiesen sich als durchaus wertvoll.

Der Cyber-Sicherheits-Check führt mit vergleichsweise kompaktem Aufwand zu einer sehr brauchbaren Bewertung der Risiken, allfälliger Schwachstellen und der Wirksamkeit von Maßnahmen. Das bewirkt Awareness und Mitwirkung des Managements, was gerade bei KMUs essentiell ist. Beim Scoring für die Exposition können sich bereits geringe Veränderungen in Einzelbereichen erheblich im Gesamtergebnis auswirken. Daher sollte die Methode von erfahrenen Auditoren durchgeführt werden.

3.2 Standardmethode nach Schalenmodell in einem Hochrisikobereich

Die primären Assets des Systems (die „Kronjuwelen“) sind Gesundheitsdaten, welche von unterschiedlichen Teilnehmern genutzt und verarbeitet werden, aber den Patienten gehören. Damit hat man mit der sensibelsten Art von Daten überhaupt, und für Angreifer äußerst wertvollen Informationen zu tun. Für Schutzmaßnahmen im Security-Bereich relevante Assets sind in erster Linie die Zugangsdaten, welche sehr heterogen strukturiert sind, was die Möglichkeiten und den Aktionsradius, somit das Gefahrenpotenzial, betrifft: Vom einzelnen Bürger über die Gesundheitsdienste bis zu zentralen Stellen. Unbeschadet genereller Leitlinien sind die von IT-Abteilungen betriebenen Systeme dezentral, unterschiedlich komplex und müssen Entscheidungsspielräume für die Akteure ermöglichen.

Das zentrale Risiko wäre ein Verlust der Vertraulichkeit, der Integrität aber auch der Verfügbarkeit von Gesundheitsdaten. Die Folgen könnten existenzbedrohende Ausmaße annehmen, sowohl in materieller Hinsicht (rechtliche Konsequenzen, Strafen,

Schadenersatz) aber auch was den Verlust an Reputation und Vertrauen betrifft. Eine besondere Problematik ergibt sich dabei aus der Struktur: Selbst wenn ein Vorfall an nur einer Stelle auftreten würde und nur ein begrenztes Ausmaß hätte, müsste mit heftigen Reaktionen der Öffentlichkeit, von Medien und der Politik gerechnet werden, welche ihren Fokus dann auf das Gesamtsystem richten und es in Frage stellen würden.

Die Riskoanalysemethode folgt einem Top-Down Ansatz: Zunächst werden Funktionen und Komponenten mit hoher Priorität identifiziert, welche sich in exponierten Bereichen befinden und Einfluss auf die Top-Assets haben. Die Fragestellung umfasst ihre jeweilige Risikoeinschätzung für sich, aber auch in welchen Bandbreiten sich ihre Restrisiken aufgrund ihrer Umgebung, verteilten Einsatzes, Eigenschaften und Zusammenwirken beeinflussen lassen. Niedrige Priorität haben dann Komponenten, bei denen man bereits ausreichende Sicherheit annehmen kann, etwa weil sie in geschützten Bereichen arbeiten resp. bereits begutachtet sind.

In der Folge werden Teilrisikoanalysen mit Hilfe eines Tools in mehreren Ebenen abgearbeitet, von den materiellen Assets über die Geschäftsprozesse, deren Relevanz auf das Gesamtsystem, die Komponenten und die Gefahren. Dies stellt den klassischen Teil der Risikoanalyse dar.

Die Ergebnisse werden für fiktive Angriffsszenarien herangezogen um die Robustheit als Grad, solche verhindern zu können, sowie die möglichen Folgen festzustellen, aber auch die Möglichkeiten sie zu erkennen und darauf effizient zu reagieren. Die gewonnenen Erkenntnisse fließen dann in Empfehlungen für die Implementierung präventiver, detektiver und reaktiver Maßnahmen ein.

Das Besondere an diesem Ansatz ist es (abgesehen vom Zusammenwirken mehrerer mit Security befasster Organisationen), einem heterogenen und aufgrund unterschiedlicher Go-Live Termine für geografische und organisatorische Einheiten dynamischen Gesamtsystem Rechnung zu tragen. Es gibt einerseits Standardverfahren, aber auch sehr spezifische resp. einzigartige Funktionen. Das erfordert menschliche Kreativität und Entscheidungsqualität und kann insgesamt nicht allein durch Befolgen von Standards hinreichend abgedeckt werden.

3.3 Risikoanalyse im Rahmen eines Qualitätsmanagements

Es handelt sich um eine sehr kleine Organisation, welche sich unter anderem mit Technologiebeobachtung befasst, Gutachten erstellt und sich dafür akkreditieren lässt. Der Zweck der Risikoanalyse ergibt sich daher zunächst aus der Notwendigkeit im Rahmen des Qualitätsmanagements und für die Pflichtversicherung. Da es sich um real vorhandene Risiken handelt, ist deren Einschätzung und Vermeidung aber auch für die Geschäftsgebarung unerlässlich.

Zu schützende Assets sind vertrauliche Unternehmens- und Produktdaten der zu prüfenden Organisationen, sowie Unterlagen und Erkenntnisse der

Technologiebeobachtung. Diese können immerhin Einfluss auf die Reputation von Systemen und deren Betreibern haben.

Das materielle Risiko liegt wie bei anderen Organisationen in deren Kompromittierung, Verlust oder Diebstahl. Die Folgen wären rechtliche Konsequenzen und Schadenersatzforderungen, welche auch hier existenzbedrohende Ausmaße annehmen könnten. Wegen der Rechtsform eines Vereins einer Teilorganisation birgt dies auch erhebliche Risiken für dessen Vorstände. Abdeckung durch Versicherungen ist nur begrenzt möglich, schon wegen der teuren Prämien in diesem Bereich.

Das Reputationsrisiko kann schon bei geringfügigen Vorfällen wie einem Einbruch mit Diebstahl der Handkassa existenzbedrohend werden, wenn damit das Vertrauen in die sichere Verwahrung von Dokumenten und das Image als Experte für Sicherheit damit in Frage gestellt würde.

Gefahren können weiters für die Integrität und Qualität der gemachten Aussagen auftreten, sowohl in inhaltlicher wie technisch-organisatorischer Hinsicht.

Bei der Risikoanalyse und dem daraus abgeleiteten Risikomanagement erfolgt die Überprüfung und schließlich der Nachweis, inwieweit die getroffenen Vorkehrungen und Maßnahmen wirksam sind. Ausgehend von den oben genannten Assets werden die maximal denkbaren Schadensszenarien abgeschätzt und welche Vorfälle sie verursachen könnten. In der nächsten Ebene (Schale) werden die kritischen Geschäftsprozesse zugeordnet und analysiert, welchen Einfluss handelnde Personen und örtliche Gegebenheiten darauf haben können. Dann wird die Stärke der Maßnahmen wie Perimeterschutz, Rollen- und Rechteverwaltung, verschlüsselte und gespiegelte Speicherung sowie für nachvollziehbare Richtigkeit der Aussagen die implementierten Review-, Freigabeprozesse und qualifizierte Signaturen bewertet und die Schlussfolgerungen gezogen.

3.4 Vergleich der Beispiele

Beispiel 3.1 hatte die Aufgabenstellung, in einem sehr kompakten Verfahren die bestehenden Sicherheitsmaßnahmen hinsichtlich allfälliger Schwachstellen zu bewerten und daraus Risiken und die Gesamtexposition zu erkennen sowie Empfehlungen zu generieren. Der gewählte Cyber-Sicherheits-Check kann dies fokussiert auf Security-Aspekte abdecken und ermöglicht auf Grund seiner Kompaktheit eine besonders aktive Mitwirkung des Managements. Erforderlich ist dazu allerdings viel Erfahrung und Übersicht bei den Auditoren und beim IT-Personal der untersuchten Organisation.

Beispiel 3.2 bearbeitet eine komplexe, heterogene und dynamische Systemlandschaft, in der es nicht möglich ist, sämtliche Einzelrisiken und ihr Zusammenwirken vollständig zu bewerten. Obwohl die Risikoanalyse sehr breit angelegt ist und mehrere Berater sowie Tools eingesetzt wurden, muss der Fokus dennoch auf den lebenswichtigen Assets und denjenigen Mechanismen liegen, die deren Funktion auch in Krisenfällen sichern. Der

Aufwand ist dementsprechend erheblich und den befassten Experten wird umfassendes Wissen, Erfahrung und Kreativität abverlangt.

Beispiel 3.3 wird für ein sehr kleines Unternehmen mit eng abgegrenzten, aber für die Organisation potenziell sehr gefährlichen Risiken verwendet. Der Vorgang ist individuell zugeschnitten, gestaltet sich allerdings auf Grund der Situation, dass die MitarbeiterInnen im Detail mit den Geschäfts- und IT-Prozessen sehr vertraut sind, als überschaubar und geradlinig. Es erfordert hohe Kompetenz der befassten Experten, aus dem begrenzten Input die Erkenntnisse nachvollziehbar zu dokumentieren und zu formalisieren, sodass sie für eine Akkreditierung brauchbar und hinreichend sind.

4 Weiteres Vorgehen

Das Österreichische Informationssicherheitshandbuch [BKA14] wird von A-SIT inhaltlich betreut und enthält ein umfassendes Kapitel über Risikoanalysestrategien und ihre Umsetzung. Dies wird nun anhand der gewonnenen Erkenntnisse und auch praktischen Erfahrungen auf den neuesten Stand gebracht. Ausgehend vom derzeit dargestellten „kombinierten Ansatz“ zur Risikoanalyse sollen das Konzept der Top-Down Vorgehensweise und das Schalenmodell konkret beschrieben und etablierte Methoden erläutert werden.

Herausfordernd dabei wird es sein, einen Leitfaden zu entwickeln, welcher einerseits generisch auf möglichst viele Fälle anwendbar ist, so umfassend als möglich ist und dennoch den Kern des Konzepts wiedergibt, wo es darum geht im konkreten Einzelfall die richtigen Prioritäten aber auch Zusammenhänge zu erkennen.

Zum einen wird man die allgemein gültigen Strukturelemente beginnend bei den lebenswichtigen Assets sowie häufige Einflussfaktoren aus der Umgebung und dem Zusammenwirken verschiedener Prozesse darstellen. Ähnlich wie im BSI Standard 100-3 [BSI08] macht es dabei auch Sinn, das Konzept und die Elemente anhand praxisnaher Beispiele zu erläutern.

5 Offene rechtliche Fragen aus der gewonnenen Erfahrung

- Da vollständige Sicherheit nicht gewährleistet werden kann, braucht es Richtwerte, was einer Organisation im Rahmen der Gesetze und Compliance an Aufwand und Zuwendung zumutbar ist. Wie weit reicht dann ihre rechtliche Verantwortung (Haftung) bzw. die ihrer Organe?
- Was sind dann die Grenzen der Prävention? Zum Beispiel können Firewalls und Virenscanner längst nicht mehr vor allen Schadprogrammen schützen, weder von der Qualität noch der Quantität her.

- Inwieweit helfen Zertifizierungen, Haftungen zu reduzieren respektive abzuwälzen? Zertifizierungen oder ähnliche Begutachtungen dienen unter anderem als Beweismittel für korrekte Gebarung oder sichere Produkte – das gilt allerdings nur für den Zustand zum Zeitpunkt der Zertifizierung.
- Soll und darf man aktiv Gegenattacken unternehmen, um einen Angreifer auszuschalten?
- Welches Restrisiko darf man in Kauf nehmen? Ein Risiko, das einen Super-GAU (Existenzverlust des Unternehmens) in Kauf nimmt, wäre wohl unangemessen. Wie kann man es aber quantifizieren?
- Was kann rechtliche Beratung in diesem Bereich leisten? Ist man auf der sicheren Seite wenn man Beratung in Anspruch genommen hat?

6 Fazit

Absolute Sicherheit ist nicht erreichbar, das zeigte sich nicht nur in den durchgeführten Risikoanalysen, sondern ist durch die teilweise spektakulären Vorfälle und Leaks der letzten Jahre belegt. Während ein Verteidiger immer aktuell sämtliche Schwachstellen und ihr Potenzial kennen muss, genügt einem Angreifer eine einzige. Ziel ist es daher, existenzbedrohende Risiken zu kennen, zu beherrschen und glaubhafte Abwehr- und Gegenstrategien für den Krisenfall vorzuhalten und umsetzen zu können.

Kann man nachweisen, alle zumutbaren Überlegungen und Vorkehrungen getroffen zu haben, verringert sich dann auch das Schadenersatz-, Straf- und Reputationsrisiko, wenngleich diesbezügliche rechtliche Aspekte nicht von vornherein abgeklärt werden können.

Die Beispiele zeigen, dass sich Risikoanalysen nach einem an Organisation und Exposition angepassten Modell, innerhalb dessen dann Risikostränge mit als gering eingestufter Priorität wie Schalen abgelöst werden, effizient durchführen lassen und zu zuverlässigen, nachvollziehbaren und vor allem aktuellen Ergebnissen führen. Kritische Erfolgsfaktoren sind dabei Know-how, Erfahrung und Kreativität der Durchführenden.

Es ist allerdings darauf zu achten, dass die Bedeutung oder der Wert sensibler oder personenbezogener Informationen nicht unterschätzt wird.

Literaturverzeichnis

[BKA14] Österreichisches Informationssicherheitshandbuch, Version 4.0.0, Bundeskanzleramt Österreich (BKA) und Zentrum für sichere Informationstechnologie – Austria (A-SIT), https://www.sicherheitshandbuch.gv.at/2013/index.php, Stand: 15.10.2014.

[BSI08] BSI Standard 100-3 „Risikoanalyse auf Basis des IT Grundschutz, Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard03/ITGStandard03_node.html, Stand: 2008.

[BSI12] BSI-Veröffentlichungen zur Cyber-Sicherheit, Empfehlung an Management, Cyber-Sicherheits-Exposition, BSI-CS 013| Version 1.00, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_013.pdf?__blob=publicationFile&v=2, Stand: 2012.

[BSI14] Leitfaden Cyber-Sicherheits-Check, Bundesamt für Sicherheit in der Informationstechnik – BSI , https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden-Cyber-Sicherheits-Check.html, Stand: 2014.

[ISO09] ISO/IEC 31000:2009: Risk management — Principles and guidelines, 2009.

[EC14] E-Control, Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft unter besonderer Berücksichtigung von Smart-Metern und des Datenschutzes, https://www.e-control.at/documents/20903/-/-/3f89d470-7d5e-433c-b307-a6443692d8f7, Stand: 2014.

[LD10] Larry Dignan: GM's Volt: 10 million lines of code, http://www.zdnet.com/article/gms-volt-10-million-lines-of-code/, Stand: 1.11.2010.

[DL11] David Lilienthal: NYC Aviation; Aviation News, Top 4 Fun Boeing 787 Technical Facts, 2011, http://www.nycaviation.com/2011/09/fun-facts-revealed-at-boeings-787-technical-panel/#.V2Utv3qQqp0, Stand: 28.9.2011.

[JM13] Zhihao Jiang und Rahul Mangharam: Entwicklung eines elektrophysiologischen Herzmodells für Regelkreistests von Herzschrittmachern in Echtzeit an der University of Pennsylvania, 2013.

[SZ16] Jürgen Schmidt, Volker Zota: heise online, Zahlen, bitte! Täglich 390.000 neue Schadprogramme, http://www.heise.de/newsticker/meldung/Zahlen-bitte-Taeglich-390-000-neue-Schadprogramme-3177141.html, Stand: 19.4.2016.