Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 609

Information Security Risk Analysis in komplexen Systemen - neue Herausforderungen und Lösungsansätze

Ingrid Schaumüller-Bichl[1], Andrea Kolberger[1]

Abstract: Die Identifikation und Bewertung von Risiken, die die Informationssicherheit bedrohen (Information Security Risk Analysis, ISRA), ist in vielen Systemen von zentraler Bedeutung. Neue Technologien und Entwicklungen, wie etwa Industrie 4.0 oder das Internet der Dinge (Internet of Things, IoT) sowie generell die zunehmende Komplexität der IT-Systeme stellen neue Herausforderungen an die Risikoanalyse und das Risikomanagement. Der Artikel diskutiert die besonderen Anforderungen an ISRA in komplexen Systemen und geht der Frage nach, wie Risikoanalyse im IT- und Informationssicherheitsbereich in Zukunft aussehen kann. Welche Ansätze können übernommen und weiterentwickelt werden, wo braucht es neue Lösungen und wie können diese aussehen?

Keywords: Risikoanalyse, Risikomanagement, Informationssicherheit, IT-Sicherheit, komplexe Systeme

1 Einleitung

Ein systematischer Ansatz zur Identifikation und Bewertung von Risiken ist in der IT- und Informationssicherheit heute wichtiger denn je. Die Risikoanalyse ist Basis für die Auswahl und Implementierung adäquater Sicherheitsmaßnahmen. Zunehmend sehen auch Rechtsvorschriften, Normen, de-facto-Standards und branchenspezifische Vorgaben eine verpflichtende Auseinandersetzung mit Risiken vor. Aktuelles Beispiel dafür ist die neue EU Datenschutz-Grundverordnung. Sie sieht sowohl eine risikogerechte Auswahl von Sicherheitsmaßnahmen vor, als auch in potentiell kritischen Fällen die Durchführung einer DPIA (Data Protection Impact Analysis, Datenschutz-Folgenabschätzung), die als eine spezielle Form der Risikoanalyse im Datenschutzbereich betrachtet werden kann. Weitere Beispiele sind etwa die in ISO/IEC 27001 zentrale Informationssicherheits-Risikoanalyse sowie die Risikoanalyse im Rahmen des BCM Prozesses.

2 Risikoanalyseansätze in der Informationssicherheit – Stand der Technik und Grenzen

Die letzten Jahre haben im Bereich der Risikoanalyse für Informationssicherheit (ISRA)

[1] FH OÖ, Information Security Compliance Center (ISCC), Hafenstraße 47-51, 4020 Linz,
{ingrid.schaumueller-bichl, andrea.kolberger}@fh-ooe.at

einen Paradigmenwechsel gebracht. Während der Risikobegriff früher als möglicher Schaden aus der Ausnutzung von Schwachstellen durch eine Bedrohung definiert war (ISO/IEC 27005: "potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization" ([ISO11]), wird er nun, angelehnt an das generelle Risikomanagement, allgemeiner gefasst. So bezieht sich seit 2013 auch die ISO/IEC 27001, der weltweit verbreitete Standard zum Informationssicherheits-Management, auf ISO 31000 und damit auf folgenden Risikobegriff: "risk is the effect of uncertainty on objectives", definiert also Risiko als Abweichung von Zielen, egal ob positiv oder negativ ([ISO09], [ISO13]). Damit wurde der "klassische" Zugang zum Informationssicherheits-Risikomanagement, nämlich die Ermittlung von Bedrohungen, Schwachstellen und Schäden zur Risikoidentifikation und die Bewertung von Eintrittswahrscheinlichkeiten sowie der Schadenshöhe zur Abschätzung der Risiken erweitert und verallgemeinert.

Risikoanalyse unterscheidet typischerweise zwischen quantitativen und qualitativen Ansätzen. Die in der Literatur teilweise dargestellten semi-quantitativen Ansätze werden in der Folge in diesem Paper unter die qualitativen Ansätze gereiht.

Wie in anderen Bereichen auch haben quantitative Ansätze im IT- und Informationssicherheitsbereich vor allem einen entscheidenden Vorteil: sie erlauben eine monetäre Abschätzung der Schäden und Risiken, und bieten damit eine gute Argumentationsgrundlage für Investitionen in den Sicherheitsbereich. Arbeiten zur Berechnung des "Return on Security Investment" (ROSI) bzw. "Return on Information Security Investment" (ROISI) finden sich u. a. in [St08] und [Ko08].

Trotz wissenschaftlich interessanter quantitativer Verfahren werden in der Praxis im Informationssicherheitsbereich überwiegend qualitative Verfahren eingesetzt. Dies liegt in erster Linie darin begründet, dass eine genaue Abschätzung von Eintrittswahrscheinlichkeiten oder Häufigkeiten in diesem Bereich sehr schwer durchzuführen ist: es gibt wenige verlässliche historische Werte, anders als etwa bei der Häufigkeit von Blitzeinschlägen, Statistiken zur Lebenserwartungen und ähnlichen Ereignissen, wo man auf langjährige Beobachtungen und relativ konstante Entwicklungen zurückgreifen kann. Der IT-Bereich ist hingegen sehr raschen Änderungen unterworfen, die Bedrohungslandschaft ändert sich laufend und mit zunehmender Geschwindigkeit. Einen guten Überblick über die aktuelle Lage und künftig zu erwartende Risiken gibt etwa die Risikolandkarte der ENISA (ENISA threat landscape [EN15]), die auch auf künftig zu erwartende Risiken ("Emerging Risks") eingeht.

In der Praxis kommen in der IT- und Informationstechnologie daher vorwiegend quantitative Verfahren, häufig auf Basis von Risikomatrizen zum Einsatz. Oft wird dabei zur Unterstützung auf vorgegebene Bedrohungs- und Schwachstellenkataloge zurückgegriffen.

Resultat einer Risikoanalyse im Informationssicherheitsbereich ist damit in der Regel eine Fülle von Einzelrisiken, die im Anschluss gesondert und im Detail behandelt werden müssen. Maßnahmen zur Risikobehandlung setzen dort an, wo die Risiken

entstehen, d.h. sie können entweder die Eintrittswahrscheinlichkeit reduzieren oder die Höhe der Auswirkungen oder auf beide Faktoren Einfluss nehmen.

Risikoaggregation und damit die Abschätzung eines Gesamtrisikos für den IT-Bereich oder bestimmte IT-Anwendungen sind in der Praxis hingegen selten anzutreffen und auch schwer zu erreichen.

Zusammenfassend ist zu sagen, dass die heute üblichen Risikoanalyse-Methoden im IT-Bereich eine gute und unabdingbare Basis für die nachfolgende Auswahl von angemessenen, eben risikogerechten, Sicherheitsmaßnahmen darstellen. Eine Abschätzung des Gesamtrisikos für die Informationssicherheit und damit der Auswirkungen auf das gesamte Unternehmen oder die Gesellschaft, ist mit gängigen Verfahren aber nicht oder nur eingeschränkt zu erreichen.

3 Information Security Risk Analysis in komplexen Systemen – spezifische Anforderungen

In komplexen Systemen, wie z.B. industriellen Systemen oder dem Internet der Dinge (IoT), bestehen eine Reihe spezifischer Anforderungen an die Risikoanalyse bzgl. Informationssicherheit und die darauffolgende Risikobehandlung. Nachfolgend werden einige davon - ohne Anspruch auf Vollständigkeit - diskutiert.

Anzahl und Diversität der Komponenten: Komplexe Systeme sind typischerweise geprägt von einer Vielzahl unterschiedlicher Einzelkomponenten. Es müssen die Schwachstellen und potentiellen Angriffspunkte dieser Komponenten sowie die korrekte Konfiguration bekannt sein, was bei einer großen Zahl an unterschiedlichen Komponenten sehr aufwendig sein kann und jedenfalls gute Systemkenntnisse erfordert.

Häufige und rasche Änderungen des Systems: Die große Anzahl an Einzelkomponenten bringt es auch mit sich, dass sich das System meist sehr schnell ändert, neue Komponenten eingebunden werden oder die Komponenten anders vernetzt werden. Jede Änderung am System bringt potentiell neue Bedrohungen, Schwachstellen und Risiken mit sich. Ein Risikoanalyseverfahren sollte möglichst einfach und effizient auf solche Änderungen reagieren können, allerdings wird es in der Praxis nicht möglich sein, Risikoanalysen immer zeitnahe nachzuziehen. Hier sind auch entsprechende Maßnahmen im Systemdesign und im Risikomanagement erforderlich, wie etwa die Entwicklung resilienter Systeme sowie die Einbeziehung von Sensormessdaten und Inputs aus dem SIEM, wie in Kapitel 4 und 5 diskutiert.

Unterschiedliche Schutzziele: Informationssicherheit umfasst immer die Gewährleistung zumindest der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, was generell erheblich zur Komplexität von ISRA beiträgt, da die Risiken in Bezug auf alle relevanten Schutzziele zu ermitteln sind. Je nach System können weitere Schutzziele von Bedeutung sein, wie etwa Authentizität, Gewährleistung der Privatsphäre (Privacy),

Zuverlässigkeit oder die Nachweisbarkeit von Aktionen (Non-Repudiation). Gerade in komplexen Systemen kann eine Vielzahl unterschiedlicher Schutzziele, die möglicherweise auch in Konflikt miteinander stehen, gegeben sein.

Konfigurationseinstellungen und deren Überwachung: Risiken entstehen in vielen Fällen nicht nur in Folge von systemimmanenten Schwachstellen, sondern auch durch unzureichende oder fehlerhafte Konfigurationen. Einstellungen müssen korrekt sein und laufend auditiert bzw. überwacht werden, Risiken aus Konfigurationsänderungen müssen in die Gesamtrisikobetrachtung einbezogen werden.

Einsatz von Low-Cost-Komponenten: In komplexen Systemen ist auch damit zu rechnen, dass aufgrund des Kostendrucks Komponenten zum Einsatz kommen, die keine oder schwache Sicherheitsfunktionen enthalten. Eine wichtige Frage für die Risikobeurteilung ist auch, ob solche Komponenten ausreichende Update- und Steuerungsmöglichkeiten haben. Neue Technologien, wie etwa Physically Unclonable Functions (PUFs), sollen dem gegensteuern und als Kern für Sicherheitsmechanismen, etwa Authentisierungsmechanismen oder kryptographisches Key-Management, auch in solchen Anwendungen fungieren. In jedem Fall ist in der Risikoanalyse diesen Komponenten besondere Aufmerksamkeit zu widmen. Ein Risikoanalyseansatz für Physically Unclonable Functions ist in [KSD14] zu finden.

Abhängigkeiten: Eine Kompromittierung von für sich alleine genommen unkritischen und aus diesem Grund unzureichend geschützten Komponente kann unter Umständen einen erfolgreichen Angriff auf andere Komponenten nach sich ziehen. Insbesondere ist dabei zu bedenken, dass die Zusammenhänge und Abhängigkeiten und die Risikopropagation in Abhängigkeit von den Schutzzielen (zumindest Vertraulichkeit, Integrität und Verfügbarkeit) unterschiedlich sein können. Während bei der Sicherstellung der Vertraulichkeit meist ein "Defense-in-Depth"-Konzept zum Tragen kommt, also unterschiedliche "Verteidigungslinien" aufgebaut werden, so dass bei Brechen einer dieser Linien noch nicht das Gesamtsystem korrumpiert ist, ist im Bereich der Verfügbarkeit eher die Gefahr gegeben, dass sich der Ausfall kleiner Komponenten kritisch auf wichtigere Komponenten und das Gesamtsystem auswirkt.

Risikoaggregation: Die heute üblichen Risikoanalyseansätze im Bereich Informationssicherheit bieten, wie in Kapitel 2 ausgeführt, eine gute Basis für die Auswahl von Sicherheitsmaßnahmen, aber nur bedingt eine Grundlage für übergreifende Geschäftsentscheidungen, da die Aggregation der Risiken zu einem Gesamtrisiko in den wenigsten Fällen zufriedenstellend gelöst ist. Gerade in komplexen Systemen ist es aber auch erforderlich, das Gesamtrisiko, das von solchen Systemen ausgeht, abzuschätzen, insbesondere Klarheit darüber zu bekommen, ob und in welchem Ausmaß dieses Risiko existenzbedrohend für ein Unternehmen sein kann oder gravierende Auswirkungen auf die Gesellschaft hat. Einen interessanten Ansatz zur Risikoaggregation auf Basis eines Graphenkonzeptes gibt [SC15].

4 Lösungsansätze

In diesem Abschnitt wird diskutiert, wie Information Security Risk Management für einen Einsatz in hochkomplexen Systemen aussehen kann. Welche Ansätze aus dem klassischen Risikomanagement können übernommen und weiterentwickelt werden, wo braucht es neue Lösungen und wie können diese aussehen?

Szenarienbasierte Impact Analyse:

Im Business Continuity Management (BCM) ist es bereits heute üblich, schon in einem frühen Stadium des BCM Prozesses eine Auswirkungsanalyse durchzuführen: in der BIA (Business Impact Analyse) wird zunächst festgestellt, welche Geschäftsprozesse die höchste Kritikalität haben, d.h. der Ausfall welcher Geschäftsprozesse den höchsten Schaden verursachen würde. Erst nachfolgend ist für diese Geschäftsprozesse eine "klassische" Risikoanalyse, allerdings konzentriert auf den Bereich Verfügbarkeit, durchzuführen. Einen ähnlichen Zugang finden wir in der neuen EU Datenschutz-Grundverordnung. Diese schreibt in Artikel 35(1) eine Datenschutz-Folgenabschätzung (Data Protection Impact Analysis, DPIA) vor, wenn "eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge (hat)". BIA und DPIA stellen jeweils auf einen spezifischen Aspekt der Informationssicherheit bzw. auf ein definiertes Schutzziel ab: die BIA auf Verfügbarkeit, die DPIA auf den Schutz personenbezogener Daten (Privacy).

Eine Impact Analyse im Bereich der Informationssicherheitsrisiken muss alle für das betrachtete System relevanten Schutzziele, also etwa Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit (Accountability), Verbindlichkeit (Non-Repudiation), oder Privacy, berücksichtigen. Als erster Schritt empfiehlt sich daher eine Feststellung der relevanten Schutzziele.

Zu diskutieren bleibt die Frage, auf welcher Ebene eine solche Impact Analyse ansetzen sollte. Die BIA im BCM setzt auf Geschäftsprozessebene an (s. etwa [BSI08c]), die DPIA bei der "Verarbeitung", also auf Ebene von Services. Auch im klassischen ISRA wird meist empfohlen, von den Geschäftsprozessen auszugehen, in der Praxis starten Risikoanalysen dennoch oft auch auf Ebene von Komponenten, wie beispielsweise Server oder Netzwerkkomponenten. Für einen durchgängigen Top-Down-Approach ist es sicherlich unumgänglich, auf einer hohen Ebene, also idealerweise auf Ebene der Geschäftsprozesse, und nicht auf Komponentenebene, anzusetzen.

Um der Komplexität der Fragestellungen gerecht zu werden, empfiehlt es sich, auf einen szenarienbasierten Ansatz zurückzugreifen. Dabei werden verschiedene Szenarien durchgedacht und ihre Auswirkungen auf die Schutzziele abgeschätzt. Bedrohungen, Eintrittswahrscheinlichkeiten und bestehende Sicherheitsmechanismen spielen in dieser Phase noch keine oder allenfalls eine untergeordnete Rolle. Die Szenarien müssen

jedoch grundsätzlich realistisch sein. Es ist zu ermitteln, welche Auswirkungen die betrachteten Sicherheitsvorfälle auf das Gesamtunternehmen und den Unternehmenserfolg haben. Die Szenarien mit dem größten Impact können dann näher untersucht werden, etwa in Form einer Top-Down-Analyse, vergleichbar mit einer Fehlerbaumanalyse (Fault Tree Analysis, FTA), wie sie in technischen Bereichen angewendet wird [DIN90]. In diesem Schritt sind dann auch detaillierte Risikoanalysen auf Basis von Komponenten durchzuführen, um konkrete Bedrohungen und Schwachstellen zu erkennen und auf deren Basis entsprechende Schutzmaßnahmen auszuwählen.

Toolunterstützung:

Eine der großen Herausforderungen an Risikoanalysen in IT-Systemen liegt in der raschen Veränderung der Parameter. Nicht nur die Bedrohungslage kann sich sehr rasch ändern, auch das System selbst ist meist vielfältigen und raschen Änderungen unterworfen: neue HW- und Softwarekomponenten, eine Änderung in baulichen Gegebenheiten oder in der Netzwerkstruktur sowie die Verarbeitung neuer Datenklassen können die Risikolage rasch verändern.

Die Erstmodellierung des Systems erfordert im Allgemeinen sehr viel Aufwand. Um zumindest rasch auf Änderungen reagieren zu können, ist es wichtig, die Modellierung toolunterstützt durchzuführen und Änderungen zeitnah einzupflegen. Eine weitgehende Automatisierung der Einbeziehung neuer Komponenten ist anzustreben.

SIEM-unterstützt:

Ein Security Information and Event Management System (SIEM) ermöglicht eine echtzeitnahe Analyse von Sicherheitswarnungen, die von Netzwerkkomponenten oder Applikationen generiert werden. SIEM-Lösungen bauen im Allgemeinen auf Log-Systemen auf und ermöglichen eine frühzeitige Erkennung von Angriffen und schnellere und bessere Reaktion auf Sicherheitsvorfälle (Security Incidents). Zunehmend werden SIEM-Lösungen heute auch zur Erkennung und Abwehr hochentwickelter zielgerichteter Angriffe (Advanced Persistent Threats, APTs) eingesetzt, da sie eine schnelle Reaktion auf die tatsächlichen Gegebenheiten in einem System ermöglichen.

Eine Einbindung von SIEM-Lösungen in das Risikomanagement ermöglicht zu einem gewissen Grad eine automatische Aktualisierung der Einschätzung der Risikolage und der Anpassung oder Einleitung von entsprechenden Sicherheitsmaßnahmen.

Eine automatisierte Einbeziehung von Messdaten und Sensoren in das Gesamtsystem erhöht die Aktualität der Risikobewertung weiter und unterstützt den Aufbau eines effizienten Risikomanagements. Ein gutes Beispiel für ein Risikoanalysesystem auf Basis von IT-Grundschutz und unter Einbeziehung von automatisierten Messdaten gibt etwa [Sc14].

5 Risikomanagementstrategien für komplexe Systeme

Wie oben ausgeführt ist eine Risikoanalyse wichtige Voraussetzung um Sicherheit in einem System zu gewährleisten. Für komplexe Systeme gilt dies in besonderem Maße. Dennoch sind gerade in komplexen Systemen auch andere Vorkehrungen, wie die Integration von Sicherheit bereits in der Entwicklung der Systeme, Absicherung durch Basisschutzmaßnahmen und die Entwicklung resilienter Systeme, unabdingbar. Einige davon werden in der Folge diskutiert.

Security by Design und Privacy-by-Design:

Im IT-Bereich werden Sicherheitsfunktionen heute oft erst im Nachhinein auf ein System aufgesetzt, was zu Fehlern führt und sehr kostenintensiv sein kann. Wünschenswert wäre eine integrierte Basissicherheit sowohl für die einzelnen Komponenten (s.u.) als auch für das Gesamtsystem ("security-by-design", "privacy-by-design"). Die Beachtung von Sicherheitsanforderungen bereits beim Systemdesign und in der Systementwicklung sowie die möglichst weitgehende Verwendung standardisierter Schnittstellen und Sicherheitsfunktionen können dazu beitragen, die Sicherheit der Systeme von vornherein entsprechend hoch zu gewährleisten.

Integrierte Sicherheit in allen Systemen und Komponenten:

In vielen Produkten des täglichen Lebens ist Sicherheit bereits ein integrierter Bestandteil. Elektroartikel, Kinderspielzeug und Autos unterliegen strengen Vorgaben, und ihre Qualität und Zuverlässigkeit wird streng geprüft. Produktrückrufe zeigen, dass zwar auch in diesen Bereichen keine 100%-ige Perfektion erreicht werden kann, dass jedoch ein gutes Prüf- und Kontrollsystem existiert und eine laufende Verbesserung vorgesehen ist. Angemessene Authentisierungsmechanismen, die Möglichkeit zu Updates und der Schutz von Vertraulichkeit und Integrität der Kommunikation sollten zum Standard-Repertoire aller Komponenten gehören. Mit Hilfe neuer Technologien, wie etwa PUFs, ist es heute möglich, auch in low-cost Komponenten, die für den Massenmarkt produziert werden, hohe Sicherheit zu gewährleisten. Dazu sind neben entsprechenden kryptographischen Verfahren (z.B. light-weight Kryptomechanismen) insbesondere auch spezifisch auf die verwendeten PUF-Technologien abgestimmte Fehlerkorrekturmechanismen erforderlich. [De15] gibt eine detaillierte Analyse und ein Design solcher Algorithmen anhand eines Prototyps zum Software-Schutz.

Basisschutz als Grundlage für das Risikomanagement:

In der Vergangenheit sehen wir unterschiedliche Zugänge zu Risikoanalyse und darauf aufbauender Risikobehandlung. Während in der 1970-er und 1980-er Jahren die "klassische" detaillierte Risikoanalyse für ein gesamtes System das Mittel der Wahl war, führte die zunehmende Komplexität der zu betrachtenden Systeme spätestens in den 1990-er Jahren zu einem Paradigmenwechsel. Mittels Basissicherheitsmaßnahmen sollten die Systeme gegen sogenannte pauschalisierte Gefährdungen geschützt werden, sehr rasch setzte sich ein kombinierter Ansatz durch, der eine Absicherung der

Systemteile und Komponenten mit normalem Schutzbedarf über generelle Sicherheitsmaßnahmen ("Grundschutzmaßnahmen") vorsieht, und für Bereiche mit sehr hohen Sicherheitsanforderungen eine detaillierte Risikoanalyse. Bekanntestes Beispiel dafür im deutschen Sprachraum ist der IT-Grundschutz des deutschen Bundesamtes für Informationssicherheit (BSI) ([BSI08a], [BSI08b]), auch das Österreichische Informationssicherheitshandbuch [BKA16] folgt dieser Vorgehensweise.

Während im kombinierten Risikoanalyseansatz meist bereits in einem frühen Stadium eine Trennung von normal- und hoch-schutzbedürftigen Systemteilen erfolgt, gehen neuere Ansätze davon aus, dass für alle Komponenten eine Basissicherung vorhanden sein sollte, auf der aufbauend weitere Standardschutzmaßnahmen sowie detaillierte Risikoanalysen für die besonders gefährdeten Szenarien / Komponenten erfolgen sollen. Der im Zuge der Modernisierung des IT-Grundschutzes des BSI gewählte Ansatz folgt dieser Vorgehensweise [BSI16]. Für komplexe Systeme ist es in besonderem Maße notwendig, dass die einzelnen Komponenten entsprechende Basisschutzmechanismen, wie etwa Authentisierungsmechanismen, haben.

Resilience:

Bereits beim Design komplexer Systeme sollte darauf geachtet werden, dass diese möglichst widerstandsfähig gegen Angriffe, aber auch gegen Fehlfunktion oder Ausfall einzelner Komponenten sind. Resiliente Systeme sind dadurch gekennzeichnet, dass sie auch im Angriffs-, Fehler- oder Katastrophenfall nicht vollständig ausfallen oder Informationen in großem Ausmaß preisgeben, und möglichst schnell und stabil wieder in ihren Ausgangszustand kommen. Sie ermöglichen per se Ausweichlösungen, wenn es zu Problemen kommt. Wichtige Mechanismen für Resilience im IT-Bereich sind etwa verteilte Verarbeitung, redundante Kommunikationsverbindungen oder Backup- und Recovery-Mechanismen.

6 Zusammenfassung und Ausblick

Risikoanalyse ist eine entscheidende, unverzichtbare Voraussetzung für die Abschätzung des Gesamtrisikos eines Systems und der Auswirkungen auf eine Organisation oder die Gesellschaft, sowie für die Auswahl von Sicherheitsmaßnahmen. Gerade im Bereich IT- und Informationssicherheit können Risikoanalysen allerdings auch für kleinere Systeme sehr aufwendig werden.

In komplexen Systemen ergibt sich eine Reihe von neuen Anforderungen an die Informationssicherheits-Risikoanalyse, die in Kapitel 3 diskutiert wurden. Es braucht neue Ansätze zur Risikoanalyse, insbesondere zur Risikoaggregation und zur Automatisierung der Risikoabschätzung (s. Kapitel 4), aber auch ein umfassendes Risikomanagement, wie in Kapitel 5 diskutiert, um die Sicherheit der Informationen und der sie verarbeitenden IT-Systeme auf Dauer zu gewährleisten.

Literaturverzeichnis

[BKA16] Österreichisches Informationssicherheitshandbuch

[BSI08a] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Bonn, 2008

[BSI08b] Bundesamt für Sicherheit in der Informationstechnik (BSI): Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Bonn, 2008

[BSI08c] Bundesamt für Sicherheit in der Informationstechnik (BSI): Notfallmanagement, BSI-Standard 100-4, Bonn, 2008

[BSI16] Bundesamt für Sicherheit in der Informationstechnik (BSI): Modernisierung IT-Grundschutz, www.bsi.bund.de/IT-Grundschutz, Stand Juni 2016

[De15] Deutschmann, M.: Mathematical Investigations on the Stability of PUF Responses Considering Different Error Correcting Mechanisms, Dissertation, Alpen Adria Universität Klagenfurt, 2015

[DIN90] Deutsches Institut für Normung e.V. (DIN): DIN 25424 Fehlerbaumanalyse

[EN15] European Union Agency for Network and Information Security (ENISA): ENISA Threat Landscape 2015, www.enisa.europa.eu/publications/etl2015, Stand Juni 2016

[ISO09] International Organization for Standardization (ISO): ISO 31000 Risk management – Principles and guidelines, 2009

[ISO11] International Organization for Standardization (ISO), International Electrotechnical Commission (IEC): ISO/IEC 27005 Information technology — Security techniques — Information security risk management, 2011

[ISO13] International Organization for Standardization (ISO), International Electrotechnical Commission (IEC): ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements, 2013

[Ko08] Kotsios, C. G.: ROISI – Investitionsentscheidungen im IKT-Sicherheitsbereich, VDM Verlag Saarbrücken, 2008

[KSB14] Kolberger, A.; Schaumüller-Bichl, I.; Deutschmann, M.: Risk Analysis of Physically Unclonable Functions, Proceedings CMS2014, LNCS 8735, 2014

[Sc14] Schiebeck, S.: An Approach to Continuous Information Security Risk Assessment focused on Security Measurements", Dissertation, Universität Wien, 2014

[Sc15] Schiebeck, S.; Latzenhofer, M.; Palensky, B.; Schauer, S.; Quirchmayr, G.; Benesch, T.; Göllner, J.; Meurers, C.; Mayr, I.: Implementation of a Generic ICT Risk Model using Graph Databases, Proc. SECUWARE 2015, pp. 146-153, Venedig, 2015

[St08] Stallinger, M.: IT-Governance im Kontext Risikomanagement, VDM Verlag Saarbrücken, 2008