Quantitative Ansätze zur IT-Risikoanalyse

Erik Tews, Christian Schlehuber

Security Engineering Group
Technische Universität Darmstadt
Hochschulstr. 10
D-64289 Darmstadt
e_tews@seceng.informatik.tu-darmstadt.de
cschlehuber@seceng.informatik.tu-darmstadt.de

Abstract: Im Bereich der Risikoanalyseverfahren für kritische IT-Systeme werden primär qualitative Analyseverfahren eingesetzt, welche auf einer Expertenschätzung des Risikos beruhen. Dieses Vorgehen birgt ein hohes Risiko für Fehleinschätzungen durch den Analysten, welches im schlimmsten Fall zu einem unbrauchbaren Sicherheitskonzept führen kann, da die Sicherheitsarchitektur entsprechend der anfänglichen Risikoanalyse gestaltet wird. Diese Arbeit stellt ein erweitertes Verfahren vor, welches durch feingranulare Schätzungen von einzelnen Faktoren die Wahrscheinlichkeit eines Fehlers minimiert und auf diese Weise einen weiteren Schritt in Richtung quantitative Methoden zur IT-Risikoanalysen beschreitet. Zu diesem Zweck kommen Bewertungsskalen zum Einsatz, welche eine spätere Berechnung von Scores ermöglichen. Hierfür wird auf den Assets der jeweiligen Domäne beginnend eine systematische Analyse von möglichen Zielen, Angreifergruppen, Angreifermitteln und denkbaren Schwachstellen durchgeführt. Die Angreifergruppen sowie die möglichen Mittel werden feingranular modelliert und in einer abschließenden Bewertung auf ihr potentielles Risiko für das System überprüft.

1 Einleitung

IT-Systeme werden in vielen sicherheitskritischen Bereichen sowie in kritischen Infrastrukturen eingesetzt. Im Rahmen dieser Verwendung muss folglich die Sicherheit von solchen Systemen sichergestellt werden, was auch durch die Politik im Rahmen des aktuellen Referentenentwurfs „Zur Erhöhung der Sicherheit in informationstechnischen Systemen“ [Bun13] in Deutschland, als auch durch ähnliche Dokumente in der EU und den USA, forciert wird.

Bei der Betrachtung der Sicherheit von IT-Systemen muss man zwischen „Safety“ und „Security“ eines Systems unterscheiden. Während „Safety“ die Ausfallsicherheit durch Fehler im System durch die eingesetzte Technik oder auch eventuelle Fehlbedienungen behandelt, befasst sich „Security“ mit gezielten Angriffen von Dritten auf ein System. Im Bereich von „Safety“ haben sich durch Industrie und Wissenschaft über die vergangen Jahre anerkannte Standards für die Risikoeinschätzung und Bewertung entwickelt, die auf quantitativen Verfahren basieren. So wurden beispielsweise durch IEC61508/IEC61511

die „Safety Integrity Level“ eingeführt [Com99]. Die Einführung solcher Verfahren im Kontext der „Security“ hat bislang nicht stattgefunden und eine Übertragung ist aufgrund des stark unterschiedlichen Bedrohungsmodells nicht ohne Weiteres möglich. Bei Analysen auf „Security“-Risiken kommen daher meist qualitative Verfahren zum Einsatz, die das Risiko für einen Angriff von Experten in vorgegeben Kategorien einstufen lassen. Durch diese subjektiven Einschätzungen kann es allerdings leicht zu fehlerhaften und intransparenten Bewertungen kommen, da selbst die Meinung von Experten durch einige externe Umstände beeinflusst werden kann, wie es von Kahneman und Tvertsky in [KT79] dargestellt wird. Durch diese Einflüsse kann es dazu kommen, das die Risikoanalyse, welche den Startpunkt jedes Sicherheitskonzeptes darstellt, Schwachstellen aufweist.

Die vorliegende Arbeit liefert einen ersten Ansatz für ein Verbesserung der Bewertung dieser Risiken durch eine feingranulare Bewertung einzelner Elemente in Verbindung mit einem systematischen Analyseprozess. Hierfür wird zuerst in Abschnitt 2 ein Überblick über andere Arbeiten auf diesem Gebiet gegeben und anschließend in Abschnitt 3 eine Gesamtüberblick über den systematischen Analyseprozess und seine Einbettung in die restlichen Entwicklungsschritte gegeben. In den Unterabschnitten 3.1 bis 3.4 werden die einzelnen Schritte der Analyse im Detail betrachtet. Die Ergebnisse werden abschließend in Abschnitt 4 zusammengefasst und weitere Arbeiten werden in Abschnitt 5 aufgezeigt.

2 Related Work

Auf dem Gebiet der Sicherheitsanalyse-Verfahren haben sich über die Jahre einige Standard-Verfahren etabliert und wurden durch verschiedene Institutionen standardisiert. So entstand von der „International Organization for Standardization“ die 2700x-Reihe [Int11], die sich mit Sicherheitsmanagement in der Informationstechnik befasst. Vom deutschen „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) wurde das IT-Grundschutzhandbuch [Bun08b] geschaffen um Unternehmen einen Leitfaden zur Herstellung eines grundlegenden IT-Schutzes an die Hand zu geben. Die genannten Verfahren stellen dem Nutzer ein einfaches Verfahren zur Risikoanalyse zur Verfügung, welches jedoch auf einer qualitativen Schätzung des Risikos für eine Gefahr beruht. Diese ist durch den Analysten, bzw. durch einen Experten durchzuführen.

Neben dem Grundschutzhandbuch wurde vom BSI auch ein Verfahren zur generellen Analyse von kritischen Infrastrukturen geschaffen (AKIS)[Bun08a], welches eine Identifikation von möglichen Angriffspunkten innerhalb eines kritischen Infrastruktur Sektors ermöglicht. Eine Auflistung von weiteren Analyseverfahren kann ISO/IEC 31010 entnommen werden [Int09].

3 Prozess

Der in dieser Arbeit vorgestellte Prozess zur Sicherheitsanalyse zielt darauf ab, die bisherige Ermittlung von zu betrachtenden Gefahren für die Implementierung und Evaluation

von sicherheitskritischen Systemen zu verbessern und die bisher oft forcierte Nutzung von „Expertenwissen“ [Bun08b] durch einen ingenieurmäßigen Prozess zu verbessern.

Dieser Prozess besteht aus einer anfänglichen semi-statischen Analyse und einem darauf folgenden kontinuierlichen rückgekoppelten Prozess (eine Übersicht bietet Abbildung 1), der sich an den Regelkreisen aus [Int05] orientiert. Die semi-statische Analyse, welche die Analyse der Assets des Systems, möglicher Ziele eines Angreifers sowie Angreiferklassen umfasst, muss nur einmalig durchgeführt werden. Es ist allerdings zu empfehlen im Falle von technischen Neuerungen eine erneute Evaluation der Bewertungen durchzuführen, da der technische Fortschritt zu einer Änderung der Mittel, beziehungsweise deren Durchführbarkeit und Komplexität führen kann.

Aus diesem ermittelten Domänenwissen wird anschließend eine Bewertung anhand gewisser Verfahren erstellt, die im Folgenden vorgestellt werden. Abschließend wird aus dieser Bewertung und einem vorgegebenen geforderten Sicherheitslevel (Security Level - SL [Com13]) ein Report erzeugt, welcher die potentiellen zu betrachtenden Gefahren für das System angibt. Dieser Report kann für einen weiteren technischen Design Prozess genutzt werden oder als Grundlage für eine spätere Evaluation der Implementierung des Systems verwendet werden. Insofern nach dem Report neue Sicherheitsmechanismen in das System eingebunden werden, so werden diese im Rahmen des technischen Design-Prozesses umgesetzt und wirken auf die Anwendbarkeit der Mittel eines Angreifers ein und erhöhen die nötigen Ressourcen, bzw. entfernen Mittel komplett. Dieser Prozess kann in beliebig vielen Iterationen wiederholt werden. Auch bereits existierende Mechanismen können auf diese Art und Weise berücksichtigt werden.

3.1 Asset-Analyse

Als Startpunkt für die Sicherheitsanalyse sollte man sich zuerst mit der Domäne des Systems vertraut machen und analysieren, welche Rahmenbedingungen (rechtliche Vorschriften, Ziele, Abläufe, etc.) in dieser gelten. Zudem müssen Experten aus der Domäne einbezogen werden, da nur durch diese ein umfangreiches Domänenwissen, gerade in Bezug auf Erfahrungswerte, eingebracht werden kann. Wenn ein entsprechendes Wissen über das Einsatzumfeld des Systems vorhanden ist, so müssen die Assets der Domäne erfasst werden, da diese den Grundstein für die folgende Analyse darstellen. Erst wenn man wirklich verstanden hat, was im zu schützenden System wichtig ist, dann bekommt man eine Vorstellung davon, was ein Gegner angreifen könnte.

In den meisten kritischen Infrastrukturen können die Assets in drei Kerngruppen unterteilt werden: Betriebliche Assets (z.B. Sicherheit des Betriebs), technische Assets (z.B. Intakte Infrastruktur) und Wahrnehmungs-Assets (wie das Image des Unternehmens).

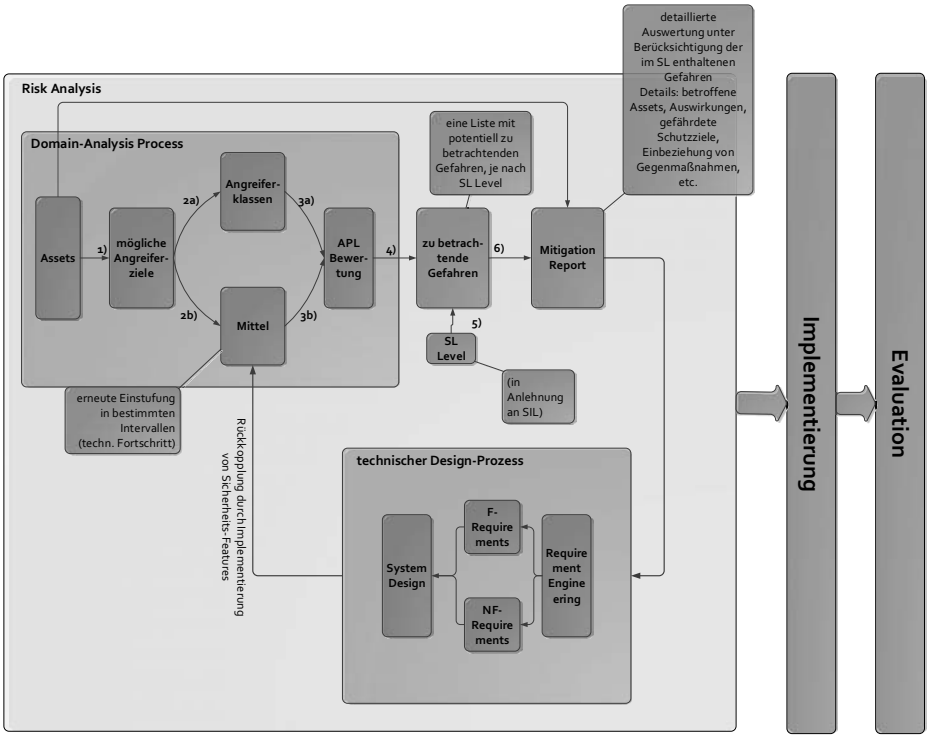

Abbildung 1: Analyseprozess im Kontext

3.2 Ziele von Angreifern

Anhand der Assets des zu betrachtenden Systems werden nun mögliche Ziele, welche ein Angreifer verfolgen könnte, abgeleitet. Hierfür führen wir anhand der Ergebnisse aus der vorausgegangenen Analyse der Domänen-Assets nun eine Identifikation von potentiellen Angreiferzielen durch. Zur Sammlung von möglichen Kandidaten bietet es sich an auch auf andere (ähnliche) Domänen zurückzugreifen und in einem folgenden Schritt zu bewerten, ob das mögliche Ziel aus dieser Domäne auch in der aktuell betrachteten Domäne realistisch ist oder nicht.

Das angewendete Vorgehen zur Identifikation von Angreiferzielen ist in Abbildung 2 veranschaulicht. Zu Beginn erfolgt die Auffüllung eines ungewerteten Ziele-Pools. Hierfür empfiehlt es sich, zur ersten Identifikation von möglichen Zielen, Experten mit einem Wissen aus der Domäne einzubeziehen und mit diesen ein gezieltes Brainstorming durchzuführen. Bei diesem Brainstorming sollte auf den bereits identifizierten Assets des Systems aufgebaut werden und zusammen mit bereits erfolgten Angriffen oder Gefährdungen auf ein Vorgängersystem ein gewisser Grundpool an Angreiferzielen gesammelt werden

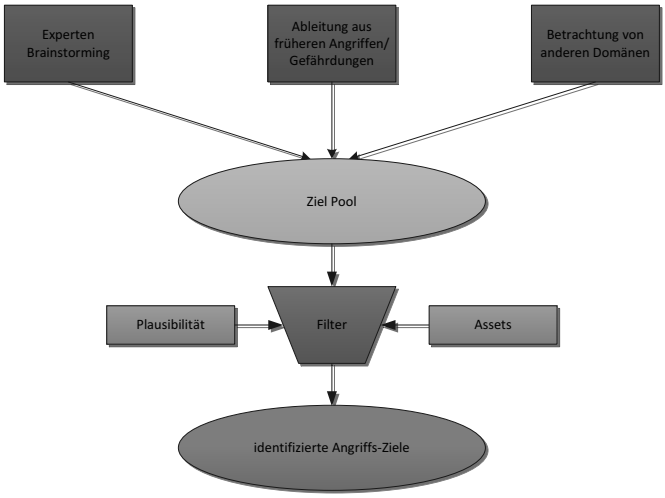

Abbildung 2: Identifikation der Angreifer-Ziele

können. Anschließend empfiehlt es sich auch einen Blick über die eigene Domäne hinaus zu werfen und zu betrachten, welche Angriffe auf andere ähnliche Sicherheitssysteme erfolgt sind und die daraus neu entstandenen Ziele mit in den Pool aufzunehmen.

Abschließend muss der Pool an identifizierten Angreiferzielen auf Plausibilität geprüft werden. Außerdem sollte geprüft werden, welches der Ziele zu welchem der Assets korrespondiert. Sollte ein Ziel zu keinem der Assets korrespondieren, so ist dieses noch einmal gezielt auf seine Plausibilität zu prüfen. Ist das Ziel plausibel, so sollte überlegt werden, ob eventuell ein Asset übersehen wurde.

3.3 Klassifikation

Nach der Identifikation der Ziele lassen sich anhand der identifizierten Ziele und Assets in einem anschließenden Schritt nun potentielle Angreiferklassen identifizieren und nach verschiedenen Charakteristika bewerten. Die Identifikation findet im Allgemeinen durch ein Brainstorming von Verantwortlichen und Experten statt und sollte klar umrissene Angreiferklassen liefern.

Generell lässt sich bei Angreifern zwischen drei Gruppen unterscheiden:

Gezielte Angreifer
Angreifer, die das aktuelle System mit einem bestimmten Ziel angreifen und sich

der Konsequenzen ihres Handelns bewusst sind (z.B. ein Hacker, der eine Firewall knackt).

Versehentliche Angreifer
Angreifer, die das System eher aus Zufall, bzw. unbeabsichtigt schädigen, z.B. ein Computer-Wurm, der eigentlich auf ein bestimmtes Ziel gerichtet war, allerdings durch eine gewisse Ähnlichkeit des zu schützenden Systems auch dieses angreift (Prominentes Beispiel: Stuxnet, dessen eigentliches Ziel Zentrifugen waren und der danach auf zahlreiche Industrieunternehmen übersprang).

Nicht-menschliche Gefahren
Hierbei handelt es sich um Gefahren, die nicht zwingend durch eine gezielte menschliche Handlung hervorgerufen werden (z.B. eine Überschwemmung oder ein Kabelbruch durch Materialermüdung). Diese werden primär durch Methoden der „Safety" behandelt.

Im Anschluss an die Identifikation findet die Klassifikation nach gewissen Charakteristika statt (im weiteren Verlauf betrachten wir nur die Gruppe der „Gezielten Angreifer"). Für diese Einstufung werden die folgenden Charakteristika genutzt und abschließend entsprechend ihrer Ausprägung gewertet:

Motivation:
1: Ein Angriff wird nur unter perfekten Bedingungen durchgeführt
5: Ein Angriff wird trotz aller Widrigkeiten stattfinden

Vorhandenes Expertenwissen, bzw. Zugriff auf Expertenwissen:
1: Expertenwissen ist für den Angreifer (nahezu) unzugänglich
5: Expertenwissen ist bei dem Angreifer bereits vorhanden, bzw. unmittelbar zugänglich

Vorhandenes Insiderwissen, bzw. Zugriff auf Insiderwissen:
1: Insiderwissen ist für den Angreifer (nahezu) unzugänglich
5: Insiderwissen ist bei dem Angreifer bereits vorhanden, bzw. unmittelbar zugänglich

Zugriff auf Spezialgeräte:
1: Sind durch den Angreifer nicht zu beschaffen
5: Sind bereits beim Angreifer vorhanden

Zugriff auf finanzielle Ressourcen:
1: Keine oder nur sehr geringe finanzielle Mittel vorhanden
5: Dem Angreifer stehen nahezu unbegrenzte Mittel zur Verfügung

Vorbereitungszeit:
1: Keine, es handelt sich um einen spontanen Täter
5: Sehr lange Zeit für eine intensive Vorbereitung

Ausgangsbasis:
1: Der Angreifer agiert vor Ort und es besteht ständig das Risiko entdeckt zu werden
5: Der Angreifer kann sich entfernt vom Ziel vorbereiten und Tests durchführen

Entdeckbarkeit des Angreifers:

1: Eine Entdeckung hätte für den Angreifer untragbare Konsequenzen
5: Eine Entdeckung wäre für den Angreifer sogar noch ein Bonus (z.B. bei terroristischen Anschlägen)

Personelle Ressourcen:

1: Es handelt sich um einen Einzeltäter
5: Es steht ein reichlicher Fundus an Personal zur Verfügung

Die einzelnen Charakteristika werden durch ein Punktesystem gewertet, welches von 1 bis 5 reicht, wobei verallgemeinert gilt: 1 = ungefährlich, da keine Ressourcen in Hinblick auf diese Charakteristik vorhanden sind; 5 = gefährlich, es sind große Ressourcen für diese Charakteristik vorhanden. Zwischen diesen Werten erfolgen jeweilige Abstufungen. Ein exemplarisches Beispiel aus der Bewertung kann Abbildung 3 entnommen werden.

	Motivation	Expertenwissen	Insiderwissen	Spezialequipment	Geld	Vorbereitungszeit	Ausgangsbasis	Entdeckbarkeit	Personal	Angreiferpotential
Vandalen	2	1	1	1	1	1	1	2	1	1,22
Hacker	3	5	2	3	2	4	3	1	1	2,67
Computerkriminelle	4	5	3	4	3	4	3	2	2	3,33
Terroristische Organisationen	5	2	2	2	4	5	5	5	3	3,67
Andere Staaten (Konflikt)	4	5	5	5	5	5	5	4	5	4,78

Abbildung 3: Auszug aus der Bewertung potentieller Angreiferklassen (Domäne: Leit- und Sicherungstechnik der Eisenbahn)

Zur Gesamtbewertung der Angreiferklasse wird noch ein abschließender Score eingeführt: das Angreiferpotential. Das Angreiferpotential ist eine einfache Abschätzung der Gesamtgefahr, die von einer bestimmten Angreifergruppe an sich ausgeht. Es wird später im Rahmen der Bewertung in Zusammenhang mit dem SL zur Selektion der relevanten Angreifer benötigt. Es berechnet sich wie folgt:

$$\begin{aligned} \text{Menge der Charakteristika } & C \\ \text{Bewertung der Charakteristik: } \forall c \in C : & \; R_c = \{1, .., 5\} \\ \text{Angreiferpotential } P_{Angreifer} = & \frac{\sum R_c}{|C|} \end{aligned} \tag{1}$$

Aus dem beschriebenen Vorgehen ergibt sich letztendlich die Bewertung für unsere betrachteten Angreifer und diese werden nach ihrem Potential gelistet. Einen ähnlichen Prozess durchlaufen auch die zur Realisierung der Ziele denkbaren Mittel der Angreifer. Diese werden analog zu den Angreifern klassifiziert, allerdings werden diese nach dem entsprechenden Bedarf an Ressourcen eingestuft.

3.4 Bewertung

In einer weiteren Phase werden nun die separat voneinander bewerteten Angreiferklassen und Angreifermittel zusammengeführt. Hierdurch wird ermittelt, auf welche Schwachstellen man sich besonders konzentrieren sollte, da deren Eintreten als wahrscheinlich anzusehen ist.

Für eine bessere Entscheidbarkeit beim gezielten Absichern gegen Schwachstellen werden wir die einzelnen Mengen nun in einem Mapping-Prozess kombinieren und auf diese Weise eine Bewertung für die jeweilige Kombination ermitteln. In einem dem Mapping-Prozess vorgelagerten Schritt wird die Angreifer-Liste gemäß dem gewählten SL-Level gefiltert. Hierdurch wird der aufwendige Mapping-Prozess nur für relevante Angreifer-Mittel Kombinationen durchgeführt.

Um diese Auswahl für die zu betrachtenden Gefahren für den Security Level des untersuchten Systems zu treffen, wurde zur Vereinheitlichung, in Anlehnung an [Com99] und [Com13], der SL eingeführt, der die Stufen 1 bis 4 umfasst. Je höher der SL, umso mehr Angreifer und damit auch Gefährdungen werden in der Liste der zu betrachtenden Gefahren berücksichtigt.

$$\text{SL1} \subseteq \text{SL2} \subseteq \text{SL3} \subseteq \text{SL4} \tag{2}$$

Als erste echte Mapping Phase werden nun die identifizierten Schwachstellen und Mittel M auf die bereits zuvor identifizierten und gefilterten Angreifer A über die Charakteristika C gemappt. Aus dem Mapping-Prozess resultiert das Gefahrenpotential P für diese spezielle Angreifer-Mittel Kombination.

Im Rahmen des Mapping-Prozesses betrachten wir die vorher ermittelten Werte der Angreifer und der Mittel als Ressourcen, bzw. Ressourcenkosten. Daher ergeben sich die folgenden Relationen:

$$\text{Expertenwissen} \leftrightarrow \text{benötigtes Expertenwissen} \tag{3}$$
$$\text{Insiderwissen} \leftrightarrow \text{benötigtes Insiderwissen} \tag{4}$$
$$\text{Spezialequipment} \leftrightarrow \text{benötigtes Spezialequipment} \tag{5}$$
$$\text{Geld} \leftrightarrow \text{Kosten} \tag{6}$$
$$\text{Vorbereitungszeit} \leftrightarrow \text{benötigte Vorbereitungszeit} \tag{7}$$
$$\text{Entdeckbarkeit} \leftrightarrow \text{Entdeckbarkeit des Angreifers} \tag{8}$$
$$\text{Personal} \leftrightarrow \text{benötigtes Personal} \tag{9}$$

Anschließend lässt sich noch ein Gesamtscore für die jeweilige Gefahr errechnen. Dieser Gesamtscore berücksichtigt bei der Berechnung speziell auch noch die Motivation des Angreifers, denn diese hat eine starke Aussagekraft darüber, unter welchen Bedingungen ein Angriff durchgeführt werden würde. Wodurch wir die folgende Berechnung für den Score erhalten:

$$\text{Score}(A_m) = \begin{cases} \frac{\text{Angreifer}_{\text{Mittel}} \times \text{Angreifer}_{\text{Motivation}}}{5} & \text{if Angreifer}_{\text{Mittel}} \geq 0 \\ \varepsilon & \text{if Angreifer}_{\text{Mittel}} < 0 \end{cases} \tag{10}$$

Zuletzt lässt sich anhand dieser Scores ein Gefahren-Report erstellen, der während der Implementierung oder während einer weiteren Design Phase verwendet werden kann um gezielt Maßnahmen gegen bestimmte Bedrohungen zu implementieren. Ein Ausschnitt aus einem exemplarischen Report ist in Abbildung 4 zu sehen.

In der „Liste der noch zu behandelnden Gefahren“ des Reports wird eine Auflistung der möglichen Gefahren aufgezeigt. In dieser sind jeder Gefahr die betroffenen Assets zugeordnet, sowie die Menge der Angreiferklassen, durch welche die Gefahr genutzt werden könnte. Unter dem Punkt „Größte Gefahr“ wird die schwerwiegendste Angreiferklasse mit deren Potential dargestellt. Die Gefahren selbst sind nach deren Gefahrenscore sortiert. Jede Gefahr aus dieser Liste lässt sich unter dem Punkt „Gefahr-Details“ im Detail anzeigen. Hierbei werden die jeweils erforderlichen Mittel zur Ausnutzung der Gefahr aufgelistet und die zur Nutzung dieses Mittels fähigen Angreifer aufgeführt. Insofern ein Mittel eine Komposition aus verschiedenen Mitteln ist, kann jedes dieser Mittel in seine Komponenten aufgelöst werden. Dies kann unter dem Punkt „Bedingungen“ gesehen werden. Hierbei sind sowohl $\wedge$ als auch $\vee$ Verknüpfungen möglich. Zur anschaulichen Visualisierung kann man die Beziehung von Gefahren und deren Mittel auch in Form eines Angriffs-Baums, wie in [Sch99] beschrieben darstellen. Abschließend kann man sich zu jedem Mittel die möglichen Angreiferklassen anzeigen lassen, hierbei sind sämtliche mögliche Klassen in einer Tabelle nach deren Angreifer-Potentialen geordnet (siehe Abbildung 4 unten).

4 Zusammenfassung

In der vorliegenden Arbeit wurde ein neuer Prozess zur Analyse der Sicherheitsanforderungen an ein sicherheitskritisches IT-System vorgestellt. Es wurde gezeigt, wie durch ein methodisches Vorgehen Assets und Ziele von Angreifern identifiziert werden können und wie diese, sowie deren Mittel selbst, gezielt analysiert und bewertet werden können. Außerdem wurde dargestellt, wie mittels einer feingranularen Schätzung über die Fähigkeiten der Angreifer und die Anforderungen von möglichen Angreifern ein Bild der existierenden Gefährdungen für das System modelliert werden kann. Im Rahmen dieser Modellierung wurde ein Verfahren zur Durchführung der Risikoanalyse im Kontext des SL vorgestellt, durch diesen SL wird ein ähnlicher Indikator, wie der SIL für die Safety eines Systems, auf Security übertragen. Abschließend wurde eine übersichtliche Darstellung in Form eines Reports vorgestellt.

Durch den hier vorgestellten Prozess erfolgt eine deutliche Steigerung der Transparenz bei der Analyse der Security Anforderungen und die Arbeit des Analysten wird weniger fehleranfällig, da er nur kleine Fragmente schätzen muss und nicht eine große Gesamtwertung. Das generelle Vorgehen ist an den „risk management process“ der ISO 27005 angelehnt. So wird in den ersten Schritten ein Kontext geschaffen, danach die Risiken identifiziert und abschließend bewertet. Die Behandlung der Risiken selbst müsste anschließend

Liste der noch zu behandelnden Gefahren

Gefahr	Betriebl. Auswirkung	Betroffene Assets	Zahl der Angreiferklassen	Größte Gefahr	Score
Modifikation der Infrastruktur (6.2.17)	b,g	(5.1.2), (5.2.1), (5.2.3), (5.2.4), (5.3.1)	4	kk – 0.6	0.6
...	...	...	...	...	...

Gefahr-Details (6.2.17)

Mittel	Nutzbar durch	Entdeckbarkeit	Mittel-Score
Extraktion von krypt. Keys (8.7.1)	ko, kk, fm, ck	Sehr gering	0.6

Mittel-Details (8.7.1) - Bedingungen

Erforderliches Vorgeschehen	Nutzbar durch	Entdeckbarkeit	Mittel-Score
DD oder MdK (8.7.6 oder 8.9.1)	to, ko, kk, fm, ha, ck, er	Sehr gering	0.78
EkS (8.7.1)	to, ko, kk, fm, ha, ck, er	Sehr gering	0.54

Mittel-Details (8.7.1) – Angreiferklassen (EkS)

Angreifer	Angreifer-Potential
ck	0.914
...	...

Abbildung 4: Auszug aus dem Gefahren Report

durch eine Änderung des Designs erfolgen, was allerdings nicht zum Umfang dieser Arbeit gehört. Der Unterschied zu den bisher existierenden Arbeiten liegt in der Feingranularität der Schätzungen: Während sich aktuell oft mit einer einfach Schätzung für die Eintrittswahrscheinlichkeit beholfen wird, wird diese Schätzung hier in einzelne Charakteristika von Angreifer und Mittel zerlegt, wodurch der mögliche Fehler minimiert wird. Die anschließende Erstellung eines Scores für die Schwere des Problems, das durch diese Kombination entsteht, beruht auf einfachen nachvollziehbaren Algorithmen. Die Entscheidung über die Relevanz der Risiken erfolgt zudem über wohl definierte SL-Werte.

Auch wenn im Zusammenhang mit dem Prozess noch einige weitere Punkte betrachtet werden müssen und es sich bei der hier vorgestellten Variante erst um ein erstes Konzept handelt, so sollte die Steigerung an Genauigkeit, das methodischere Vorgehen und die Minimierung möglicher Fehlerquellen bereits gut erkennbar sein.

5 Zukünftige Arbeiten

Die weiteren Arbeiten auf dem Gebiet dieser Arbeit sind vielfältig: Zum einen wird eine Methodik geschaffen werden, welche es ermöglicht Angreifer nicht nur als einzelne Individuen, sondern auch als kooperierende Subjekte zu betrachten und abzubilden. Außerdem wird zur Steigerung der Aussagekraft in Hinblick auf das Schadensausmaß einer Gefahr eine Bewertung der Assets eingeführt werden, welche eine automatisierte Schätzung des möglichen Schadens auf ein System durch eine Gefahr ermöglicht. Um die spätere Arbeit der Analysten weiter zu erleichtern und die Analysen wirtschaftlicher zu machen wird des weiteren versucht eine Möglichkeit zu schaffen aus dem Report direkt ein „Protection Profile“ nach „Common Criteria“ abzuleiten oder zumindest Dokumente zu liefern, welche bei der Erstellung eine gute Hilfestellung geben.

Literatur

[Bun08a] Bundesamt für Sicherheit in der Informationstechnik. *Analyse Kritischer Infrastrukturen - Die Methode AKIS*. Bundesamt für Sicherheit in der Informationstechnik, 2008.

[Bun08b] Bundesamt für Sicherheit in der Informationstechnik. *Risikoanalyse auf der Basis von IT-Grundschutz (Standard 100-3)*. Bundesamt für Sicherheit in der Informationstechnik, 2008.

[Bun13] Bundeministerium des Innern. *Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme*. Bundeministerium des Innern, März 2013.

[Com99] International Electrotechnical Commission. *Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/elektrisch programmierbarer Systeme (IEC 61508)*. International Electrotechnical Commission, 1999.

[Com13] International Electrotechnical Commission. Industrial communication networks - Network and system security (IEC 62443). *International Electrotechnical Commission*, 2013.

[Int05] International Organization for Standardization. *Information security management systems - Requirements (ISO/IEC 27001:2005)*. International Organization for Standardization, 2005.

[Int09] International Organization for Standardization. Risk Management - Risk assessment techniques (ISO/IEC 31010:2009). *International Organization for Standardization*, 2009.

[Int11] International Organization for Standardization. *Information security risk management (ISO/IEC 27005:2011)*. International Organization for Standardization, 2011.

[KT79] Daniel Kahneman und Amos Tversky. Prospect Theory: An Analysis of Decision under Risk. *ECONOMETRICA*, 47(2):263–292, March 1979.

[Sch99] Bruce Schneier. Attack Trees - Modeling security threats. *Dr. Dobb's Journal*, December 1999.