Bestimmung des technical-Value at Risk mittels der bedingten Wahrscheinlichkeit, Angriffsbäumen und einer Risikofunktion

Wolfgang Boehmer

wboehmer@cdc.informatik.tu-darmstadt.de
Technische Universität Darmstadt, Morneweg Str. 30, CASED building,
64293 Darmstadt, Germany

Abstract: In diesem Artikel wird ein Vorschlag zur Berechnung eines technical-Value at Risk (t-VaR) diskutiert. Dieser Vorschlag basiert auf der Risikoszenarientechnik und verwendet die bedingte Wahrscheinlichkeit gemäß Bayes. Zur Ermittlung der Bedrohungen werden Angriffsbäume und Angriffsprofile eingesetzt. Die Schwachstellen sind empirisch für eine Versicherung im Jahr 2012 ermittelt worden. Die Angriffsbäume werden gewichtet mit einer Risikofunktion, die die kriminelle Energie beinhaltet. Zur Verifizierung dieser Vorgehensweise ist die VoIP-Telefonie einer Versicherung der t-VaR berechnet worden. Es zeigt sich, dass dieses Verfahren hinreichend gute Ergebnisse erzielt und für den technischen Bereich eine wirkungsvolle Methode darstellt[1].

Bedingte Wahrscheinlichkeit; Bayes Theorem; Angriffsbäume; Bedrohungsprofile; Risikofunktion; Risikoszenarien.

1 Einleitung

In den Anfangszeiten der Absicherung der IT, also in den frühen 90-er Jahren, lag der Schwerpunkt rein auf der technischen Absicherung. Denn man hatte zu der Zeit erkannt, dass die IT verwundbar ist. Diese oftmals kostenintensiven Maßnahmen waren zu der Zeit nicht immer an betriebswirtschaftliche Überlegungen gebunden und ein Bezug zu den Geschäftsprozessen wurde nur rudimentär hergestellt. Einen Meilenstein stellt daher der BASEL II Accord im Jahre 2004 dar, da dieser die operationellen Risiken gleichberechtigt neben den Markt und Finanzrisiken stellte. Im gleichen Zeitraum hat sich bei den Markt- und Finanzrisiken eine Bemessungsgröße für die Risiken durchgesetzt, die mit Value at Risk (VaR), respektive seine kohärente Variante der C-VaR, bezeichnet wird. Ferner wurden für die operationellen Risiken in etlichen theoretischen Modellen versucht entsprechende Bemessungsgrößen zu dem VaR zu ermitteln, die sich in der Praxis jedoch nie durchgesetzt haben. In Folge dessen entstanden die qualitativen und die quantitativen Risikoverfahren, die bis heute noch nebeneinander stehen.

[1] Dieser Beitrag ist in abgewandelter Form in englischer Sprache auf der ARES 2013 Konferenz in Regensburg (`http://www.ares-conference.eu/ares2013/`) vorgestellt und ist im Tagungsband abgedruckt.

Eine wesentliche Besonderheit in der Berechnung der Risiken zwischen den Markt- und Finanzrisiken einerseits und den operationellen Risiken andererseits liegt nun darin, dass im Bereich der operationellen Risiken die IT-Infrastruktur durch Bedrohungen und vorhandenen Schwachstellen geprägt ist[2]. Somit führt der bei den Markt- und Finanzrisiken weit verbreitete Ansatz, eine Monte Carlo Simulation zur Ermittlung der Wahrscheinlichkeitsverteilung zu verwenden, bei den operationellen Risiken zu keinen befriedigenden Ergebnissen.

Generell basiert die Risikoanalyse auf die Betrachtung zweier Verteilungen. Die erste Verteilung beschreibt die Eintrittswahrscheinlichkeit von Risikoereignissen und die zweite Verteilung stellt die Auswirkung des Risikoereignisses dar, wenn das Risiko eingetreten ist. Anschließend werden die beiden Verteilungen gefaltet. Diese gefaltete Verteilung ist eine neue Verteilung, die Risikoverteilung. Wird von dieser z.B. ein 5%-Quantil als erwarteter Verlust definiert, so ist der VaR bestimmt. Allein die Frage bleibt, wie werden realitätsnahe Verteilungen gefunden. Die Type der Eingangsverteilung bestimmt einen spezifischen Teil im Bereich des opRisk. Wir gehen im Anhang weiter auf diese Zusammenhänge ein.

Die Forschungsfrage besteht nun darin eine Methode zu entwickeln mit der ein VaR für den technischen Bereich möglich ist (t-VaR) und die Besonderheiten einer IT-Infrastruktur berücksichtigt, jedoch im Ergebnis mit den VaR der Markt- und Finanzrisiken gleich zu setzen ist.

Der restliche Artikel ist wie folgt organisiert: Im Anhang wird das zu Grunde liegende Modell diskutiert. Im Abschnitt 2 wird die Datenerhebung zur Ermittlung der Schwachstellen, die Bedrohung und die Anwendung des Models zur Berechnung des t-VaR am Beispiel einer Versicherung für deren VoIP-Anlage diskutiert. Anschließend folgt im Abschnitt 3 die Diskussion der Ergebnisse. Im Anhang und dort im Abschnitt 5.2 wird die relevante Literatur diskutiert. Der Artikel schließt mit einer kurzen Zusammenfassung, weiterführenden Überlegungen und Vorschlägen zu weiteren Untersuchungen ab.

2 Data acquisition

Gemäß dem Model, beschrieben im Anhang, wird in diesem Abschnitt die Datenerhebung bzgl. der Schwachstellen vorgenommen und, darauf abgestimmt, der attack-tree mit den dazugehörigen threat agent (actor) analysiert, um Risikoszenarien gemäß der Gleichungen 5.9 - 5.12 zu entwickeln. Dabei repräsentiert ψ die VoIP-Telephony. Andere Systeme werden nicht untersucht und so ist $\Psi = \psi$. Dies bedeutet, dass sich alle Schwachstellen, Bedrohungen und Risikoszenarien auf ψ = VoIP-Telefonie beziehen.

In der Abbildung 1 ist die VoIP-Telefonie der Versicherungsfirma grob skizziert. Es handelt sich um zwei Lokationen A, B. Die beiden Lokationen (A, B) sind über ein nicht öffentliches Netz (MPLS Cloud) verbunden und an dem Switch an der Lokation A und B werden sowohl der Datenverkehr als auch der Sprachverkehr abgehandelt. Die MPLS

[2] Anzumerken ist, dass die operationellen Risiken mehr beinhalten als nur die IT-Infrastruktur gemäß Basel II.

Cloud wird von einem Service Provider unterhalten, der neben diesen Kunden auch andere Kunden in seiner MPLS Cloud versorgt. Die Kunden des Versicherungsunternehmens wählen von außen die softphones der Mitarbeiter der Versicherung an. Neben der Erreichbarkeit (Verfügbarkeit) ist ebenso die Vertraulichkeit der Gespräche ein Sicherheitsziel für die Versicherung.

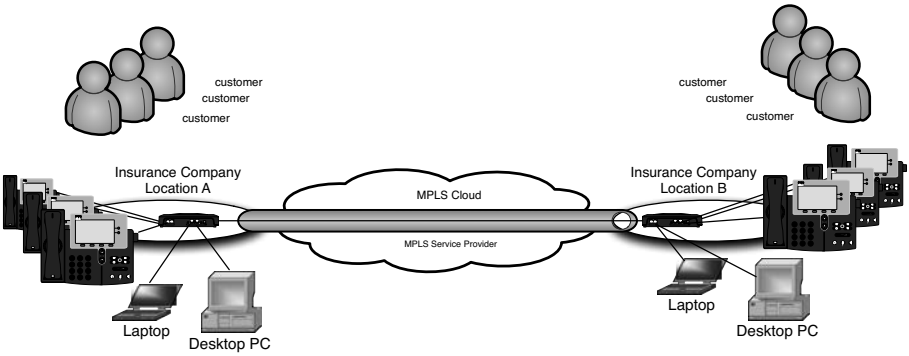

Abbildung 1: VoIP Architektur der Versicherung

2.1 Analyse der Schwachstellen

Die empirische Untersuchung in 2012 für die Versicherungsfirma hatte zum Ziel die gegenwärtigen Schwachstellen in dem Scope der VoIP-Telefonie zu analysieren. In diesem Abschnitt werden Schwachstellen exemplarisch diskutiert, um die Vorgehensweise des Models (vgl. Anhang) zu zeigen.

Die Analyse wurde in zwei Schritten durchgeführt. Im ersten Schritt wurde das VoIP-Modul (B. 4.7) der IT-Grundschutzkataloge des BSI verwendet [BSI08, mOfSiIT05]. Es wurden mittels Interview die technische Abteilung befragt. Im zweiten Schritt wurde ein *white box pentest* durchgeführt, um die Aussagen zu verifizieren und um weitere Schwachstellen zu finden. Erwähnenswert ist, dass es zwischen der VoIP-Telephony und dem Internet keine Verbindung existiert.

In der Untersuchung wurde unter anderem erkannt, dass die Sprachdaten (RTP- Stream) nicht verschlüsselt übertragen werden und die Ports an den *Softphones* und die *Patchdosen* in den Räumen nicht gegen unerlaubte Nutzung gesichert waren (IEEE 802.1x, Port Based Network Control, PBNC). Weiterhin wurde erkannt, dass keine Firewall zwischen dem MPLS Netz und dem LAN der Insurance Company existierte ebenso wurden die Sprachdaten in dem MPLS-Netz unverschlüsselt übertragen.

Basierend auf diesen Schwachstellen wurde im Anschluß eine Bedrohungsanalyse durchgeführt.

2.2 Analyse der Bedrohungen

Die Bedrohungsanalyse basiert auf den identifizierten Schwachstellen und beinhaltet drei Elemente, die Bedrohungsszenarien, die dazu passenden Bedrohungsprofile und die jeweilige Funktion der kriminellen Energie.

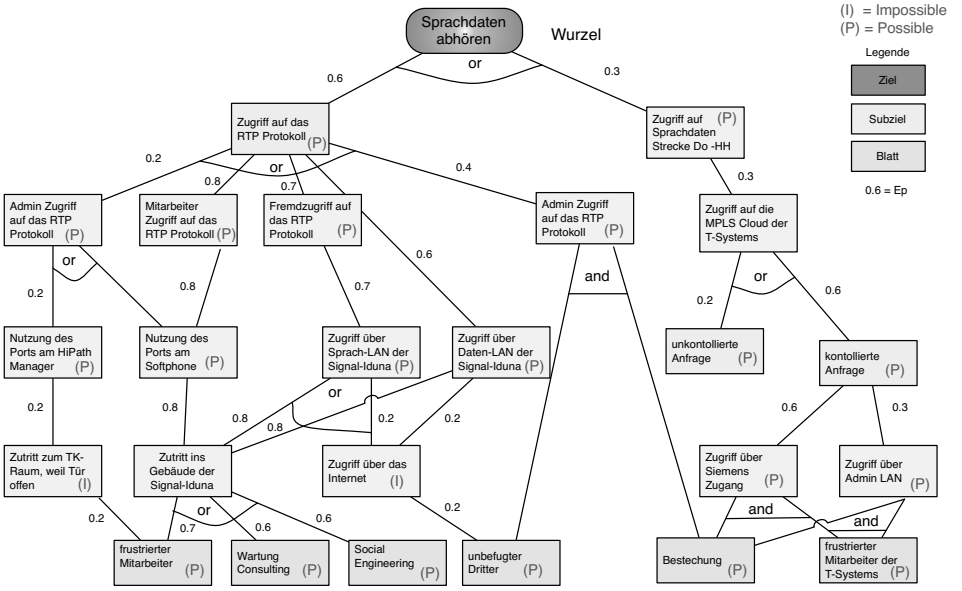

Abbildung 2: Angriffsbaum mit Werten der kriminellen Energie

In der Bedrohungsanalyse zeigen wir exemplarisch wie für das Schutzziel Vertraulichkeit der VoIP-Telefonie die aktuelle Bedrohungssituation für die Versicherungsfirma gegeben ist. Vertraulichkeit für die VoIP-Telefonie bedeutet, dass die Gespräche zwischen den Mitarbeitern der Versicherungsfirma mit ihren Versicherten nicht abgehört werden dürfen. Ebenso müssen die Gespräche zwischen den Standorten A und B vertraulich behandelt werden. Denn durch das Abhören könnte ein Schaden für die Versicherungsfirma entstehen.

Wie groß die Bedrohung tatsächlich und welches Bedrohungsprofil passend ist für die Versicherungsfirma wird in diesem Abschnitt diskutiert.

Die Abbildung 2 zeigt mögliche Bedrohungspfade für die Versicherungsfirma vom Blatt bis zur Wurzel. Zwischen den Pfaden sind entweder *oder* oder *und* Verbindungen. Die *und* Verbindung besagt, dass beide Pfade, die mit dem *und* verbunden sind, erfüllt sein müssen, um das nächste Teilziel zu erreichen. Zwischen den Teilzielen ändert sich die Funktion der kriminellen Energie. Die einzelnen Blätter stellen die Akteure dar. Die Wurzel stellt das Ziel des Angriffs (Abhören des Sprachverkehrs) dar. Die Ziffern stellen die Funktion der kriminellen Energie dar, die nach dem Muster der Gleichung 5.13 - 5.15 ermittelt wurden.

Die Indizes (I) = Impossible und (P) = Possible unterscheidet mögliche Pfade die aufgrund von Policies oder baulichen Gegebenheiten möglich oder nicht möglich sind.

Wie groß das Risiko des Abhörens (eavesdropping) tatsächlich ist wurde mit Risikoszenarien (vgl. Gleichungen 5.9 - 5.12) gemäß der Bayesian Statistik, den Angriffsbäumen, den *threat agent* und der *crimal function* abgeschätzt. Dabei wurde als *threat agent* ein Innentäter postuliert, weil sich der unverschlüsselte *voice traffic* nur in dem LAN der Versicherungsfirma bewegt und ebenfalls unverschlüsselt in der MPLS Cloud des Providers transportiert wird. Denn es ist keine Internet Verbindung für den Voice Traffic der Versicherungsfirma vorhanden und die MPLS Cloud ist ebenfalls nicht mit dem Internet verbunden. Somit kommt als Innentäter nur jemand aus der Versicherung oder jemand aus dem Umfeld (Administrator) des MPLS Cloud Providers in Frage.

Als Bedrohung wurde das Abhören (thr_1) von sensiblen Sprachdaten der Versicherungsfirma angenommen, die von einem Innentäter (threat agent) vorgenommen werden könnten. Ebenso könnte der Innentäter auch durch Service Personal (thr_2) oder als Eindringling (thr_3) dargestellt werden. Zu jedem Bedrohungsbaum und Innentäter wird eine eigene *criminal function* bzw. Risikofunktion aus den Abb. 5, Abb. 6 und Abb. 7 mit der Gleichung 5.16 abgeschätzt. Die Blätter in der Abb. 2 stellen die unterschiedlichen Bedrohungsprofile und Akteure dar. Über das Verhalten von Innentätern sind bereits eine Reihe von Artikeln erschienen, stellvertretend ist hier der Artikel von I. J. Martinez-Moyano et al. [MMRC$^+$08] zitiert. Es wird mit ψ_1 die VoIP-Infrastruktur bezeichnet und die Schwachstelle der nicht verschlüsselten Sprachdaten mit Vul_1 bezeichnet.

Der möglich entstehende Schaden für die Versicherung durch den Innentäter resultiert durch das Bekanntwerden der abgehörten Sprachdaten in der Öffentlichkeit und dem damit verbundenen Image Schaden. D.h. für das Szenario Sprachdaten abhören wird eine Annahme vorgenommen, dass 25 Versicherte ihren Vertrag im laufenden Jahr kündigen. Der Verlust durch die Vertragskündigung wird mit l_{25c} dargestellt. Der Verlust von 25 Versicherungsverträgen in einem Zeitraum von einem Jahr liegt auch deutlich oberhalb der normalen Fluktuation (Fluktuationsverlust), die mit 11 Verträgen pro Jahr (T) angegeben wurde und somit deutlich oberhalb des Erwartungswertes. Die Zahl der Verluste mit 25 Verträgen entspricht ca. einem Faktor zwei des Fluktuationsverlustes mit 11 Verträgen. Der Faktor 2 - 3 ist aus ähnlichen Reputationsverlusten (ADAC[3]) abgeschätzt.

Wir können mit den Gleichungen 5.9 - 5.12 wie folgt für die Bedrohungsprofile bzw. Akteure und Angriffsbäume dieser empirischen Fallstudie (ψ = VoIP Telefonie der Versicherung) die Risikoszenarien mit dem möglichen Verlust von 25 Verträgen unter der Berücksichtigung der Gl. 5.16 ausdrücken.

Neben dem Schutzziel der Vertraulichkeit und den Risikoszenarien wie unter $R_{sz1} - R_{szn}$ (5.9 - 5.12) beschrieben, wurden auch Risikoszenarien für die anderen beiden Schutzziele, der Verfügbarkeit und der Integrität vorgenommen. Somit wurden für das Schutzziel Verfügbarkeit und Integrität analoge Bedrohungsbäume mit passenden Akteuren entwickelt, um dann die bedingte Wahrscheinlichkeit und somit die Risikoszenarien bestimmen zu können.

[3] zum Jahreswechsel 2013/2014 sind ebenfalls Vereinsmitglieder mit einem Faktor zwei (56000 Mitglieder) gegenüber der regulären Jahreskündigung (15000)

3 Ergebnisse

In diesem Abschnitt werden die Ergebnisse der Untersuchung zur VoIP-Telefonie diskutiert.

Der Geschäftserfolg einer Versicherung lässt sich u.a. an der Menge der Versicherungsverträge ($|C|$) bestimmen. Dabei schwankt die Zahl der Versicherungsverträge ($c_i \in C$) durch natürliche Fluktuation durch Kündigungen zwischen 8 und 11 Versicherungsverträge für die empirische Fallstudie. Die Zielerwartung ist pro Jahr nicht mehr als 8 Versicherungsverträge zu verlieren, jedoch ist der Verlust von 11 Versicherungsverträgen noch akzeptabel und bildet den Wert α. Damit liegt der Erwartungswert $E_w^T(C)$ für ein Jahr bei 8 Versicherungsverträgen und entspricht dem Zielwert 1 in der Abbildung 3. Der Betrachtungszeitraum beträgt ein Jahr (T).

Die Gleichung 3.1 beschreibt die negative Schwankung um den Zielwert von 1 ($l_{c8} = 8$ verlorene Verträge). Es werden die pro Jahr hinzugekommenen Verträge in unserer empirischen Fallstudie zunächst nicht betrachtet. Aus diesem Grund wird nur die untere Verteilung (LPM) betrachtet. Die Streuungsbreite liegt bei 3 Verträgen und erreicht z.T. somit auch den Verlust von 11 Verträgen pro Jahr. Die Gleichung 3.1 beschreibt nun den Einfluss der technischen Infrastruktur mit den Schutzzielen (Confidentiality, Integrity, Availability) auf die Mächtigkeit der Menge der Verträge $|C|$.

$$\text{t-Var(C)} = \sigma_C^2 = \sum_{i=1}^{|C|} (c_i - E_w^T(C))^2 \cdot Pr\,(C = c_i). \tag{3.1}$$

Diese Erfahrungswerte der Fluktuation sind aus Beobachtungen der letzten 10 Jahre abgeleitet.

Für die Versicherung ist die Erreichbarkeit für ihre Kunden von sehr großer Bedeutung. Wenn die Kunden nicht per Telefon ihr Anliegen vorbringen können, sind diese ungehalten und bereit die Versicherung zu wechseln.

Bei dem Verlust der Vertraulichkeit entsteht ein Reputationsschaden für die Versicherung und es kündigen eine Reihe von Kunden. Es gibt interne Untersuchungen der Versicherungsfirma, die diesen Sachverhalt belegen. Dies ist einer der Gründe weshalb die Risikoanalyse durchgeführt wurde. Es hat sich gezeigt, dass durch die Risikoszenarien in der empirischen Fallstudie die Möglichkeit besteht, deutlich mehr Verträge zu verlieren, als durch den Fluktuationsschaden erwartet.

Die Abbildung 4 zeigt die LPM Verteilung in einer anderen Darstellung. Diese Darstellung wird sehr häufig für Verlustbetrachtungen vorgenommen. Es handelt sich um die diskreten Werte der Risikoszenarien, die in empirischen Fallstudien analysiert wurden. Es lässt sich zeigen, dass der erwartete Verlust zwischen 8 und 11 Verträgen deutlich überschritten wird. Es handelt sich also um einen unerwarteten Verlust.

Abschließend lässt sich für unsere Fallstudie festhalten, dass die Versicherung u.a. entschied, entsprechende Maßnahmen zur Verschlüsselung im Bereich des LAN und auf der Strecke in der MPLS-Cloud vorzunehmen. Dabei wurde darauf geachtet, dass die Kosten der Maßnahmen die möglichen Verluste nicht überschreiten.

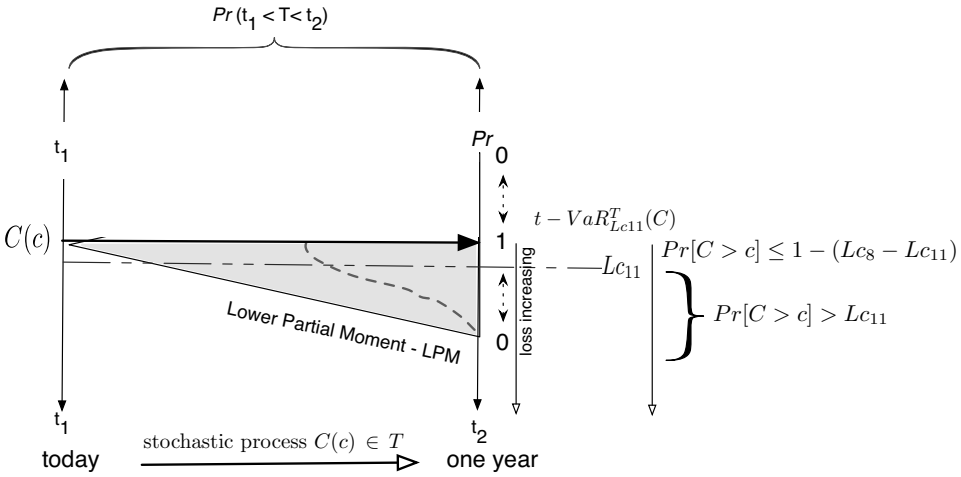

Abbildung 3: Technischer VaR für die Versicherung

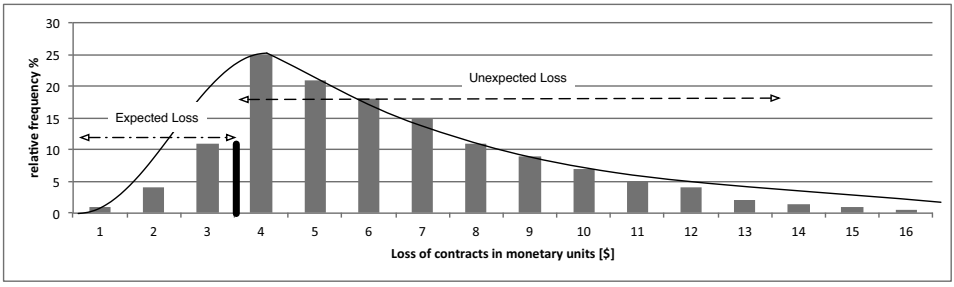

Abbildung 4: Verlustverteilung an Verträgen c_i durch den bekannt gewordenen Vertraulichkeitsverlust bei der VoIP-Telefonie

4 Kurzbeschreibung und weitere Untersuchungen

Es wird in diesem Artikel eine Methode vorgestellt, die einerseits einen technischen VaR ermittelt und andererseits auf die Besonderheiten einer IT-Infrastruktur eingeht. Am Beispiel der VoIP-Telefonie einer Versicherung wurde der t-VaR untersucht. Im Ergebnis lässt sich zeigen, dass der t-VaR eine adäquate Methode zur Bestimmung des VaR für den technischen Bereich im Rahmen der operationellen Risiken ist. Weiterführende Überlegungen zielen darauf ab für weitere Bereiche der IT-Infrastruktur einen t-VaR zu bestimmen, um dann eine Risikoaggregation zur Bestimmung des Gesamtrisikos im technischen Bereich durchzuführen.

Literatur

[BSI08] BSI. *BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise*. Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de/gshb, 2.0. Auflage, 05 2008.

[EFK03] Paul Embrechts, Hansjörg Furrer und Roger Kaufmann. Quantifying Regulatory Capital for Operational Risk. *Derivatives Use, Trading and Regulation*, 9:217–233, 2003.

[Ing] T. R. Ingoldsby. *Fundamentals of Capabilities-based Attack Tree Analysis*. Amenaza Technologies Limited, 406 – 917 85th St SW, m/s 125.

[KMMS10] Barbara Kordy, Sjouke Mauw, Matthijs Melissen und Patrick Schweitzer. Attack-defense trees and two-player binary zero-sum extensive form games are equivalent. In *Proceedings of the First international conference on Decision and game theory for security*, GameSec'10, Seiten 245–256, Berlin, Heidelberg, 2010. Springer-Verlag.

[MEL01] A. P. Moore, R. J. Ellison und R. C. Linger. Attack Modeling for Information Security and Survivability. Technical Note CMU/SEI-2001-TN-001, Carnegie Mellon University, 2001.

[MHB85] Ali Mosleh, E. Richard Hilton und Peter S. Browne. Bayesian probabilistic rsika analysis. *ACM SIGMETRICS – Performance Evaluation Review*, 13, June 1985.

[MMRC+08] Ignacio J. Martinez-Moyano, Eliot Rich, Stephen Conrad, David F. Andersen und Thomas R. Stewart. A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach. *ACM Transactions on Modeling and Computer Simulation*, 18(02), April 2008.

[mOfSiIT05] Federal Office for Security in Information Technology. IT Baseline Protection Handbook. *Bundesanzeiger, Cologne*, 2003 - 2005.

[Sch99] B. Schneier. Attack Trees. *Dr. Dobb's Journal*, 24(12):21–29, 1999.

[SW04] O. Sheyner und J. Wing. *Tools for Generating and Anaylzing Attack Graphs*, Seiten 344–371. FMCO 2003, LNCS 3188. Springer-Verlag Berlin Heidelberg, 2004.

[Wei91] J. D. Weis. A System Security Engineering Process. *Proceedings of the 14th National. Computer Security Conference*, 1991.

5 Anhang

5.1 Grundlagen

Ausgehend von dem allgemeinen linearen Zusammenhang zwischen dem Risiko ($\mathcal{R}$), der Eintrittswahrscheinlichkeit (Pr) und dem monetären Ergebnis (I), wie in der Gleichung 5.1 ausgedrückt,

$$\mathcal{R} = Pr \times I \ [\mathbb{R}], \tag{5.1}$$

$$R_{sz} = E_p(b|S) \cdot I \tag{5.2}$$

$$R_{sz} = \left(\frac{E_p(b \cap S)}{E_p(b)} \right) \cdot I \tag{5.3}$$

$$\tag{5.4}$$

wird diese Form der Risikobetrachtung nicht verwendet, sondern in diesem Beitrag wird die Verlustvariante (Lower Partial Moment vgl. Abb. 4) herangezogen.

Wie diese in Gleichung 5.5 dargestellt ist, wird nachfolgend ganz allgemein für ein System Ψ gezeigt. Denn es wird für ein System nur das negative Ergebnis als Schaden [$\mathbb{R}^-$] betrachtet, wie es im Bereich des opRisk typisch ist (vgl. Embrecht et al. [EFK03]). Diese führt den möglichen Schaden (I) und den möglichen Eintritt eines negativen bedingten Ereignisses (Ep), d.h. einer existierenden Bedrohung (thr) unter der Bedingung (|), dass eine Schwachstelle (vul) existiert, zusammen. Die bedingte Wahrscheinlichkeit sagt etwas darüber aus, wie wahrscheinlich der Eintritt eines bereits bekannten Ereignisses ist, wenn ein (bestimmtes) anderes Ereignis bereits vorher eintrat. Mit dem Risiko als Maß geht dieses als Messgröße für einen Wahrscheinlichkeitsraum und der Verlustansatz (LDA) einher.

$$\mathcal{R} = \left(Pr_E \times L \right) [\mathbb{R}^-] \ \mapsto \Psi \tag{5.5}$$

In Gleichung 5.5 wird für die Eintrittswahrscheinlichkeit (Pr) eines Ereignisses (E) nicht die frequentistische Wahrscheinlichkeit, sondern die bedingte Wahrscheinlichkeit für ein Ereignis (Pr_E) gemäß dem Satz von Bayes verwendet.

Entsprechend der Bayes Statistik wird eine Hypothese aufgestellt, die hier besagt, dass eine Schwachstelle nur unter der Bedingung (|) von einer Bedrohung mit einem dazu passendem Bedrohungsprofil *(threat agent)* ausgenutzt werden kann. Oder vice versa, dass eine Bedrohung sich nur entfalten kann, wenn eine entsprechende Schwachstelle vorhanden ist. Die Bedrohung wird mit (thr) und die Schwachstelle mit (vul) bezeichnet. Somit kann die Gleichung 5.5 in die Gleichung 5.6 umgeformt werden.

$$\mathcal{R} = \left(Pr_E \left(vul \,|\, thr \right) \times L \right) [\mathbb{R}^-] \ \mapsto \Psi \tag{5.6}$$

Somit wird die bedingte Wahrscheinlichkeit, dass eine vorhandene Schwachstelle von ei-

ner Bedrohung ausgenutzt wird in der Gleichung 5.7 überführt mit

$$Pr_E(vul \,|\, thr) = \frac{Pr_E\,(thr \cap vul)}{Pr_E\,(thr)}. \tag{5.7}$$

Das heisst, der Zähler in der Gleichung 5.7 beschreibt die Schnittmenge zwischen der Menge der Bedrohungen und der Menge der Schwachstellen in der Wahrscheinlichkeitsebene Pr_E. Für das Zustandekommen der Schnittmenge wird gemäß der Bayes Statistik exogenes Wissen benötigt. Dieses notwendige exogene Wissen wird über Angriffsbäume und Angriffsprofile in die Wahrscheinlichkeitsebene gebracht, so dass sich damit die Wahrscheinlichkeit der Schnittmenge abschätzen lässt, wie wir in Abschnitt 5.2 zeigen.

Wird nun in die Definition 5.5 die Gleichung 5.7 eingesetzt, entsteht die nachfolgende Gleichung 5.8 für das System Ψ. Diese besagt, dass das Risiko ($\mathcal{R}$) einen Schaden ($L\ [\mathbb{R}^-]$) zu erleiden von dem Ereignis (E) abhängt, das wiederum von einer bedingten Wahrscheinlichkeit (Pr) für das Eintreten der Schnittmenge von Schwachstelle (vul) und Bedrohung (thr) abhängt.

$$\mathcal{R} = \left(\frac{Pr_E\,(thr \cap vul)}{Pr_E\,(thr)}\right) \times L\ [\mathbb{R}^-]\ \mapsto \Psi. \tag{5.8}$$

Aus der Gleichung 5.8 können einzelne Risikoszenarien $\mathcal{R} = \{R_{sz1}, ..., R_{szn}\}$ für verschiedene Systeme $\Psi = \{\psi_1, ..., \psi_n\}$ entwickelt werden, wie die nachfolgenden Gleichungen 5.9 bis 5.12 zeigen.

$$R_{sz1} = PrE_{p1}(vul_1 \,|\, thr_1) \cdot l_{25c} \mapsto \text{VoIP-Telefonie} \tag{5.9}$$
$$R_{sz2} = PrE_{p2}(vul_1 \,|\, thr_2) \cdot l_{25c} \mapsto \text{VoIP-Telefonie} \tag{5.10}$$
$$R_{sz2} = PrE_{p3}(vul_1 \,|\, thr_3) \cdot l_{25c} \mapsto \text{VoIP-Telefonie} \tag{5.11}$$
$$\vdots$$
$$R_{szn} = PrE_{pn}(vul_n \,|\, thr_n) \cdot l_{25c} \mapsto \text{VoIP-Telefonie} \tag{5.12}$$

Die Wahrscheinlichkeit $PrE_{p1} - PrE_{pn}$ wird wie oben beschrieben mit der bedingten Wahrscheinlichkeit der Gl. 5.7 abgeschätzt.

Während Schwachstellen real vorhanden sind, sind Bedrohungen hypothetischer Natur. Um eine quantitative Aussage zur Risikolage einer Firma zu bekommen, ist es daher notwendig die Bedrohungen genauer zu analysieren. Denn nicht jede Bedrohung wirkt sofort und unmittelbar. Weiterhin wird vorausgesetzt, dass hinter jeder aktiven Bedrohung auch ein Akteur vorhanden sein muss. Historisch gesehen wurde zuerst 1991 von J.D. Weis das Konzept der Bedrohungsbäume (threat trees) von [Wei91] diskutiert.

5.2 Angriffsbäume und Bedrohungsprofile

Die Idee der Angriffsbäume (*attack trees*) geht auf die Arbeit von Weis [Wei91] zurück. In dem Artikel werden diese als logische Angriffsbäume beschrieben. Allgemein werden Angriffe mit graphischen Entscheidungsbäumen modelliert. Wenige Jahre später wird die

Idee der Bedrohungsbäume unter anderen von B. Schneier aufgegriffen und weiterentwickelt [Sch99]. Diese Arbeiten von B. Schneier führten zu weitreichenden Erweiterungen und Verbesserungen dieser Technik wie z.B. bei A.P. Moore et al. [MEL01] publiziert wurde. Etliche Tools sind entwickelt und publiziert worden, stellvertretend wird hier die Arbeit von [SW04, Ing] genannt; die Autoren geben einen Überblick über die Techniken und Tools. Die Gemeinsamkeit von Angriffsbäumen und Szenarienbetrachtung durch die Spieltheorie ist bei Kordy et al. in 2012 [KMMS10] heraus gearbeitet worden. Somit könnte ein ähnlicher Lösungsweg für die Bedrohungsszenarien und Bedrohungsprofilen mittels der Spieltheorie durchgeführt werden.

In dieser Arbeit wird die Idee von T. R. Ingoldsby [Ing] erweitert. Allgemein besitzen Bedrohungsbäume eine Wurzel bzw. Angriffsziel. Auf dieses Angriffsziel können verschiedene Zweige (Knoten) hinführen, die auch als Teilziele zu betrachten sind und jeweils von einem Blatt ausgehen. Hinter jedem Blatt verbirgt sich ein Angreifer mit unterschiedlichen Motiven. Die Blätter und Zweige werden gewichtet bei [Ing] und mit einem Akteur versehen. Die Gewichtung entspricht der Kriminellen Energie (Criminal Power, Cp) und erfolgt mittels drei Funktionen. Die Abschätzung der drei Funktionen spiegeln das Expertenwissen wider, das z.B. in der Bayesian Statistik erforderlich ist (vgl. Gleichung 5.7).

Bereits im Jahr 1985 haben A. Mosleh et al. sich Gedanken über die Bayesian Statistik in der Risikoanalyse gemacht [MHB85] und auf die beiden zentralen Verteilungen einer Risikoanaylse hingewiesen. Es ist zum einen die Verteilung des Eintretens eines Ereignisses. Da es sich um seltene Ereignisse handelt, wird hier die Poisson Verteilung vorgeschlagen, die später auch von vielen anderen Autoren verwendet wird. Die einparametrige Poisson Verteilung gibt gut die Abschätzung wieder, dass kleine Planabweichungen häufiger als größere Planabweichungen auftreten, wie z.B. in der Abb. 4 mit dem Lower Partial Moment (LPM) ausgedrückt wird. Die Herausforderung besteht nun darin eine gute Abschätzung für die Parameter der Verteilung zu bekommen. Diese Abschätzung wird in dieser Arbeit über die Bedrohungen und Angriffsbäume in Kombination mit der Funktion der Kriminellen Energie vorgenommen.

Auf der anderen Seite wird in dem Artikel von A. Mosleh et al. [MHB85] die Verlustverteilung durch die Log Normal Verteilung approximiert. Auch diese Verteilung entsprach für lange Zeit der Vorstellung, dass kleine Verluste häufiger als große Verluste auftreten. Diese Vorstellung wurde durch die Black Swan Theorie (Extrem Wert Theorie) revidiert und wird nun häufig durch eine Generalisierte Pareto Verteilung (GPD) ersetzt. Oftmals ist die Verlustverteilung einfacher zu bestimmen als die Häufigkeitsverteilung, wenn die Auswirkungen (Schaden) auf die Geschäftsprozesse bezogen werden.

Die Risikofunktion der kriminellen Energie (Cp) entspricht der *criminal function*, die wiederum additiv durch drei Funktionen zusammengesetzt wird, repräsentiert das Expertenwissen für die Bayesian Risikoanalyse (vgl. Gleichung 5.9 - 5.12). Die Kriminelle Energie wird durch die Kostenfunktion *(cost of attack)*, die technische Machbarkeitsfunktion *(technical function)* und die Bemerkbarkeitsfunktion *(noticeability function)* repräsentiert. Die drei Funktionen sind bereits bei T. R. Ingoldsby [Ing] erwähnt und müssen der jeweiligen Untersuchung (Inspektion) angepasst werden.

Die Abbildung 5 besagt, dass ein Akteur für einen Angriff auf die VoIP-Telefonie der Ver-

sicherung bereit ist (Willingness to spend) Geld für tools auszugeben. Diese Bereitschaft bewegt sich zwischen 0 - 1 (Ordinate) sinkt mit zunehmenden Kosten (Abzisse). Dies lässt sich einfach erklären, da im Internet eine ganze Reihe von kostenfreien Werkzeugen (tools) zu finden sind, die alle gut geeignet sind eine VoIP-Telefonie zu bedrohen.

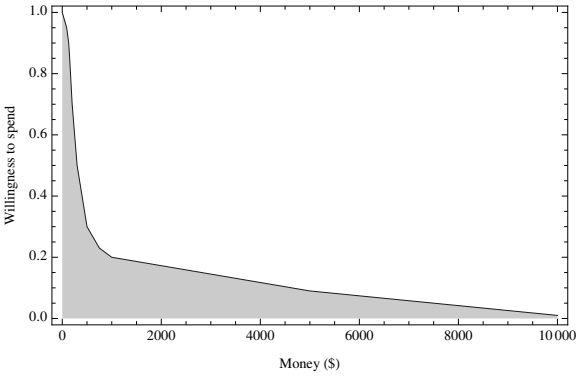

Abbildung 5: Funktion der Kosten für einen Angriff

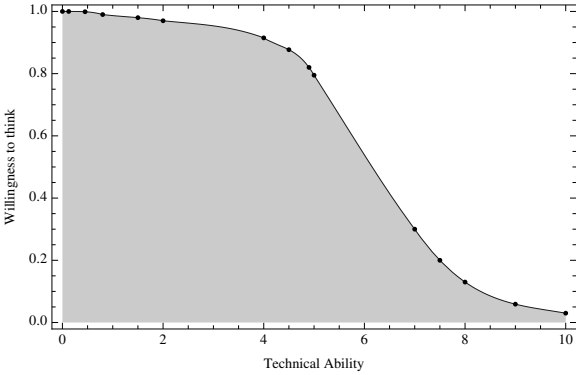

Abbildung 6: Funktion der zu verwendenden Technologie

Die Abb. 7 zeigt die Bemerkbarkeitsfunktion, die ausdrückt wie ein Akteur seinen Angriff verschleiern will, damit er nicht entdeckt wird. Aus diesen drei Funktionen ist die Bedrohung eines Angriffs näher zu bestimmen. Diese wird als kriminelle Energie bezeichnet. Diese Funktionen müssen jeweils auf die Situation angepasst werden und spiegeln das exogene Wissen wider, das bei der bedingten Wahrscheinlichkeit notwendig ist.

Als ein Beispiel für die technischen Möglichkeiten sei ein Wert von 0,5 auf einer Skala von 1.0 Werten und ein Wert von 0,3 auf der Bemerkbarkeitsfunktion verzeichnet. Wenn

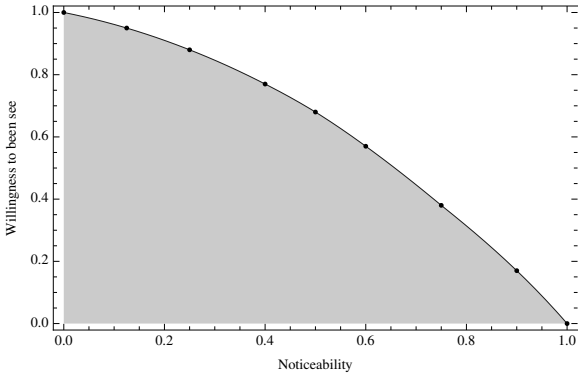

Abbildung 7: Funktion der Entdeckung

diese Werte verwendet werden, so ergeben sich die folgenden Werte:

$$f_{cost}\,(25) = 0.9 \tag{5.13}$$

$$f_{tech\,ability}\,(05) = 0.9 \tag{5.14}$$

$$f_{noticeabiity}\,(0.3) = 0.85 \tag{5.15}$$

und daraus die kriminelle Energie, die als Risikofunktion verstanden wird.

$$CE = f_{cost} \cdot f_{tech\,ability} \cdot f_{noticeabiity} \tag{5.16}$$

$$CE = 0.6885 = 0.9 \cdot 0.9 \cdot 0.85 \tag{5.17}$$

Die Diskussion über die Motivation und Vorteile eines Angreifers wird in diesem Artikel nicht behandelt.