Proseminar

Model-based risk assessment with CORAS

Denis Malkic

1. Februar 2014

Technische Universität Dortmund Fakultät Informatik

Lehrstuhl 14 Software Engineering – Prof. Dr. Jan Jürjens

betreut durch: Jens Bürger

Denis Malkic

Denis.Malkic@tu-dortmund.de
Matrikelnummer: 152984
Studiengang: Bachelor Informatik

Werkzeugunterstützung für sichere Software
Thema: Model-based risk assessment with CORAS

Eingereicht: 1. Februar 2014

Betreuer: Jens Bürger

Prof. Dr. Jan Jürjens Lehrstuhl 14 Software Engineering
Fakultät Informatik
Technische Universität Dortmund
Otto-Hahn-Straße 14
44227 Dortmund

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und noch nicht veröffentlicht.

Dortmund, den 1. Februar 2014 _____

Unterschrift

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die Sicherheit von IT-Systemen ist ein viel diskutiertes Thema in unserer heutigen Gesellschaft, in der Computer und Internet nicht wegzudenken sind. Schwächen im System ergeben sich immer wieder, sodass beispielsweise Angreifer von außen oder Fehler von Mitarbeitern zu weitreichenden Konsequenzen führen können. Umso wichtiger ist dabei das Risikomanagement, welches effektiv dabei helfen soll, Risiken zu minimieren und negative Folgen zu vermeiden. Die Risikoanalyse bildet das Kernstück des Risikomanagements und bezieht Identifikation, Dokumentation und Behandlung von Risiken ein [FOSAD11].

Diese Ausarbeitung beschäftigt sich mit dem CORAS Verfahren, mit welchem modellbasierte Sicherheitsrisikoanalysen durchgeführt werden. Das Verfahren besteht aus der CORAS Methode, der CORAS Sprache und dem CORAS Tool. Die CORAS Methode ist die Anleitung zur Durchführung der Risikoanalyse in der Praxis. Die mit CORAS durchgeführte Analyse besteht aus 8 Abschnitten, wobei in jedem Abschnitt verschiedene Ziele verfolgt und unterschiedliche Aufgaben bearbeitet werden. Die CORAS Sprache ist eine Risikomodellierungssprache, die anfangs auf der Form eines UML Profils basierte, später allerdings den Bedürfnissen des CORAS Verfahrens weiterentwickelt und gepasst wurde. Die Sprache benutzt simple Grafiken und Relationen um Diagramme zu erstellen, wodurch die Sprache als Medium die Kommunikation zwischen den Teilnehmern an der Analyse erleichtern soll und zudem eine Struktur bereitstellt um die bei der Analyse gesammelten Informationen zu dokumentieren. Das CORAS Tool unterstützt die CORAS Sprache und ist faktisch ein grafischer Editor mit dem man alle möglichen CORAS Diagramme erstellen kann. Letztlich sollen mithilfe von CORAS alle nicht akzeptierbaren Risiken identifiziert und minimiert werden, solange es sich vom Preis-Leistungs-Verhältnis rentiert.

Seinen Ursprung hat CORAS in dem gleichnamigen europäischen Forschungsprojekt, welches von 2001 bis 2003 betrieben wurde. Seitdem wird das Verfahren mithilfe von Erfahrungen, die man bei der Anwendung von umfassenden Risikoanalysen mit CORAS in verschiedenen Bereichen der Industrie sammelt, weiterentwickelt.

1.1 Motivation

In einer Umwelt voller Ungewissheit können Risiken für Unternehmen sowohl ökonomische als auch ökologische Folgen nach sich ziehen. Insbesondere die starke Abhängigkeit von digitalen Informationssystemen und Netzwerken macht die Informationssicherheit wichtiger als je zuvor. Selbst ein einzelner Zwischenfall kann enorme Auswirkungen haben. Beispielsweise kann der Diebstahl von Kunden-Daten durch Hacker bei einem Finanzdienstleister neben wirtschaftlichem Schaden auch den Ruf des Unternehmens dauerhaft schädigen, wodurch das Unternehmen aus dem Geschäft gedrängt werden kann. Ein anderes Beispiel ist der sogenannten Northeast Blackout von 2003, der teilweise durch einen Softwarefehler entstanden ist und zum Ausfall des Stromnetzes von 50 Millionen Menschen führte [BUCH]. Das

Risikomanagement ist deshalb von essentieller Bedeutung, um Risiken zu erkennen, zu minimieren und folglich negative Vorfälle zu vermeiden. Die Risikoanalyse bildet das Kernstück des Risikomanagements. Was Risikomanagement und Risikoanalyse genau bedeuten, wird in den nächsten Kapiteln genauer erklärt. Um Risiko Management effektiv und erfolgreich betreiben zu können, muss das angewandte Risikoanalyse Verfahren von Personen unterschiedlicher Kompetenzen leicht nutzbar und verständlich sein. Genau das verspricht das CORAS Verfahren.

1.2 Aufbau der Arbeit

Diese Proseminararbeit setzt sich mit der Funktionsweise des CORAS Verfahrens auseinander und soll Einblicke in die modellbasierte Sicherheitsrisikoanalyse verschaffen. Die Ausarbeitung gliedert sich in sechs Kapitel. Nach der Einleitung werden zunächst in dem zweiten Kapitel diverse Grundlagen wie „Was ist eine Risikoanalyse?“ und das Konzept von CORAS geklärt, denn wenn von Risikoanalysen die Rede ist, muss genau definiert werden, um welche Analyse es sich genau handelt und wie diese aussieht. Als Nächstes wird die CORAS Sprache erläutert und das CORAS Tool kurz vorgestellt. Anschließend folgt die Anwendung der CORAS Methode unter Verwendung der bereits vorgestellten CORAS Sprache. Abschließend gibt es noch eine persönliche Bewertung des Verfahrens.

2 Grundlagen

In diesem Kapitel werden Grundlagen zu Risikoanalysen und zum CORAS Verfahren vermittelt, um ein besseres Verständnis zu gewährleisten.

2.1 Risikoanalyse

Um das CORAS Verfahren verstehen zu können, ist es essentiell überhaupt zu wissen, was Risiko Management und Risikoanalyse bedeuten. CORAS basiert auf dem ISO 31000 Standard für Risikomanagement. Die folgende Grafik ist eine Adaption aus dem ISO 31000 Risikomanagement Standard und veranschaulicht die sieben Aktivitäten des Risikomanagement-Prozesses. Die fünf Aktivitäten in der Mitte bilden sozusagen die Risikoanalyse. In dem ersten Schritt „Establish the context“ wird das Fundament für die Analyse geschaffen. Es wird festgestellt, welche Schwächen das zu analysierende System hat und wer die Anspruchsberechtigten (stakeholder) an den zu analysierenden Elementen sind. Zudem wird in diesem Schritt festgelegt, auf welchen Bereich des Systems sich die Analyse fokussiert. Die nächsten drei Schritte beschäftigen sich mit der Identifizierung von Risiken, derer Wahrscheinlichkeit und der Priorisierung dieser um festzustellen welche Risiken behandelt werden müssen. Im letzten Schritt werden passende Behandlungen der Risiken ermittelt.

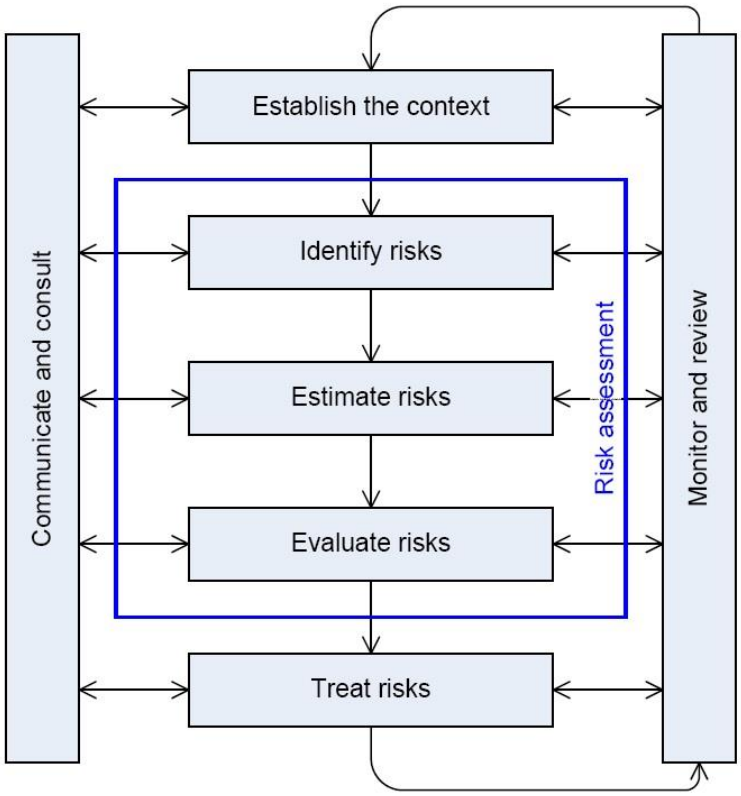

Abbildung 2.1: ISO 31000 Risk Management Standard [LS11]

2.2 Das Konzept von CORAS

Mit CORAS führt man defensive Risikoanalysen durch, das bedeutet, dass die Analyse darauf abzielt das zu schützen, was bereits vorhanden ist. Man nennt das Verfahren deshalb auch „asset-driven“. Mit „asset“ ist das gemeint, was einen Wert für die Beteiligten hat, die die Analyse veranlassen und das zu schützen gilt. Deswegen werden die assets oder auch Güter zu Anfang der Analyse ausgewählt, nach denen sich danach die ganze Analyse richtet. Ein Gut könnte dabei z.B. die Goldreserve der Bank von England oder der Ruf von Airbus sein. Die Güter können also physisch oder auch abstrakt sein. Offensive Risikoanalysen dagegen meinen Risiken, die man eingeht um einen bestimmten „Gewinn“ zu erzielen [BUCH]. Das Konzept von CORAS, nach welchem man die Risikomodellierung durchführt, ist zusätzlich als UML Klassendiagramm in Abbildung 2.2 modelliert.

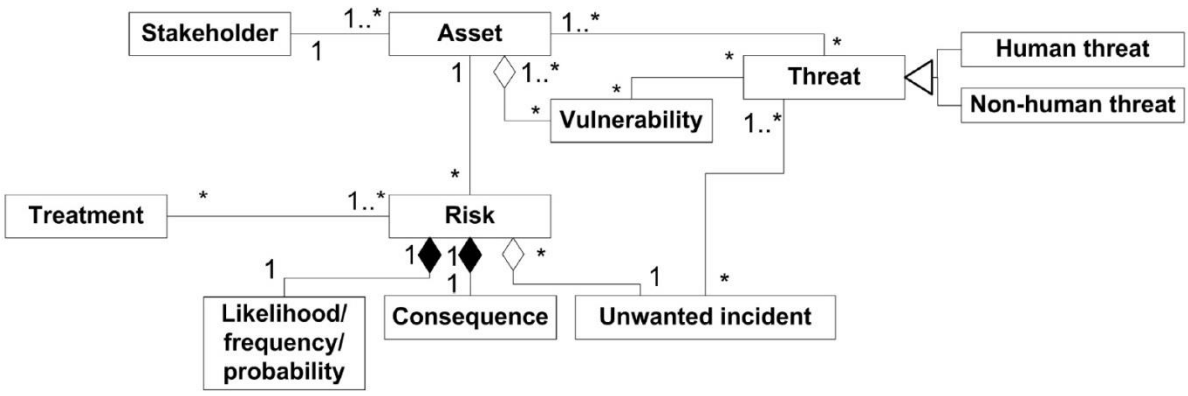

Abbildung 2.2: CORAS conceptual model [IH06]

3 CORAS Sprache

Dieses Kapitel widmet sich der Modellierungssprache von CORAS. Erst im 5. Kapitel wird die CORAS Methode vorgestellt, in denen die Sprache in der Praxis eingesetzt wird. Die Erklärung der Sprache wird es leichter machen die CORAS Methode im späteren Kapitel zu verstehen. Die Sprache bedient sich simpler grafischer Symbole und Relationen zwischen diesen, um Diagramme zu produzieren, welche einfach zu lesen sind und der Kommunikation zwischen den an der Analyse teilnehmenden Personen, aber auch der Dokumentation von Analyseergebnissen, dient. Die Übersicht aller grafischen Symbole ist der Abbildung 3.1 zu entnehmen. Der Hauptteil der Sprache wird auch „basic CORAS language“ genannt und bietet fünf verschiedene Diagramm-Typen, wobei jeder Typ einen bestimmten Abschnitt in der CORAS Methode unterstützt..

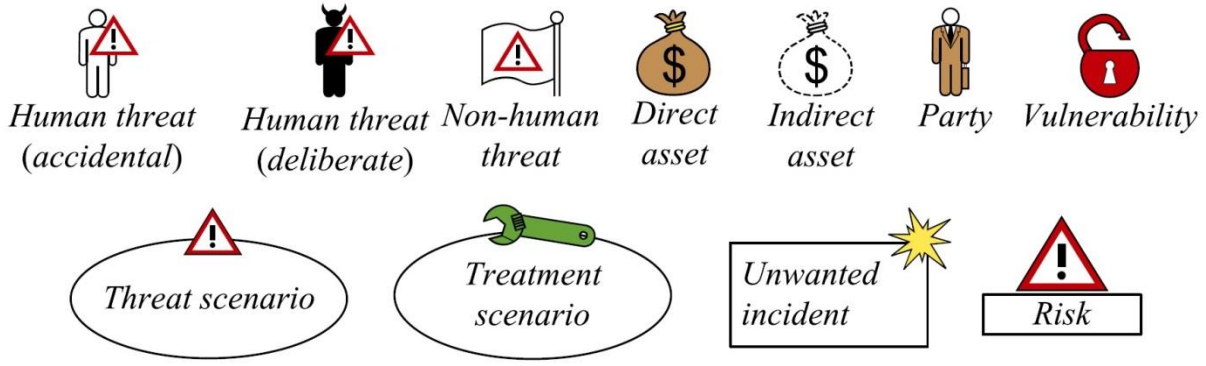

Abbildung 3.1: CORAS Grafiksymbole [MS10]

3.1 Asset Diagram

Dieses Diagramm wird hauptsächlich dazu genutzt, um die relevanten Güter zu definieren und zu dokumentieren. Für dieses Diagramm können drei grafische Symbole benutzt. Diese sind „Direct asset“, „Indirect asset“ und „Party“. Für „Party“ wird in dieser Ausarbeitung der deutsche Begriff Partei benutzt. Eine Partei ist eine Organisation, ein Unternehmen, eine Gruppe oder eine Person in deren Auftrag die Analyse durchgeführt wird. Die in dem Diagramm abgebildeten Güter gehören der Partei. Normalerweise gibt es je Risikoanalyse nur eine Partei. Es kann aber vorkommen, dass gewünscht wird, weitere Parteien miteinzubeziehen. In diesem Fall wird für jede Partei ein separates Diagramm erstellt. Indirekte Güter können nur Schaden nehmen, indem andere Güter zuvor Schaden genommen haben und dies auch durch eine „Harm relation“ gekennzeichnet ist. Dies wird in der Abbildung 3.2 verdeutlicht. In der Abbildung erkennt man Werte hinter den Gütern wie „high“ oder „critical“.

In der Regel werden die Güter von der Partei der Wichtigkeit nach eingestuft. Die Einordnen von Gütern gehört zu den Grundprinzipien von CORAS.

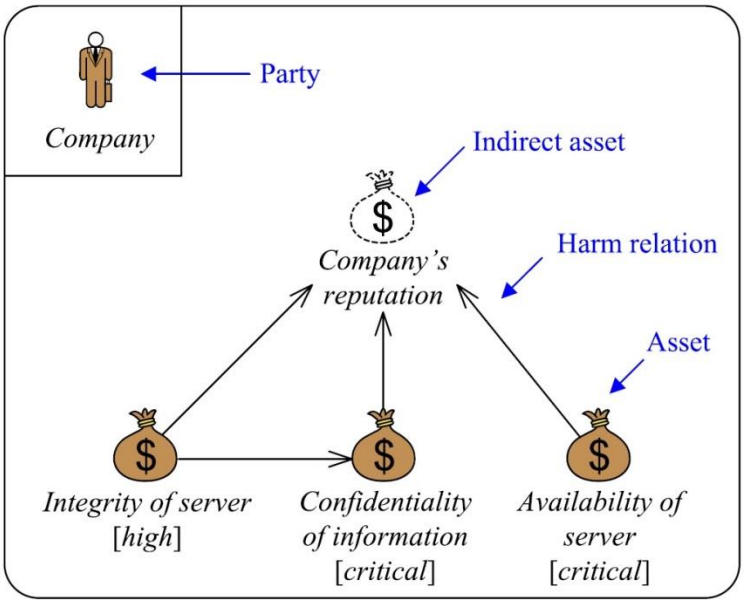

Abbildung 3.2: CORAS asset diagram [MS10]

3.2 Threat Diagram

Das threat diagram wird dazu genutzt, mögliche Ereignisse die von threats (Bedrohungen) ausgehen und die Güter gefährden können, anschaulich zu machen. Bei diesem Diagramm können sieben verschiedene grafische Symbole zum Einsatz kommen. Threat (deliberate) (gezielte Bedrohung), threat (accidental) (unabsichtliche Bedrohung), threat (non-human) (nicht-menschliche Bedrohung), vulnerability (Schwäche), threat scenario (Bedrohungsszenarien), unwanted incidentes (ungewolltes Ereignis) und asset (Gut).

Anhand des Beispiels eines Bedrohungsdiagrammes in Abbildung 3.3, wird nun der Aufbau eines solchen Diagrammes erläutert. Zunächst werden die Relationen benannt, die wie in jedem Diagramm als Pfeile vorkommen. Pfeile von Bedrohungen zu Bedrohungsszenarien oder ungewollten Ereignissen, werden initiates relations (einleitende Relation) genannt. Pfeile von einem Bedrohungsszenario zu einem ungewollten Ereignis oder zwischen zwei Bedrohungsszenarien oder zwei ungewollten Ereignissen werden leads-to relations (führt zu Relation). Die dritte und letzte Relation die durch Pfeile dargestellt werden kann, ist die impact relation (Auswirkungsrelation), die zwischen einem ungewollten Ereignis oder einem Bedrohungsszenario und einem Gut vorkommt. Diese ersten beiden Relationen können mit Schwächen und Wahrscheinlichkeiten annotiert werden. Die impact relation kann mit Kon-

sequenzwerten annotiert werden, welche aussagen wie hoch der verursachte Schaden an dem Gut ist. Des Weiteren ist zu erkennen, dass bei Bedrohungsszenarien und ungewollten Ereignisse informelle Wahrscheinlichkeiten angegeben sind, bei den Relationen allerdings feste Werte. Dies ist in der Regel möglich, es wird aber in den Vorbereitungen einer Risikoanalyse genau festgelegt, welche Werte genutzt werden sollen. Wenn z.B. bei einer leads-to relation keine Wahrscheinlichkeit angegeben ist, dann bedeutet das, dass der jeweilige Fall zutreffen wird.

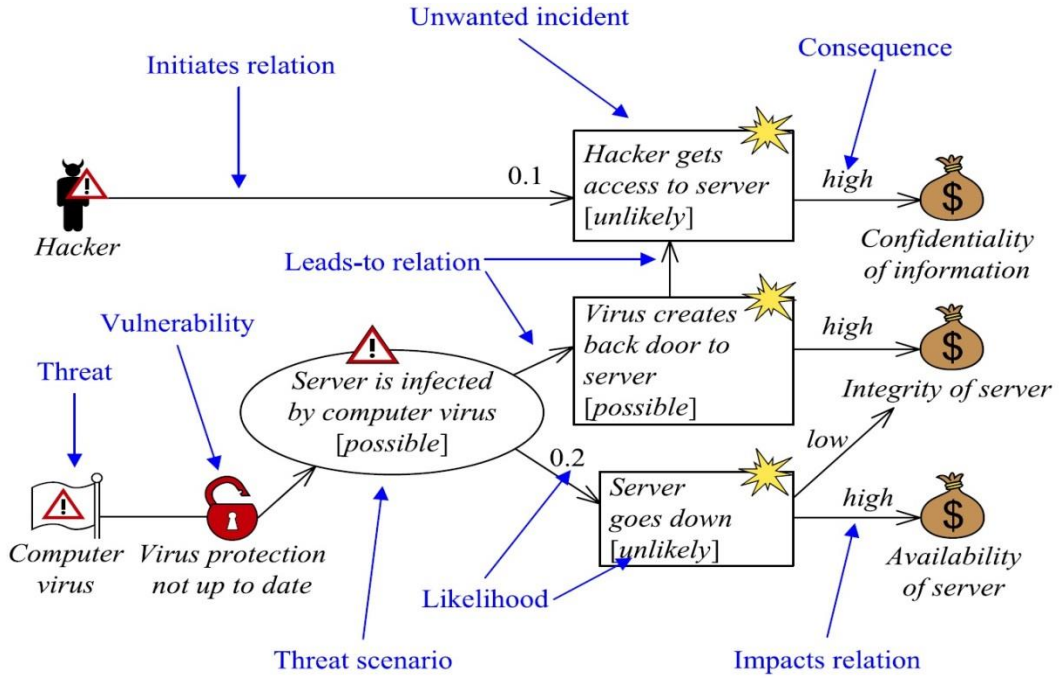

Abbildung 3.3: CORAS threat diagram [MS10]

3.3 Risk Diagram

Ein risk diagram baut auf dem threat diagram auf und fasst die Bedrohungsszenarien und ungewollte Ereignisse als risk (Risiko) Symbole zusammen. Das Schwächesymbol wird bei diesem Diagramm nicht beachtet. Es existieren für das risk diagram die gleichen Relationen wie beim threat diagram, allerdings werden nicht die gleichen Symbole benutzt. Die Symbole die benutzt werden sind die drei Bedrohungssymbole, das Risikosymbol und das Güter Symbol. Ausgehend von einem Bedrohungssymbol, werden die initiates relations benutzt. Zwischen zwei Risikosymbolen wird die leads-to relation verwendet und zwischen einem Risikosymbol und einem Gut die impact relation. Das Risikosymbol besitzt eine Beschreibung und ein risk level. Das risk level, der Wert des Risikos nimmt in der Abbildung 3.4 die Werte „acceptable“ und „unacceptable“ an. Diese Werte setzen sich aus den Wahrscheinlichkeiten der ungewollten Ereignisse und den Konsequenzwerten zusammen, weswegen der Konse-

quenzwert in diesem Diagramm auch fehlt. Jedes Paar das aus einem ungewollten Ereignis und einer impact relation besteht, repräsentiert ein risk, weswegen man auch in Abbildung 3.3 zwei scheinbar identische risks sieht.

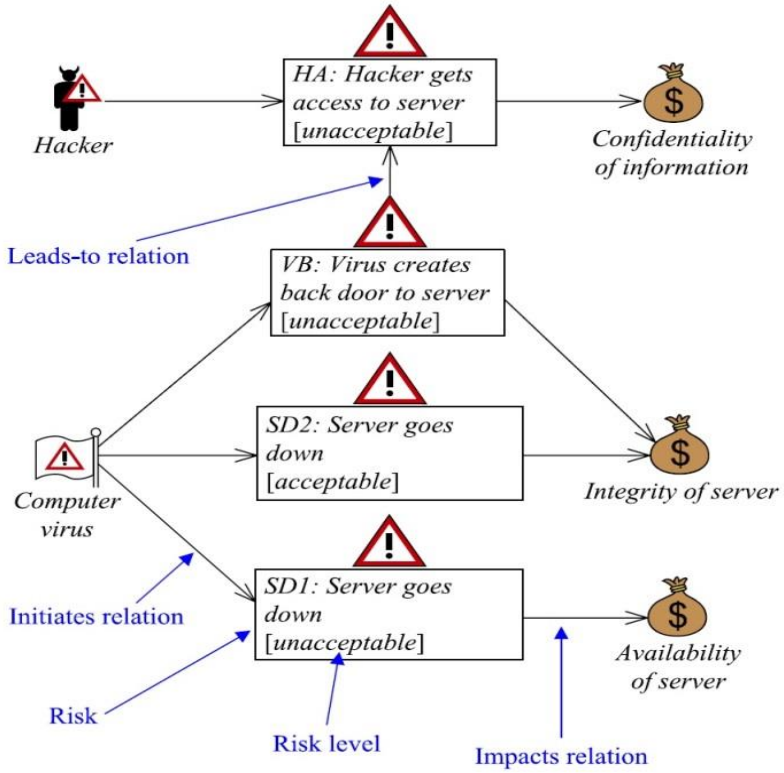

Abbildung 3.4: CORAS risk diagram [MS10]

3.4 Treatment Diagram

Das treatment diagram wird dazu benutzt Behandlungen von Risiken zu dokumentieren. Das in Abbildung 3.6 dargestellte treatment diagram, baut auf den vorherhigen Diagrammen auf und ähnelt einer Vereinigung von threat und risk diagram. Zusätzlich zu den beiden vorherigen Diagrammen wird in diesem auch das Behandlungsszenariosymbol verwendet. Ein Behandlungsszenario ist die Implementation oder Ausführung von angemessenen Maß-

Definition 4.19 A *treatment category* is a general approach to treating risks. The categories are:

- *Avoid*: Avoid risk by not continuing the activity that gives rise to it.
- *Reduce consequence*: Reduce risk level by reducing the harm of unwanted incidents to assets.
- *Reduce likelihood*: Reduce risk level by reducing the likelihood of unwanted incidents to occur.
- *Transfer*: Share the risk with another party or other parties.
- *Retain*: Keep risk at current level by informed decision.

Abbildung 3.5: CORAS treatment category [MS10]

nah-men um das risk level zu reduzieren. Das Behandlungsszenario wird mit einem gestrichelten Pfeil bspw. mit einem Risiko oder einer Schwäche verbunden. Diese Relation wird treat rela-tion bezeichnet. Diese Relation kann optional mit einer Behandlungskategorie annotiert werden. Die Behandlungskategorie dient der Kategorisierung der Behandsszenarien und be-schreibt in welcher Weise das Risiko behandelt wird. Eine Übersicht der Kategorieren ist in Abbildung 3.5 dargestellt.

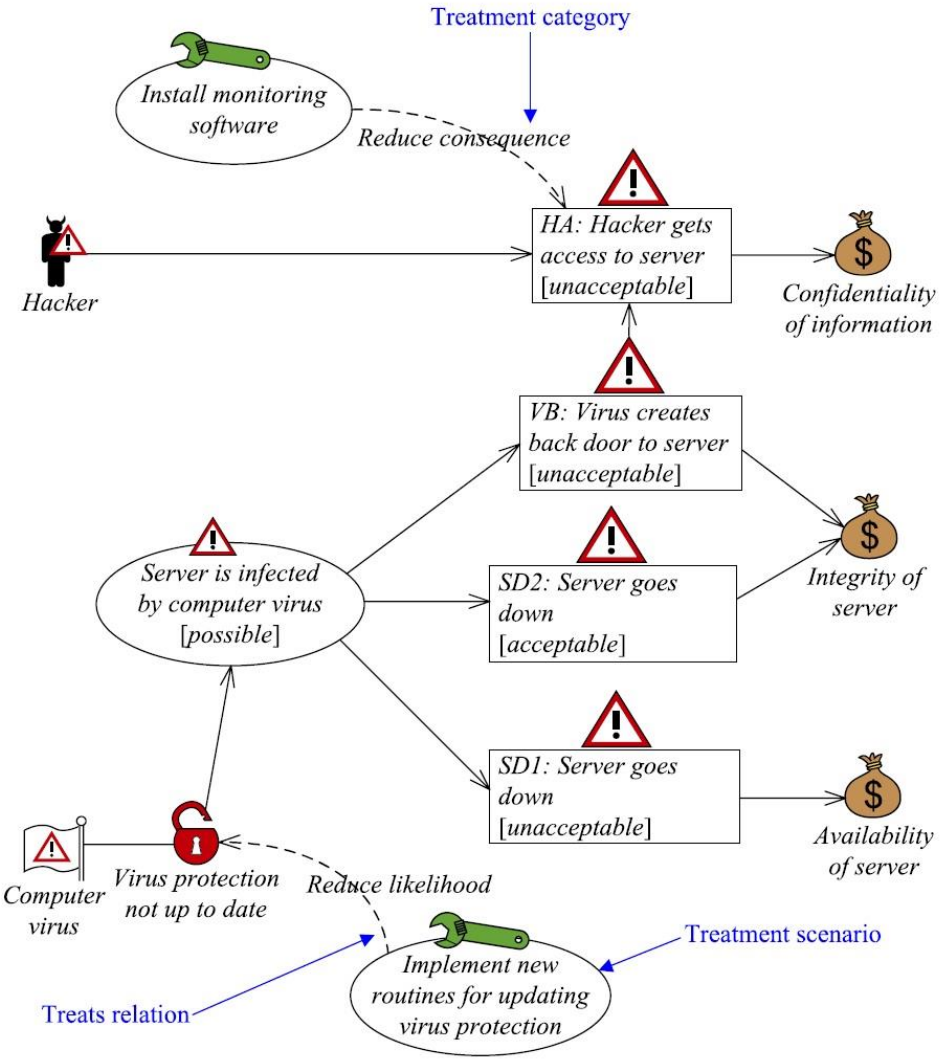

Abbildung 3.6: CORAS treatment diagram [MS10]

3.5 Treatment Overview Diagram

Das treatment overview diagram ist ein um die Bedrohungsszenarien- und Schwächensymbole reduziertes treatment diagram. Es stellt lediglich eine Übersicht des treatment dia-

grams dar. Die Behandlungsmaßnahmen wären dann z.B. bei Abbildung 3.6 direkt mit den Risiken verbunden.

4 CORAS Tool

Das CORAS Tool wurde basierend auf den Prinzipien und Anforderungen der CORAS Sprache und Methode entwickelt, um alle möglichen CORAS Diagramme zu entwerfen und diese dann im Nachhinein auch zu bearbeiten. Der an die CORAS Sprache angepasste grafische Editor ist kostenlos als Open Source Programm auf http://coras.sourceforge.net erhältlich.

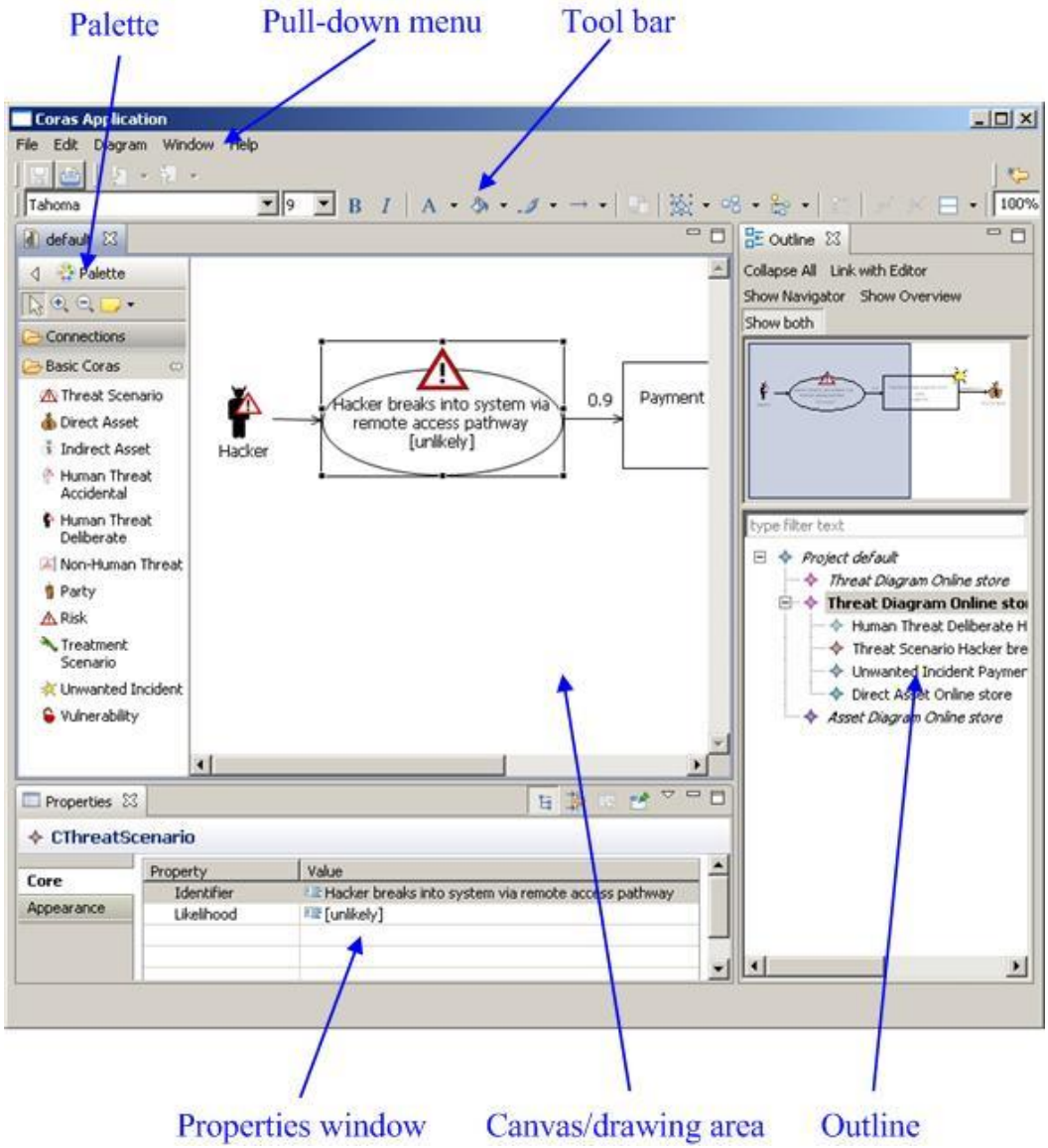

Abbildung 4.1: CORAS Tool [CO11]

5 CORAS Methode

In diesem Kapitel wird die CORAS Methode, die aus acht Abschnitten besteht, vorgestellt und näher erläutert. Die ersten vier Abschnitte sind eine Vorbereitung auf die eigentliche Analyse, die in den letzten vier Abschnitten stattfindet. In der Vorbereitung soll festgelegt werden, worauf sich die Analyse spezialisieren soll, also auf welche Bereiche man sich konzentrieren soll, die es wert sind, geschützt zu werden. Während der Vorbereitung sollen Annahmen und Einschränkungen der Ziele dokumentiert werden, um später bei der eigentlichen Analyse als Basis zu dienen. In Abbildung 5.1 werden die einzelnen Abschnitte veranschaulicht. An einer Analyse mit CORAS sollten ein Analyse Leiter und ein Analyse Sekretär

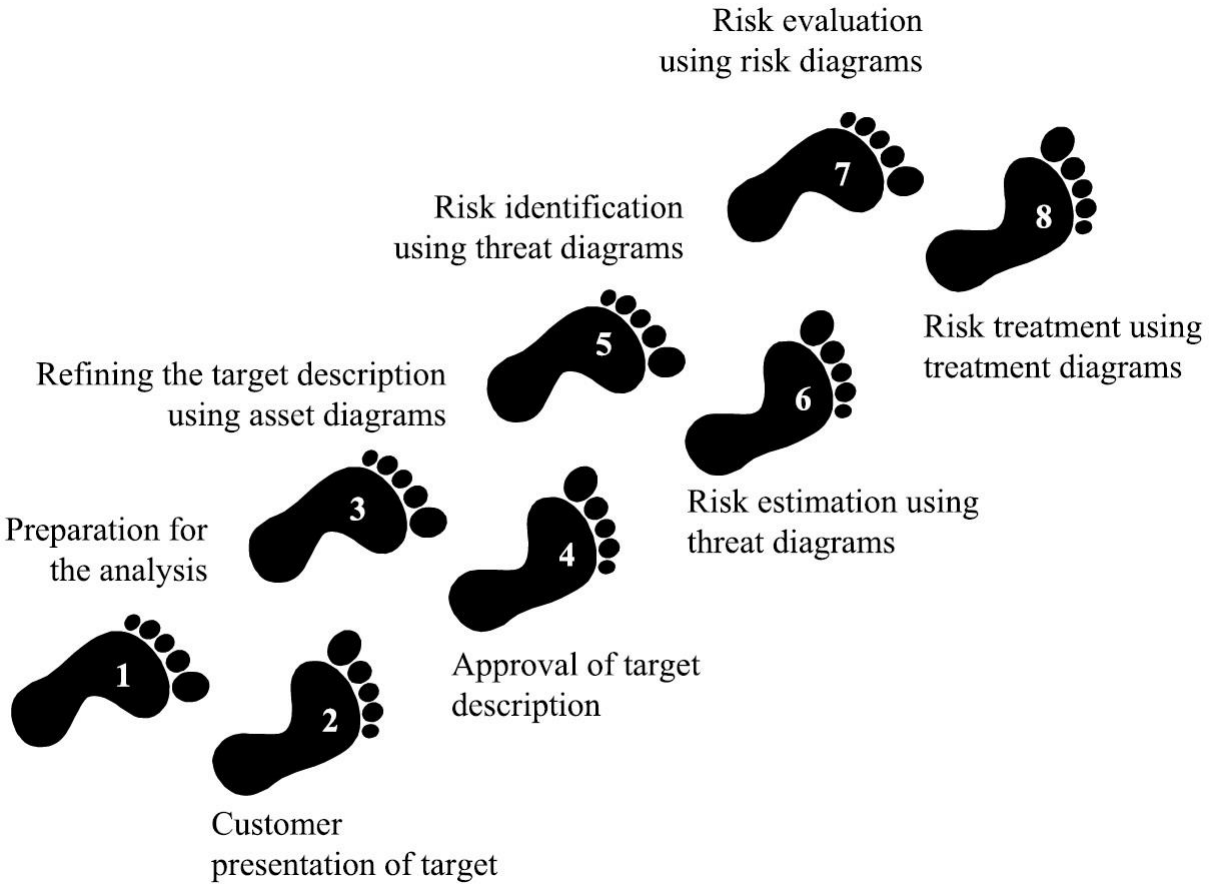

Abbildung 5.1: CORAS 8 Schritte [MS10]

teilnehmen. Unter den Vertretern des Kundens, sollten Entscheidungsträger und technische Fachkräfte teilnehmen.

5.1 Preparation for the analysis

In diesem Abschnitt der Methode geht es darum den Rahmen der Analyse festzulegen. Der Kunde, der die Analyse in Auftrag gegeben hat, hat den Analysten alle notwendigen Dokumente und Hintergrundinformationen bereitzustellen. Infolgedessen können die Analysten abschätzen wie viele Arbeitsstunden für die komplette Analyse notwendig sind oder sinnvoll erscheinen, außerdem wird ein vorläufiger Besprechungsplan ausgearbeitet. Der Analyst nennt die Ziele der verschiedenen Besprechungen und ihre Anforderungen, wie z.B. technische Expertise oder weitere Materialien.

5.2 Customer presentation of target

Der zweite Schritt der Methode umfasst eine Einführungsbesprechung zwischen den Analysten und dem Kunden bzw. den Vertretern des Kunden. Ziel des Ganzen ist, zu erfahren was der Kunde zu analysieren bzw. zu schützen wünscht. Dieses Wissen ist essentiell für die Risikoanalyse. Wichtig ist auch, dass die Analysten und der Kunde zu einem gemeinsamen Verständnis kommen, was Fokus, Güter die geschützt werden sollen und Annahmen machen, angeht. Nachdem der Kunde seine Ziele vorgestellt hat, stellen die Beteiligten abschließend einen Plan für den Rest der Analyse mit Terminen für Besprechungen und dem Abliefern von Berichten auf. Zudem wird festgelegt, wer an welchen Besprechungen teilnimmt, um zu garantieren, dass bspw. Fachpersonal des jeweiligen Bereiches des Unternehmens an der Besprechung und Analyse beteiligt sind.

5.3 Refining the target description using asset diagrams

Das Ziel dieses Abschnittes ist, zu einem konkreteren Verständnis der Ziele und Wünsche des Kunden zu kommen. Auch dieser Schritt setzt eine Besprechung zwischen den Analysten und dem Vertreter des Kunden voraus. Diese Besprechung lässt sich in drei Teile gliedern. Diese sind (1) Präsentation der Ziele, wie sie von den Analysten verstanden wurden, (2) Güter Identifikation und (3) high-level risk analysis. Im ersten Teil der Besprechung stellen die Analysten die Ziele der Analyse vor, wie sie sie von den Vertretern des Kunden wahrgenommen haben. Dabei werden sie von diesen korrigiert, um Missverständnisse aus dem Weg zu räumen. Das Resultat soll eine Beschreibung der zu analysierenden Ziele sein, bei der sich alle einig sind. Im zweiten Teil der Besprechung werden die Güter identifiziert. Damit sind die Güter gemeint, die es zu analysieren und schützen gilt und wegen derer die Analyse auch hauptsächlich durchgeführt wird. Die identifizierten Güter werden mithilfe von asset diagrams doku-mentiert. Ein Beispiel eines asset diagrams ist in Kapitel 3.1 zu finden. Die high-level risk analysis soll bei einem kurzen Brainstorming die wichtigsten Bedrohungen und Schwächen der zuvor identifizierten Güter bestimmen. Dies hilft dem Analysten dabei zu wissen, wo er mit der Analyse anfangen soll.

5.4 Approval of the target description

Der vierte Schritt wird typischerweise auch bei einer Besprechung behandelt, allerdings ist es alternativ auch möglich diesen via E-Mail oder andere Kommunikationsmittel zu behandeln. In diesem Abschnitt der Methode soll die Beschreibung der zu analysierenden bzw. schützenden Güter festgelegt und durch den Kunden genehmigt werden. Dies schließt sämtliche Annahmen, Skalen für Wahrscheinlichkeiten und Konsequenzen und die risk evaluation criteria. Die risk evaluation criteria bestimmt das risk level der Risikosymbole in den Risiko- und Behandlungsdiagrammen und entscheidet darüber, ob eine Behandlung eines Risikos nötig ist. Die Formulierung dieser Skalen und der risk evaluation criteria ist Teilaufgabe dieses Abschnitts. Hierfür werden Tabellen benutzt, die von den Vertretern des Kunden definiert werden. In Abbildung 5.2 sieht man eine Güter Tabelle, in welcher die Güter jeweils einen Wert für Wichtigkeit besitzen. Diese Werte werden von den Vertretern der Kunden festgelegt. Bei dieser Tabelle bedeutet ein niedrigerer Wert eine höhere Wichtigkeit. Die Gesundheit der Patienten wäre von den vier Gütern das wichtigste Gut das es zu beschützen gilt. Die Wahrscheinlichkeitsskala wird auch von den Vertretern des Kunden festgelegt.

Table 3.2 Asset table

Asset	Importance	Type
Health records	2	Direct asset
Provision of telecardiology service	3	Direct asset
Public's trust in system	2	Indirect asset
Patients' health	1	Direct asset

Table 3.3 Likelihood scale

Likelihood value	Description	Definition
Certain	Five times or more per year	$[50, \infty\rangle : 10y = [5, \infty\rangle : 1y$
Likely	Two to five times per year	$[20, 50\rangle : 10y = [2, 5\rangle : 1y$
Possible	Less than twice per year	$[5, 20\rangle : 10y = [0.5, 2\rangle : 1y$
Unlikely	Less than once per two years	$[1, 5\rangle : 10y = [0.1, 0.5\rangle : 1y$
Rare	Less than once per ten years	$[0, 1\rangle : 10y = [0, 0.1\rangle : 1y$

Abbildung 5.2: Asset table & likelihood scale [MS10]

Für jedes direkte Gut aus der Güter Tabelle wird eine separate Konsequenzenskala erstellt, da ungewollte Ereignisse unterschiedliche Auswirkungen auf die jeweiligen Güter haben können. In Abbildung 5.3 ist so eine Konsequenzenskala dargestellt. Wenn über 1000 Gesundheitsakte betroffen sind, dann ist die Konsequenz katastrophal. Neben den betroffenen Gesundheitsakten könnten in der Beschreibung noch z.B. gelöschte Gesundheitsakten stehen. Man könnte also unterschiedliche Fälle in die Beschreibung nennen. Unter der Konsequenzskala befindet sich die risk evaluation matrix oder auch Risikobewertungsmatrix. Die Matrix gibt die Werte der Risiken anhand der Frequenzen und Konsequenzen eines ungewollten Ereignisses an. Ein Risiko kann akzeptierbar oder nicht akzeptierbar sein. Die nicht akzeptierbaren Risiken werden in der Regel behandelt um das Risiko zu mildern, allerdings ist es nicht immer möglich alle nicht akzeptierbaren Risiken zu behandeln, da es sich vom Preis-Leistungs-Verhältnis nicht immer lohnt oder aber nicht genügend Ressourcen zur Ver-

fügung stehen. Demnach müssten sie dann doch akzeptiert werden. Die grünen Flächen in der Abbildung stehen für akzeptierbare Risiken und die roten für die nicht akzeptierbaren Risiken. Basierend auf den festgelegten Zielen bei den Besprechungen, könnte es auch vorkommen, dass eine andere Verteilung der grünen und roten Flächen gewählt wird.

Die Risikoanalyse befindet sich so lange in dem vierten Abschnitt, bis die von den Analysten vorbereitete Dokumentation vom Kunden genehmigt wird.

Table 3.4 Consequence scale for *Health records*

Consequence value	Description
Catastrophic	1000+ health records are affected
Major	101–1000 health records are affected
Moderate	11–100 health records are affected
Minor	1–10 health records are affected
Insignificant	No health records are affected

Table 3.5 Risk evaluation matrix

		Consequence				
		Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Frequency	*Rare*					
	Unlikely					
	Possible					
	Likely					
	Certain					

Abbildung 5.3: Konsequenzskala & risk evaluation matrix [MS10]

5.5 Risk identification using threat diagrams

Ziel des fünften Abschnittes ist, so viele Bedrohungen, Bedrohungsszenarien, Schwächen und ungewollte Ereignisse ausfindig zu machen wie möglich. Dieser Schritt wird als strukturiertes Brainstorming verstanden und als Workshop ausgeführt. Der Gedanke dahinter ist, Personen mit unterschiedlichen Kompetenzen und Hintergründen an den Tisch zu bringen, da Personen aus unterschiedlichen Fachbereichen auch unterschiedliche Vorgehensweisen haben. Während des Brainstormings werden von einem Analysten alle Ergebnisse mithilfe von threat diagrams bzw. Bedrohungsdiagrammen, die wir bereits in Kapitel 3.2 kennengelernt haben, dokumentiert

5.6 Risk estimation using threat diagrams

Nachdem die threat diagrams im vorherigen Kapitel erstellt wurden, müssen nun in einem weiteren Brainstorming die Wahrscheinlichkeiten und Konsequenzen ermittelt werden. Das ist die Hauptaufgabe dieses Abschnittes, um die risk level zu berechnen. Dadurch würde man dann wissen, welche Risiken akzeptabel sind und welche nicht. Die Teilnehmer am Brainstorming geben Wahrscheinlichkeiten ihrer Erfahrung nach an oder geben Ratschläge wie die Wahrscheinlichkeit aus historischen Daten abgeleitet werden kann. Da das risk level durch die Wahrscheinlichkeit der ungewollten Ereignisse berechnet wird, liegt unser Hauptaugenmerk auf den ungewollten Ereignissen. Die Wahrscheinlichkeit der ungewollten Ereignisse zu bestimmen ist aber oftmals sehr schwer, sodass versucht wird mithilfe der Wahrscheinlichkeiten der Bedrohungsszenarien die Wahrscheinlichkeit der ungewollten Ereignisse abzuleiten. Die Dokumentation der Bedrohungsszenarien ist auch sehr wichtig, da diese die wichtigste Quelle von Risiken sind, wodurch sich Behandlungsmöglichkeiten erschließen. Die Werte die für die Wahrscheinlichkeiten und Konsequenzen verwendet werden, wurden bereits im Kapitel davor definiert.

5.7 Risk evaluation using risk diagrams

In diesem Abschnitt wird dem Kunden das erste Gesamtbild der Risiken übergeben, dabei werden in den meisten Fällen die bisher dokumentierten Informationen korrigiert und angepasst. Desweiteren ist das Ziel in diesem Arbeitsschritt zu bestimmen, für welche von den identifizierten Risiken eine Behandlung in Erwägung gezogen wird. Zusätzlich zu den vorherigen Kapiteln der CORAS Methode, werden die indirekten Güter miteinbezogen.

5.8 Risk treatment using treatment diagrams

Im letzten Schritt werden alle nicht akzeptierbaren Risiken in einem Workshop genauer untersucht, um mithilfe von treatment diagrams, die bereits in Kapitel 3.4 vorgestellt wurden, Maßnahmen zu finden, welche kosteneffizient sind und die Risiken reduzieren. Die Risiken müssen dabei so reduziert werden, dass sie wieder akzeptabel sind. Die finalen Ergebnisse werden dann als treatment overview diagram dem Kunden präsentiert.

6 Fazit

Viele ungewollte Ereignisse, die bspw. in Unternehmen geschehen, werden durch opportunistische Attacken verursacht, die man hätte vermeiden können, wenn man denn Sicherheitsmanagement betrieben hätte. Mit CORAS wurde ein Verfahren zur modellbasierten Sicherheitsrisikoanalyse vorgestellt, welches auf dem ISO 31000 Risk Management Standard basiert. Ich bin der Ansicht, dass das CORAS Verfahren kein Garant für eine erfolgreiche Sicherheitsrisikoanalyse ist, da das Verfahren doch sehr stark von den an der Analyse mitwirkenden Personen abhängt. Zudem scheint es auf große Unternehmen ausgelegt zu sein, da es bei kleinen Unternehmen mit wenig Umsatz nicht kosteneffizient wäre. Die erforderliche Arbeitszeit der Analysten und der Mitarbeiter des Unternehmens, die an einer Analyse teilnehmen würden, würde die Kosten in die Höhe treiben, wenn man als Resultat ein unwahrscheinliches Risiko behandeln würde. Dennoch ist CORAS meines Erachtens ein sehr guter Ansatz um Sicherheitsrisikoanalysen durchzuführen, da die Methode sehr gut strukturiert ist und noch zusätzlich mit der CORAS Sprache die Dokumentation erleichtert. Es gibt sicherlich Alternativen für die CORAS Sprache, diese Sprache wurde aber speziell an die Methode angepasst um ein effektives Arbeiten zu ermöglichen. Zudem wird das Verfahren mithilfe von Erfahrungen aus der Industrie weiterentwickelt, wodurch es nur noch besser werden kann.

Literaturverzeichnis

[MS10] Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. Model-Driven Risk Analysis. The CORAS Approach. Springer, 2010.

[LS11] Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. Risk analysis of changing and evolving systems using CORAS. Foundations of Security Analysis and Design VI (FOSAD'11), number 6858 in Lecture Notes in Computer Science, pages 231-274, Springer 2011.

[IH06] Ida Hogganvik, Ketil Stølen. A Graphical Approach to Risk Identification, Motivated by Empirical Investigations. In 9th International Conference on Model Driven Engineering Languages and Systems (MoDELS 2006), number 4199 in Lecture Notes in Computer Science, pages 574-588, Springer, 2006. (©2006 Springer)

[FB07] Folker den Braber, Ida Hogganvik, Mass Soldal Lund, Ketil Stølen, Fredrik Vraalsen. Model-based security analysis in seven steps – a guided tour to the CORAS method. BT Technology Journal, 25(1):101-117, January 2007. (©2007 Springer)

[CO11] CORAS Tool: http://coras.sourceforge.net/coras_tool.html