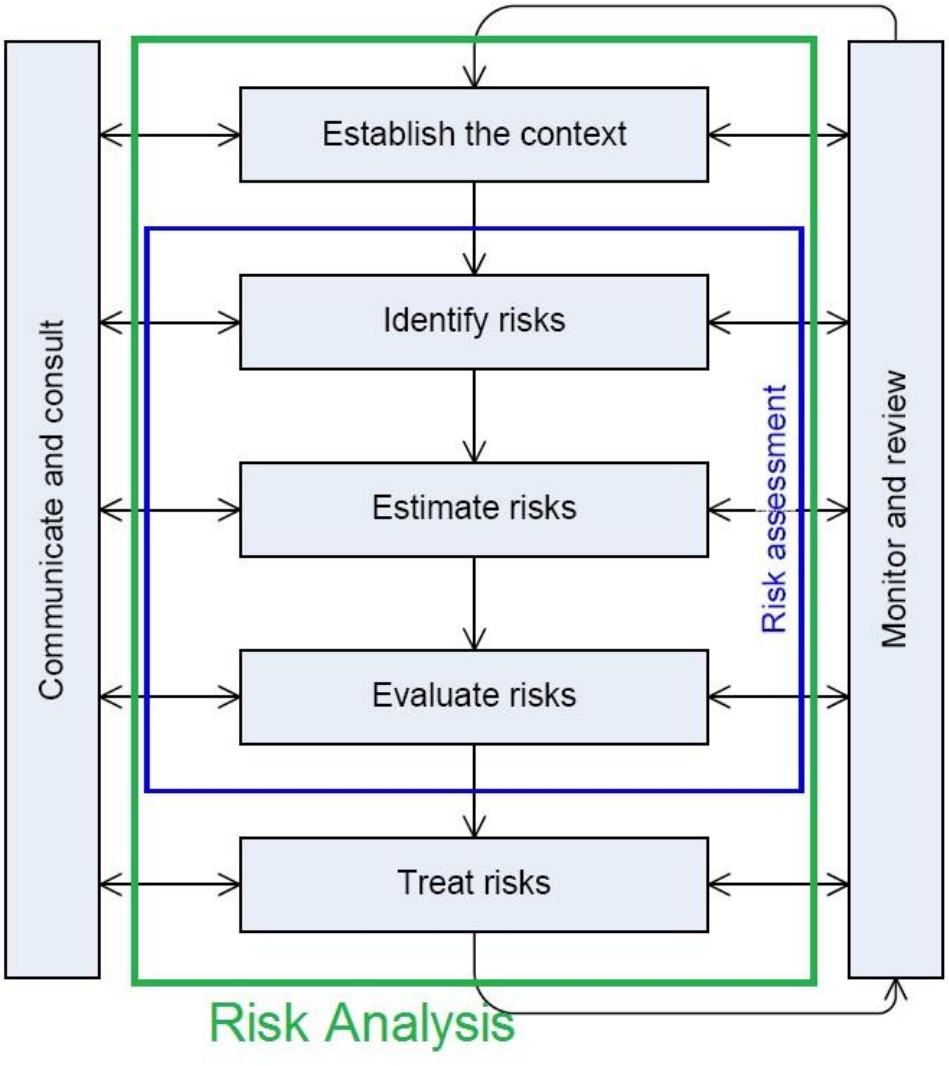
Werkzeugunterstützung für sichere Software

Model-based risk assessment with CORAS

Inhaltsverzeichnis

Grundlagen
Risikoanalyse



- Die Abbildung zeigt den ISO 31000 Risiko Management Standard, auf welchem CORAS basiert.
- Systematischer Gebrauch von vorhandenen Informationen um Risiken zu bestimmen.
- Das Ziel ist das Reduzieren von *inakzeptablen* Risiken durch die Anwendung geeigneter Behandlungsmethoden.

Grundlagen
Begriffe

asset (Gut) 

indirect asset (indirektes Gut) 

Partei 

menschliche böswillige Bedrohung 

menschliche unbeabsichtigte Bedrohung 

nicht-menschliche Bedrohung 

Verletzbarkeit 

Bedrohungsszenario 

Behandlungsszenario 

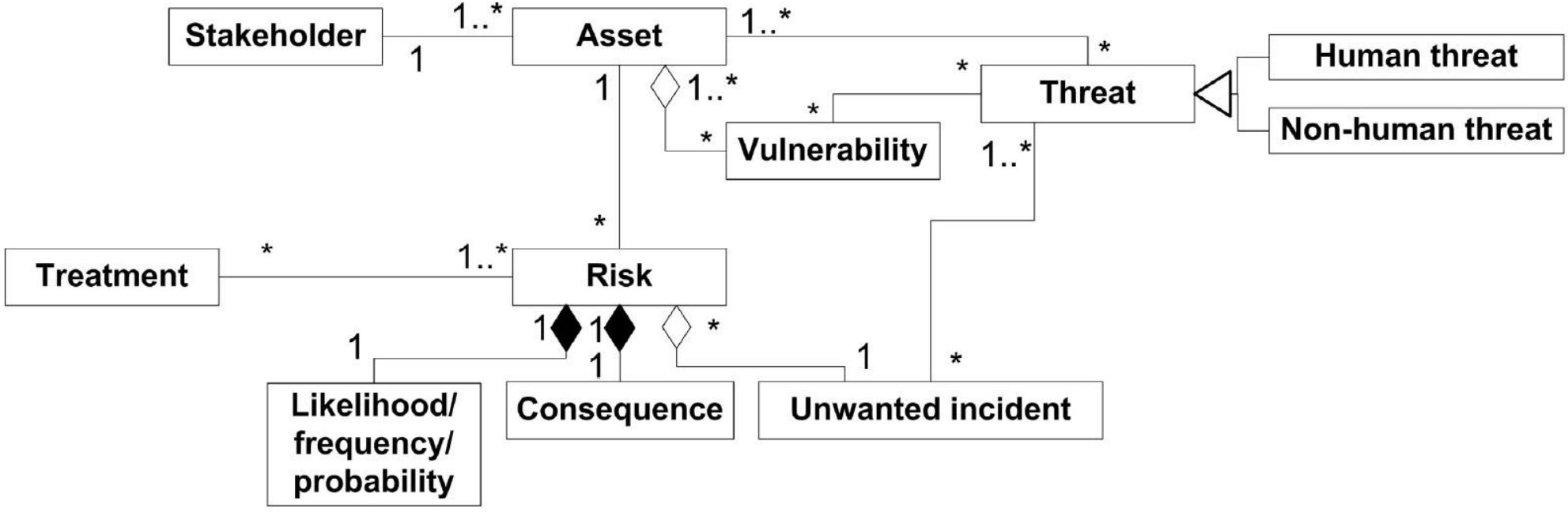
ungewolltes Ereignis 

Risiko 

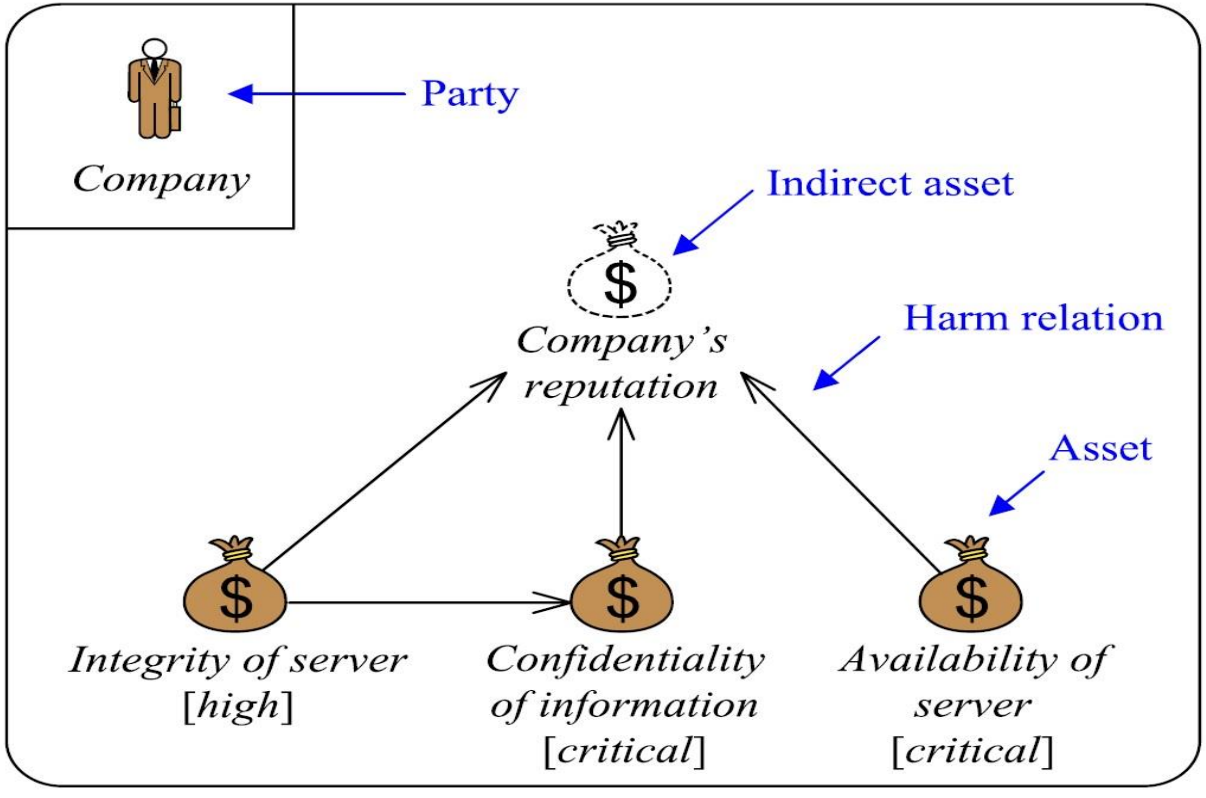
Das CORAS Verfahren
Das Konzept

- CORAS ist ein Verfahren um modellbasierte Sicherheitsrisikoanalysen durchzuführen.
- Modellbasierte Sicherheitsrisikoanalysen bieten grafische Modelle, welche die drei folgenden Funktionen erfüllen:
  - Abstraktion
  - Medium für Kommunikation
  - Dokumentation
- CORAS besteht aus den drei Artefakten Sprache, Methode und Tool.
- Die mit CORAS durchgeführten Analysen sollen bereits vorhandene Güter schützen, deswegen spricht man auch von defensiver Risikoanalyse.

Das Konzept von CORAS:

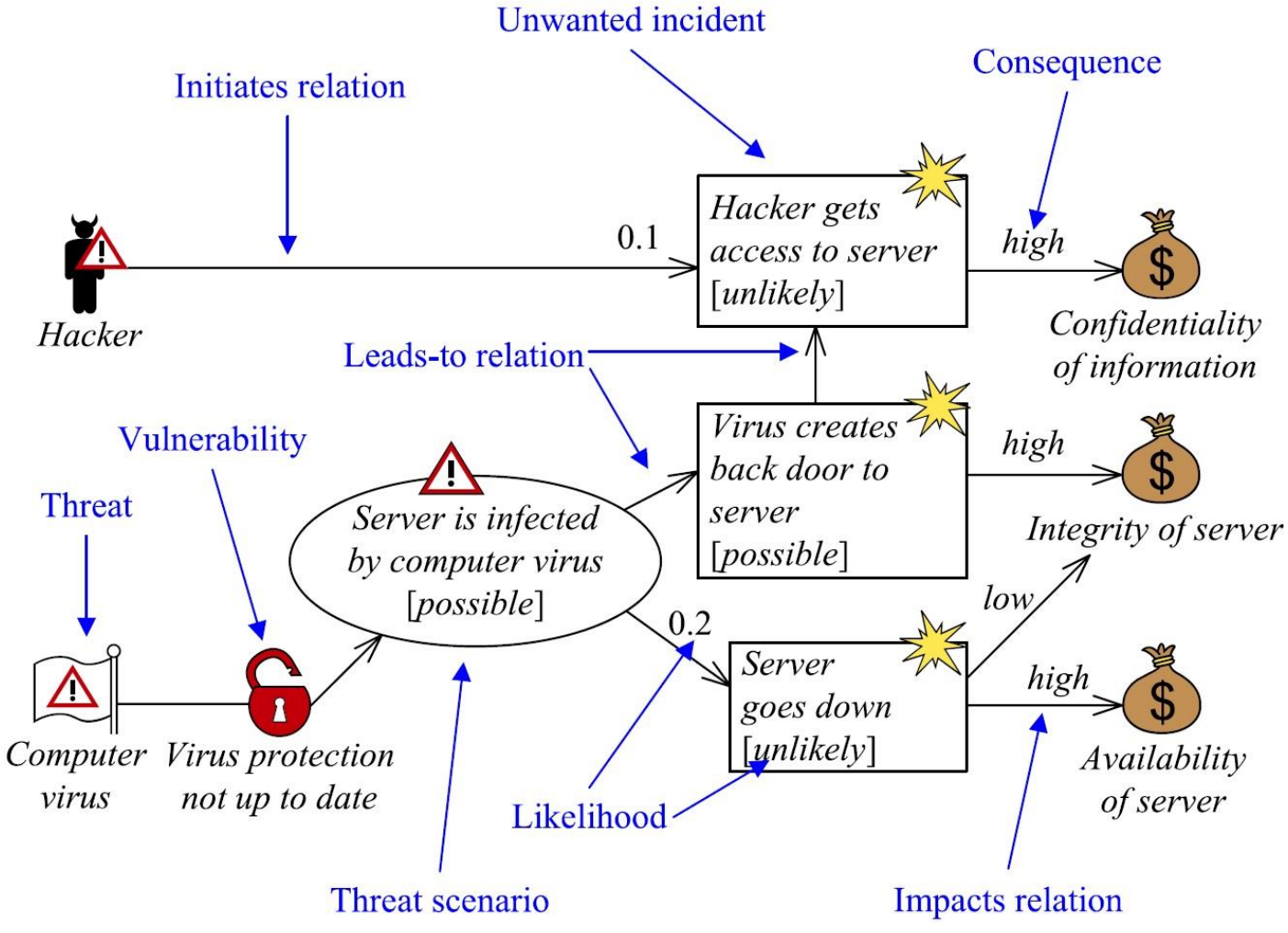


Die CORAS Sprache
Asset Diagram



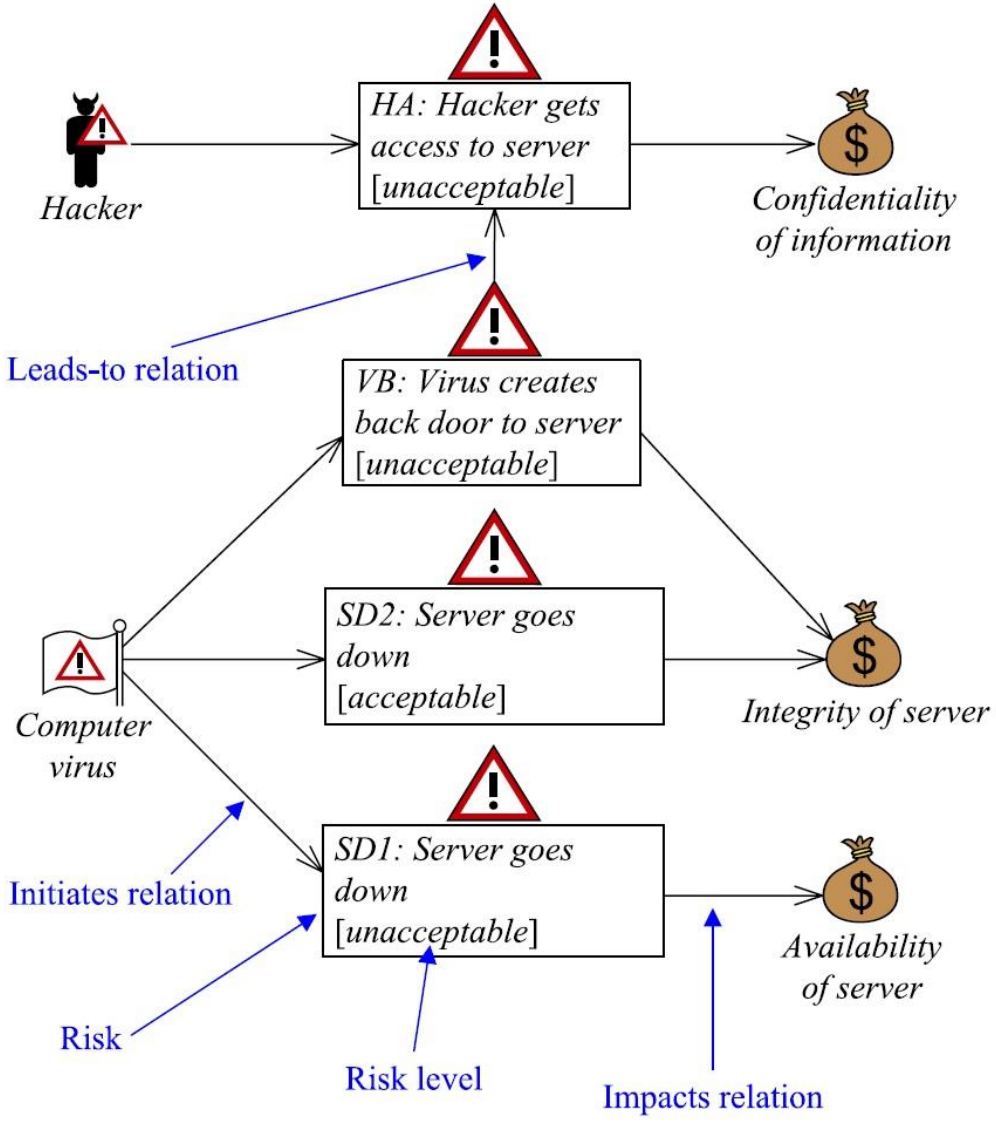
Ein indirektes Gut kann nur verletzt werden, wenn ein direktes Gut verletzt wurde und in Beziehung zu einem indirekten Gut steht.

Die CORAS Sprache
Threat Diagram



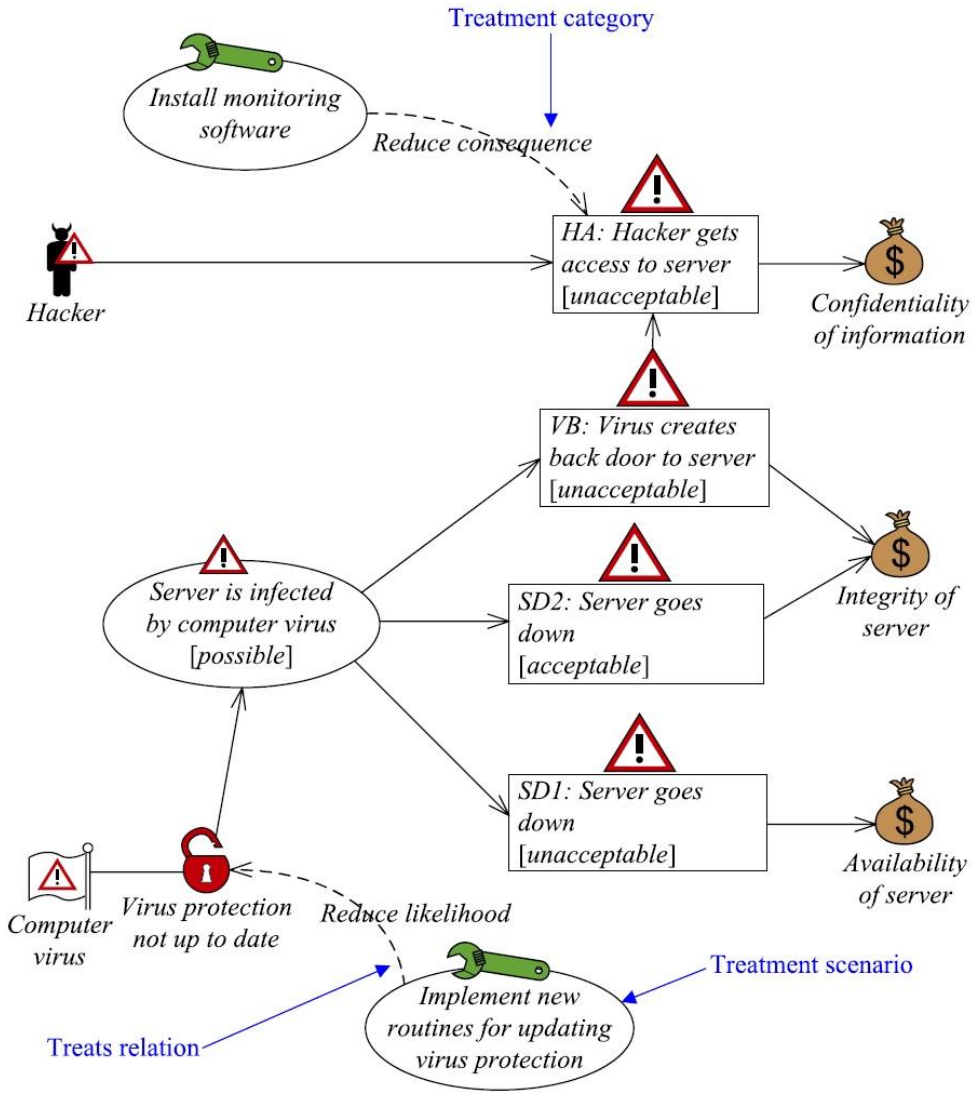
Die Güter wurden aus dem vorherigen Asset Diagramm übernommen.

Die CORAS Sprache
Risk Diagram



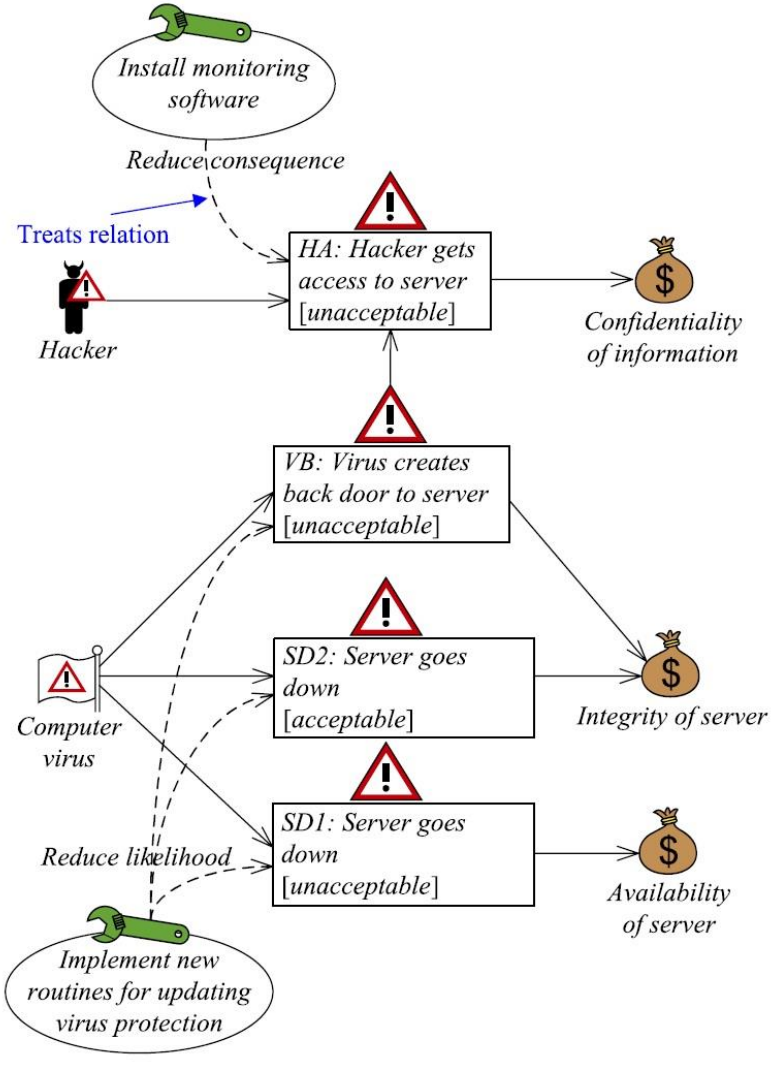
- Umwandlung des vorherigen Threat Diagrammes
- Jedes Paar aus ungewolltem Ereignis und impact relation repräsentiert ein Risiko
- Das Risiko Level wird aus der Wahrscheinlichkeit und der Konsequenz des ungewollten Ereignisses berechnet

Die CORAS Sprache
Treatment Diagram



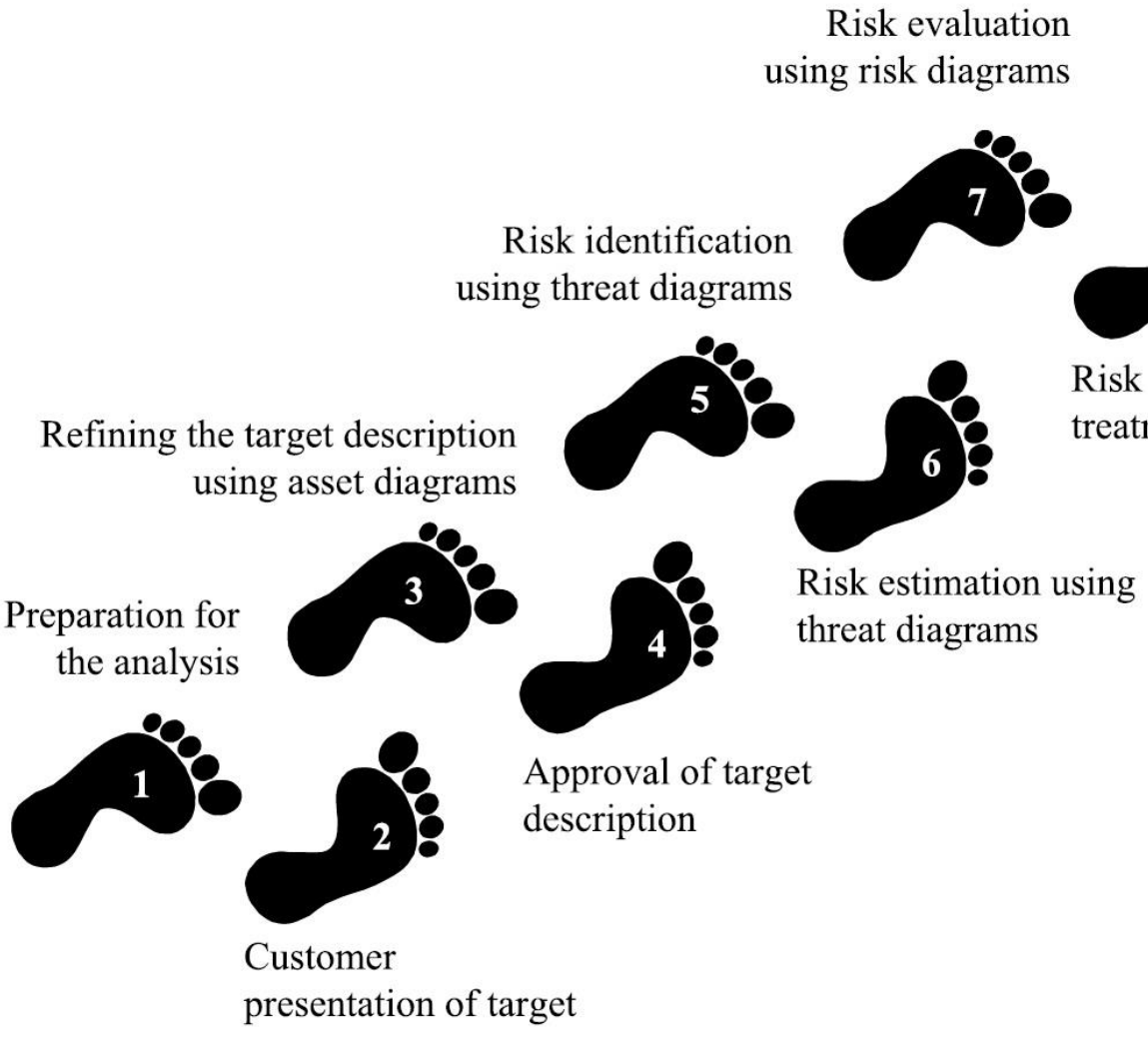
- Es werden mögliche Behandlungen dargestellt.
- Typischerweise werden die verletzbaren Stellen behandelt.
- Fünf Behandlungskategorien:
  - Avoid
  - Reduce consequence
  - Reduce likelihood
  - Transfer
  - Retain

Die CORAS Sprache
Treatment Overview Diagram



- Vereinfachtes Treatment Diagram das der Übersichtlichkeit dient
- Ist das Resultat der Analyse, welches dem „Kunden“ vorgestellt wird

Die CORAS Methode



Die Methode kommt mit genauen Richtlinien die erläutern wie die verschiedenen Phasen der Analyse in der Praxis durchgeführt werden.

Die ersten vier Schritte bilden die Vorbereitung für die Analyse. Die eigentliche Analyse findet in den letzten vier Schritten statt.

Die CORAS Methode
1. Schritt - Preparation

- Der Rahmen der Analyse wird festgelegt.
- Alle notwendigen Dokumente und Hintergrundinformationen werden vom Kunden bereitgestellt.
- Ein vorläufiger Besprechungsplan wird ausgearbeitet, welcher ungefähre Termine für Workshops und Meetings beinhaltet. Der Analyst nennt die Ziele der verschiedenen Besprechungen und ihre Anforderungen.

Die CORAS Methode
2. Schritt – Customer presentation

- Es findet eine Einführungsbesprechung zwischen Analysten und Kunden bzw. Vertretern des Kunden statt.
- Dabei soll geklärt werden, was der Kunde geschützt bzw. analysiert haben will.
- Am Ende stellen die Beteiligten einen festen Plan mit Terminen für Besprechungen und Abgaben von Berichten auf. Zudem wird festgelegt, welche Personen, welche Besprechungen wahrnehmen → Fachpersonal

Die CORAS Methode
3. Schritt – Refining target description

- Präsentation der Ziele wie sie vom Analysten verstanden wurden
- Güter Identifikation und Dokumentation mithilfe von Asset Diagrammen
- High-level risk analysis: Brainstorming im Workshop um die wichtigsten Bedrohungen und Schwächen zu bestimmen

Die CORAS Methode
4. Schritt - Approval

- Die Charakterisierung der Ziele und Güter muss vom Kunden genehmigt werden, bevor man mit dem 5. Schritt fortfahren kann.

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	$[0, 1\rangle : 10y = [0, 0.1\rangle : 1y$

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					

Die CORAS Methode
5. Schritt – Risk identification

- Strukturiertes Brainstorming
- So viele Bedrohungen, Bedrohungsszenarien, Verletzbarkeiten und ungewollte Ereignisse wie möglich finden und in Threat Diagrammen festhalten.

Die CORAS Methode
6. Schritt – Risk estimation

- Die Skalen wurden zuvor im 4. Schritt definiert, nun müssen aber die Wahrscheinlichkeiten, dass ungewollte Ereignisse eintreten und deren Konsequenzen abgeschätzt werden. Nur mit diesen Werten ist das Bestimmen des Risikos möglich.

- Möglichkeiten für die Abschätzung:
  - Historische Daten, Statistiken, Sicherheitsvorfälle
  - Persönliche Erfahrungen
  - Ableiten der Wahrscheinlichkeiten der Bedrohungsszenarien

Die CORAS Methode
7. Schritt – Risk evaluation

- Dem Kunden wird das erste Gesamtbild der Risiken übergeben und es erfolgt ggf. eine Anpassung der dokumentierten Informationen.

- Zusätzlich werden in diesem Arbeitsschritt auch die indirekten Güter betrachtet.

- Es werden die Risiken bestimmt, deren Behandlung in Erwägung gezogen wird.

Die CORAS Methode
8. Schritt – Risk treatment

- Alle nicht akzeptierbaren Risiken werden in einem Workshop genauer untersucht.
- Mithilfe von Treatment Diagrammen sollen Maßnahmen gefunden werden, um die jeweiligen Risiken kosteneffizient zu reduzieren, sodass sie wieder akzeptierbar sind.
- Diese Behandlungsmaßnahmen werden dem Kunden als finale Ergebnisse in Form von Treatment Overview Diagrammen präsentiert.

Das CORAS Tool

Fragen soweit?

→ *Live-Demonstration*

Literatur

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