# Risiken Verstehen mit Hilfe der Attack Tree Analyse

Übersetzung aus der kanadischen Originalausgabe:

Understanding Risk Through Attack Tree Analysis



# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Risiken Verstehen mit Hilfe der Attack Tree Analyse

## Attack Tree Theorie

## Einführung

### Hintergrund

Jeden Tag aufs Neue treffen wir Entscheidungen, bei denen wir mögliche Risiken abwägen. Tatsächlich ist es kaum möglich irgendeine Wahl zu treffen, ohne ein gewisses Risiko einzugehen. Soll ich lieber ein Thunfischsandwich oder doch lieber einen Cheeseburger zu Mittag essen? Der Fisch ist möglicherweise verdorben, der Burger hat aber einen höheren Fettgehalt und ist daher schlecht für mein Herz. Ein anderer Faktor ist der Preis, der bei meiner Entscheidung ebenfalls eine Rolle spielt. Die meisten dieser Abwägungen sind persönlicher und informeller Art. Mit Hilfe unserer Erfahrungen haben wir gelernt einzuschätzen, welche unserer Entscheidungen letztlich mehr Risiken bergen als wir bereit sind einzugehen und unternehmen daher Schritte sie entweder zu vermeiden, zu mindern oder auch zu teilen.

Die Welt wird immer komplexer. Moderne Technologien ermöglichen weltweit die Ernährung, Kleidung, Unterbringung und das Freizeitvergnügen von Millionen von Menschen auf der ganzen Welt. Dies bringt auf der einen Seite eine Steigerung unserer Lebensqualität mit sich, führt aber auch dazu, dass wir angreifbarer sind. 2003 mussten aufgrund eines massiven Stromausfalls (aus noch ungeklärtem Grund) Millionen von Menschen in den USA und Kanada tagelang ohne Elektrizität leben. Das Problem war nicht nur völlig unvorhergesehen aufgetreten, sondern hat darüber hinaus noch Wochen später Experten rätseln lassen. Es steht außer Frage, dass durch diese Komplexität Situationen geschaffen werden, die auch durch persönliche Erfahrungen der meisten Menschen nicht mehr kalkuliert werden können. Das wiederum bereitet ihnen Schwierigkeiten, ein Risiko intuitiv einzuschätzen.

Geschichtlich gesehen haben wir versucht dieser Herausforderung mit Hilfe von Statistiken zu begegnen. Auch wenn kein Individuum allein über die notwendige Erfahrung bezüglich bestimmter Ereignisse verfügt um deren Häufigkeit angemessen einschätzen zu können, so kann die Gesellschaft als Ganzes dieser Herausforderung möglicherweise Genüge tun. Durch das Aufzeichnen von Daten willkürlicher Ereignisse sind wir in der Lage die kollektive Erfahrung der Gesellschaft zu nutzen um rationale, wohlbegründete Voraussagen zu treffen. Ohne die technischen Details zu verstehen, die mit einem erwarteten Zwischenfall assoziiert werden, machen es Statistiken möglich die Wahrscheinlichkeit eines möglicherweise eintreffenden Ereignisses vorauszusehen um dann angemessene Maßnahmen zu treffen. Die Tatsache zum Beispiel, dass es alle paar Jahre zu einem Stromausfall kommt, sollte für Unternehmen eine Warnung sein, Notstromversorgungen für kritische Computersysteme vorzuhalten. Dank solcher Präventivmaßnahmen konnte beim Stromausfall 2003 auf so genannte Störfallpläne ausgewichen werden die, wenn man das Ausmaß des Stromausfalls betrachtet, längerfristige Schäden überraschenderweise gering hielten.

Leider ist es bei der Betrachtung eines Risikos nicht möglich, bereits geschehene Ereignisse als Grundlage **aller** heutzutage auftretenden Situationen heranziehen. Das ist besonders dann schwierig, wenn wir das Risiko bewusst durchgeführter, feindseliger Angriffe betrachten. Der Einsatz von moderner Technologie erlaubt Einzelpersonen oder auch kleineren Gruppen, einen - gemessen an der Zahl der involvierten Personen - unverhältnismäßig großen Schaden anzurichten. 2001 beispielsweise haben ein paar Duzend Terroristen mit einem geschätzten Budget von weniger als 500.000 Dollar eine Art menschlich gesteuerte Rakete benutzt um damit tausende von Menschen zu töten und einen Wolkenkratzer im Wert von 40 Milliarden Dollar zu zerstören, der von mehreren Tausend Menschen über Jahre hinweg gebaut wurde. Wenn man jetzt auch noch die Kosten berechnet, die für den von den USA durchgeführten Vergeltungsschlag aufgebracht wurden, haben die Terroristen ihre Opfer mehr als 200 Milliarden gekostet - ca. 40.000 mal soviel, als das was sie selbst investiert haben!

Ein eher banales Beispiel sind Hacker. Meist handelt es sich dabei um junge Teenager, die regelmäßig und mit einem minimalen Arbeits-, sowie Kostenaufwand Viren erzeugen und damit Unternehmen zehntausende Arbeitsstunden (und Millionen von EURO) kosten, um die Schäden zu beheben. Diese Beispiele verdeutlichen wie es heutzutage ein leichtes ist mit einfachen Mitteln unvorhersehbar großen Schaden anzurichten. Das ist ein vorher nie dagewesenes Phänomen unserer Zeit.

Sich mit dieser neuen Art von Bedrohung auseinanderzusetzen geht weit über die persönliche Erfahrung der meisten Menschen hinaus und auch die vorhandenen Mittel um sich zu schützen, sind leider begrenzt. Obgleich es möglich ist Vorsichtsmaßnahmen für fast alle potentiell auftretenden Gefahren zu treffen, ist es dennoch unmöglich sich hundertprozentig zu schützen.

Unabhängig davon was wir tun, können wir für unsere Entscheidungen kritisiert werden. Angenommen es passiert etwas Schlimmes (und wir waren darauf nicht vorbereitet): Wie können wir dann beweisen, dass unsere Maßnahmen nicht unbegründeter weise (und auch nicht aus Geiz) zu optimistisch waren?

Oder wie beweisen wir, wenn etwas Schlimmes, das wir vorausgesagt hatten **nicht** eintrifft, dass wir aufgrund unserer Paranoia nicht unnötig Geld zum Fenster hinausgeworfen haben?

Die Antwort auf diese Fragen ist Dreh- und Angelpunkt der Risikoanalyse.

## Risiko - Theorie und Definitionen

Die Definition von Begriffen, die sich auf Risiko beziehen unterscheidet sich je nach Autor leicht voneinander. An dieser Stelle geben wir einen Überblick über die Definitionen, die wir im Laufe dieses Textes verwenden werden.

### Risiko – traditionelle Definition

In der Regel wird der Begriff **Risiko** mit einem bestimmten Ereignis verbunden und kann somit definiert werden als:

***Risiko****Ereignis* **= (Wahrscheinlichkeit des Ereignisses) x (Auswirkung des Ereignisses)**

Mag es noch so zufriedenstellend sein eine Formel zu verwenden um Risiko zu beschreiben, gibt es dennoch viele Situationen, in denen diese Formel nicht anwendbar ist. Auch wenn es noch so einfach (und öde) erscheint einen möglichen Schaden einzuschätzen, der bei einem hypothetischen Ereignis entstehen könnte, ist es dennoch keineswegs immer einfach einen Wert für die *Wahrscheinlichkeit eines Ereignisses* zu finden. Der Wert dieses Terms (für gewöhnlich durch einen Zahlenwert zwischen 0 und 1 ausgedrückt) ist das Ergebnis vieler Faktoren, die nicht alle ohne weiteres bestimmt werden können.

### System

Jedes Mal wenn wir ein Risiko betrachten, müssen wir festlegen, wie groß der Analyseraum ist. Philosophen würden wahrscheinlich behaupten, dass ein Ereignis bei dem jemand verletzt wird letzten Endes jeden und alles auf der ganzen Welt in einer Weise beeinträchtigt; und zwar heute und für alle Ewigkeit. Die meisten anderen Menschen begrenzen ihre Bedenken auf diejenigen Dinge, für die sie sich direkt verantwortlich fühlen, oder die sie auf direkte Art und Weise betreffen. Den Raum in dem wir unsere Betrachtungen anstellen, nennen wir normalerweise **System**.

Schauen wir in *Meyers deutschem Wörterbuch* unter dem Wort **System** nach, finden wir folgende Definition: „Regelmäßig aufeinander einwirkende oder unabhängig voneinander agierende Faktoren, die im Zusammenspiel ein einheitliches Ganzes bilden.“ Auch wenn ein **System** fast immer aus einer Vielzahl physischer Komponenten (beispielsweise Computer, Gebäude, etc.) besteht, können auch Menschen Teil dieses Systems sein, die mit den jeweiligen Komponenten und den daraus entstehende Prozessen in Wechselwirkung stehen. Ein erster Schritt der Risikoanalyse ist es zu entscheiden aus welchen Komponenten das untersuchte **System** zusammengesetzt ist.

### Verwundbarkeit

Jedes System weist ein oder mehrere Schwachstellen auf. Unter einer Schwachstelle verstehen wir eine mögliche Angriffsfläche eines Systems. Es ist sozusagen ein Mechanismus durch den ein System beschädigt wurde, seine Ressourcen auf nicht autorisiertem Wege missbraucht, oder in einen unerwünschten Zustand gebracht wurden. Ein Computersystem das

Nutzer durch ein Passwort authentifiziert, birgt beispielsweise die Schwäche, dass das Passwort durchaus erraten werden kann. Der griechische Held Achilles war übrigens auch nur an (s)einer Ferse verwundbar.

### Bedrohung

Eine **Bedrohung** ist eine mögliche Gefahr für ein System. Eine **Bedrohung** ist etwas, dass die Möglichkeit hat zu agieren. Sie kennt eine spezifische oder gar eine ganze Reihe von Schwächen und ist dadurch in der Lage anzugreifen. Die reine Existenz einer **Bedrohung** bedeutet nicht automatisch, dass die Schwäche ausgenutzt werden wird, sondern zeigt vielmehr dass es potenziell möglich ist. Eine **Bedrohung** kann einerseits von einem feindseligen, intelligenten Angreifer, der bewusst Schaden zufügen will ausgehen, kann aber andererseits auch Folge zufälliger, natürlicher Umstände sein. Die Möglichkeit auf in Bäume geschlagene Metallstangen zu treffen, ist beispielsweise eine **Bedrohung** für sicher durchführbare Baumfällarbeiten. Die Möglichkeit vom Blitz getroffen zu werden stellt eine **Bedrohung** für Leute dar, die gerne bei Gewitter spazieren gehen.

### Bedrohungsagenten

Eine bestimmte Art oder Gruppe von Menschen, die eine Bedrohung für ein System darstellen, werden **Bedrohungsagenten** genannt. Wenn wir uns das vorher genannte Beispiel genauer anschauen, könnte der **Bedrohungsagent** der Metallstangen in Bäume rammt um ein Fällen zu verhindern ein radikaler Umweltschützer sein. Auf der anderen Seite könnte der **Bedrohungsagent** auch ein verärgerter ehemaliger Angestellter sein, der seinem früheren Chef finanziellen Schaden zufügen will. Handelt sich bei Ihnen um jemand der Computersysteme mit wichtigen Firmengeheimnissen schützten soll, kommt als **Bedrohungsagent** sowohl ein Industriespion als auch ein experimentierfreudiger Teenager in Frage.

Manche Autoren betrachten jegliche Art von Individuen die das Potential haben, einen Angriff auf ein System auszuüben als legitimen **Bedrohungsagenten**. Wenn man es genau nimmt, ist dies auch tatsächlich der Fall. In der gesamten Analyse werden wir jedoch den Gebrauch des Begriffs auf die Gruppen reduzieren, die einen nachvollziehbaren Grund oder Wunsch haben ein System zu beschädigen. Das bedeutet laut unserer Definition, dass z.B. die US Armee keine plausible Bedrohung für die Bank von New York darstellt. Obwohl die US Armee mit Sicherheit das Potential hat, die Bank zu überfallen um alles Geld zu stehlen, können wir uns keinen Grund vorstellen, warum sie das tun sollte. Um also noch einmal zu unterstreichen, dass wir bei dem Gebrauch des Begriffs davon ausgehen, dass eine bestimmte Motivation vorhanden ist, werden wir oft von plausiblen oder denkbaren **Bedrohungsagenten** sprechen.

### Exploit - Ausnutzen von Sicherheitslücken

Eine Bedrohung stellt eine eher abstrakte Art dar aus einer Schwäche Vorteile zu ziehen. Sprechen wir dagegen konkret vom Ausnutzen eines Sicherheitsproblems (einem sog. Exploit), beziehen wir uns auf den detaillierten Ablauf dieses Prozesses. Oft benutzen wir diesen Ausdruck, wenn es um Angriffe auf Computersysteme geht. Wir wissen beispielsweise, dass es bei manchen Anwendungen leicht zu einem Speicherüberlauf (Buffer-Overflow) kommen kann.

Ursache dafür sind schlicht Programmierfehler, die zur Folge haben, dass ein Buffer überschrieben werden kann. Das Ausnutzen der Schwachstelle wäre hier sozusagen der Prozess der zur Störung des Programms führen würde. Dazu gehört die Übertragungsmethode der Daten, die Zeichensequenz und alle anderen Details, die für das Ausnutzen einer Schwachstelle notwendig wären. Das Verb „exploit", (*deutsch„ausnutzen/benutzen/ausbeuten")* bezieht sich auf das Durchführen einer böswilligen Handlung.

## Vorfälle und Ereignisse

Zitieren wir noch einmal das Lexikon, so finden wir in *Meyers deutschem Wörterbuch* für den Begriff **Vorfall „*eine Tat die wahrscheinlich schwere Konsequenzen hat".*** Im Klartext bedeutet das, dass wir dann von einem **Vorfall** sprechen, wenn eine Bedrohung aufhört lediglich eine hypothetische Möglichkeit darzustellen, sondern ein tatsächlicher Angriff stattfindet.

In vielen Fällen handelt es sich bei einem **Vorfall** um das Resultat einer Abfolge oder Kombination verschiedener aufeinander einwirkender **Ereignisse**. Ein Auto beispielsweise hat vielleicht einen Unfall als Folge einer Reifenpanne. Auf den ersten Blick ist die Reifenpanne der Vorfall, der den Unfall verursacht hat. Die Reifenpanne war jedoch die Folge eines Nagels, der den Reifen durchstochen hatte. Der Nagel wiederum war von einem vorbeifahrenden Lastwagen gefallen, da ein Baustellenarbeiter die Nägel nicht ordnungsgemäß in den Werkzeugkasten geräumt hatte.

Jedes einzelne Ereignis ist ein **Vorfall**, der einen daraus resultierenden **Vorfall** verursacht hat. Manche dieser Vorfälle haben zu einem sofort eintretenden Schaden geführt, andere hingegen haben lediglich unangenehme Folgen mit sich gebracht.

Der Begriff **Ereignis** beschreibt meist Vorgänge, die vielleicht - vielleicht aber auch nicht - sofortige Konsequenzen haben. Der Terminus **Vorfall** wird in der Regel für Ereignisse, verwendet, die einen höheren Stellenwert in der Kausalkette einnehmen, da sie direkt mit den entstehenden *schlimmen Konsequenzen* assoziiert werden. Diese Unterscheidung ist allerdings eher künstlicher Natur, da fast alle Ereignisse von anderen vorhergegangenen Ereignissen ausgelöst werden. **Vorfälle** und **Ereignisse** sind daher praktisch Synonyme.

## Angriffe und Missgeschicke

Es gibt zwei Arten von **Vorfällen**. Einen Vorfall, der absichtlich und bewusst durch das Ausnutzen einer Schwachstelle herbeigeführt wurde, nennt man einen **Angriff**. **Vorfälle**, die Folge eines ungewollten oder zufälligen Ereignisses sind, nennt man **Missgeschicke**.

## Auswirkung auf das Opfer und Vorteile für den Angreifer

Vorfälle und Ereignisse bedeuten in der Regel einen Schaden für das betroffene System. Wir sprechen dabei von der **Auswirkung auf das Opfer**, oder vereinfacht von der **Auswirkung.**

Stellt der Vorfall die Folge eines absichtlichen Angriffs dar, mag dies durchaus eine positive Auswirkung oder einen Nutzen für den Angreifer haben. Wir sprechen daher auch vom **Vorteil des Angreifers**.

In manchen Fällen ist die **Auswirkung auf das Opfer** genauso groß wie der **Vorteil des Angreifers**. Wenn zum Beispiel ein Angreifer 1000 EURO stiehlt, verliert die eine Seite diese 1000 EURO und die Andere gewinnt sie. Das ist jedoch eher die Ausnahme und nicht die Regel. Vandalismus macht dies ganz besonders deutlich. Das Opfer trägt unter Umständen einen beträchtlichen finanziellen Schaden, während der Angreifer nichts an Geldwert dazugewinnt.

Die **Auswirkung** kann auf verschiedene Art und Weise gemessen werden. Obgleich Geld den gebräuchlichsten Maßstab darstellt, kann fast alles das von Wert ist, herangezogen werden. Die Anzahl von Opfern beispielsweise, oder der geringe/mittlere/große Verlust an Ansehen können Maßstäbe für die Auswirkung sein. Davon abhängend auf welche Schwäche des Systems abgezielt wird und auf welche Art und Weise die Schwäche ausgenutzt wird, variiert die **Auswirkung**.

## Fehlerbäume

Ein Vorfall ist das Ergebnis anderer vorhergegangener Vorfälle und Ereignisse. Die Beziehung zwischen dem Vorfall und den dazu beitragenden Ereignissen können grafisch dargestellt werden. Eine Darstellung, die sich in den Untersuchungen über Systemausfälle in Unternehmen als durchaus nützlich erwiesen hat, nennt sich **Fehlerbäume**.

**Fehlerbäume**[1] dienen besonders der Darstellung von möglicherweise auftretenden Problemen in kritischen Systemen. In chemischen Betriebsanlagen beispielsweise wird die sog. Fehlerbaumanalyse verwendet, um mögliche Konsequenzen eines beschädigten Rohrs zu ermitteln. Bei den Untersuchungen der (Raumschiff) „Challenger"-Katastrophe[2] und dem Verlust der Raumsonde Columbia wurde in beiden Fällen die Fehlerbaumanalyse herangezogen.

Auch wenn die **Fehlerbäume** nicht alle Möglichkeiten in Betracht ziehen, die bei einem vollständigen Bedrohungs-Risiko Modell eine Rolle spielen, ist es doch eine Grundlage, auf die wir uns stützen können. Betrachten wir daher einmal ein einfaches Beispiel, das das Konzept der **Fehlerbäume** verdeutlicht.

### Ampelbeispiel

Eine Kleinstadt überlegt ihr manuelles Verkehrsampelsystem auf Computerbertrieb umzustellen. Die Stadt ist sehr klein und hat nur eine einzige Ampel, die sich auf der Hauptstraße befindet. Der Bürgermeister gilt als (für manche gar übertrieben) progressiv und möchte für sein Dörfchen eine zentral betriebene Ampelanlage, ähnlich dem einer Großstadt. Er hat daher ein zentral gesteuertes Computersystem vorgeschlagen, das sämtliche Anweisungen per Netzwerkverbindung zur Ampel sendet. Der Bürgermeister wirbt mit

[1] „Fault Tree Development", 3. Auflage März 2002, Sutton Books, http://www.swbooks.com/#monographs

[2] htttp://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf

Kosteneinsparungen, um die Ampelanlage zu rechtfertigen. Ihm zufolge sei es dann nicht mehr länger notwendig, Arbeitskräfte anzufordern, um Änderungen an der Anlage vorzunehmen. Da das Steuerungssystem so programmiert werden kann, dass die jeweiligen Phasen automatisch je nach Tageszeit entweder kürzer oder länger sind, könne man zusätzlich auch noch den Verkehrsfluss optimieren.

Die Kritik an der Idee des Bürgermeisters bezog sich auf die anfallenden Kosten für das neue System. Um diesem Zweifel zu entgegnen hat der Bürgermeister das System so minimiert, dass die Ampelanlage so einfach wie möglich aufgebaut ist – d.h. sie funktioniert nicht ohne Kommunikation mit der Zentrale. Die Ampelanlage verfügt zwar über einen batteriebetriebenen Akku, der die Lichter im Falle eines Stromausfalls noch eine zeitlang am Laufen halten würde, jede andere Fehlerquelle würde jedoch zu einem totalen Zusammenbruch des Systems führen. Seine Kritiker verlangen daher nun, dass das vom Bürgermeister vorgeschlagene System auf seine Verlässlichkeit hin geprüft wird.

Nach einigen Überlegungen wurden die folgenden Punkte als Hauptgefahrenquelle für das Versagen der Ampelanlage herausgearbeitet:

1. Stromausfall
2. Hardwareproblem
3. Softwareproblem

In zusätzlich durchgeführten Studien kam man zu der Erkenntnis, dass jeder einzelne dieser Punkte Folge eines oder mehrerer Vorfälle sein kann. Diese werden in der unten aufgeführten Liste näher erläutert. Die Liste zeigt die verschiedenen Bedingungen unter denen es zu einem Versagen des Verkehrskontrollsystems kommt. Die detalliertere Version wird durch Unterpunkte in der Liste (deutlich eingerückt) dargestellt. Innerhalb einer bestimmten Ebene wird die Bedingung anhand eines vorangestellten ▲ markiert, wenn sie durch lediglich eine Unterbedingung erfüllt werden kann, oder durch ein ♣, wenn alle Unterbedingungen erfüllt werden müssen.

1 ▲ Stromausfall

1.1 ▲ Stromversorgung zum zentralen Computersystem ist unterbrochen

1.1.1 Fehler im zentralen Stromnetz (Stromausfall)

1.1.2 Unterbrochene Stromversorgung

1.1.3 Problem mit der Stromversorgung innerhalb des Gebäudes

1.2 ♣ Stromversorgung der Ampelanlage versagt

1.2.1 Versagen der Batterie – Notstromversorgung

1.2.2 ▲Versagen der Hauptstromversorgung

1.2.2.1 Fehler im zentralen Stromnetz (Stromausfall)

1.2.2.2 Unterbrochene Stromversorgung

2 ▲ Hardware Problem

2.1 Computerkomponenten in der Zentrale versagen

2.2 Netzwerkkomponenten zwischen Zentrale und Zwischenversorgung versagen

2.3 Teile der Ampelanlage versagen

3 ▲ Software Problem

3.1 ▲ Zentrales Verkehrskontrollsystem ist nicht funktionsfähig (zusammengebrochen)

3.1.1 Versagen des Betriebssystems

3.1.2 Versagen der Echtzeitanwendung

3.2 Zentrales Verkehrskontrollsystem sendet fehlerhafte Information zum Mikroprozessor der Ampelanlage

Um das zu veranschaulichen betrachten wir den Hauptfehler 1. Stromausfall und die dazugehörigen untergeordneten Fehler. Es gibt zwei Hauptmöglichkeiten aufgrund dessen ein Stromausfall vorkommen kann. Entweder handelt sich um die Bedingung 1.1 Stromversorgung zum zentralen Computersystem ist unterbrochen oder Punkt 1.2 Versagen der Stromversorgung der Ampelanlage.

Die "ODER-Beziehung" wird durch das ▲Symbol unter Punkt *1 Stromausfall* gekennzeichnet. Wenn wir nun Punkt *1.1* ***Stromversorgung zum zentralen Computersystem ist unterbrochen*** näher betrachten, stellen wir fest, dass diese Bedingung durch eine der drei folgenden Möglichkeiten erfüllt werden kann:

- Es könnte ein Fehler im zentralen Stromnetz vorliegen (Stromausfall) (Fehler *1.1.1*)
- Die Stromleitung zur Zentrale ist möglicherweise durchtrennt (Fehler *1.1.2*)
- Teile der Infrastruktur in der Zentrale sind vielleicht beschädigt (z.B. der Trenn- oder Ausschalter) (Fehler *1.1.3*)

Jede einzelne dieser Bedingungen würde zu einem Absturz des zentralen Computers führen, was wiederum die Ampelanlage lahmlegen würde.

Ein Stromausfall in der Ampelanlage verursacht möglicherweise ebenfalls einen Absturz des Systems, aber dank der Batterien in der Ampel, müsste es in dem Fall sowohl zur Erfüllung der Bedingung ***1.2.1 Versagen der Batterie - Notstromversorgung*** der Ampel als auch ***1.2.2 Versagen der Hauptstromversorgung der Ampelanlage*** kommen. Die "UND - Bedingung" bei Punkt ***1.2 Versagen der Stromversorgung der Ampel*** wird durch das ♣ Symbol gekennzeichnet, und verlangt die Erfüllung beider Unterbedingungen von Punkt ***1.2.1*** und Punkt ***1.2.2***.

Die Aufzählung von Vorfällen, Bedingungen und Ereignissen könnte sogar noch detaillierter aufgeschlüsselt werden. Leider wird es, je länger die Liste wird, immer schwieriger die einzelnen Punkte nachzuvollziehen. Dieselbe Information kann weitaus übersichtlicher grafisch anhand eines so genannten **Fehlerbaums** dargestellt werden.

Jeder möglicherweise eintretende Vorfall bzw. jedes Ereignis wird als *BLATT* oder *Knoten* in einer Baumgrafik dargestellt. Im Unterschied zu den natürlichen Bäumen, wachsen diese **Fehlerbäume** von oben nach unten. Innerhalb des **Fehlerbaums** wird der oberste Knoten *Wurzelknoten* genant und stellt den Zustand bzw. die Bedingung dar, die wir vermeiden wollen. Diejenigen Knoten, die direkt unter den Wurzelknoten stehen sind Bedingungen oder Ereignisse die dazu beitragen, dass die Wurzel erreicht wird. Diese Knoten werden *Kinder* der Wurzeln genannt, was bedeutet, dass die Wurzel ihr Ursprung ist. Knoten die einen gemeinsamen Ursprung haben werden *Geschwister* genannt.
Je weiter man die Zwischenknoten im Baum nach unten hin verfolgt, desto präziser wird die Übersicht. Die *Kinder* eines jeden Knotens geben uns eine jeweils genaue Information über ihren Zustand, Bedingungen oder Bedrohungen, die letztlich alle zu ihrem durch die Wurzel dargestellten Ursprung führen.

Die untersten Knoten nennt man BLATT-Knoten. BLATT-Knoten sind bereits so präzise, dass man sie nicht weiter aufschlüsseln muss. Drüber hinaus stellen sie nicht nur eine Bedingung, sondern auch eine Handlung oder ein Ereignis dar, die zu einem durch einen Wurzelknoten dargestellten Vorfall auf höherer Stufe (möglicherweise zusammen mit anderen Vorfällen) führen kann.

Es ist daher von Vorteil, sich auf eine grafische Darstellung zu einigen, um zwischen den logischen Beziehungen und verschiedenen Knotentypen unterscheiden zu können[3]. *UND*-Knoten repräsentieren die Zustände, die nur erreicht werden können, wenn alle durch ihre Kinder dargestellten Zustände erfüllt werden. Innerhalb dieses Textes haben wir uns darauf verständigt, die *UND*-Knoten durch 8-seitige, blaue Vielecke darzustellen. *ODER*-Knoten symbolisieren Zustände, die eintreffen, wenn ein als Kind dargestellter Knoten erreicht wird. Grafisch dargestellt werden letztere als grüne Rechtecke mit abgerundeten Ecken. BLATT-Knoten zeichnen wir als graue, scharfkantige Rechtecke.

Abbildung 1 stellt einen Fehlerbaum dar, der anhand dieser Symbole das ***Versagen einer Ampelanlage*** grafisch erklärt. Achten Sie darauf, wie anhand des **Fehlerbaums** die drei Stufen der verschiedenen Möglichkeiten - die letztlich zu einem Versagen der Ampel führen können - sichtbar werden (*Stromausfall, Hardware Problem, Software Problem*).

[3] Andere Autoren verwenden leicht unterschiedliche grafische Symbole bei der Erstellung von *Fehlerbäumen*. Unsere Darstellung soll in die eher komplexeren grafischen Strukturen, die wir später kennen lernen werden, einführen

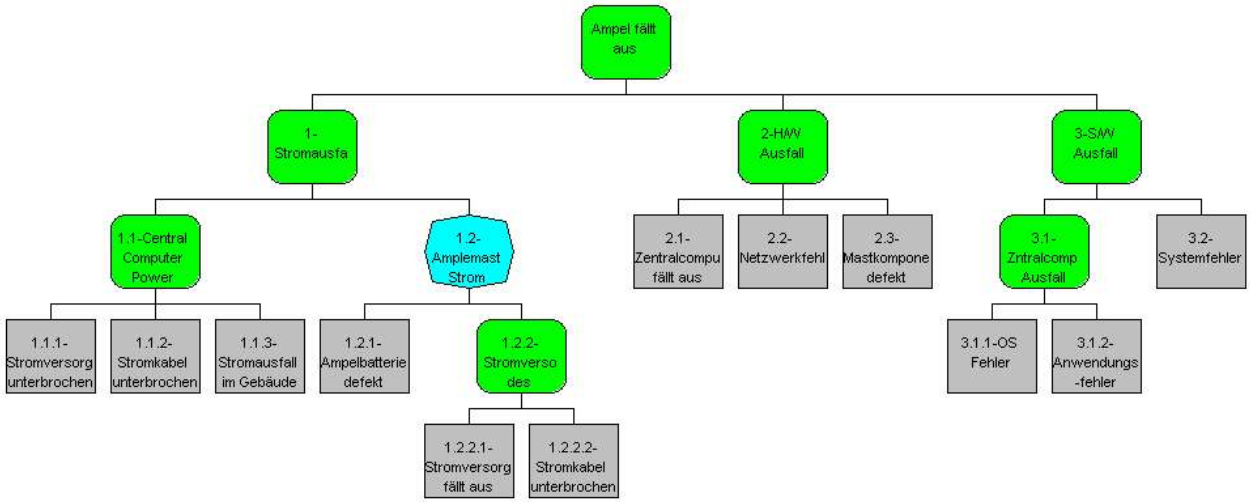


***Abbildung 1:*** *Fehlerbaum einer Ampelanlage*

Dieser **Fehlerbaum** beschreibt **wie** ein Ereignis eintreffen kann, jedoch nicht **ob** es möglicherweise eintritt. Das einfache Fehlerbaummodell ist daher in seiner Aussagekraft begrenzt.

## Erweiterter Fehlerbaum

Die Möglichkeiten aufgrund derer das geplante Ampelsystem versagen könnte, können ohne Probleme durch das Betrachten des Fehlerbaums ausgemacht werden. Leider ist das für eine Risikoanalyse nicht immer ausreichend. Die Stadtverwaltung muss in unserem Beispiel wissen, welche der theoretischen Schwachpunkte maßgeblichen Einfluss auf das Funktionieren der Ampelsignale haben. Bevor sie also dem Konzept des Bürgermeisters zustimmt, verlangt die Stadtverwaltung eine Zuverlässigkeitsprognose des gesamten Systems. Ebenfalls interssiert sie, welche der Schwachstellen die meisten Probleme verursachen werden und wie man diesen vorbeugen könnte. Glücklicherweise kann dies berechnet werden.

Die meisten Hersteller von Geräten/Maschinen verfügen über Daten die über die Verlässlichkeit ihrer Produkte Auskunft geben. Die Verlässlichkeit ihrer Komponenten wird durch die *mittlere Ausfallzeit eines Gerätes, MTBF (Mean Time Between Failure) und die mittlere Reparaturdauer eines Gerätes, MTTR (Mean Time to Repair)* ausgedrückt. Diese Werte können verwendet werden, um die Wahrscheinlichkeit eines Zusammenbruchs eines untergeordneteten Systems oder einer einzelnen Komponente auszurechnen[4]. Die Werte für das Verkehrsampelsystem sind in Tabelle 1 dargestellt.

[4] Nehmen wir zum Beispiel an, dass ein System bekannterweise einen MTBF von 8760 Stunden hat (entspricht einem Jahr). Bricht es zusammen, hat es einen MTTR von nur noch 4 Stunden. Wir kalkulieren dass das System im Durchschnitt 4 von 8760 Stunden, bzw. 0,0004566 (circa 0,045%) der Zeit nicht betriebsfähig ist.

| *Wahrscheinlichkeit des Ausfalls von Komponenten einer Ampelanlage* | | | | | | |
|---|---|---|---|---|---|---|
| Komponente | MTBF (h) | Ausfälle pro Jahr | MTTR (h) | Ausfallzeit (Jahr/h) | Ausfallzeit/ Gesamtlaufzeit | % Ausfallzeit |
| Betriebsstrom | 8760 | 1,00 | 1 | 1 | 0,00011416 | 0,0114% |
| Starkstromleitung | 17520 | 0,50 | 4 | 2 | 0,00022831 | 0,0228% |
| Gebäudeenergie | 4380 | 2,00 | 0,25 | 0,5 | 0,00005708 | 0,0057% |
| Ampelbatterie | 35040 | 0,25 | 4 | 1 | 0,00011416 | 0,0114% |
| Netzwerk | 1460 | 6,00 | 2 | 12 | 0,00136986 | 0,1370% |
| Hardware der Steuerungszentrale | 2190 | 4,00 | 4 | 16 | 0,00182648 | 0,1826% |
| Betriebssystem | 8760 | 1,00 | 1 | 1 | 0,00011416 | 0,0114% |
| Applikationssoftware | 4380 | 2,00 | 1 | 2 | 0,00022831 | 0,0228% |
| Ampelpfosten | 8760 | 1,00 | 2 | 2 | 0,00022831 | 0,0228% |
| Systemermüdung | 8760 | 1,00 | 4 | 4 | 0,00045662 | 0,0457% |

Dadurch, dass wir ausrechnen können, wie hoch die Wahrscheinlichkeit ist, dass ein untergeordnetes System einem Fehler unterliegt, können wir auch kalkulieren inwieweit andere, von diesem Subsystem abhängige Komponenten, beeinträchtigt werden[5]. **Abbildung 2** zeigt den Fehlerbaum der Ampel und enthält die Zusatzinformation bezüglich der Wahrscheinlichkeit eines Versagens.

Der erweiterte Fehlerbaum dient uns als Modell, um das zu untersuchende System besser verstehen zu können. Wie bei allen Modellen vereinfacht der Fehlerbaum der Verständlichkeit halber die Situation ohne jedoch diejenigen Eigenschaften außer Acht zu lassen, die das Funktionieren des Systems betreffen[6].

Der erweiterte Fehlerbaum verdeutlicht, dass die Ampel durchschnittlich 40 Stunden im Jahr funktionsunfähig ist, was natürlich nicht akzeptabel ist. Die größte Fehlerquelle scheint die Hardware (dargestellt durch die untergeordneten Bäume) zu sein, welche mit 0,34% oder fast 30 Stunden zum Ausfall der Ampel beitragen. Circa ⅔ aller Stromausfälle werden durch Fehler in der Zentrale verursacht, die verbleibenden ⅓ hängen mit Netzwerkproblemen zusammen.

[5] Bei *n* unabhängigen Ereignissen ist die Wahrscheinlichkeit, dass alles gleichzeitig eintreffen wird das Ergebnis der individuellen Ereignis–Wahrscheinlichkeiten, P= a x b x ...x n.

Diese Formel kann auch verwendet werden um die Wahrscheinlichkeit einer UND- Beziehung bei einem Knoten zu erreichen, sofern die Wahrscheinlichkeiten der Kinder der UND-Knoten individuell betrachtet werden können. Da die Wahrscheinlichkeit des Eintreffens einer oder mehrerer unabhängiger Ereignisse durch P = 1 – [ ( 1-a) (1-b)....(1-n)] gegeben ist, kann diese Formel auch zur Berechnung von ODER- Knoten herangezogen werden

[6] Wie bereits erwähnt beschreibt das Modell nur die einfache Situation, in der das Ampelkontrollsystem aus einer einzigen Ampel auf der Hauptstraße besteht. Wenn die Stadt mehrere Ampelanlagen besäße, müsste man 1.2.1, 1.2.2.2 und 2.3. wiederholen. Ginge es tatsächlich um eine große Anzahl von Ampeln, würde das Modell schnell unübersichtlich werden. In dem Fall wäre es wahrscheinlich besser sich der Realität anzunähern, indem man einen Gesamtwahrscheinlichkeitswert für Fehler einer ganzen Reihe von Ampelanlagen errechnet.

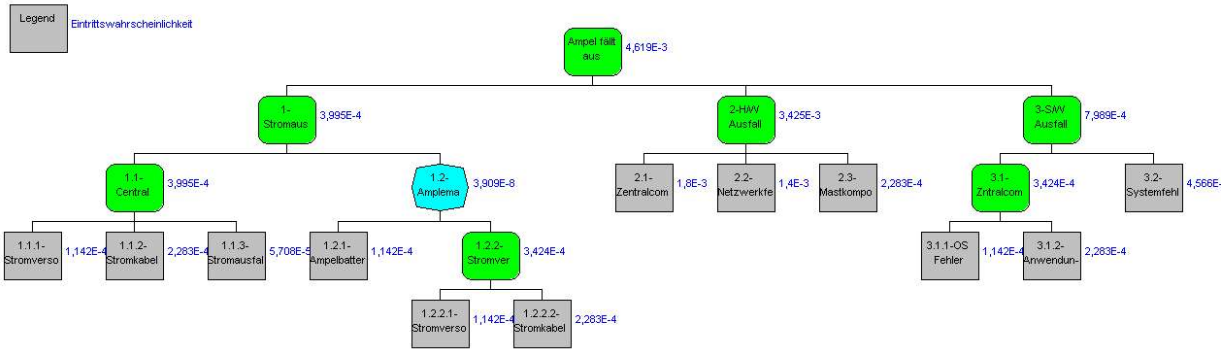


***Abbildung 2:*** *Wahrscheinlichkeiten des Ausfalls einer Ampelanlage*

Das System kann verlässlicher gemacht werden, indem die Anzahl der Stromausfälle in der Zentrale verringert und das Netzwerks verbessert wird. Eine andere Möglichkeit ist die Installation von hochwertiger Hardware in der Ampelanlage, die sie von den Anweisungen der Zentrale unabhängig machen würde. Da es sich in unserem Beispiel um nur eine Ampel handelt, entschied man sich dafür, die Hardware der Ampel zu verbessern. Hätte die Stadt mehrere Ampeln, wäre möglicherweise eine andere Entscheidung getroffen worden. Das System könnte dann so verändert werden, dass die Auswirkungen der Veränderungen deutlich werden würden.

In unserem Beispiel handelte es sich bei allen möglichen Ursachen des Systemausfalls um nicht bösartige, eher zufällige Fehler einzelner Teile. Aufgrund dessen, dass wir Zugriff auf Verlässlichkeitsstatistiken einzelner Komponenten hatten, konnten wir anhand des erweiterten Fehlerbaums die voraussichtliche Verlässlichkeit des gesamten Systems errechnen. Das wiederum hat uns gezeigt welche Teile des Systems problematisch sein könnten und gab Anhaltspunkte zur Verbesserung des Systems.

Der erweiterte Fehlerbaum verdeutlicht die Wahrscheinlichkeit eines Fehlers im Ampelsystem. Fehler führen voraussichtlich zu Unfällen, Staus (was zu einem Produktionsverlust führt) und Überstunden für die Polizei, die den Verkehr auf der Straßenkreuzung regeln muss. Anhand einiger Überlegungen und Recherchen wäre es möglich die Auswirkung des Ampelversagens abzuschätzen. Die Risikogleichung

**Risiko**Vorfall **= (Wahrscheinlichkeit eines Vorfalls) x (Auswirkung ausgelöst durch Vorfall)**

hilft uns den voraussichtlichen Verlust in einem vorgegebenen Zeitraum (normalerweise jährlich) zu berechnen. Dieser Wert wird **jährliche Verlusterwartung (annual loss expectancy, ALE)** genannt. Wenn die Kosten für eine Verbesserung (und Instandhaltung) des Systems unter dem ALE-Wert liegen, empfehlen gängige Risiko Management Systeme normalerweise eine Verbesserung des Systems.

Fehlerbäume erleichtern es uns das Risiko eines Systems auszumachen, welches über ausreichende Informationen ihrer untergeordneten Komponenten verfügt. Obgleich dies von großem Nutzen ist, wird die Anwendbarkeit von Fehlerbäumen deutlich durch die Verfügbarkeit von Statistiken begrenzt. Darüber hinaus bedeutet allein die Tatsache, dass wir über Statistiken

verfügen, dass wir in einem bestimmten Gebiet ausreichend Erfahrung haben, um uns eigentlich auf unsere Intuition verlassen zu können - was uns wiederum erlauben würde gänzlich auf formale Analysen zu verzichten.

Leider werden viele Vorfälle durch Ereignisse verursacht die weder zufällig noch Ursprung unglücklicher Umstände sind. Auslöser dieser Ereignisse sind feindliche Angriffe mit bösartiger Absicht. Möglicherweise gibt es Statistiken für Situationen, in denen es regelmäßig zu diesen Angriffen kommt. Die hohe Rate von Autodiebstählen beispielsweise ist wohlbekannt, und doch sind Statistiken hier oft nicht verfügbar. In dem Fall müssen, wenn wir eine Wahrscheinlichkeit ermitteln wollen, andere Techniken entwickelt werden. Manchmal werden zum Beispiel Checklisten verwendet, um Faktoren zu erkennen, die die Wahrscheinlichkeit eines Vorfalls erhöhen. Sicherheitsexperten im Computerbereich greifen oft auf Checklisten zurück, die risikosteigernde Elemente wie z.B. Modems, Internetverbindungen, nicht ausreichende technische Sicherheit etc., berücksichtigen. Diese Elemente werden dann in empirisch abgeleitete Formeln[8] eingesetzt, um abschätzen zu können wie wahrscheinlich es ist, dass das System einen Vorfall erleiden wird. Wir sind fest davon überzeugt, dass diese Techniken in der Regel nur sehr mangelhafte Ergebnisse erzielen.

Der nächste Abschnitt erweitert das Fehlerbaummodell noch ein wenig, so dass selbst diejenigen Risiken abgeschätzt werden können, für die es keine Statistiken gibt.

## Möglichkeiten-orientierte Fehlerbäume (Attack Trees)

Bereits 1994 wurde von Amoroso[9] das Konzept der „*Bedrohungsbäume*“ diskutiert. Unlängst entwickelte Bruce Schneier[10] (ein anerkannter Kryptologe) die dank ihm heutzutage weit verbreitete Idee eines *Attack Tree – Modells*, das auch von anderen Wissenschaftlern aufgegriffen und weiterentwickelt wurde[11].

Amenaza Technologies Ltd. hat sich von all diesen Sicherheitsmodellen, die sich an dem Baumsystem orientieren, inspirieren lassen und sie mit Hilfe neuer Methoden und Software weiterentwickelt. Wir von Amenaza nennen diesen Ansatz *Möglichkeiten-orientierte Attack Tree*[12]*Analyse.* Die damit verbundene Software ist unter dem Namen *SecurITree*® bekannt. Die

[8] Dadurch, dass die Formel fast ausschließlich auf Erfahrung basiert, kann man durchaus sagen, dass der Checklistenansatz als grundsätzlich informelle Art von Statistik gilt.

[9] Edward G. Amoroso, Fundamentals of Computer Security Technology, Prentice-Hall, ISBN0131089293

[10] B. Schneier, Attack Trees, Dr. Dobb's Journal, v. 24, n. 12, December 1999, pp. 21-29.
B. Schneier, Attack Trees: Modeling Actual Threats, SANS Network Security 99 **–** The Fifth Annual Conference on UNIX and NT Network Security, New Orleans, Louisiana. Wednesday, October 6th, 1999, Session Two, Track One - Invited Talks
B. Schneier, Seminar session given at a Computer Security Institute conference in November, 1997. See also http://www.counterpane.com/attacktrees.pdf

[11] Moore, A., Ellison, R. and R. Linger, "Attack Modeling for Information Security and Survivability", March 2001, http://www.cert.org/archive/pdf/01tn001.pdf

[12] Wir haben lange darüber diskutiert ob Threat Tree **(Bedrohungsbaum)** oder Attack Tree (**Angriffsbaum)** der passendere Ausdruck ist. Bezogen auf die vorhergegangenen Definitionen würde ein Bedrohungsbaum sowohl bösartige, absichtliche Angriffe von intelligenten Gegnern ausgehend, als auch Gefahren die zufälliger Art oder umgebungsbedingt sind, berücksichtigen. Unsere Analyse ist durchaus in der Lage sowohl feindselige als auch umweltbedingte Bedrohungen darzustellen, so dass **Bedrohungsbaum** ein passender Name ist. Auf der anderen Seite würde ein **Attack Tree** (laut unserer Definitionen) sich auf diejenigen Vorfälle beschränken, die absichtlich verursacht wurden. Ungeachtet der anscheinenden Missachtung unserer Definitionen haben wir uns für den Ausdruck **Attack Tree** entschieden. Dies haben wir aus zwei verschiedenen Gründen getan: Erstens wurde durch B. Schneiers Veröffentlichungen zu diesem Thema der Terminus **Attack Tree** eingeführt. Wir sind der Meinung, dass es nur verwirren würde einen anderen Ausdruck zu verwenden, auch wenn er uns eigentlich passender erschien. Unsere **Attack Tree** Modelle wären zwar in der Lage zufällige Missgeschicke mit einzubeziehen, unser Fokus wird aber hauptsächlich auf absichtlich durchgeführte Angriffe gelenkt sein. Daher werden wir den Begriff **Attack Tree** statt

Attack Tree Analyse ist besonders dort auf ein positives Echo gestoßen, wo sich Menschen mit der Sicherheit von Informationstechnologie beschäftigen. Als Antwort auf dieses Interesse hat Amenaza eine Art Archiv geschaffen, in der vordefinierte *SecurITree®* Modelle zu finden sind, um uns die Analyse gängiger Computersysteme zu erleichtern**. Die Attack Tree Analyse gilt jedoch nicht nur für die gängigen, sondern für fast alle Systemarten.**

Wie wir zuvor festgestellt haben, gibt es oft keine Statistiken für Bedrohungen, die von einem intelligenten, feindseligen Gegner ausgehen. Obwohl das natürlich stimmt, ist es dennoch möglich Faktoren auszumachen, die das Verhalten des Angreifers beeinflussen. Auf welche Art und Weise diese Faktoren Einfluss nehmen, hängt davon ab, ob und wie der *Bedrohungsagent* angreift. **Auch ein hoch motivierter Bedrohungsagent kann einen möglichen Angriff nur dann durchführen, wenn die Ressourcen, die ihm zur Verfügung stehen denen entsprechen, die notwendig sind um das fehlerhafte System auszunutzen**. Ein Mangel an Ressourcen bedeutet eine Einschränkung für das Verhalten des Bedrohungsagenten. Als Ressourcen verstehen wir sowohl Geld und technische Fähigkeiten, als auch die Bereitschaft den Preis für seine Tat zu bezahlen. Die Attack Tree Analyse arbeitet mit genau diesen Einschränkungen, um die Wahrscheinlichkeit der Angriffe genauer zu bestimmen.

## Beispiel eines Attack Trees

Um das Konzept einer Attack Tree Analyse zu verdeutlichen, stellen wir uns noch einmal eine hypothetische Situation vor. Dieses Mal wenden wir uns der Sicherheitsfrage zu, die sich ein typischer Eigentümer für sein Haus in einem Vorstadtviertel stellt. Obgleich wenige Hausbesitzer ein formelles Sicherheitsrisikogutachten für ihr Haus erstellen würden, haben wir uns bewusst für dieses Beispiel entschieden, da sich alle Leser etwas darunter vorstellen können.

Das Haus, das wir im Kopf haben ist ein typisches Einfamilienhaus, zu dem auch eine Garage gehört. Der Vorfall, der uns hier beschäftigen wird ist die Möglichkeit eines Einbruchs in eben dieses Haus. Diese Annahme wird durch den obersten Knoten des Attack Trees als *Einbruch in das Haus* dargestellt. Nach einigen Überlegungen können wir sieben verschiedenen Möglichkeiten ausmachen, wie ein Dieb in das Haus gelangen könnte, um einen Einbruch zu begehen:

1. Türen (die Vorder- und Hintertür, durch die man in der Regel hinein- bzw. hinausgeht)
2. Fenster
3. Durch die an das Haus angrenzende Garage
4. Wände (das Dach eingeschlossen)
5. Schornstein
6. Fußboden (im Falle eines Angriffs von unten)
7. Social Engeneering (Bewohner überzeugen die Tür zu öffnen)

---

**Bedrohungsbaum** verwenden.

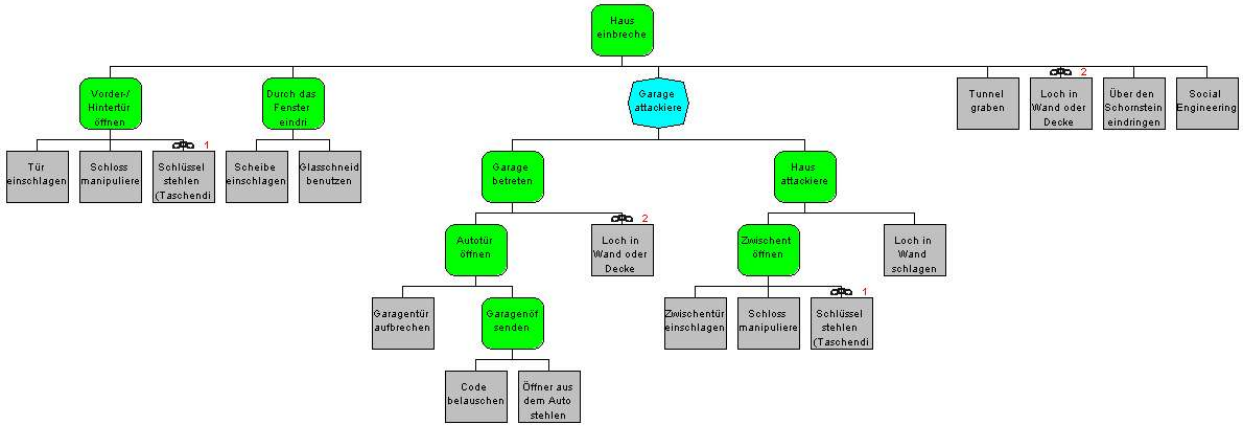


***Abbildung 3:*** *Attack Tree - Wege in ein Haus einzubrechen*

Diese Angriffe, die teilweise noch in detaillierte Schritte aufgeschlüsselt wurden, sind in **Abbildung 3** dargestellt. Um unser Beispiel zu vereinfachen haben wir die Aufschlüsselung der Angiffsvektoren auf *Öffnen der Vorder/Hintertür, Zugang über Fenster und Garage* beschränkt. Was die Angriffsmöglichkeiten durch *Loch in die Wand oder Dach bohren, Angriff über den Schornstein, Tunnel durch den Fußboden und Social Engeneering* betrifft, könnte man durchaus auch hier noch mehr ins Detail gehen.

Wie aus dem Diagramm ersichtlich wird, gibt es drei verschiedene Arten von Angriffen über die Durchgangstüren. Die Türen können entweder mit Gewalt aufgebrochen, die Türschlösser manipuliert, oder aber der Schlüssel durch Diebstahl entwendet werden. Ähnlich kann der Einbrecher das Fensterglas entweder herausschneiden oder einschlagen. Um über die Garage in das Haus zu gelangen, muss der Einbrecher zunächst in die Garage selbst eindringen und dann weiter ins Haus (entweder durch die Wand oder die Durchgangstür, die von der Garage ins Haus führt).

Die Aufschlüsselung von Ereignissen in mehrere, bzw. präziser definierte Ereignisse kann fast unendlich weitergehen. Für unsere Zwecke reicht es aus solange weiterzumachen, bis eine weitere Aufschlüsselung nicht automatisch mit einem besseren Verständnis des Modells einhergeht. Der BLATT-Knoten *Fensterglas zerschlagen* beispielsweise könnte in die Schritte *einen Stein aufheben und gegen das Fenster werfen* aufgeschlüsselt werden. Das allerdings ist unnötig, da es allgemein bekannt ist, wie man ein Fenster einschlägt. Auf der anderen Seite könnte und sollte der BLATT-Knoten *Öffnungscode belauschen* in mehrere Schritte zerlegt werden. Das würde nämlich zu einem besseren Verständnis derjenigen führen, die die einzelnen Schritte des Einbrechers versuchen nachzuvollziehen.

Bis zu diesem Punkt ähnelt unser Attack Tree in den Grundzügen dem zuvor betrachteten Fehlerbaum. Wir wollen nun auf der Struktur des Fehlerbaums aufbauen, indem wir die *Indikatoren für verhaltensabhängige Auswirkungen* einführen.

**Indikatoren für verhaltensabhängige Auswirkungen**

In den Attack Tree Modellen beginnen die Vorfälle mit den Ereignissen, die durch BLATT-Knoten dargestellt werden. Kommt es zu einer passenden Kombination von BLATT-Knoten-Ereignissen (festgelegt durch die UND/ODER-Baumstruktur), werden automatisch die Zwischenstufen oder Ereignisse (dargestellt durch Eltern oder BLATT-Knoten) erreicht. Das Ereignis geht stufenförmig aufwärts, erreicht andere Knoten und endet schließlich im Wurzelknoten (was automatisch bedeutet, dass es zu einem Vorfall gekommen ist).

Ob die BLATT-Knoten-Ereignisse letzten Endes eintreffen oder nicht, hängt vom Bestehen einer Bedrohung ab, die sowohl bereit als auch fähig ist, genügend Ressourcen aufzubringen, um die Verteidigungsstrukturen des Systems zu überwinden. Bei unabsichtlichen Vorfällen (wie das zuvor erläuterte Beispiel der Verkehrsampel), müssen passende umgebungsbedingte Bedingungen erfüllt werden, damit ein oder mehrere BLATT-Knoten-Ereignisse eintreffen. Die tatsächlichen Ursachen von naturbedingten Ereignissen sind meist nicht vollständig nachvollziehbar[13], wenn auch ihre Häufigkeit anhand von Statistiken wiedergegeben werden kann. Überschwemmungen beispielsweise kommen bekanntermaßen in bestimmten Gebieten einmal jährlich vor. Die Zahlen für die *mittlere Ausfallzeit eines Gerätes (MTBF) und die mittlere Reparaturdauer eines Gerätes (MTTR)* bei der Verkehrsampel stellen ein weiteres statistisch darstellbares Beispiel dar. Tippfehler[14] sind ein Beispiel nicht bösartiger menschlicher Bedrohung, die ebenfalls statistisch dargestellt werden kann. Die Wahrscheinlichkeit des Eintreffens ist also ein Maß für das Verhalten eines umweltbedingten Bedrohungsagenten[15]. Das ist das einfachste Beispiel eines verhaltensabhängigen Indikators.

Im Falle eines feindseligen Angriffs muss der Bedrohungsagent seine Ressourcen soweit erweitern, dass er am passenden BLATT-Knoten zuschlagen kann. Bösartiges Verhalten von Bedrohungsagenten wird stark von Faktoren, wie zum Beispiel den *Kosten um den Angriff durchzuführen, notwendiges technisches Wissen*, *Verfügbarkeit spezieller Materialien* oder der *Wahrscheinlichkeit erwischt und bestraft zu werden*, beeinflusst. Da diese Faktoren das Verhalten des Bedrohungsagenten beeinflussen, werden sie dementsprechend **verhaltensabhängige Indikatoren** genannt.

Je nachdem ob die Bedrohungen absichtlicher oder zufälliger Natur sind, können die verhaltensabhängigen Indikatoren verwendet werden, um genauer zu bestimmen ob ein Vorfall eintreffen könnte.

## Die Funktion verhaltensabhängiger Indikatoren

Um genauer festlegen zu können, ob ein bestimmtes Ziel im Baummodell erreicht werden kann, müssen wir untersuchen ob eine bestimmte Art von Bedrohungsagent über die

[13] Chaostheoretiker mögen darüber spekulieren, ob ein Hurrikan im Golf von Mexiko mit dem Flügelschlag eines afrikanischen Schmetterlings begonnen hat. Realistisch gesehen kann das Wissen über alle beitragenden Ereignisse nicht genau bestimmt werden. Das bedeutet, dass das durch den BLATT-Knoten dargestellte Ereignis nicht weiter aufgeschlüsselt, aber durchaus statistisch festgehalten werden kann.

[14] Tippfehler mag zwar harmlos klingen, waren aber einst die Ursache, dass eine Raumsonde den Planeten Mars verfehlt hat!

[15] Der Begriff *Bedrohungsagent* wirkt im Beispiel einer umweltbedingten Bedrohung ein wenig Fehl am Platz. Wer ist schuld an einer Flutkatastrophe? Wie wir bald sehen werden, passt diese Terminologie besser zu feindseligen, intelligenten Gegnern Wenn es Ihnen hilft, können Sie *Mutter Natur,* oder vielleicht *Murphys Law,* als Bedrohungsagenten bei umwelbedingten Gefahren nennen.

notwendigen Ressourcen verfügt, um das angestrebte Level zu erreichen[16]. Durch das Miteinbeziehen der notwendigen Ressourcen in das Bedrohungsmodell, ermöglicht man genauere Prognosen für das System.

Es ist zum Glück nicht notwendig explizit auf die Zahlenwerte der ressourcenabhängigen Voraussetzungen von jedem Knoten im Attack Tree einzugehen. Wie auch schon im vorhergegangen Beispiel der Verkehrsampel ist es möglich automatisch Ressourcen zu kalkulieren, die notwendig sind um einen Knoten zu erreichen, der dem Zahlenwert seiner Kind-Knoten entspricht. Das funktioniert für alle Knoten, außer den BLATT-Knoten. Sie haben keine Kinder und deren Werte müssen explizit eingegeben werden.

Im **Abbildung 4** und **5** sind zwei einfache Attack Trees dargestellt, die die Kosten zeigen, die ein Bedrohungsagent aufbringen müsste, um mehrere Ziele zu erreichen. Im Beispiel von **Abbildung 4** sind die Eltern von Ziel #1 und Ziel #2 ein UND-Knoten, was zur Folge hat, dass beide Kinder erreicht werden müssen, um zu den Eltern zu gelangen Es erscheint logisch, dass der Angreifer 500€ aufbringen muss um Ziel #1 und zusätzlich 200€ um Ziel #2 zu erreichen. Um auf die Ebene des UND-Knotens zu gelangen, müssten also 500€ + 200€ = 700€ aufgebracht werden.

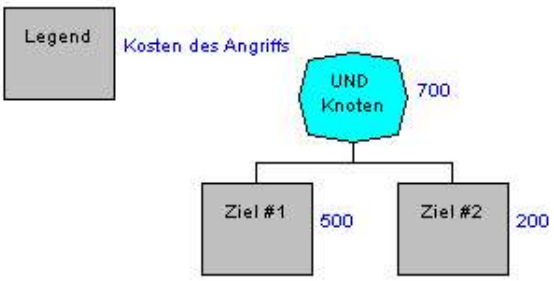


***Abbildung 4:*** *UND-Kosten eines Angriffs*

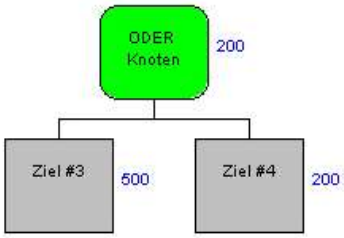


***Abbildung 5:*** *ODER-Kosten eines Angriffs*

Die Funktion, die mit dem verhaltensabhängigen Indikator *Angriffskosten* für UND-Knoten verbunden wird, entspricht daher der *Summe aller Unterpunkte*. Der Terminus hierfür lautet *Kosten für den verhaltensabhängigen Angriffsindikator UND-Funktion* oder einfach *Angriffskosten UND-Funktion.*

Auf ähnliche Art und Weise kann im **Abbildung 5** der ODER-Knoten erreicht werden, wenn entweder Ziel #3 oder Ziel #4 erlangt wurde. Wenn wir davon ausgehen, dass der Angreifer die günstigste der beiden Möglichkeiten wählen wird, wird der Preis um zum ODER-Knoten zu kommen der *Mindestbetrag der Unterpunkte* sein. Wir nennen das *verhaltensabhängiger Angriffsindikator ODER Funktion*, oder einfach *Angriffskosten ODER-Funktion.* Es lohnt sich zu erinnern, dass es zwei separate Wege gibt, auf denen der Angreifer das ODER-Ziel erreichen kann – der $200 - Wert, dargestellt durch den ODER-Knoten entspricht dem Weg mit den geringsten Kosten – welcher möglicherweise nicht gewählt wird, wenn der Angreifer über die Ressourcen für einen kostspieligeren Weg verfügt.

[16] Wie zuvor besprochen, setzt unsere Definition des *Bedrohungsagenten* voraus, dass eine Motivation besteht das System zu schädigen.

Die Indikatoren werden dem Baum zugeordnet, sofern sie offensichtlich problemrelevant sind. Typischerweise werden drei oder vier Indikatoren verwendet. Zu wenige Indikatoren führen zu einem oberflächlichen, eindimensionalen Verstehen derjenigen Kräfte, die bei einem Vorfall eine Rolle spielen. Eine zu große Anzahl von Indikatoren macht das Ganze möglicherweise so komplex, dass man den Wald vor lauter Bäumen nicht mehr sieht.[17]

Idealerweise sollten die Indikatoren orthogonal verlaufen. Das bedeutet, dass ein verhaltensabhängiger Indikator jeweils unabhängig von einem anderen ist. Der Kontostand eines Angreifers zum Beispiel ist bei einem Angriff relativ schwer zu erfassen. Die Indikatoren für *Angriffskosten* und die *Wahrscheinlichkeit seiner Ergreifung* sind orthogonale Indikatoren. Manchmal kommt es jedoch zu unvermeidbaren Abhängigkeiten zwischen den Indikatoren. In manchen Fällen zum Beispiel ist es möglich, das der Bedrohungsagent seine technischen Fähigkeiten durch Zeit und Geld erweitern kann. Daher stehen die *Angriffskosten* und *Technische Fertigkeiten* nicht komplett orthogonal zueinander. Obwohl die Indikatoren so gewählt werden sollten, dass die Abhängigkeiten so weit wie möglich reduziert sind, ist eine absolute Unabhängigkeit nicht immer erreichbar.

Wenn der Fokus auf feindseligen Angreifern liegt, sollten die verhaltensabhängigen Indikatoren Faktoren wiedergeben, die in einem möglichst weitläufigen Spektrum das Verhalten der Gegner beeinflussen. Die meisten Angreifer werden durch ähnliche Dinge beeinflusst: Kosten, technische Fähigkeiten, Gefahr erwischt zu werden, etc.

Die Indikatoren die wir für Bedrohungen aus der Natur verwenden, beruhen in der Regel auf Wahrscheinlichkeitsrechnungen (wie auch im Beispiel der Verkehrsampel). Es gibt jedoch noch andere Möglichkeiten, die ebenfalls umweltbedingte Situationen widerspiegeln. Ein möglicher Indikator könnte die *Höhe des Wasserspiegels bei Überschwemmung* sein.
Ein bestimmter Indikatorwert für den *„Höhe des Wasserspiegels bei Überschwemmung-Knoten“* könnte den Wasserstand anzeigen, bei dem ein Damm durchbrechen und in Fole dessen Schaden entstehen würde.

Indikatoren werden idealerweise je nach Projekt oder in standardisierter Version für das gesamte Unternehmen unterschiedlich und je nach Bedarf gewählt. Für jeden Ansatz gibt es Vor- und Nachteile. Indem wir eine Standardauswahl an Indikatoren verwenden, vereinfachen wir die Verfahrensweise verschiedener Projekte. Eine individuelle Auswahl von Indikatoren gibt wahrscheinlich eher die spezifische Situation eines Projektes wieder. Die beste Idee ist daher wahrscheinlich ein Standardset von Indikatoren zu verwenden, das jedoch bei Bedarf noch erweitert werden kann, falls kein erkennbarer Einfluss auf den Bedrohungsagenten ausgeübt wird.

Die Auswahl passender Indikatorfunktionen verlangt ein gewisses Verständnis für mathematische Zusammenhänge und Statistiken. Glücklicherweise sind die Funktionen der häufigsten Indikatoren den meisten bekannt.

[17] Ihnen ist es bestimmt klar gewesen, dass wir dieses Wortspiel irgendwann in unserer Darstellung verwenden würden, oder?

| *Verhaltensabhängige Indikatoren und zugehörige Funktionen* | | |
|---|---|---|
| **Indikator** | **UND** | **ODER** |
| Kosten | a + b + c +...+ n | Minimum (a,b,c,...,n) |
| Wahrscheinlichkeit entdeckt zu werden | 1-[(1-a) + (1-b) + (1-c) + ... + (1-n)] | Minimum (a,b,c,...,n) |
| Wahrscheinlichkeit des Erfolgs | a x b x c x ... x n | 1-[(1-a) + (1-b) + (1-c) + ... + (1-n)] |
| Technischer Schwierigkeitsgrad | Maximum (a,b,c, ..., n) | Minimum (a,b,c,...,n) |

Nachdem die passenden Indikatoren ausgewählt wurden, müssen die verhaltensabhängigen Indikatorfunktionen für jeden einzelnen Indikator definiert und Auskunft über die Werte der notwendigen Ressourcen von BLATT-Knoten erteilt werden[18].

Die Indikatorwerte der BLATT-Knoten orientieren sich an der *Expertenmeinung*, die wiederum auf einem gewissen Verstehen der Vorgänge basiert. Im nächsten Schritt können dann anhand der ausgewählten Formeln diese sog. Ressourcenwerte aller nicht-BLATT-Knoten des Attack Trees errechnet werden.

Problematisch wird es dann, wenn ein Modell versucht sowohl umweltbedingte, als auch bösartige Bedrohungen zu integrieren. Wie wir bereits festgestellt haben, sind die Wahrscheinlichkeitswerte, die wir normalerweise für Bedrohungen zufälliger Art verwenden, für absichtliche Attacken nicht vorhanden. Genauso können wir uns fragen, was die finanziellen Kosten der Natur bei einer Überschwemmung sind? Es gibt keine perfekten Antworten auf diese Fragen, obgleich wir im Folgenden noch auf ein paar Strategien eingehen werden (Seite 34).

## Wege um Indikatorenwerte für Knoten zu berechnen

Zunächst ist es wichtig die Bedeutung der berechneten Werte der Zwischenknoten und des Wurzelknotens zu verstehen. Obgleich es letztendlich davon abhängt welche Indikatorfunktionen in den Berechnungen verwendet werden, gibt der Wert eines bestimmten Knotens in der Regel die Voraussetzungen der notwendigen Ressourcen wieder, die aufgebracht werden müssen, um den Weg/die Wege mit dem geringsten Kostenaufwand zu erreichen. Werden aber verschiedene Indikatoren innerhalb eines bestimmten Baumes verwendet, wird jeder Knoten jeweils einen Wert für jeden Indikator anzeigen**. Die Berechnungen für einen bestimmten Indikator haben keinen Einfluss auf die Berechnung anderer Indikatoren.** Jeder Indikatorwert repräsentiert einen spezifischen Weg von einem oder mehreren BLATT-Knoten zu dem jeweiligen Punkt im Attack Tree. Der oder die Wege, die zu einem bestimmten Knoten führen oder den geringsten Kostenaufwand mit sich bringen sind in der Regel für jeden Indikator unterschiedlich.

[18] Obgleich es keinen Grund gibt, warum die Werte für BLATT-Knoten nicht gleichzeitig mit der Knotendefinition hinzugefügt werden kann, finden es die meisten Menschen einfacher zuerst den Baum zu erstellen um dann noch einmal die BLATT-Knoten durchzusehen und diese Information nachträglich einzugeben.

 

## Wege von beeinflussenden Knoten

Die Indikatorenwerte eines bestimmten Knoten im Baum werden aus den Werten der darunter liegenden Knoten berechnet. Die unteren Knoten haben unterschiedlichen starken Einfluss, abhängig von ihrer UND/ODER Struktur, ihrer Berechnungsfunktion und ihrer Knotenwerte. Es ist wichtig diejenigen Knoten herauszufinden, welche den größten Einfluss auf die Indikatorwerte der Elternknoten haben.

Das Problem ist, dass „Einfluss“ ein relativ subjektiver Ausdruck ist. Hat ein Knoten beispielsweise „großen Einfluss“ wenn er den Wert der Eltern in irgendeiner Art verändert? Um 50%? Um 10%? Es gibt keine klare, mathematisch korrekte Antwort auf diese Frage, sondern es hängt vielmehr davon ab, was die Person, die diese Frage stellt damit erreichen möchte.

## Kritischer Pfad

Wir veranschaulichen das Ganze indem wir den *kritischen Pfad* definieren. Der *kritische Pfad* enthält alle Knoten die einen Einfluss auf die zuvor berechneten Knoten ausüben. Genauer gesagt ist ein Knoten dann auf dem kritischen Pfad, wenn sein Löschen (oder das Löschen aller Geschwisterknoten mit demselben Wert) den Elternwert ändern oder seine Definition für diese Indikatorfunktion verlieren würde. Unsere Definition ist keine Standardlösung – es gibt viele andere.

Das Berechnen und Betrachten des kritischen Pfades eines Baumes ist hilfreich, um zu sehen welche BLATT-Knoten den geringsten Aufwand für jede einzelne Ressource aufweisen. Das ist besonders dann von Bedeutung, wenn die kritischen Pfade verschiedener Indikatoren sich überlappen. **Das ist ein deutlicher Hinweis darauf, dass die Schwachstelle bzw. Schwachstellen in den sich überlappenden kritischen Pfaden ein Schwachpunkt im System sind.**

Allgemein gesagt ist es aber relativ schwierig die Bedeutung des kritischen Pfades zu verstehen. Wir werden nun andere, leichter verwendbare Analysemethoden vorstellen.

## Attack Tree Schneiden – Möglichkeitenbedingte Analyse

Zuvor haben wir das Attack Trees Modell zu Rate gezogen, um verschiedene Wege zu zeigen, durch die die Sicherheit eines Hauses gewährleistet werden konnte. Darüber hinaus wurden Ressourcen herausgearbeitet die für jeden Angreifer notwendig gewesen wären, um in das Haus zu gelangen. Obwohl dies natürlich interessant und wichtig ist, reicht es dennoch nicht aus um vorauszusagen, wer auf welche Art und Weise angegriffen wird. Die *Möglichkeitenbedingte Analyse* erlaubt uns das Attack Tree Modell zu verwenden, um genau diese Fragen zu klären und das Verhalten der Angreifer vorherzusagen!

Die *Möglichkeitenbedingte Analyse* von Attack Trees basiert auf einer einfachen Annahme das Verhalten von Angreifern betreffend:

„**Wenn Angreifer wollen UND die Möglichkeiten haben werden sie es auch tun.“**

Mit anderen Worten: Gibt es Gegner, die motiviert sind das System zu schädigen, über die für die Durchführung ihrer Tat notwendigen Ressourcen verfügen, als auch bereit sind die Konsequenzen[19] zu akzeptieren, werden sie früher oder später einen erfolgreichen Angriff auf das System durchführen.

Es gibt nur ganz wenige Situationen, in denen das nicht der Fall ist. Die Gegner greifen möglicherweise nicht an, weil sie nicht wissen, dass das System überhaupt existiert[20]. Sie greifen vielleicht auch nicht sofort an, wenn es viele andere Systeme mit ähnlichen Schwachstellen gibt und sie ganz einfach noch nicht auf dem richtigen Weg sind um genau das System zu treffen[21].

## Schwachstellen im System

Die klassische Definition von Risiko bezieht die Wahrscheinlichkeit eines Vorfalls mit ein. Statistiken werden anhand von Ereignissen erstellt, die aufgrund einer Anhäufung zugrunde liegender Faktoren eintreffen und maßgeblich mitbestimmen, ob es zu einem Vorfall kommt oder nicht. Kommt es aufgrund des Zusammentreffens dieser Faktoren nur selten zu einem Ereignis, kann auch keine Statistik erstellt werden. Das erschwert das Aufzeigen von Wegen, die die Wahrscheinlichkeit eines eintreffenden Vorfalls verringern.

Anstatt also auf das Eintreffen von Vorfällen zu warten um bessere Statistiken erstellen zu können, können wir genausogut die grundsätzlichen Auslöser betrachten, aufgrund derer es zu Vorfällen kommt? Nehmen wir doch einen Moment lang an, dass die Gegner das System angreifen wollen: was bestimmt letztlich ob sie es schaffen? Eine allgemein bekannte Formel lautet:

**Vorfallswahrscheinlichkeit = Bedrohung x Schwachstelle**

Das anfängliche Attack Tree Modell wurde aktualisiert (siehe Abbildung 6), um die notwendigen Ressourcen für die Durchführung eines BLATT-Knotenangriffs bereitzustellen und danach eine höhere Ebene im Attack Tree zu erreichen. Die erforderliche Anstrengung um einen Angriff durchzuführen, ist ein Maßstab für die Größe einer bestimmten Schwachstelle im System. Der Attack Tree aus Abbildung 6 stellt also den Ausdruck der *Schwachstelle* der oben genannten Gleichung dar. Wenn wir die Größenordnung einer *Bedrohung*, der ein System ausgesetzt ist, bestimmen können, ist die Gleichung vollständig.

### Möglichkeiten der Bedrohungsagenten

Zuvor hatten wir festgestellt, dass Bedrohungen von *Bedrohungsagenten* ausgehen. Ein *Bedrohungsagent* ist eine Gruppe von Gegnern, die gleiche Eigenschaften aufweisen und deren Vorhaben die Schädigung eines Systems[22] ist. Feindselige *Bedrohungsagenten*

[19] Unsere Definition von *Möglichkeit* bedeutet das Zugeständnis des Angreifers Scham, finanziellen Verlust, persönlichen Schaden oder gar Tod in Kauf zu nehmen. Es erscheint uns daher der passendste Ausdruck zu sein.

[20] Wenn die Geheimhaltung des Systems ein bedeutender Teil der Abwehr des Systems ist, sollten die Wege auf denen das System enttarnt werden kann, im Attack Tree dargestellt werden.

[21] Das Angreifen anderer Ziele könnte einen größeren Nutzen für den Angreifer haben oder die Kosten für den Angriff anderer Ziele niedriger sein.

[22] Um die Natur mit einzubeziehen dehnen wir unsere Definition soweit, dass auch umweltbedingte Gefahren miteinbezogen werden.

versuchen Bedingungen zu schaffen, um Schwachstellen ausnutzen zu können. *Bedrohung* kann daher auch folgendermaßen dargestellt werden:

**Bedrohung = Möglichkeit x Motivation**

In unserer Definition des *Bedrohungsagenten* gehen wir davon aus, dass eine Motivation vorhanden ist. Daher hängt der Bedrohungsgrad ausschließlich von der Möglichkeit[23] des Angreifers ab. Das wiederum bedeutet:

**Bedrohung = Möglichkeit**

Möglichkeit ist also ein Maßstab für die Ressourcen, die einem *Bedrohungsagenten* zur Verfügung stehen. Darunter verstehen wir z.B. Geld, Geschick und Wissen, Zeit und die Bereitschaft schädliche Konsequenzen zu tragen.

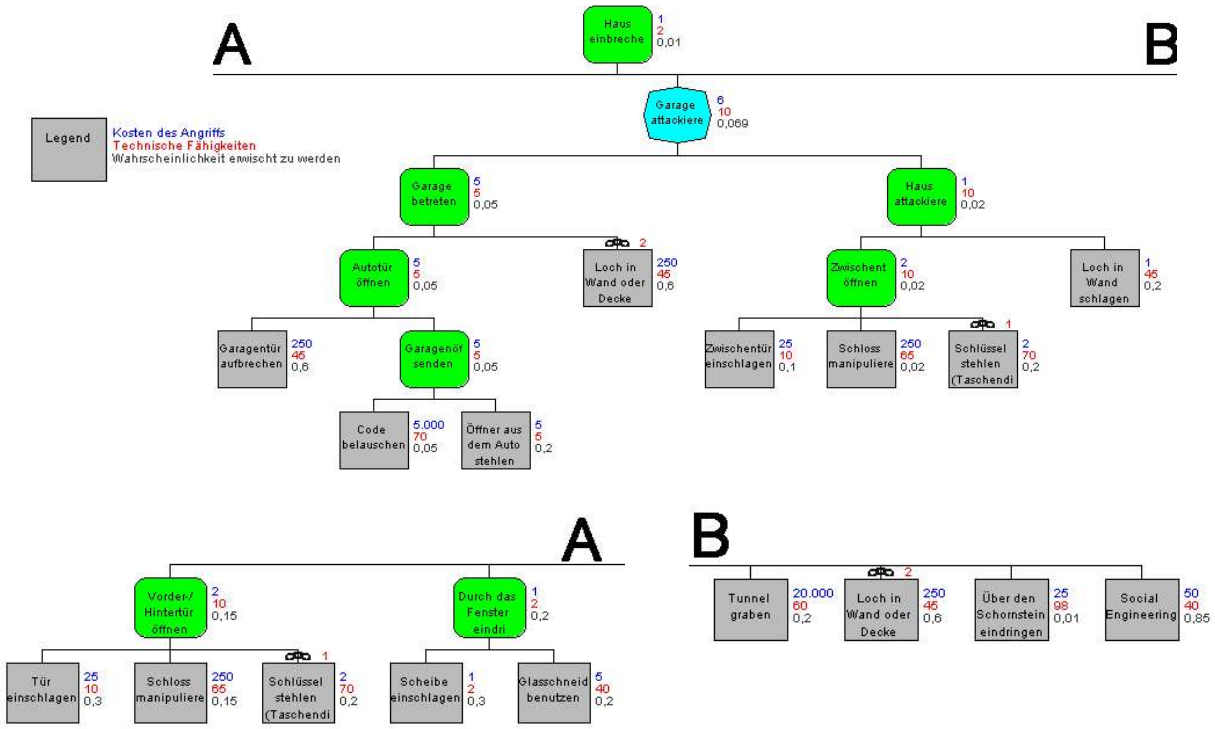


***Abbildung 6:*** *Attack Tree eines Hauseinbruchs und die dafür erforderlichen Ressourcen*

Das Identifizieren von Bedrohungsagenten, die vorhaben ein System zu schädigen, verlangt Menschenkenntnis. Es handelt sich hierbei meist um einen nachvollziehbaren Prozess. Banken zum Beispiel machen sich sowohl Sorgen um Bankräuber, als auch um Betrüger und Hacker, deren Intention es ist über das Computersystem zuzuschlagen. Sie haben vielleicht, je nachdem was in den Tresoren der Kunden aufbewahrt wird, keinen Grund sich um Juwelendiebe Gedanken zu machen und befürchten normalerweise auch keinen militärischen Angriff. Auf der anderen Seite lohnt es sich über ein paar unwahrscheinliche Gegner nachzudenken, die über außergewöhnliche Ressourcen verfügen, um zu sehen wie sich ein

[23] Später werden wir sehen, wie die Motivation des Angreifers in das Baummodell integriert werden kann. Das wird die Tatsache widerspiegeln, dass Motivation des Bedrohungsagenten = Möglicher Nutzen vom Angriff für den Bedrohungsagenten ist.

System verhalten wird, wenn es sich mit einem außergewöhnlichen Gegner auseinandersetzen muss.

Der Analyst sollte daher ein Profil für jede nur vorstellbare Art von Bedrohungsagent erstellen. Das Profil beschreibt die Ressourcen des Bedrohungsagenten, die jedem einzelnen Indikator des Attack Tree Modells entspricht. Wird ein Bedrohungsagent, der motiviert ist das System zu schädigen, nicht miteinbezogen, können Risiken, die von diesem Agenten ausgehen, nicht berücksichtigt werden. Es ist daher ratsam ein eher größeres als ein zu kleines Spektrum von Bedrohungsagenten zu berücksichtigen.

Betrachten wir zwei mögliche Bedrohungsagenten für unser Haussicherheitsmodell.

| ***Bedrohungsagent*** | ***Finanzielle Ressourcen*** | ***Akzeptierte Wahrscheinlichkeit entdeckt zu werden*** | ***Technische Möglichkeiten Skala 1-100*** |
|---|---|---|---|
| Jugendlicher Straftäter | 50,00 € | 50% | 25 |
| Einbrecher | 5.000,00 € | 10% | 70 |

Der jugendliche Straftäter ist ein verärgerter Teenager der nicht viel Geld hat, um es in einen Hauseinbruch zu investieren. Er oder sie hat keine Angst erwischt zu werden. Eine vergeudete Jugend hat aber unseren Schurken davon abgehalten technische Fertigkeiten zu entwickeln.

Unser Einbrecher dagegen ist ein Profi. Er ist ein verbrecherischer katzenhafter Dieb und betrachtet Einbrechen als seinen Beruf. Er ist bereit Geld auszugeben, um Geld zu verdienen und ist darauf vorbereitet bis zu 5000€ für Werkzeug auszugeben. Wie jeder Profi hat er sein Fach gut studiert und hat keine Probleme Schlösser aufzubrechen, einfache Alarmanlagen zu deaktivieren und Fensterscheiben zu zerschlagen. Die einzige Sache, die er nicht bereit ist zu akzeptieren, ist ins Gefängnis zu gehen.

Diese Profile sind Vermutungen, die auf uns zugänglichen Information und der Meinung von Experten basieren. Die Genauigkeit unserer Prognosen hängt davon ab, wie präzise unsere Vermutungen über den Bedrohungsagenten sind.

## Schneiden (Eliminieren) nicht erreichbarer Ziele

Der Attack Tree in **Abbildung 6** beschreibt sowohl die notwendigen Ressourcen, um ein Angreifen auf einem BLATT-Niveau durchzuführen, als auch Ziele und Zwischenstufen innerhalb des Attack Trees. Das Profil des Bedrohungsagenten geht auf die, einem potentiellen Angreifer zugänglichen, Ressourcen näher ein. Indem man beide vergleicht, können alle Knoten des Attack Trees geschnitten[24] oder ausgelöscht werden, die über die Möglichkeiten des Bedrohungsagenten hinausgehen. In **Abbildung 7** sind zum Beispiel die möglichen Angriffe eines jugendlichen Straftäters auf das Einfamilienhaus dargestellt. Im Vergleich dazu die Angriffe eines professionellen Einbrechers (**Abbildung 8**). Das Verhalten der beiden

[24] Ein „geschnittener" Attack Tree ist ein Attack Tree, dem Knoten durch das Filtern von Kriterien gelöscht wurden.

Angreifer-Typen wird ziemlich unterschiedlich sein. In beiden Fällen sind die möglichen Angriffe das, was wir intuitiv erwarten würden[25]. Jugendliche Täter tendieren dazu eine Menge kaputtzumachen. Einbrecher dagegen sind raffiniert und unauffällig.

Angenommen, das Modell ist präzise und unsere Vermutungen über die Bedrohungsagenten sind zutreffend, so werden von einem geschnittenen Baum alle möglichen Angriffe beschrieben. Sind die Bedrohungsagenten dazu noch motiviert anzugreifen, steht es außer Frage, dass die nach dem Schneiden verbliebenen Angriffe wahrscheinlich sind. Es gibt nicht genügend Information um die Wahrscheinlichkeit zu messen, aber wir können annehmen, dass sie relativ hoch ist.

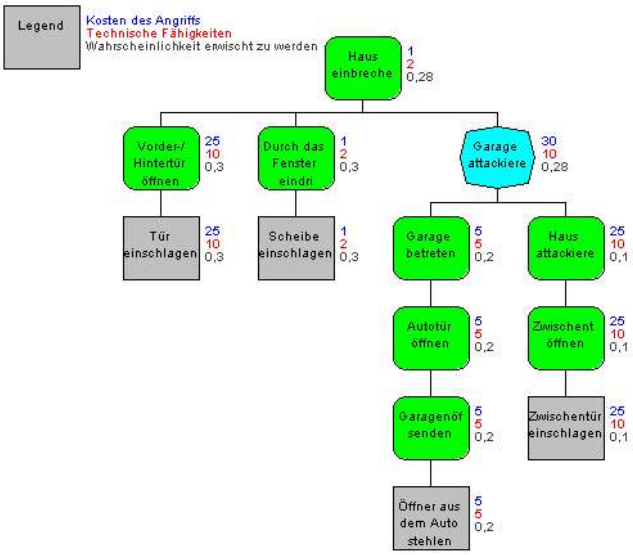


***Abbildung 7:*** *Geschnittener Attack Tree (Jugendlicher Straftäter)*

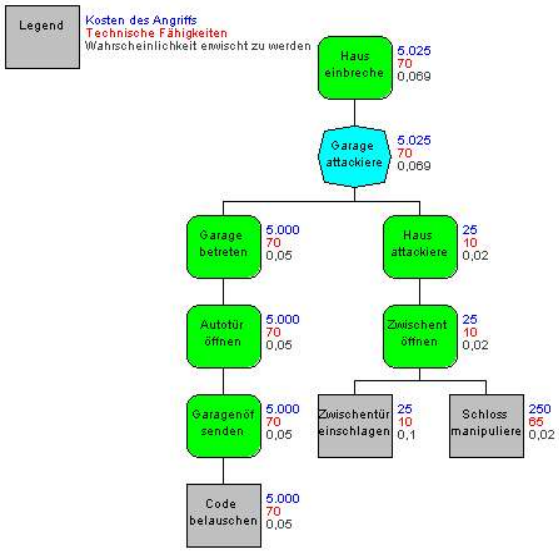


***Abbildung 8:*** *Geschnittener Attack Tree (Einbrecher)*

Die größte Einschränkung des geschnittenen Attack Trees ist, dass der Indikatorwert für einen bestimmten Knoten ebenso wie beim Original Attack Tree eine Reihe verschiedener Wege reflektiert, die diesen Punkt erreichen. Der geschnittene Attack Tree zeigt zwar mehrere Knoten, an die die Bedrohungsagenten anknüpfen können, gibt jedoch keine Hinweise auf spezifische Pfade, auf denen sie ihr Ziel erreichen können.

## Angriffsszenarien

Ein *Angriffsszenario* ist ein bestimmter Pfad, oder eine Reihe von Pfaden der mit einer minimalen Anzahl von einem oder mehreren BLATT-Knoten zur Wurzel führt. Minimal in dem Sinne, dass das Schneiden eines einzigen BLATT-Knotens den Weg zur Wurzel versperrt.

[25] Wie schon zuvor angemerkt können wir uns in Situationen, in denen wir über viel Erfahrung verfügen, überraschend gut auf unsere Intuition verlassen.

*Angriffsszenarien* gibt es für den ganzen Attack Tree. Das vollständige Spektrum von Angriffszenarien eines Attack Trees zeigt alle Angriffe, die ein Angreifer durchführen kann, der über unbegrenzte Ressourcen und Möglichkeiten verfügt.


***Abbildung 10:*** *Angriff eines jugendlichen Straftäters #1*


***Abbildung 9:*** *Angriff eines jugendlichen Straftäters #2*

Generell ist es hilfreich die Reihe von Angriffsszenarien für einen geschnittenen Attack Tree zu berechnen, da es deutlich macht welche Angriffe für welche Art von Bedrohungsagent möglich sind. Der jugendliche Straftäter beispielsweise kann bei einem geschnittenen Attack Tree zwischen drei verschiedenen Einbruchsszenarien wählen **(Abbildung 7)**

1. Die Vorder- bzw. Hintertür aufbrechen **(Abbildung 9)**
2. Das Fenster einschlagen **(Abbildung 10)**
3. Den Garagenöffner aus dem Auto des Hausbesitzers stehlen (um sich Zugang zur Garage zu verschaffen) UND die Durchgangstür zwischen Garage und Haus aufbrechen **(Abbildung 11).**

Ein Angriffsszenario zeigt nur einen kleinen Teil des Weges. Das heißt, dass die für die Knoten berechneten Werte die spezifischen Ressourcen darstellen, die ein Angreifer auf seinem Weg aufbringen muss.

Die mit einem bestimmten Angriffsszenario assoziierten Ereignisse auf BLATT-Niveau, können uns bei bestimmten Angriffsarten behilflich sein. Obwohl das in diesem Beispiel mehr als offensichtlich erscheint, kann das bei komplexen Situationen und mehreren hundert oder tausend Angriffsszenarien durchaus von Vorteil sein.

So wäre es zum Beispiel möglich ein Angriffserkennungssystem zu entwickeln um Ereignisse auf BLATT-Niveau mit Angriffsszenarien zu vergleichen und einen Alarm auszulösen wenn ein Angriff erkannt wird.

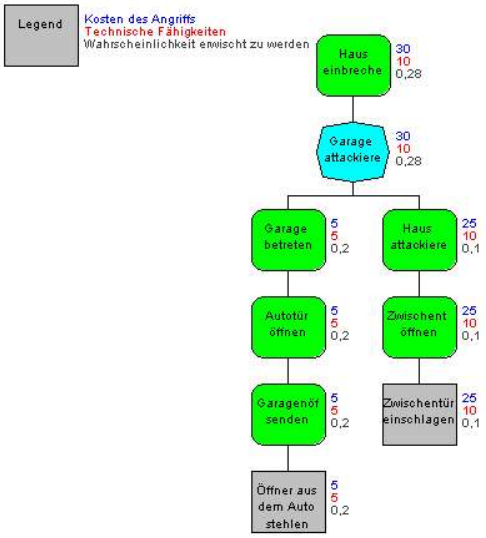


***Abbildung 11:*** *Angriff eines jugendlichen Straftäters #3*

## Risikobestimmung durch Möglichkeitenabhängige Analyse

Zuvor haben wir Risiko definiert als

***RisikoVorfall = (Vorfallswahrscheinlichkeit) x (Auswirkung durch Vorfall).***

Wir haben dann aufgezeigt, dass falls

***Bedrohung = Möglichkeit x Motivation***

was für einen motivierten Angreifer auf

***Bedrohung = Möglichkeit***

reduziert werden kann, dann ist die

**Vorfallswahrscheinlichkeit = Bedrohung x Schwachstelle.**

Folglich ist

***RisikoVorfall = (Bedrohung x Schwachstelle) x (Auswirkung durch Vorfall).***

Da ein Modell des geschnittenen Attack Trees den Terminus *Bedrohung x Schwachstelle* mit einbezieht, können wir auch die *Auswirkungen* in unser Modell integrieren und somit das Risiko besser bestimmen.

## Effektindikatoren

Genauso wie wir zuvor die verhaltensabhängigen Indikatoren geschaffen haben um Faktoren mit einzubeziehen, die das Verhalten des Angreifers beeinflussen, werden wir jetzt das Konzept der *Effektindikatoren* einführen. *Effektindikatoren* werden zunächst verwendet um den Einfluss oder den Effekt, den ein Angriff auf das Opfer hat, darzustellen. Sie können jedoch auch verwendet werden, um die Vorteile eines Angreifers herauszuarbeiten.

Die Werte für verhaltensabhängige Indikatoren werden durch Dateneingabe auf BLATT-Niveau berechnet. Sind erst einmal die genauen Formeln ausgewählt und auf die Anfangswerte übertragen, läuft der Rest automatisch ab.

Die Effektindikatoren verlangen eine genauere Betrachtung. Während einige Werte durchaus berechnet werden können, kann die Mehrheit nur dadurch bestimmt werden, indem man die Arbeitsprozesse genauer untersucht, die bei bestimmten Angriffen beeinträchtigt werden. Auch wenn alle erfolgreichen Angriffe dasselbe Wurzelziel verfolgen, beeinflussen verschiedene Pfade durch den Attack Tree (Angriffsszenarien) das Opfer auf unterschiedliche Art und Weise.

Nehmen wir zum Beispiel an, dass ein Attack Tree verschiedene Wege aufzeigt, ein Computerprogramm zu stören. Ein Angriffsszenario könnte das Durchdringen einer Internet Firewall sein, wodurch der Zugang zum lokalen Netzwerk ermöglicht wird und solange manipulierte Information an den Computer verschickt werden, bis dieser kapituliert und neu gestartet werden muss. Ein anderer Ansatz wäre beispielsweise einen Lastwagen voller Diesel und Dünger neben das Gebäude zu parken und explodieren zu lassen, das Haus somit zum Einstürzen und den Server zum Verbrennen zu bringen. Beide Angriffe erreichen das Ziel, das Computersystem zum Erliegen zu bringen, wenn auch eine der beiden Arten weit mehr Schaden als die andere anrichtet.

Das gilt auch, wenn es darum geht Vorteile für einen Angreifer aufzuzeigen. In der Sicherheitsbranche ist es allgemein bekannt, dass es viel nützlicher für einen Gegner ist, ein Geheimnis zu stehlen ohne erwischt zu werden als einen Aufmerksamkeit erregenden Angriff durchzuführen. Angriffsszenarien denen ein heimlicher Angriff zugrunde liegt lohnen sich daher viel eher für den Angreifer. Dies wiederum beeinflusst möglicherweise die Wahl des Bedrohungsagenten für welche Art von Angriff er sich letztlich entscheidet.

Um die Auswirkungen richtig darzustellen, sollte das Modell die Möglichkeit offen lassen, ob man externe Informationen nutzt, um die Werte der Effektindikatoren eines Knoten darzustellen oder ob sie vollständig anhand der Werte der „Kinderknoten“ kalkuliert werden können. Die Effektwerte können sich nach verschiedenen Maßstäben richten. Auch wenn Geld als das am häufigsten auftretende Maß gilt, kann es durchaus auch an anderen Dingen wie z.B. der Anzahl von notwendigen Bedingungen gemessen werden.

Betrachten wir nun das uns bereits bekannte Haussicherheitsmodell (**Abbildung 3**). Die Risikoanalyse schätzt, dass Angreifer, wenn sie es schaffen in ein Haus zu gelangen Gegenstände im Wert von 15.000€ stehlen oder beschädigen werden. In unserem speziellen Beispiel verfügt der Besitzer über eine Menge wertvoller Werkzeuge und Sportgeräte, die in der Garage aufbewahrt werden. Laut Untersuchungen wird davon ausgegangen, dass der Angreifer diese Gegenstände übersieht wenn er direkt in das Haus einbricht. Kommt der Einbrecher jedoch durch die Garage, wird er die Wertsachen mit Sicherheit wahrnehmen und stehlen. Zusätzlich muss das Modell also alle möglichen Kollateralschäden wiederspiegeln, die durch den Angriff entstehen können. Miteinbezogen werden zerbrochene Fensterscheiben, beschädigte Türen, geklaute Schlüssel, etc. Um diese Details in das Modell mit einzubeziehen, muss jeweils neu entschieden werden, ob eine allgemeine Formel oder das „Injizieren“ von Werten in die Knoten letztlich anzuwenden ist.

Dies kann am ehesten dargestellt werden, indem die Angriffsszenarien des Haussicherheits Attack Trees genauer untersucht werden, der gestutzt wurde, um die möglichen Angriffe eines jugendlichen Straftäters aufzuzeigen.

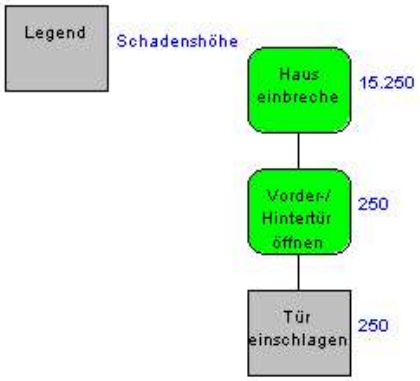


***Abbildung 12:*** *Finanzieller Schaden durch jugendlichen Straftäter #1*

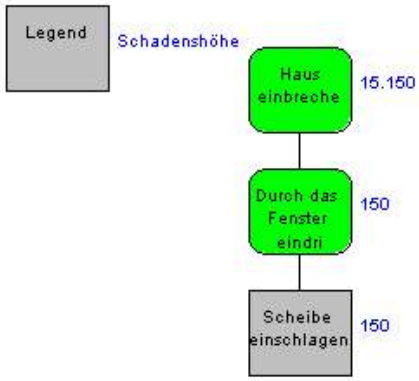


***Abbildung 13:*** *Finanzieller Schaden durch jugendlichen Straftäter #2*

Diese Szenarien, vervollständigt durch finanzielle Effektwerte, werden in **Abbildung 12**, **Abbildung 13** und **Abbildung 14** dargestellt.

**Abbildung 13** ist das Angriffsszenario mit den geringsten Folgen für den Hauseigentümer. Der Schaden beläuft sich auf 150€, um eine zerschlagene Fensterscheibe zu reparieren, zuzüglich der 15.000€ für die gestohlenen Gegenstände, was sich auf insgesamt 15.150€ beläuft. Der Angriff von **Abbildung 12** ist auch nur geringfügig teurer da 250€ für die Reparatur der Tür eine nur relativ geringe Differenz zu den Kosten für eine neue Scheibe ausmachen. Ein deutlich größerer Sprung den Schaden des Opfers betreffend wird aus **Abbildung 14** ersichtlich.

In diesem Szenarium schlägt der jugendliche Straftäter ein Autofenster ein (200€), um den Garagenschlüssel zu klauen (50€). In der Garage wird er auf die „Goldmine“ von Sportartikeln aufmerksam und macht sich mit zusätzlichen 3.000€ davon. Zum Schluss bricht er noch die Durchgangstür zum Haus auf (250€) und stiehlt Wertgegenstände für 15.000€. Die Endsumme beläuft sich letztendlich auf 18.500€.

Ohne weitere Informationen über die Vorlieben von jugendlichen Straftätern zu kennen, ist es durchaus nachvollziehbar anzunehmen, dass die Wahrscheinlichkeit aller drei Angriffsarten ungefähr gleich hoch ist. Das bedeutet, dass der Angriff mit dem größten Effekt (Angriffsszenario#3) auch das größte Risiko birgt.

Es ist durchaus wichtig zu verstehen warum das so ist. Die dargestellten Angriffe sind wahrscheinlich, weil sie von einem Bedrohungsagenten, der motiviert ist anzugreifen, durchführbar sind. Das ist der erste Teil der Risikogleichung. Die Auswirkungen vervollständigen letzten Endes die Gleichung und zeigen das relative Risiko auf.

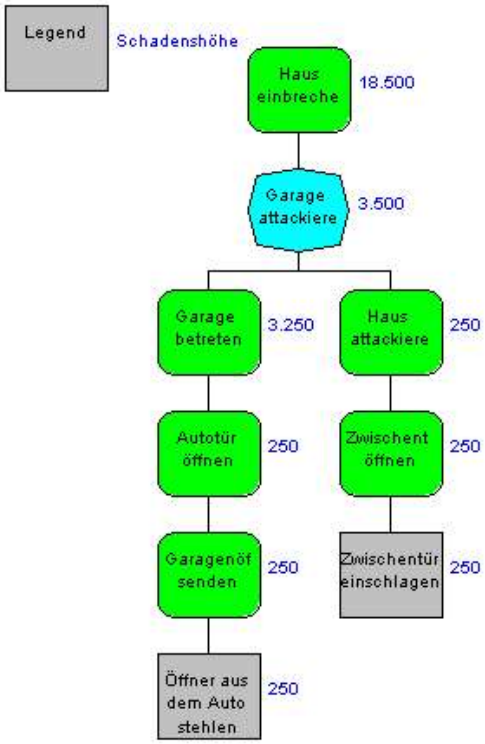


***Abbildung 14:*** *Finanzieller Schaden durch jugendlichen Straftäter #3*

## Motivation des Bedrohungsagenten

Bis jetzt haben wir unsere Analyse insoweit vereinfacht, dass wir davon ausgegangen sind, dass alle Bedrohungsagenten gleich stark motiviert sind, das System zu schädigen.

Das ist natürlich nicht immer so. Glücklicherweise können wir, sofern wir die Psychologie von Angreifern verstanden haben, die Motivation eines Angreifers in ein Attack Tree Modell integrieren.

Angreifer können durch viele Dinge motiviert werden. Das Haussicherheitsmodell, das wir zuvor besprochen haben, geht davon aus, dass die Einbrecher in das Haus eindringen und Wertsachen stehlen. Das kann ohne Probleme dargestellt werden, indem wir einen Effektindikator schaffen, der den finanziellen Nutzen des Angreifers zeigt. Dieser wird ähnlich hoch wie der Schaden des Opfers sein, außer dass der Angreifer keine Vorteile aus dem Beschädigen von Sicherheitskomponenten (wie z.B. Schlösser, Fenster) ziehen wird, wohingegen das Opfer sicherlich beeinträchtigt wird. Indem wir eine Liste von Angriffszenarien schaffen, können wir herausfinden welche Angriffe am attraktivsten für den Bedrohungsagenten sind. Es ist also mit anderen Worten möglich zu sehen, welche Angriffe ihn wahrscheinlich am meisten motivieren werden.

Indem wir die vom Bedrohungsagenten aufgewendeten Ressourcen in einem bestimmten Angriffsszenario mit dem gewonnenen Nutzen vergleichen, kann für den Angreifer sogar ein Return on Investment (ROI) errechnet werden. Das macht einen sogar noch genaueren Blick auf die Motivation des Bedrohungsagenten möglich. Bei dieser Art von Analysen[26] ist jedoch Vorsicht geboten, da sie stark vom Verständnis der Psychologie eines Bedrohungsagenten abhängen. Verwirrte Personen, oder Personen aus Kulturen mit einem sehr unterschiedlichen Wertesystem, denken und urteilen auf eine Art und Weise, die wir nicht voraussagen können. Indem wir also annehmen, dass das Verhalten des Bedrohungsagenten stark von seinen Fähigkeiten abhängt, sind wir damit auf der sicheren Seite. Sogar Supermann kann nur das erreichen, was seine Ressourcen ihm erlauben. Das ist der Vorteil von möglichkeitenabhängiger Analyse.

## Die Kombination von Wahrscheinlichkeiten und Möglichkeiten bei Verhaltensindikatoren

Einige der Analysemodelle sind rein auf der Wahrscheinlichkeitsebene angesiedelt. Andere wiederum betrachten nur die feindlichen Bedrohungen. In diesen Situationen gibt es keine Frage, wie die verhaltensbedingten Indikatoren einzuschätzen sind. Probleme entstehen wo ein Modell beide Arten von Bedrohungen berücksichtigt.

Der einfachste Fall ist dann, wenn sich die wahrscheinlichen und feindseligen Bedrohungen eines Systems wenig oder überhaupt nicht gegenseitig beeinflussen. Die Inhaber einer Produktionsstätte beispielsweise machen sich möglicherweise Sorgen über feindselige Bedrohungen in Form eines Einbruchs, bei dem Waren oder Maschinen gestohlen werden können. Gleichzeitig befindet sich die Fabrik in einer Flussebene, in der es häufig zu Überschwemmungen kommt und daher befürchtet werden muss, dass der Fluss über das Ufer tritt und es zu einem Wasserschaden bei den Waren kommen könnte. Ein Feuer im nahe gelegenen Wald könnte dem Gelände und der Fabrik ebenfalls zu nahe kommen. Der einfachste Weg mit dieser Situation umzugehen wäre zwei verschiedene Attack Trees zu erstellen und die Analyse jeweils getrennt vorzunehmen.

In manchen Fällen jedoch stehen die Bedrohungen in Wechselbeziehung zueinander **(Abbildung 15)**. Nehmen wir einmal an die Produktionsanlage hat ein Einzugsgebiet, dass aus Zäunen mit Alarmanlagen und Wachposten besteht. Diese Schutzvorrichtung ist normalerweise schwierig zu durchbrechen. Eine Flut könnte aber die Schutzvorrichtungen insofern schwächen, als dass die Alarmanlagen oder Wachposten nicht wie gewohnt funktionieren können. Die Flut ermöglicht gewissen Bedrohungsagenten (deren Bemühungen sonst vereitelt worden wären) das Eindringen in die Fabrik.

[26] Im Beispiel des Hauseinbruchs könnte man leicht darauf verfallen einen Effektindikator, in Form des Wertes der gestohlenen Gegenstände, als Indiz für die Motivation des Angreifers zu nehmen. Unser Modell jedoch basiert auf der Tatsache, dass der Angreifer sich nicht über die Wertsachen in der Garage bewusst ist und sie nur zufällig entdeckt, sofern sich gewisse Angriffszenarien abspielen. Das ist oft der Fall. Die Täter werden regelmäßig von den Resultaten ihres Angriffs überrascht.

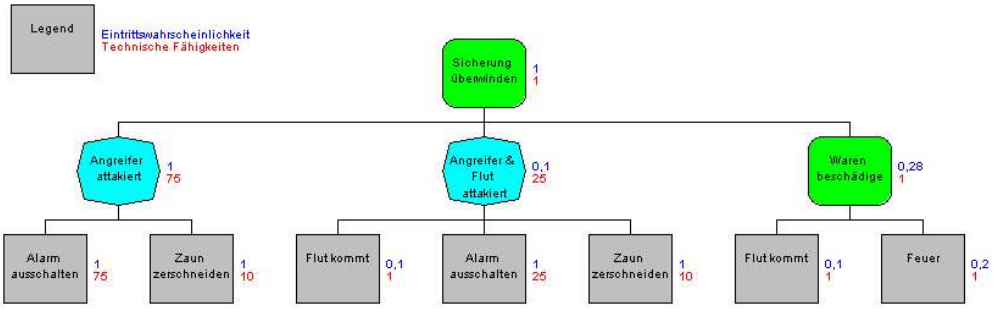


***Abbildung 15:*** *Gemischte Bedrohung gegen eine Sicherungsanlage*

Wenn es auch keine perfekten Techniken gibt unterschiedliche Verhaltensindikatoren aufeinander abzustimmen, gibt es doch einen guten Trick um sich dem Problem zu nähern. Die Verhaltensindikatoren des Attack Trees sollten in zwei Kategorien aufgeteilt werden; und zwar in umweltbedingte und ursächliche Kategorien. Die umweltbedingten Indikatoren spiegeln die Vorfallswahrscheinlichkeit. Die ursächliche Reihe von Indikatoren bezieht sich auf die Fähigkeiten von Bedrohungsagenten (z.B. Angriffskosten, technische Fertigkeiten). BLATT-Knoten, die Ereignisse in der Umwelt darstellen, müssen daher ihren umweltbedingten Verhaltensindikatoren Werten zuordnen die sie aus statistischen Quellen haben. Die ursächlichen Verhaltensindikatoren für die Umweltknoten müssten den „einfachen“ Werten zugeordnet werden, d.h. die Schwellenwerte sollten von jedem Bedrohungsagenten erreichbar sein.

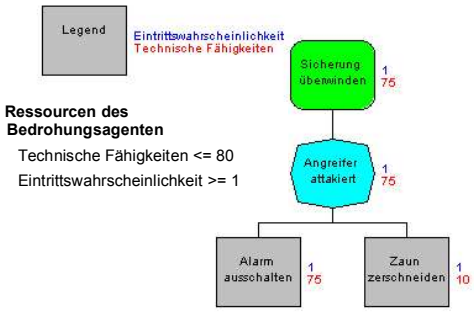


***Abbildung 16:*** *Nur ein Angreifer*

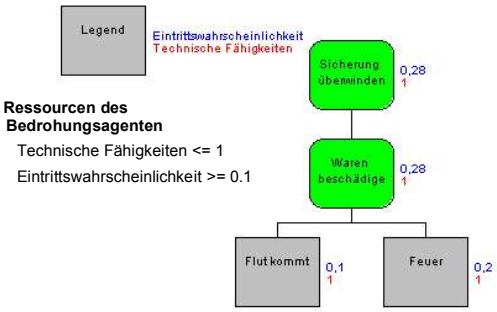


***Abbildung 17:*** *Naturereignisse*

Umgekehrt sollten die BLATT-Knoten ihre Umwelt-Schwellenwerte vereinheitlichen. Das bedeutet, dass deren Wahrscheinlichkeit vollständig vom Verhalten der Angreifer kontrolliert wird. In einem nächsten Schritt kann der Baum nun geschnitten werden, um drei Situationen näher zu betrachten. Welche der eintreffenden Vorfälle werden lediglich auf der Fähigkeit des Gegners basieren (**Abbildung 16**), welche basieren ausschließlich auf der Wahrscheinlichkeit (**Abbildung 17**) und welche Vorfälle treten dann ein, wenn ein bestimmtes Level von Fähigkeit und Wahrscheinlichkeit des Gegners gegeben ist (**Abbildung 18**)? Es ist Vorsicht geboten beim interpretieren von Situationen gemischter Indikatoren.

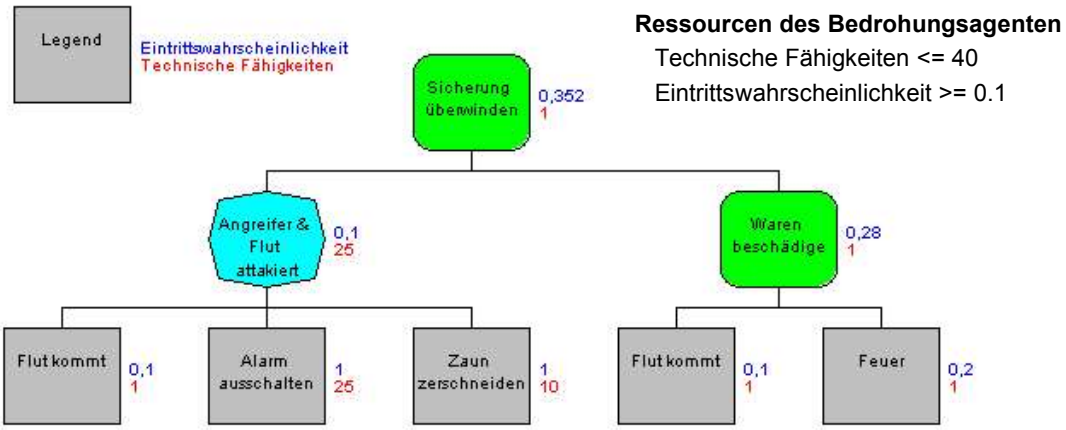


***Abbildung 18:*** *Kombination von Naturereignissen und einem Semi-Professionellen Angreifer*

## Warum wir Analyse-Tools brauchen

Die zuvor beschriebenen Techniken basieren auf einfachen Konzepten. Die gezeigten Beispiele waren fast alle klein genug, um von einer Person mit Papier und Bleistift durchgeführt zu werden. Diese Operationen werden allerdings schnell unhandlich, wenn es um sehr komplexe Situationen geht. Der Wunsch mit dem Modell zu experimentieren, indem man den Attack Tree verändert und Vermutungen über die Bedrohungsagenten modifiziert, würde sich schnell legen, sobald man sich über den Aufwand bewusst wird, der notwendig ist um Angriffsszenarien „zurechtzustutzen“ oder zu berechnen.

Mit Hilfe eines Software-Tools das in der Lage ist mit einem Mausklick diese Operationen durchzuführen, können einige komplexe Situationen vereinfacht werden. Genauso wie ein Tabellenkalkulationsprogramm die Aktualisierung von Daten überflüssig macht, kommt es mit Hilfe eines Analyse-Tools für Attack Trees nicht mehr darauf an, dass ein Analyst sämtliche Parameter im Auge behält.

Amenaza hat ein solches Software-Tool entwickelt. *SecurITree*® ist das erste kommerziell erhältliche Attack Tree - Entwicklungs- und Analysetool der Welt. Mit *SecurITree*® können Sie tatsächlich den Wald vor lauter Bäumen sehen!

## Vorteile von Attack-Tree-Analysen gegenüber klassischen Risikoanalyse-Methoden

Die konventionelle, auf Statistiken basierende Risikoanalyse kann möglicherweise aussagen, wie hoch die Wahrscheinlichkeit ist, dass jemand in ein Haus einbricht und welcher Schaden dadurch entsteht. Jedoch gibt diese Art von Risikoanalyse lediglich ungefähre Richtlinien vor, wie man sich schützen kann.

Die Attack Tree Analyse ermöglicht uns die zugrunde liegenden Tatsachen zu erkennen, die das Verhalten des Angreifers determinieren. Dem Hausbesitzer fällt beim Entfernen des Garagentorschlüssels aus dem Auto möglicherweise auf, dass er den risikoreichsten Angriff eines jugendlichen Straftäters damit ausgeschlossen hat.

Auch wenn es Statistiken für Hauseinbrüche gibt, ist das nicht automatisch für andere Arten illegaler Aktivitäten der Fall. Ohne Statistiken ist es anhand der konventionellen Risikoanalysen nicht möglich überzeugend vorauszusagen welche Angriffe wahrscheinlich eintreffen. Die Analysten müssen sich daher auf Vermutungen verlassen, die, auch wenn sie später zutreffen, nicht auf Tatsachen beruhen. Falls der Analyst sich entscheiden sollte das System zu ändern um gewisse Risiken zu minimieren, bietet die konventionelle Risikoanalysemethode keine Vorschläge effektiver Veränderungsmöglichkeiten. Die Folge ist eine Reihe rein subjektiver Entscheidungen für die es keine nachvollziehbare Argumentationskette gibt. Früher oder später kommen Probleme auf und niemand wird sich an den rationalen Hintergrund der Vorschläge erinnern können.

Attack Tree Modelle erklären sich zum großen Teil selbst. Die Vermutungen über die Schwachstellen des Systems manifestieren sich im Attack Tree selbst, die Vermutungen über die Bedrohungsagenten sind in der Tabelle „Möglichkeiten von Bedrohungsagenten“ aufgeführt. Die Lösungen ergeben sich aus den mathematischen Schlussfolgerungen, indem wir das Profil des Bedrohungsagenten in das Modell integrieren (durch „Schneiden“ des Attack Trees). Das ist viel verlässlicher als die Erinnerungsfähigkeit eines Analysten.

Gängige Ansätze von Risikoanalysen sind sehr zeitintensiv. Das führt dazu, dass die Analysten im Falle einer system– oder umweltbedingten Änderung nur widerwillig Updates durchführen. Das führt auch dazu, dass nur ein kleiner, zufälliger Teil des Systems zu einem bestimmten Zeitpunkt berücksichtigt wird. Wenn die Analyse dann endlich vollständig ist, ist sie nicht mehr relevant, da sich das System bereits verändert hat. Attack Tree Modelle können (mit Hilfe der richtigen Tools) innerhalb weniger Minuten aktualisiert und neu bewertet werden.

# Methodologie

## Ergebnisse der Attack Tree orientierten Risikoanalysen

Der vorangegange Teil hat die theoretischen Grundlagen *möglichkeitenbedingter Attack Tree Analysen* beschrieben. Damit uns diese Prinzipien etwas nützen, müssen wir sie strukturiert anwenden. Wir nennen das *Methodologie*. In der Regel werden bei einer Risikoanalysen-Methodologie drei Dinge untersucht:

### Eine zuverlässige und *vorschriftsgemäße* Abwehr

Wir sind keine Anwälte. Generelle Rechtsberatung ist nur von bedingtem Nutzen, da Gesetze je nach Gerichtsbarkeit, Branche und jeweiliger Situation variieren. Soweit uns bekannt ist, verlangt die allgemeine Rechtsprechung, dass ein Betrieb in der Lage ist deutlich zu machen, dass potentielle Risiken untersucht und nach wohlüberlegten Gesichtspunkten gehandhabt wurden. Eine Attack Tree Analyse ist ein formeller Weg Risiken zu identifizieren und anhand dessen Entscheidungen zu fällen.

Nur zu oft vergessen Betriebe den wohlüberlegten Prozess zu dokumentieren, anhand dessen sie entscheiden welche Risiken sie berücksichtigen oder welche Strategien sie bezüglich der Schadensminderung anwenden. Ein Attack Tree Modell ist in der Lage

a) die Argumentationskette bestimmter Entscheidungen zu dokumentieren.
b) die Abhängigkeit von menschlicher Erinnerungsfähigkeit auszuschließen bzw. zu reduzieren.
c) die Plausibilität von Entscheidungen aufzuzeigen.

Auch wenn Ihre Analysten Genies sind, die keine Tools und Techniken verwenden, um die richtigen Entscheidungen zu treffen, mag es doch in bestimmten Situationen notwendig sein ihre Handlungen rechtfertigen und nachvollziehen zu können.

### Identifizieren von effektiven Sicherheitslösungen

Menschen in leitenden Positionen sind es oft leid, sich auf Lösungsstrategien zu verlassen, die anscheinend niemals das leisten was sie zuvor versprochen hatten. Das ist besonders im Bereich der Informationstechnologie der Fall. Nur zu oft betrachtet das Management einer Firma die mit der Sicherheit betrauten Leute als die „Schneider des Kaisers“. Wie Sie sich vielleicht erinnern, fiel einst ein bestimmter Kaiser einem betrügerischen Schneider zum Opfer, der vorgab Kleider aus einem magischen Stoff zu nähen, der alle möglichen wundervollen Qualitäten hatte. Der Kaiser konnte diese versteckten Eigenschaften des besagten Kleidungsstücks nicht so recht sehen und kaufte dem Schneider die vielversprechenden Kleider ab. Nachdem er jedoch nackt in der Öffentlichkeit erwischt wurde, schwor er nie wieder auf Scharlatane hereinzufallen. Der Kaiser ist jetzt Ihr Chef und glaubt nichts, solange es nicht

hundertprozentig nachweisbar ist. Die Attack Tree Analyse ermöglicht es Ihnen aufzuzeigen, was Lösungstrategien leisten können bevor Sie sie kaufen oder anwenden.

### Nachweisbar kosteneffektive Sicherheitslösungen

Die erarbeitete Lösung muss nicht nur funktionieren, die entstehenden Kosten sollen auch im Hinblick auf das Risiko gerechtfertigt sein. Die Berechnung des Return On Security Investment (ROSI) für IT-Sicherheitslösungen ist aber schon immer schwierig gewesen, da das verwendete Datenmaterial meist so unpräzise ist, dass auch die Mathematik zu keiner Entscheidungsgrundlage verhilft.

Attack Tree Modelle und Szenarienanalysen zeigen hingegen nachvollziehbar welche Situationen wahrscheinlich auftreten und wie viel Schaden dadurch entstehen wird. In diese Analysen können dann verschiedene Lösungen integriert werden und sowohl die dadurch entstehenden Kosten als auch Einsparungen verdeutlicht werden. Damit ist eine notwendige Grundlage zur Aufstellung einer Return On Security Investment (ROSI) Rechnung gegeben. Die aus einem Attack Tree ermittelten Werte bilden so eine nachvollziehbare und solide Basis auf derer ein Return On Security Investment (ROSI) kalkuliert werden kann.

## Universelle Methodologie

Die genauen Details einer Methodologie müssen angepasst sein an die Strukturen und Arbeitsvorgänge des betreffenden Betriebes. Amenaza empfiehlt in der Regel einen vierstufigen Risikoanalyseprozess.

1. Erstellen eines Attack Tree Modells das darstellt wie es zu einem Vorfall kommen kann. Darstellung der Schwachstellen und notwendigen Ressourcen, um sie ausnutzen zu können sowie die Auswirkung verschiedener Angriffe auf das Opfersystem. Das Modell zeigt Techniken, die verwendet werden können, um das System angriffsicherer zu machen oder seine Gestaltung zu verbessern.
2. Herausfinden welche Schwachstellen von einem bestimmten Bedrohungsagenten ausgenutzt werden. Finden Sie heraus, wer ihre Feinde sind, wo und wie sie zuschlagen werden.
3. Erstellen einer Prioritätenliste für Risiken die jede Angriffsart berücksichtigt. Nur wenige Betriebe sind in der Lage jede Schwachstelle zu korrigieren. Die Prioritätenliste beinhaltet die notwendigen Informationen um zu rechtfertigen, welche Probleme gelöst werden müssen und ob der Verbesserungsvorschlag kostengerecht ist.
4. Effektive Vermeidungsstrategien vorschlagen. Zeigen Sie, wie sich verschiedene Veränderungen am System auswirken und finden Sie die effektiven (und kostengerechte) Verbesserungen.

## Beispiel einer Informationstechnologie-Methodologie

Wie bereits oben erwähnt, variieren detaillierte Risikoanalysen abhängig von der Art des untersuchten Systems. Die Schritte, die in diesem Teil untersucht werden sind speziell für

Anwendungen in der Informationstechnologie. Wir hoffen, dass Menschen, die in anderen Branchen tätig sind inspiriert werden und ein ähnliches, ihrem Aufgabenbereich angepasstes Modell, anwenden können.

## Schritt Eins: Abbildung des Informationssystems in einem Attack Tree

### Definitionsbereich

Bevor wir Risiken eines bestimmten Informationssystems auswerten können, müssen wir zunächst definieren, was das System ausmacht. Im Fachjargon von Risikonanalysten wird das System oft „*zu prüfendes System*[27]“ genannt. Logischerweise ermöglicht das „*zu prüfende System*“ die Verarbeitung und Übertragung von Information. Verlässt man sich auf die Sicherheit der Netzwerkinfrastruktur hat dies möglicherweise einen beträchtlichen Einfluss auf die Computer, die die Information verarbeiten.

Menschen, die mit der Information arbeiten sind auch Teil des Systems. Sie zu identifizieren ist weitaus schwieriger als es klingt. Es ist zwar möglich den Kabeln zu folgen und festzustellen welche Computer miteinander verbunden sind, es ist jedoch nicht immer offensichtlich wie Menschen miteinander kommunizieren.

Es gibt auf Erfahrungen basierte Grenzen eines Systems. Zwar ist es verlockend, in eine Risikoanalyse alle Komponenten eines Netzwerks mit einzubeziehen. Die Tatsache jedoch, dass die meisten Netzwerke heutzutage mit dem Internet (das wiederum öffentlich zugänglich ist) verbunden sind, macht diese Verlockung nicht nur unpraktikabel, sondern birgt auch Gefahren! Vielmehr müssen wir unser System um jene Computer bauen, deren Funktionalitäten am anfälligsten für den Informationsverlust des zu untersuchenden Systems sind.

#### *Fragen zur Erkennung der wichtigsten Systemkomponente*

Beantworten Sie die folgenden Fragen, um herauszufinden welche Computer die wichtigsten Komponenten des zu untersuchenden Systems sind:

- Wie heißt die die zu untersuchende Anwendung?
- Welches Betriebssystem haben sie?
- Handelt es sich um eine Benutzeranwendung oder um eine Infrastruktur?
- Erfüllt das System den Mindestsicherheitsstandard des betreffenden Unternehmens? Ist es beispielsweise untersucht worden und entspricht den unternehmenseigenen Sicherheitspraktiken?
- Wessen Tätigkeit hängt primär von diesem System ab?
- Arbeitet das System mit Prozesssteuerung?
- Arbeitet das System mit Finanzdaten?
- Arbeitet das System mit Informationen das Personal betreffend?

[27] Wir verwenden generell den Ausdruck „System“, es sein denn er ist in einem bestimmten Zusammenhang missverständlich. Es ist jedoch wichtig, dass Sie mit dem Begriff vertraut sind, da er häufig von Risikoanalysten verwendet wird.

- Kommen Kundendaten im System vor? Wenn ja, was für Daten?
- Arbeitet das System mit personenbezogenen Daten?
- Welche Abteilungen genau verwenden das System?
- Wer, außerhalb des Betriebs, verwendet das System? (z.B. Geschäftspartner, teilweise oder vollständig unterstellte Tochtergesellschaften)

Der Systemzugang erfolgt :

- Über das unternehmenseigene Netzwerk?
- Durch eine Einwahlverbindung?
- Durch eine virtuelle, private Netzwerkverbindung (VPN)?

Wie verläuft die Passworterkennung (Authentifizierung)?

- Durch ein Internetportal?
- Durch Verbindungen über eine Standleitung (WAN)?

## Fragen zur Erkennung von unterstützenden und abhängigen Komponenten

Die zentralen Server verlangen normalerweise einen Netzwerkzugang, um angemessen arbeiten zu können. Dabei haben sie Zugang zu den Nameservern, den Fileservern, dem Server zur Authentifizierung und auch den Zeitservern. Die Administartoren verfügen in der Regel über die dafür notwendigen Information. Folgenden Fragen können dabei helfen unterstützende und abhängigen Komponenten zu erkennen.

- Welche internen Computer tauschen Daten mit dem zu prüfenden System aus?
- Welche externen Systeme tauschen Informationen mit dem zu untersuchenden System aus?
- Werden von dem System Informationen mit Rechnern ausgetauscht, die vom Internet aus zugänglich sind?
- Werden Informationen ausgetauscht, die über Kommunikationswege übertragen werden, die nicht Teil des betriebseigenen Netzwerkes (LAN) sind?
    - Welches System überträgt Daten auf das zu untersuchende System? (Vergessen Sie nicht Fileserver in die Liste mit aufzunehmen)
    - Was passiert mit diesen Informationen wenn das zu prüfende System keine Daten aufnehmen kann?
    - Wird dies das System des Senders beeinträchtigen?
    - Auf welche Datenbänke hat das zu prüfende System Zugriff?
    - Wer ist zuständig für die Wartung und Administration des zu prüfenden Systems? Versichern Sie sich, dass Sie alle Aspekte berücksichtigen: Hardware, OS, Programme, Daten.

Um zu bestimmen welche unterstützenden Komponenten in die Untersuchungen miteinbezogen werden sollen, wird ein großes Maß an Urteilsvermögen seitens des Analysten verlangt. Wenn Sie zu viele irrelevante Komponenten in der Analyse berücksichtigt werden, wird die Aufgabe möglicherweise unlösbar. Werden aber unterstützende Komponenten, die den

zentralen Server am laufen halten vergessen, werden der Analyse aber wichtige Schwachstellen des Systems entgehen. Daher ist es meistens besser ein paar der irrelevanten Konponenten zu viel in die Analyse mit einzubeziehen.

Wir sind an denjenigen Komponenten interessiert, die das zu prüfende System unterstützen, da sie potentielle Schwachstellen verdeutlichen (Angriffspunkte). Daher können wir keine Systeme ignorieren, die von Informationen oder Diensten vom zu prüfenden System abhängen. Jede Auswirkungen eines Versagens des zu prüfenden Systems auf abhängige Systeme muss bei der Analyse berücksichtigt werden.

### *Systeme ohne direkten Bezug*

Macht es überhaupt Sinn die Rolle von nicht-abhängigen Systemen in der Risikoanalyse zu betrachten? Normalerweise lautet die Antwort NEIN. Der Analyst muss jedoch die Erwartungen derjenigen verstehen, die sie mit der Risikoanalyse beauftragt haben. Die typische Erwartungshaltung ist „die Risiken aufzuspüren, die ein Versagen des zu prüfenden Systems zur Folge haben“. Für die meisten Menschen bedeutet das „was kann passieren, dass die Authentizität, die Verfügbarkeit oder Integrität der Information des untersuchten Systems beeinträchtigt? Und welche Auswirkungen hat das auf mein Unternehmen?“ Um diese Frage zu beantworten müssen wir lediglich die wichtigsten unterstützenden und abhängigen Komponenten in die Untersuchungen miteinbeziehen.

Es wird vom Analysten auch erwartet, dass er Situationen erkennt, in denen ein erfolgreicher Angriff gegen das zu prüfende System den Angreifer in eine Position bringen kann, andere, „unabhängige“ Systeme zu schädigen. Systeme, die vom unternehmerischen Standpunkt aus „unabhängig“ erscheinen, sind vielleicht vom Gesichtspunkt des Angreifers aus alles andere als „unabhängig“.

Der Analyst sollte klar und deutlich auf die möglichen Risiken aufmerksam machen. Wenn das Management erwartet, dass Angriffe, die das zu prüfende System als Sprungbrett nutzen, Teil des Auftrags sind, wird das den Umfang der Analyse deutlich erweitern. Es ist durchaus denkbar, dass alle Systeme des Unternehmens dabei berücksichtigt werden! Das wiederum würde dazu führen, dass ein Attack Tree für jedes System des Netzwerks erstellt werden muss. Diese Attack Trees würden sich auf das Aufspüren von Gefahren konzentrieren, was eine unglaubliche Menge an Arbeit bedeuten würde. Diese Art von Risikoanalyse würde in einen ständigen Prozess übergehen, der keinen Abschluss fände und damit unbrauchbar werden würde.

Ein möglicher Ausweg aus diesem Dilemma wäre, dass die Folgen eines Angriffs auf das zu prüfende System vermieden werden könnten, wenn das System sicher ist. Wenn dies nicht möglich oder finanzierbar ist, würde ein Intrusion-Detection-System es den Administratoren zumindest ermöglichen ein Eindringen in das System festzustellen bevor es als Sprungbrett genutzt werden kann.

### *Identifizierung der Mensch - System Beziehungen*

Jede Personengruppe, die das System[29] direkt verwendet, sollte in der Risikoanalyse-Diskussion berücksichtigt werden. Falls das System gar indirekt mit Finanzen, Personal oder anderen Bereichen in denen wichtige Entscheidungen getroffen werden arbeitet, sollten diese unbedingt miteinbezogen werden. Die Interessen derjenigen Gruppen, die das System nur indirekt nutzen, sollten von solchen Gruppen vertreten werden, die mit der Infrastruktur und dem Computersystem vertraut sind.

Die meisten Unternehmen befürchten ganz besonders einen Vorfall der Kunden betrifft. Es ist jedoch nicht immer möglich, die Kunden direkt zu integrieren, auch wenn ihre Bedürfnisse und Meinungen möglichst berücksichtigt werden sollten. Der Analyst sollte deren Anforderungen in seine Untersuchung mit einbeziehen.

### *Identifizierung von systemabhängigen Unternehmensprozessen*

Schlüsselentscheidungsprozesse hängen möglicherweise vom System ab. Manager und andere Führungskräfte machen ihre Entscheidungen von den, ihnen zur Verfügung stehenden, Informationen abhängig. Diese Führungsebene verwendet oft nicht direkt das Computersystem. Sie verlassen sich eher auf Berichte, die aus zuvor eingeholten Systeminformationen bestehen. Das Erkennen von allen Menschen, die Teil dieses Informationsflusses sind kann manchmal schwierig sein. Trotzdem ist es essentiell wichtig auch für diese Gruppe die Auswirkungen eines kompletten oder teilweisen Systemausfalls zu erkennen. Die folgenden Fragen sollen uns dabei helfen.

- Welche Entscheidungsprozesse würden leiden, wenn das zu prüfende System nicht zugänglich wäre oder die von ihm produzierten Informationen ungenau sind?
- Wer wäre an seiner Arbeit gehindert, wenn aufgrund eines Systemfehlers keine Informationen fließen könnten?
- Welche Alternativen können aufgrund eines Systemfehlers möglicherweise nicht wahrgenommen werden? Inwieweit können mögliche Alternativen durch einen Systemfehler beeinträchtigt werden?
- Wie lange könnten Sie ohne dieses System überleben und welche Bereiche wären bei einem längeren Ausfall nicht mehr arbeitsfähig?

## Kommunizieren Sie mit Interessensvertretern

Zu diesem Punkt der Untersuchung wurden bereits einige Interessensvertreter herausgearbeitet, die in den Risikoanalyseprozess mit einbezogen werden sollten. Treten Sie mit jeder dieser Gruppen in Kontakt. Erklären Sie, dass eine Risikoanalyse für ein, von Ihnen verwendetes, Systems erstellt wird. Erklären Sie wie wichtig es ist, Ihre Perspektive zu kennen und laden Sie sie ein sich zu beteiligen. Falls die Abteilung die Einladung abschlägt, muss Stellvertretend die IT-Abteilung die Verantwortung für diese Abteilung übernehmen. Die IT-Abteilung gewährleistet damit, dass die Interessen aller Abteilungen berücksichtigt werden. Der

[29] Manchmal ist das zu analysierende System Teil einer Infrastruktur. In dem Fall hat dies wahrscheinlich Auswirkungen auf eine Menge anderer Systeme (und Abteilungen). Es ist möglicherweise nicht praktikabel alle in Frage kommenden Gruppen in die Analyse mit einzubeziehen, weshalb wir vorschlagen ein repräsentatives Beispiel zu wählen.

Analyst sollte dafür eine Tabelle für das zu prüfende System anlegen. Ein Beispiel ist die unten aufgeführte Tabelle für ein hypothetisches Bestandssystem:

| *Teilnehmer bei der Risikobewertung* | | |
|---|---|---|
| **Geschäftseinheit** | **Beziehung zum System** | **Beauftragter** |
| IT-Service Abteilung | Support für die Hardware und das Betriebssystem | Selber vertreten |
| Datenbank Support | Support für die Firmendatenbank | Selber vertreten |
| Produktionsabteilung | Direkte Nutzung der Anwendung | Selber vertreten |
| Stategische Marktplanung | Indirekte Nutzung der Anwendung | IT-Abteilung |
| Marketing Vorstand | Trifft Entscheidungen basierend auf täglichen Informationen aus dem System | IT-Abteilung /Revision |

## Deren Traum, Ihr Alptraum – Identifizierung der Angriffsziele

Ein elementarer Schritt in der Attack Tree Analyse ist das Identifizieren des obersten Ziels, des „Root Goals“. Es repräsentiert, was ein Angreifer erreichen möchte (das, was die Verteidigung des Systems verhindern möchte). In der Regel ist es möglich ein oberstes Ziel auszumachen, das für eine große Zahl von Angreifern und Situationen Sinn macht .

Die Sicherheit in der Informationstechnologie setzt auf Diskretion, Verfügbarkeit und vertrauliche Behandlung von Informationen[31]. Wenn der Angreifer mehr oder weniger die selbe Anstrengung unternehmen wird, um jede dieser Prinzipien zu gefährden, wird ein einzelnes „Root Goal“ wahrscheinlich genügen. Wenn die Angriffe oder die Auswirkung aber deutlich variieren, wird es notwendig sein verschiedene Ziele zu definieren, und zwar für jede einzelnen Sicherheitsaspekt.

## Erstellen von Attack Tree Modellen

Verwenden wir die gesammelten Informationen und die obersten Ziele, die wir ausfindig gemacht haben, sind wir in der Lage ein Attack Tree Modell zu erstellen. In das Modell sollten sowohl die verhaltensbedingten- als auch die Effektindikatoren einfließen und diese sollten mit den Informationen aus den vorhergegangenen Phasen vervollständigt werden. Vergessen Sie

[30] Vorschriften den Datenschutz betreffend machen es notwendig gewisse persönliche Informationen zu verschlüsseln, egal ob sie anderweitig geschützt sind oder nicht.

nicht diese Schritte ausführlich zu dokumentieren, da das Modell letzten Endes einer sorgfältig vorbereiteten Abwehr dienen könnte.

### Wiederverwendung von Wissen

Die meisten kommerziellen Informationssysteme basieren auf einer kleinen Reihe von so genannten Kernanwendungen. Es werden meist nur eine begrenzte Anzahl von Betriebssystemen und Datenbanken verwendet. Sind diese Komponenten erst einmal untersucht und in ein Attack Tree Modell überführt worden, können diese Informationen in einer Art Bibliothek aufbewahrt und immer wieder verwendet werden.

Amenaza Technologies bietet ein Set von Attack Tree Bibliotheken für häufig verwendete Komponenten bei der Informationstechnologie. Unternehmen können auch eigene Bibliotheken anlegen, die speziell auf sie ausgerichtet sind. Unabhängig davon, auf welche Anwendung sich diese Bibliotheken beziehen, ist es notwendig, importierte Bibliotheken auf ihre Verwendbarkeit zu prüfen und sie, falls nötig, anzupassen. Denn nicht jeder wendet dieselben Komponenten auf dieselbe Art und Weise an.

Beim Anlegen einer Bibliothek sollte der Analyst sich auf den Aufbau und die Struktur des Produkts konzentrieren. Er sollte eine oder mehrere der zahlreichen Datenbanken, die auf die Schwachstellen hinweisen verwenden, um eine Liste der Schwachstellen und bekannten Angriffspunkte anlegen zu können. Diese Liste der Schwächen wird strukturelle Defizite im System sichtbar machen. Ein Beispiel spezifischer Schwachstellen sollte ebenfalls in die Bibliothek eingefügt werden, obgleich es normalerweise unnötig ist jeden einzelnen bereits bekannten Fehler zu finden.

## Schritt Zwei: Erkennen von ausnutzbaren Schwachstellen

Das Attack Tree Modell zeigt alle Angriffe auf, die von einem unendlich reichen, mächtigen, mutigen und intelligenten Feind ausgeführt werden könnten. Diese Reihe sollte reduziert werden auf diejenigen Angriffe, die für einen relevanten Feind wahrscheinlich sind.

### Auswahl und Definition von Bedrohungsagenten

Alles und Alle die das System schädigen wollen sind Bedrohungsagenten. Es mag hilfreich sein die Bedrohungsagenten in zwei Kategorien zu unterteilen: absichtlich und unabsichtlich. Absichtliche Bedrohungsagenten sind zum Beispiel Hacker, böswillige Angestellte und spezielle Interessensgruppen (Konkurrenten, etc.). Sie greifen das System mit Viren, Trojanischen Pferden, nicht autorisiertem Zugang und dem Verweigern von Befehlen an.

Der erste unabsichtliche Bedrohungsagent ist die Natur. Sie kann uns mit Umweltkatastrophen wie zum Beispiel Überschwemmungen, Bränden, Erdbeben oder Wirbelstürmen Schaden zufügen. Darüber hinaus zählen wir noch ungeplante menschliche Irrtümer zu der Kategorie von unabsichtlichen Bedrohungen. Wenn wir dem Bedrohungsagenten der für dumme Fehler verantwortlich ist einen Namen geben wollen, so können wir ihn „Murphy“ oder „Murphys Law[31]“ nennen.

[31] Wenn etwas schief gehen kann, kann man sich darauf verlassen, dass es schief gehen wird.

Vor einiger Zeit gab es einen Vorfall, wo versehentlich die Netzwerkverbindungen eines großen Kommunikationsservers vertauscht wurden. Ohne zu sehr ins Detail zu gehen, war die Folge doch, dass einige Netzwerkswitches nicht mehr reagierten. Es war schwierig das Problem einzugrenzen und die Kommunikation über das Netzwerk wurde dadurch in die Knie gezwungen. Das System war tagelang funktionsunfähig. Obwohl der Fehler ein Unfall war, war er nicht weniger schädlich als ein absichtlicher Angriff.

In vielen Fällen kann ein Unternehmen das Potential von Naturkatastrophen relativ gut einschätzen. Es werden schon zufriedenstellende Maßnahmen getroffen, um diese Risiken zu mindern. In diesem Fall, kann der Analyst festhalten, dass die Analyse lediglich absichtliche Angriffe untersuchen wird. Diese Entscheidung verlangt aber die Unterstützung durch andere TeilnehmerInnen der Risikoanalyse, als auch die Rückendeckung von dem/derjenigen, der sie in Auftrag gegeben hat.

Falls dies nicht der Fall sein sollte werden sowohl umweltbedingte, als auch absichtliche Bedrohungen in die Untersuchung mit aufgenommen. Treten diese zwei Arten der Bedrohungen nicht unabhängig voneinander auf, ist es wahrscheinlich am besten zwei getrennte Attack Trees zu erstellen. Der Baum, der absichtliche Bedrohungen darstellt, benutzt Indikatoren, welche die für einen Angriff notwendigen Ressourcen zeigen. Der zufällige oder umweltabhängige Baum basiert auf Statistiken.

Sind die zwei Bedrohungen unabhängig voneinander, oder ist ein Bedrohungstyp deutlich dominant, sollte möglichst ein einziger Baum erstellt werden. Das erfordert möglicherweise ein paar Tricks, die wir zuvor beim Analysieren von gemischten Bedrohungen gezeigt haben.

Manchmal gibt es Probleme den Unterschied zwischen Bedrohungsagenten und Bedrohungen zu verstehen. Anhand einiger Beispiele möchten wir das Konzept hier noch einmal verdeutlichen.

| ***Bedrohungsagenten und Angriffe*** | | |
|---|---|---|
| **Bedrohungsagent** | **Typ** | **Bedrohungsbeispiel** |
| Hacker | vorsätzlich | Malware – Viren, Würmer, Trojanische Pferde |
| Angestellter | vorsätzlich | Informationen zu eigenem Gunsten abändern |
| Wettbewerber | vorsätzlich | Informationsdiebstahl zur Verbesserung der eigenen Marktposition |
| Natur | unbeabsichtigt | Flut, Feuer, Tornado... |
| Murphy | unbeabsichtigt | Das Stromkabel ziehen, Tippfehler |

Der beste Weg um sich auf einen Bedrohungsagenten zu einigen, ist ein Brainstorming mit allen TeilnehmerInnen der Risikoanalyse. Das ist praktikabel wenn die Zahl der TeilnehmerInnen gering ist, bei größeren Gruppen aber nur schwer durchzuführen. Wenn

letzteres der Fall ist, sollte der Risikoanalyst jeden einzelnen Teilnehmer interviewen, um deren Meinung bezüglich der zu berücksichtigenden Bedrohungsagenten einzuholen.

Stellen Sie die folgenden Fragen, um mögliche Bedrohungsagenten zu ermitteln:

- Was sind Ihre schlimmsten Albträume über mögliche Gründe warum dieses System zusammenbrechen könnte?
- Was ist das Ungewöhnlichste oder Bizarrste was Ihrer Meinung nach mit dem System passieren könnte?
- Wer würde sich darüber freuen, wenn Sie keinen Zugang zu Ihrem System hätten oder nicht auf die Informationen des Systems zurückgreifen könnten?

Wenn Sie nicht sicher sind, ob Sie einen Bedrohungsagenten berücksichtigen sollen oder nicht, ist es im Normalfall immer besser diesen zu berücksichtigen.

Erstellen Sie eine Tabelle, in die Sie die verschiedenen bekannten Bedrohungsagenten eintragen. Die Tabelle sollte die geschätzten Ressourcen der Bedrohungsagenten für jeden Indikator im Attack Tree erfassen. Versichern Sie sich der Gründe für die Wahl der eingetragenen Werte.

| ***Ressourcen der Bedrohungsagenten*** | | | |
|---|---|---|---|
| **Bedrohungsagent** | **Verfügbare finanzielle Mittel** | **Technische Fähigkeit (1 – 100)** | **Toleranz entdeckt zu werden** |
| Hacker | 50 € | 35 | 50% |
| Angestellter | 50 € | 25 | 5% |
| Wettbewerber | 10.000 € | 75 | 2% |

## Ausschalten von Angriffen über die Möglichkeiten der Bedrohungsagenten

Vergleichen Sie die Ressourcen eines jeden Bedrohungsagenten, die benötigt werden um jede Schwachstelle im Attack Tree Modell auszunutzen. Wenn die Möglichkeiten des Bedrohungsagenten dem Angriff nicht gewachsen sind, schneiden Sie es aus dem Attack Tree. Die Schwachstellen, die noch übrig bleiben, sind die, die wahrscheinlich sind (für jede Art Bedrohungsagent).

### *Vertrauenseinschätzung*

Was die Wahrscheinlichkeit von Angriffen betrifft, können verschiedene Techniken verwendet werden, um die Verlässlichkeit einer Voraussage einzuschätzen. Die Erste ist als *Anfälligkeitsanalyse* bekannt. Um eine Anfälligkeitsanalyse durchzuführen, müssen die Möglichkeiten die jedem Bedrohungsagenten zugeordnet sind ein wenig erweitert werden und der Attack Tree noch einmal „geschnitten“ werden. Kommt es durch diese

Anpassungsmaßnahmen zu keinen neuen Resultaten (oder nur geringfügigen Veränderungen), kann man guten Gewissens behaupten, dass die Voraussage über den Bedrohungsagenten bei diesem Indikator nicht anfällig für Fehler ist.

Eine weitere Hilfe ist das Erstellen einer Liste mit allen Knoten, die „geschnitten“ worden sind (aufgrund eines vorhandenen Bedrohungsagenten). Die Liste sollte genau ersichtlich machen, welche Einschränkungen bezüglich der Ressourcen dazu geführt haben, dass der Knoten entfernt wurde. Knoten, die bei zahlreichen Indikatoren „geschnitten“ wurden sind für den ausgewählten Bedrohungsagenten kaum angreifbar.

## Schritt Drei: Erstellen einer Risiko-Prioritäten-Liste von Angriffsszenarien

Indem wir wissen welche Angriffe von jedem Bedrohungsagenten durchgeführt werden, haben wir nur die halbe Schlacht gewonnen. Um das Risiko, das mit einem Angriff assoziiert wird zu verstehen, ist es wichtig dessen Auswirkung zu kennen.

### Erstellen von Angriffsszenarien für jeden Bedrohungsagenten

Erstelle eine Reihe von Angriffsszenarien für alle in Betracht kommenden Bedrohungsagenten. Somit werden alle möglichen Wege abgedeckt, die ein Bedrohungsagent nehmen könnte um das System anzugreifen.

### Priorisieren von Angriffsszenarien nach Auswirkung

Das Attack Tree Modell sollte ein oder mehrere Indikatoren beinhalten, die den Schaden oder Verlust anzeigen, die ein Opfer bei einem Vorfall erleiden wird. Sortieren Sie die Angriffsszenarien je nach Auswirkungsgrad. Das sollte einmal für jeden Auswirkungsindikator des Modells vorgenommen werden. Das Ergebnis sind Listen für das Opfer, auf denen das Risiko aufgezeigt wird, einen bestimmten Schaden durch einen spezifischen Bedrohungsagenten zu erleiden.

## Schritt Vier: Erkennen von effektiven Eingrenzungsstrategien

In gewissen (seltenen) Fällen verdeutlicht die Risikoanalyse, dass die Risiken die mit einem System assoziiert werden allesamt akzeptabel für das Unternehmen sind. Generell aber wird der Analyst ersucht eine Empfehlung abzugeben, die sich auf außergewöhnliche hohe Risiken bezieht. Dabei kann entweder versucht werden das bestehende Risiko über eine Versicherung abzudecken oder, und das ist viel häufiger der Fall, es wird versucht werden Veränderungen am System vorzunehmen, um die Wahrscheinlichkeit eines Angriffs zu minimieren. Die Attack Tree Analyse ist ideal um vorhandene und neue Lösungen für Sicherheitsprobleme genauestens zu untersuchen. Lösungen können sowohl eine Änderung von Taktiken, als auch von Arbeitsvorgängen oder bestimmten Techniken sein.

Die genaue Untersuchung von Angriffsszenarien führt oft zu einem besseren Verständnis über Mängel in der Sicherheitsstruktur. Der Analyst kann sich eine Vielzahl von Lösungen vorstellen und das Attack Tree Modell jeweils den Veränderungen anpassen. Das heißt, dass

 

der Analyst wieder bei Schritt Eins (Schritt Eins - Integrieren des Informationssystems in einen Attack Tree) beginnt und dann Schritt Zwei und Drei wie zuvor durchläuft. Lösungen die „funktionieren“ führen zum Ausscheiden von Angriffsszenarien. Indem wir die Folgekosten eines Angriffsszenarios mit den Realisierungskosten einer vorgeschlagenen Lösung vergleichen, können wir rentable und effektive Lösungen herausfinden. Indem wir die Kosten und Effizienz einer Vielzahl von vorgeschlagenen Lösungen vergleichen, können wir die beste Lösung herausfinden.

Einen ähnlichen, iterativen Prozess sollten wir immer dann anwenden, wenn wir Veränderungen an einem System vornehmen. Das ermöglicht der Risikoanalyse vorausschauend statt rückwirkend zu agieren.

### Zukunftswege

Die vier Stufen die wir in dieser Methodologie vorgestellt haben, sind erprobt und zuverlässig. Sie führen zu außergewöhnlich guten Ergebnissen, auf schnellem und verteidigungsfähigem Weg. Da die Entwicklungen am Modell stetig weitergehen, können möglicherweise bald weitere Schritte hinzugefügt werden, die zu noch mehr Vorteilen der Attack Tree Analyse führen.

Eine verlockende Idee ist die Integration des Attack Tree Models in Angriffserkennungssysteme (IDS). Gegenwärtige IDS basieren auf dem Abgleich von Strukturen mit einer „Signatur-“ oder „Pattern-“ Liste. Irgendwann in der Zukunft, ist es vielleicht möglich Attack Tree Modelle für Vergleichszwecke und als Erkennungssystem zu verwenden.

## Schlussfolgerung

Dieses Dokument hat die grundlegenden Konzepte einer Möglichkeiten-orientierten Attack Tree Analyse dargestellt. Darüber hinaus wurde ein Beispiel für eine Methodologie aufgezeigt, das für ein Informationstechnologie-System geeignet ist. Hoffentlich werden auch Menschen aus anderen Bereichen von diesem Beispiel inspiriert und erstellen in ihrem eigenen Umfeld angemessene Methodologien.

Der beste Weg um über Attack Tree Analysen etwas zu lernen, ist das hier vorgestellte Konzept zu nehmen und einige der Probleme die Sie betreffen zu lösen. Amenaza Technologies Limited gilt in diesem Bereich als weltweit führend. Wir würden Ihnen gerne helfen, indem wir Training, Software-Tools oder Kundenberatung anbieten. Ebenso freuen würden wir uns, wenn Sie uns Ihre Erfahrungen mit dem Attack Tree Modell mitteilen wollen.

Amenaza
Technologies Limited