Softwaregestützte Bedrohungsanalyse durch Angriffsgraphen

Software-supported threat analysis using attack graphs

Markus Heinrich | Lukas Iffländer

Zur Bestimmung von Bedarfen im Cybersecurity-Kontext ist eine Bewertung der Bedrohungen unter anderem nach Auswirkung und Eintrittswahrscheinlichkeit notwendig. Bisherige Softwarewerkzeuge sind nicht in der Lage, die Komplexität im Eisenbahnsektor ausreichend abzubilden. Die Methodik der Angriffsgraphen und ein quelloffenes Softwarewerkzeug unterstützen die Risikoanalyse der IT- und OT-Sicherheit durch Darstellung der Bedrohungen und ihrer Wirkung auf das Asset. Die vorgenommene Bewertung in einem Attributvektor wird durch das Werkzeug zu einem Gesamtrisiko aggregiert. Die Aggregation erfolgt unter Berücksichtigung der bereits etablierten Gegenmaßnahmen und ihrer risikomindernden Wirkung.

1 Einleitung

Die IT- und OT-Sicherheit (=Security) erfordert eine ganzheitliche und regelmäßige Risikobewertung. Ein eigenständiges Produkt, das den Schutz vor Cyberangriffen sicherstellt, existiert genauso wenig wie eine einmalig zu integrierende Lösung. Stattdessen muss der Betrachtungsgegenstand (Asset) regelmäßig einer Risikoanalyse unterzogen werden, die die sich ständig verändernde Bedrohungslage berücksichtigt. Die einschlägigen Methoden gehen im Kern auf die bekannte Gleichung:
Risiko = Eintrittswahrscheinlichkeit x Schadensausmaß
zurück. Während man in der funktionalen Sicherheit (Safety) von Gefährdungen spricht, wird in der IT-/OT-Sicherheit das Risiko einer Bedrohung betrachtet. Insbesondere die Eintrittswahrscheinlichkeit einer Bedrohung kann dabei häufig nicht durch einen Dezimalbruch angegeben werden, sondern wird auf andere, semi-quantitative Art bewertet (bspw. niedrig, mittel, hoch). Der Eintritt eines IT/OT-Sicherheitsereignisses (ein Angriff) folgt keinem stochastischen Prozess, der sich durch eine Wahrscheinlichkeit beschreiben lässt. Die TS 50701 bspw. modelliert die Wahrscheinlichkeit (als Likelihood) über die Attribute Exposition und Verwundbarkeit des betrachteten Systems, die in Stufen von 1 bis 3 bewertet werden. Die DIN VDE V 0831-104 folgt dem Ansatz der IEC 62443 und fordert die Bewertung jeder Bedrohung durch das Wissen, die Ressourcen und die Motivation des Angreifers, was als indirekte semi-quantitative Modellierung der Eintrittswahrscheinlichkeit interpretiert werden kann.
Allen Risikoanalysemethoden ist gemein, dass sie eine Vielzahl von Bedrohungen auf das Asset berücksichtigen müssen, aus der eine umfangreiche Dokumentation resultiert, um die Einschätzung des Risikos aus jeder Bedrohung nachvollziehbar zu machen. Darüber hinaus kann ein hundertprozentiger Schutz vor Angriffen nicht existieren, weil sich die Bedrohungslage stetig ändert und Gegen-

Threat assessments, including assessments of their impact and probability of occurrence, are necessary in order to determine the requirements within the cybersecurity context. Previous software tools have not been able to adequately depict the complexity of the railway sector. The attack graph methodology supported by an open-source software tool supports IT and OT security risk analysis by displaying the threats and their effects on the asset. The tool aggregates the assessment made in an attribute vector in order to form an overall risk that takes into consideration any established countermeasures and their risk-reducing effect.

1 Introduction

IT and OT security require a holistic and regular risk assessment. There is no such thing as a stand-alone "fire-and-forget" product that ensures protection against cyber-attacks. Instead, a holistic security approach requires a regular risk analysis that considers the constantly changing threat situation for the protected asset.
The relevant methods are based on the well-known equation:
risk = probability_of_occurence · extent_of_damage
While functional safety deals with hazards, IT and OT security considers the risk of threats. A threat occurrence probability cannot be determined to within a decimal fraction in contrast to safety hazards. Instead security models use different semi-quantitative methods (e.g., low, medium, high). The occurrence of IT and OT security events (attacks) does not follow a stochastic process that can be described using a probability. The TS 50701, for example, models the probability as a likelihood according to the attributes of the exposure and vulnerability of the system under consideration using levels from 1 to 3. DIN VDE V 0831-104 follows the approach of IEC 62443 requiring the assessment of each threat based on the knowledge, resources and motivation of the attacker, interpreted as indirect semi-quantitative occurrence probability modelling.
All risk analysis approaches face the challenge of considering a multitude of threats to the asset. This results in extensive documentation to comprehensibly assess the risk from each threat. In addition, complete protection against attacks cannot exist, because the threat situation is constantly changing and countermeasures must be drawn from limited financial and human resources. Therefore, the task of any risk analysis and its documentation is to determine which risks to mitigate against and which risks to accept. Risk analysis thus provides

maßnahmen aus beschränkten finanziellen und personellen Ressourcen geschöpft werden müssen. Daher ist die Aufgabe der Risikoanalyse und ihrer Dokumentation zu bestimmen, welche Risiken zu mitigieren und welche Risiken zu akzeptieren sind. Damit liefert die Risikoanalyse eine priorisierte Liste von Maßnahmen zur Risikominderung. Gleichzeitig müssen bereits existierende Gegenmaßnahmen abgebildet werden, um eine valide Einschätzung des Risikos zu erhalten.

2 Angriffsgraphen

Zur Unterstützung der Risikoanalyse wird im Forschungsprojekt „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“ [1] die Methodik der Angriffsgraphen entwickelt und mithilfe eines Softwarewerkzeuges abgebildet, das die Analyse automatisiert. Durch das Tool werden der Arbeitsaufwand und die Fehleranfälligkeit des Prozesses reduziert sowie die Nachvollziehbarkeit und Aussagekraft erhöht. Eine Analyse bisher existierender Softwarewerkzeuge hat gezeigt, dass es keine Software gibt, die die Anforderungen der Angriffsgraphen komplett abbildet. Es wurden sowohl Software aus der IT-Sicherheitsforschung als auch kommerziell oder frei verfügbare Produkte betrachtet. Daher wurde entschieden, eine Software gemäß den Anforderungen zu entwickeln und quelloffen zur Verfügung zu stellen.

Die Angriffsgraphen basieren auf den Angriffsbäumen (Attack Trees). Attack Trees sind eine Methode, die in der Informationssicherheit verwendet wird, um Bedrohungen zu analysieren und Bedingungen darzustellen, die gelten müssen, um aus einer Bedrohung einen erfolgreichen Angriff durchzuführen. Es hat sich jedoch gezeigt, dass es von Vorteil ist, auf einige Eigenschaften von Bäumen aus der Graphentheorie zu verzichten. Zum einen erfordern Angriffsgraphen nicht, dass alle Knoten zusammenhängend sind, sodass voneinander unabhängige Angriffspfade auf ein Asset modelliert werden können. Zum anderen erlaubt der Verzicht auf die Anforderung, dass zwischen zwei Knoten nur genau ein Pfad existieren darf, die Wiederverwendung von Teilschritten eines Angriffes und ihrer Bewertung, die in unterschiedlicher Verkettung auch zu unterschiedlichen Konsequenzen führen können.

Ein Angriffsgraph analysiert genau einen Betrachtungsgegenstand (Asset) auf hinreichend spezifischem Abstraktionsniveau. Ein durch einen Angriffsgraphen analysierter Betrachtungsgegenstand könnte z. B. die intelligente Instandhaltung einer Weiche sein. Bei der intelligenten Instandhaltung (Predictive Maintenance) wird durch Überwachung der Betriebsparameter und maschinelles Lernen vorhergesagt, wann mit einem Versagen zu rechnen ist, um rechtzeitig vorher eine Instandhaltung durchzuführen. Die exakte Definition des Assets ist nicht Teil der Angriffsgraphen-Methodik. Das Asset wird im Graphen durch ein Trapez dargestellt (Bild 1).

Durch Angriffe auf das Asset entstehen unterschiedliche Angriffsfolgen („Consequence“) oder Schadensereignisse, die im Graphen durch Rechtecke mit abgerundeten Ecken dargestellt werden. Zur Bestimmung der Folgen kommen durch Unternehmen vordefinierte Kataloge von schädlichen Ereignissen, wie z. B. Personenschaden, Reputationsschaden, finanzieller Schaden oder Einschränkung des operativen Geschäfts, infrage. Genauso erlaubt die Methodik auch die Definition von Folgen durch die Analystin oder den Analysten, falls kein Katalog angewendet werden soll oder eine Erweiterung eines angewendeten Kataloges erfolgen soll.

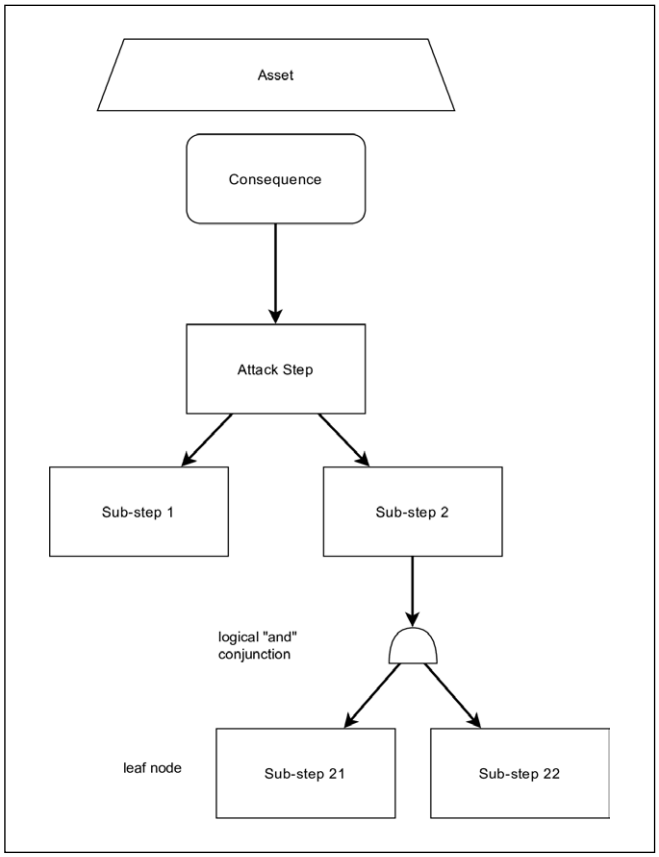

Bild 1: Beispiel eines Angriffsgraphen für ein Asset
Fig. 1: An example of an attack graph for an asset

a prioritised list of risk reduction measures. At the same time, the risk analysis must map out the existing countermeasures in order to obtain a valid assessment.

2 Attack graphs

We developed the attack graph methodology and a software tool to automatically analyse them as part of the “Security Requirements Forecast and Evaluation of Possible Security Concepts” research project [1] in order to support risk analysis. The tool reduces the amount of work and the susceptibility to errors and increases traceability and meaningfulness. A study of existing software tools has shown that no software fully maps out the requirements of the attack graph. Both software from IT security research and commercially or freely available products were considered. Therefore, we decided to develop software according to the requirements and to make it available as open source.

Attack graphs are based on attack trees. Attack trees are a method used in information security to analyse threats and present conditions that must apply in order to turn a threat into a successful attack. However, experience has shown that it is advantageous to omit some of the tree properties from graph theory. Firstly, attack graphs do not require all the nodes to be connected, so independent attack paths on an asset can also be modelled. On the other hand, waiving the requirement that only one path may exist between two nodes allows the reuse of the sub-steps in an attack and their evaluation, which can also lead to different consequences in different concatenations.

3 Bedrohungskataloge und Threat Mining

Jede Angriffsfolge kann durch einen oder mehrere Angriffe ausgelöst werden („Attack Step" in Bild 1). Diese Beziehung wird im Graphen durch eine gerichtete Kante von der Folge zum Angriffsschritt dargestellt. Durch diese Verknüpfung erhöhen die Angriffsgraphen die Nachvollziehbarkeit der Risikoanalyse, da sie die mögliche n:m-Beziehung zwischen Angriff und Schaden graphisch darstellen können.

Zur Identifikation der Angriffe können existierende Bedrohungskataloge (bspw. die Elementaren Gefährdungen des BSI [2]) und Methoden des Threat Modellings (bspw. STRIDE [3]) herangezogen werden. Das sog. Threat Modelling ist ein Prozess, um strukturiert IT-Sicherheit bezogene Schwachstellen auf ein System zu identifizieren und so seine Angriffsfläche zu bestimmen. Als Angriff ist hier die Realisierung oder Ausführung einer Bedrohung zu verstehen. Im Beispiel der intelligenten Instandhaltung ist ein Angriff die Manipulation der Vorhersage durch den Angreifer und daraus resultierendes Materialversagen ohne rechtzeitige Vorhersage. Die Folge des Angriffes könnte finanzieller Schaden durch Entgleisen eines Zuges wegen der defekten Weiche sein. Die Verwendung von Katalogen und Threat Mining stellt die hinreichende Vollständigkeit der Bedrohungsanalyse sicher. Angriffsgraphen unterstützen die Analyse durch die grafische Aufbereitung und die Zerlegung der Angriffe in Teilschritte (Sub-step 1 und Sub-step 2) zur Verfeinerung der Analyse und der folgenden Risikobewertung. Teilschritte setzen sich immer durch logische Disjunktion („oder") und Konjunktion („und") zusammen, sodass Fallunterscheidungen in den Angriffsschritten modelliert werden können. Die Methodik erlaubt die Verschachtelung der logischen Verknüpfung und ist prinzipiell auf weitere logische Verknüpfungen erweiterbar.

Eine Aufteilung eines Schrittes in Teilschritte wird durch eine gerichtete Kante zwischen den Knoten dargestellt. Für die Darstellung der Disjunktion und Konjunktion werden entsprechende Knoten zwischen zwei Angriffsschritten erstellt (Bild 1). Eine direkte Verbindung zwischen zwei Angriffsschritten stellt implizit eine Disjunktion dar. Die Zerlegung der Angriffsschritte wird iterativ fortgesetzt, bis Teilschritte vorliegen, die hinreichend präzise durch die Attribute zur Bewertung der Eintrittswahrscheinlichkeit (bspw. Ressourcen, Wissen, Motivation nach IEC 62443) beschrieben werden können.

4 Risikobewertung

Die Blattknoten der Angriffsgraphen werden in der Analyse durch einen zuvor gewählten Vektor von Attributen bewertet, um die Eintrittswahrscheinlichkeit zu modellieren. Die Attribute können grundsätzlich frei gewählt werden, um sie der gängigen Praxis der betrachteten Domäne, existierenden Standards und der Risikoaffinität der analysierenden Organisation anpassen zu können. Die DIN VDE V 0831-104 verwendet die aus der IEC 62443 bekannten Attribute „Ressourcen" sowie „Wissen" und ersetzt die Motivation durch drei bahnspezifische Risikofaktoren, von denen wir den „Ort" als Beispiel aufnehmen. So ergibt sich der Attributvektor (Ressourcen, Wissen, Ort), der im Beispiel verwendet wird. Die Attribute werden im Softwarewerkzeug über einen Dialog für den Angriffsgraphen festgelegt oder aus einer Vorlage übernommen. Die Einschätzung der Belegung der Attribute erfolgt typischerweise in Workshops mit Expertinnen und Experten und wird in den Angriffsgraphen in die Blattknoten eingetragen und mithilfe von Icons visualisiert (siehe Bild 2 und Legende in Bild 3).

Der Mehrwert der Angriffsgraphen entsteht durch die atomaren Blattknoten, für die sich die Einschätzung der Attribute leich-

An attack graph analyses exactly one system at a sufficiently specific level of abstraction. For example, the predictive maintenance of a railway switch could be the object analysed by an attack graph. With predictive maintenance, the monitoring of operating parameters and machine learning are used to predict when a failure is expected in order to enable maintenance to be performed in time. The exact definition of the asset is not part of the attack graph methodology. The graph represents the assets by means of a trapezoid (fig. 1).

Attacks on the asset result in different attack sequences ("consequences") or damage events, represented on the graph by rectangles with rounded corners. Companies use predefined catalogues of harmful events, such as personal injury, reputational damage, financial damage or restrictions to business to determine the consequences. The methodology also allows the analyst to define the consequences, if no catalogue is available or an existing catalogue has been expanded.

3 Threat catalogues and threat mining

Each attack sequence can be triggered by one or more attacks ("Attack Step" in fig. 1). The graph shows this relationship by means of a directed edge from the sequence to the attack step. The attack graphs use this link to increase the traceability of the risk analysis, since they can graphically represent the possible n:m relationship between the attack and the damage.

Existing threat catalogues (e.g. the elementary threats of the German Federal Cybersecurity Authority – BSI [2]) and threat modelling methods (e.g., STRIDE [3]) support attack identification. So-called threat modelling is a process used to systematically identify IT security weaknesses in a system and thus determine its attack surface. An attack is understood as the realisation or execution of a threat within this context. Using the example of predictive maintenance, a possible attack involves prediction manipulation by the attacker and the material failure that results from the lack of a timely prediction. The attack could result in financial damage due to a train derailing due to a defective switch. Catalogues and threat mining ensure that the threat analysis is sufficiently complete. Attack graphs support the analysis by graphically processing and breaking down the attacks into sub-steps (Sub-step 1 and Sub-step 2) in order to refine the analysis and the subsequent risk assessment. Sub-steps always consist of logical disjunctions ("or") and conjunctions ("and") to the model case distinctions in the attack steps. The methodology allows for nested logical operators and is open to extension with other logical operators.

A directed edge between the nodes represents the division of a step into sub-steps. Corresponding nodes between two attack steps represent disjunctions and conjunctions (fig. 1). A direct connection between two attack steps implicitly represents a disjunction. The breakdown of the attack steps continues iteratively until reaching steps with sufficient attributive precision to evaluate the probability of occurrence (e.g., resources, knowledge and motivation according to IEC 62443).

4 Risk Assessment

During the analysis, the tool evaluates the attack graph leaf nodes by means of a previously selected vector of attributes in order to model the probability of occurrence. In principle, the tools allow the attributes to be freely adapted to the current practice of the domain under consideration, the exist-

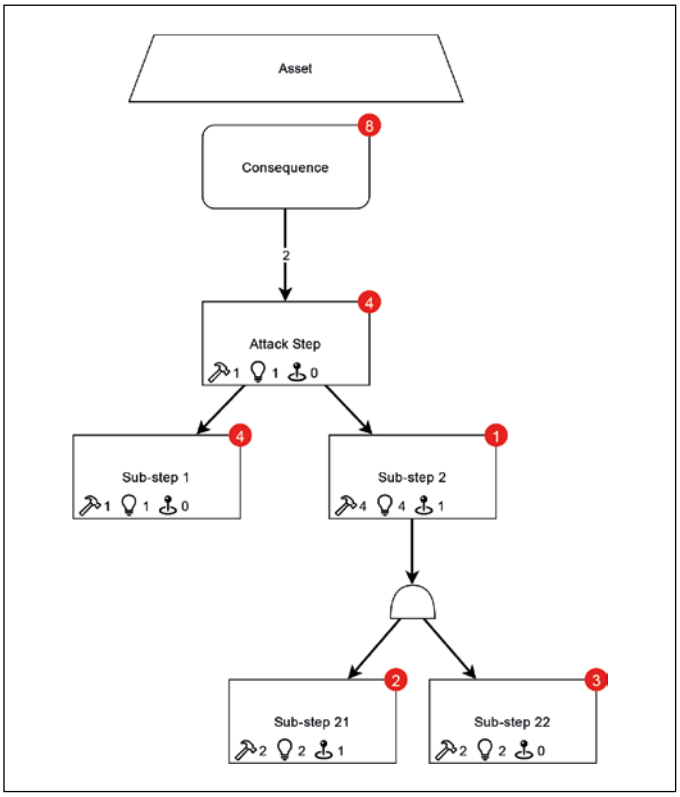

Bild 2: Angriffsgraph mit erfolgter Bewertung und Aggregation
Fig. 2: An attack graph, including assessment and aggregation

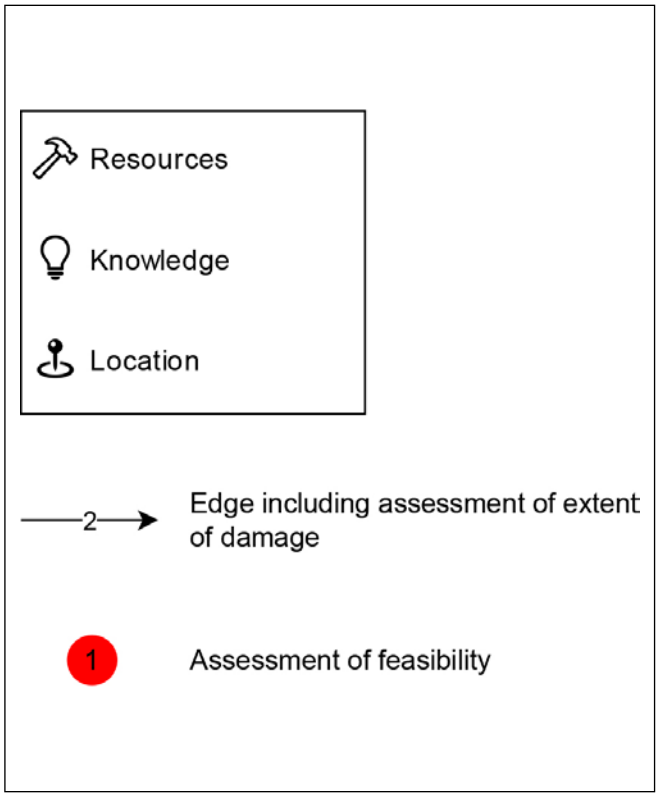

Bild 3: Legende zum Angriffsgraph
Fig. 3: The attack graph legend

ter vornehmen lässt als für komplexere, zusammengesetzte Angriffe. Daraus folgt allerdings die Notwendigkeit, die Bewertung der Blattknoten entlang des Pfades zur Angriffsfolge zu aggregieren, um die Teilschritte wieder zu einer Gesamtbewertung zusammenzusetzen. Das Softwarewerkzeug für die Angriffsgraphen unterstützt die Analystin durch vorbereitete und automatisierte Verknüpfung der Teilschritte gemäß der in der Zerlegung definierten logischen Verknüpfungen. Der vorgeschlagenen Disjunktion liegt die Annahme zugrunde, dass sich der Angreifer von mehreren möglichen Teilschritten zur Umsetzung eines Angriffsschrittes für den am leichtesten durchführbaren entscheidet. Eine mathematische Ordnungsrelation über die Attributvektoren erlaubt den Vergleich der Durchführbarkeit der Teilschritte und die Bestimmung der höchsten Durchführbarkeit. In Bild 2 ist zu erkennen, dass die Bewertung von „Sub-step 1" in „Attack Step" übernommen wird, da er die höhere Durchführbarkeit im Vergleich zu „Sub-step 2" aufweist.

Aus der Konjunktion mehrerer Teilschritte folgt die erschwerte (geringere) Durchführbarkeit des zusammengesetzten Schrittes. Die für einen erfolgreichen Angriff benötigten Ressourcen sowie das benötigte Wissen steigen (ähnlich der arithmetischen Addition), wie in Bild 2 zu sehen ist. Zur Illustration werden hier über den zwischengeschalteten Und-Knoten die Attribute der Kindknoten „Sub-step 21" und „Sub-step 22" addiert.

Das Softwarewerkzeug unterscheidet zwischen Aggregationsfunktionen und Funktionen zur Berechnung eines abgeleiteten Attributes. Aggregationsfunktionen dienen zur logischen Verknüpfung der Attributvektoren der Kindknoten zu einem Attributvektor des betrachteten Knotens. Ein abgeleitetes Attribut, wie die Durchführbarkeit, ist ein aus dem lokalen Attributvektor abgeleiteter Skalar (roter Kreis oben rechts im Knoten). Eine mit-

ing standards and the risk affinity of the analysing organization. DIN VDE V 0831-104 uses the attribute's "resources" and "knowledge" taken from IEC 62443 and has replaced motivation with three railway-specific risk factors, of which we have taken "location" as an example. This results in the attribute vector (resources, knowledge and location) in the example graph. The tool allows us to define the attributes via a dialogue or to import them from a template. Expert workshops typically perform the attribute assignment. Analysts then enter this assignment into the attack graphs in the leaf nodes. The tool visualises them with the help of icons (see fig. 2 and the legend to fig. 3).

The added value of attack graphs comes from the atomic leaf nodes. Their attribute assessment is simpler than for more complex, compound attacks. However, this means that it is necessary to aggregate the evaluation of the leaf nodes along the path to the attack sequence in order to reassemble the sub-steps into an overall assessment. The software tool for the attack graphs supports analysts by means of the prepared and automated linking of the sub-steps according to the logical operators defined in the breakdown. The proposed disjunction assumes that the attacker chooses the most easily executable step out of several possible sub-steps to implement an attack step. A mathematical order relation over the attribute vectors allows the feasibility of the partial steps to be compared and the highest feasibility to be determined. In fig. 2, the evaluation of "Sub-step 1" carries over to the "Attack Step" because it has a higher feasibility compared to "Sub-step 2".

The conjunction of several sub-steps results in the more complex (and lower) feasibility of the combined step. The resources and knowledge required for a successful attack increase (like arithmetic addition), as shown in fig. 2. For illustration, the in-

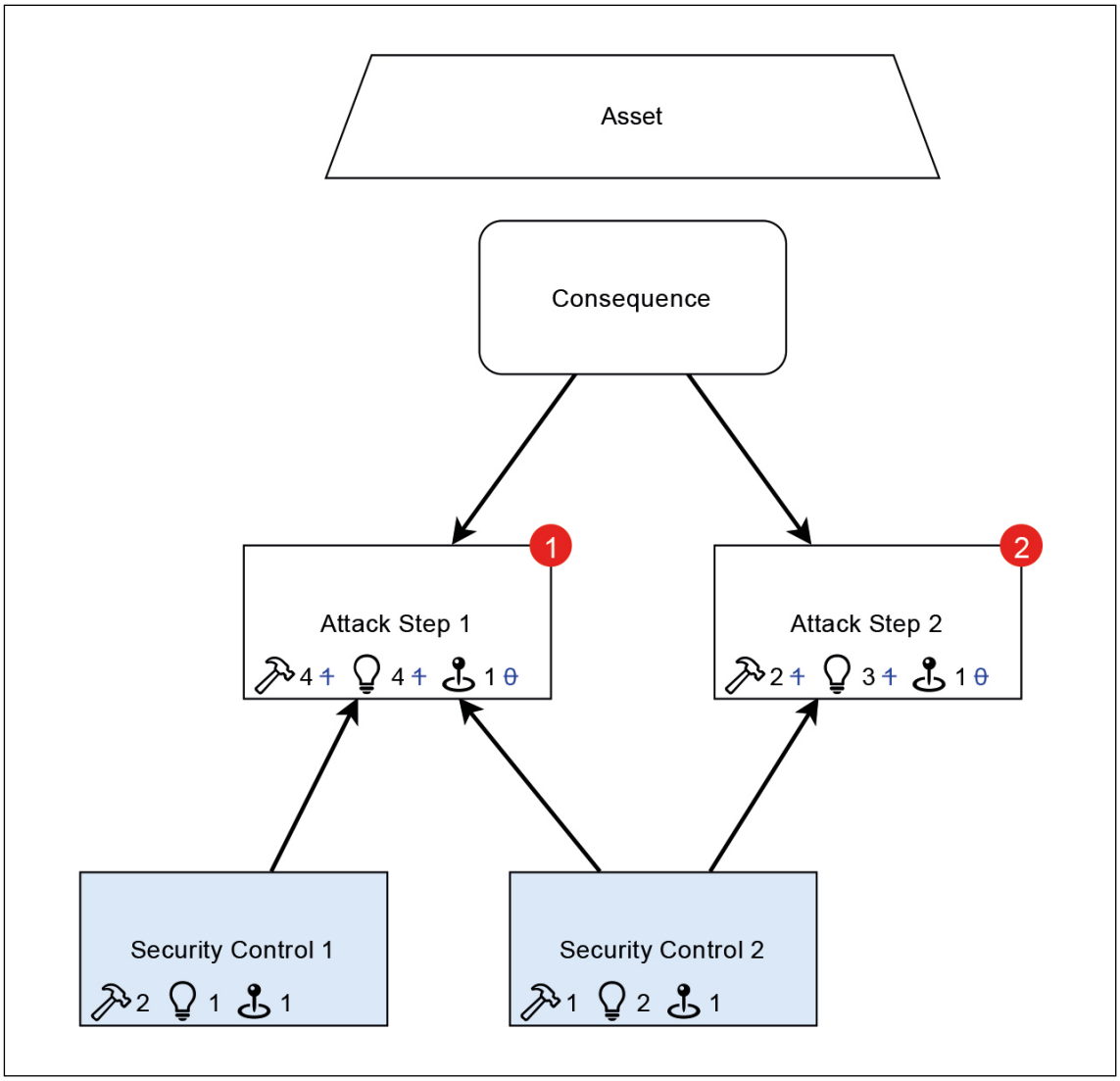

Bild 4: Der Angriffsgraph stellt die Wirkung der Gegenmaßnahmen dar
Fig. 4: The attack graph depicts the effect of a countermeasure

gelieferte Vorlage für die Angriffsgraphen beinhaltet bereits Vorschläge für die Umsetzung sowohl der Aggregationsfunktionen als auch der abgeleiteten Attribute. Sie sind in der Programmiersprache JavaScript implementiert und können durch die Benutzerin über einen Dialog betrachtet und modifiziert werden. Zur Abbildung eigener Risikoanalysemethoden erlaubt das Werkzeug die Definition eigener Funktionen über die vorgegebenen hinaus. Nach der Hinterlegung global pro Angriffsgraph lassen sich neu definierte Funktionen sowie bestehende für jeden Knoten individuell auswählen. Über eine Namenskonvention werden Knoten zur Dis- und Konjunktion automatisch mit den Funktionen „OR" bzw. „AND" belegt.

Über die Funktionen werden die Attributvektoren automatisch bis zum Angriffsschritt („Attack Step" in Bild 2) vor den Knoten mit den Angriffsfolgen aggregiert (gegen die Richtung der Kanten). Beim Übergang von Angriffsschritt auf Angriffsfolge wird das Ausmaß eines Angriffes oder dessen Einfluss auf eine bestimmte Folge durch Expertinnen und Experten bewertet. Die Bewertung wird als Skalar, als Kantengewicht der Kante zwischen den beiden Knoten dargestellt, sodass die n:m-Beziehung zwischen Angriff und Schaden mit unterschiedlicher Stärke bewertet werden kann. Eine Aggregationsfunktion im Angriffsfolgeknoten nimmt pro Kindknoten den Attributvektor sowie das Kantengewicht entgegen, verknüpft diese zum Betrag des Risiko terposed "AND" node adds the attributes of the child node's "Sub-step 21".

The software tool distinguishes between aggregation functions and functions used to calculate a computed attribute. Aggregation functions are used to logically link the attribute vectors of the child nodes to an attribute vector of the node under consideration. A computed attribute, such as feasibility, is a scalar derived from the local attribute vector (the red circle in the top-right corner of the node). The supplied template for the attack graph already contains suggestions for implementing both the aggregation functions and the computed attributes. We have implemented the function using the JavaScript programming language and allow the functions to be viewed and modified via a dialogue. The tool allows its own functions to be defined in order to map out the distinct risk analysis methods. Newly defined and existing functions can be individually selected for each node after the global filing of each attack graph. The disjunction and conjunction nodes are automatically assigned the functions "OR" or "AND" using a naming conventions

The use of the functions aggregates the attribute vectors automatically towards the attack step ("Attack Step" in fig. 2) in front of the nodes with the attack sequences (against the direction of the edges). Experts evaluate the extent of an at-

kos und kann somit den Angriff mit dem höchsten Risiko für das im Knoten beschriebene Schadensereignis bestimmen. In Bild 2 wird dies beispielhaft mit nur einem Angriffsschritt dargestellt:
Risiko = Durchführbarkeit * Schadensausmaß = 4 x 2 = 8
Die in den Bildern gezeigten Werte dienen der Illustration und spiegeln keine konkrete Risikobewertung wider. Die genaue Definition und Feinjustierung der Aggregationsmethodik wird im weiteren Verlauf des Forschungsprojektes vorgenommen.

5 Gegenmaßnahmen

Die Risikoanalyse und Bewertung der Bedrohungen werden zunächst ohne Berücksichtigung der Gegenmaßnahmen durchgeführt. Grundsätzlich sollen im iterativen Prozess der Risikoanalyse jedoch bereits etablierte Gegenmaßnahmen berücksichtigt, bewertet und dargestellt werden. Die Angriffsgraphen und das Softwarewerkzeug erleichtern daher auch die Erfassung der Wirkung von Gegenmaßnahmen auf Angriffsschritte. Auch hier ist eine n:m-Beziehung zwischen Angriff und Maßnahme anzunehmen, da typischerweise je nach Fallkonstellation eine einzelne Maßnahme gegen mehrere Angriffe schützen kann und umgekehrt mehrere Maßnahmen zum Schutz vor einem Angriff zur Auswahl stehen können oder erst die Kombination mehrerer Maßnahmen einen wirksamen Schutz darstellt.
Das Beispiel in Bild 4 zeigt die Wirkung von zwei Gegenmaßnahmen auf zwei Angriffsschritte. Auch die Gegenmaßnahmen werden mit demselben Attributvektor bewertet und nehmen so Einfluss auf den Angriff. Die ursprüngliche Bewertung des Angriffsschrittes wird mit blauer Schriftfarbe und durchgestrichen im Knoten weiterhin dargestellt, während die schwarz gedruckten Werte auch den Einfluss der Gegenmaßnahmen enthalten und so das durch die Maßnahme reduzierte Risiko widerspiegeln. Auf „Attack Step 1" wirken beide Gegenmaßnahmen mit im Beispiel addiertem Effekt. Auf „Attack Step 2" hingegen wirkt nur „Security Control 2", sodass hier bei gleicher Ausgangsbewertung wie „Attack Step 1" eine geringere Reduktion der Durchführbarkeit erfolgt.

6 Fazit und Ausblick

Mit dem Softwarewerkzeug für Angriffsgraphen lassen sich verschiedene Risikoanalysemethoden abbilden, automatisieren und auf die Bedürfnisse und die Risikoaffinität der analysierenden Organisation abstimmen. Die Angriffsgraphen ermöglichen die explizite Zuordnung von Bedrohungen zu daraus folgenden Schäden inklusive einer Bewertung der Schadenshöhe. Durch die Verfeinerung der Bedrohungen in Angriffsschritte werden die semi-quantitative Bewertung der Eintrittswahrscheinlichkeit sowie der risikomindernde Einfluss von Gegenmaßnahmen mit denselben Attributen wie ein Angriffsschritt transparent und nachvollziehbar. Durch diesen Schritt wird ein harmonisiertes Risikomanagement im Unternehmen möglich. Die Semi-Quantifizierung unterstützt IT-Sicherheitsverantwortliche dabei, Maßnahmen für Fachpersonale und Management gleichermaßen nachvollziehbar in ihrer Wirkung darzustellen. Dies erhöht Verständnis, Bewusstsein und Sicherheit in der Qualität der Einschätzung.
Das Werkzeug stellt eine JavaScript-Schnittstelle zur automatisierten Aggregation der Attribute im Angriffsgraphen bereit. Die Definition der Funktionen wird im weiteren Verlauf des Projektes „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn" vorgenommen und verfeinert. Das Werkzeug wird in diesem Forschungsprojekt dazu verwendet, eine Risikoanalyse der prognostizierten Anwendungsfälle vorzunehmen und Abuse-Cases

tack or its influence on a specific sequence at the transition from the attack step to the attack sequence. The scalar rating is presented as the edge weight of the edge between the two nodes, so that the n:m relationship between the attack and the damage can be evaluated at different strengths. An aggregation function in the attack sequence node accepts the attribute vector and the edge weight for each child node, links them to the amount of risk and can thus determine the attack with the highest risk for the damage event described in the node. Fig. 2 shows this as an example with just one attack step:
risk = feasibility • extent_of_damage = 4 • 2 = 8.
The values shown in the figures are for illustrative purposes only and do not reflect a specific risk assessment. The exact definition and fine-tuning of the aggregation methodology is subject to the further course of the research project.

5 Countermeasures

Risk analysis and threat assessment do not initially consider any pre-existing countermeasures. However, these measures should be reflected in the risk analysis process. Therefore, attack graphs and the software tool also make it easier to record the effect of any countermeasures on the attack steps. Here, too, we assume an n:m relationship between the attack and the measure, since a single measure can typically protect against several attacks and, conversely, multiple measures can also protect against the same attack or only the combination of several measures can provide adequate protection.
Fig. 4 shows the effect of two countermeasures on two attack steps. The countermeasure evaluation uses the same attribute vector and thus influences the attack. The tool represents the original assessment in the blue font and crossed out in the node, while the values printed in black also contain the influence of the countermeasures and thus reflect the risk reduced by the measure. Both countermeasures work on "Attack Step 1" with the added effect in the example. On the other hand, only "Security Control 2" acts on "Attack Step 2," so there is a minor reduction in feasibility with the same initial evaluation as "Attack Step 1".

6 Conclusion

We have presented a software tool for attack graphs that can map out various risk analysis methods and is automated and tailored to the needs and risk affinity of the analysing organisation. Attack graphs enable the explicit assignment of threats to the resulting damage, including the assessment of the amount of damage. By refining the threats into attack steps, the semi-quantitative assessment of the probability of occurrence and the risk-reducing influence of any countermeasures with the same attributes as an attack step become transparent and comprehensible. This step enables harmonised risk management in a company. The semi-quantification supports those responsible for IT security in presenting the effects of measures to specialist staff and management in an equally comprehensible manner. Thereby, this possibility increases understanding, awareness and surety with regard to the quality of the assessment.
The tool provides a JavaScript interface for the automated aggregation of attributes in the attack graph. We will define and refine the functions in the further course of the "Security Requirements Forecast and Evaluation of Possible Security Concepts" project. In this project, the tool allows a risk analysis of the predicted use

für sie zu entwickeln und zu bewerten. Das Softwarewerkzeug wurde als Plug-in für die frei verfügbare Diagrammsoftware Draw.io [4] entwickelt und steht quelloffen unter der MIT Lizenz auf GitHub zum Herunterladen zur Verfügung [5].

Forschungsförderung

Die vorgestellte Lösung entstand im Rahmen des vom Deutschen Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt beauftragten und finanzierten Projekts „Prognose Securitybedarf und Bewertung möglicher Sicherheitskonzepte für das System Bahn“.

cases to be carried out and abuse cases to be developed and evaluated for them. We have realised the software tool as a plug-in for the freely available Draw.io software [4] and made it available for download under the MIT license on GitHub [5].

Research funding

The presented solution has been created as part of the “Security Requirements Forecast and Evaluation of Possible Security Concepts” project commissioned and financed by the German Centre for Rail Traffic Research at the Federal Railway Authority.

LITERATUR | LITERATURE

[1] https://www.dzsf.bund.de/SharedDocs/Standardartikel/DZSF/Projekte/Projekt_49_Securitybedarf.html
[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html
[3] https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
[4] https://www.diagrams.net/
[5] https://github.com/incyde-gmbh/drawio-plugin-attackgraphs

AUTOREN | AUTHORS

Dr.-Ing. Markus Heinrich
Expert IT Security
INCYDE GmbH
Anschrift /*Address*: Schaumainkai 91, D-60596 Frankfurt am Main
E-Mail: markus.heinrich@incyde.com

Dr. rer. nat. Lukas Iffländer
Wissenschaftlicher Referent Cybersicherheit
Deutsches Zentrum für Schienenverkehrsforschung
beim Eisenbahn-Bundesamt
Anschrift /*Address*: August-Bebel-Straße 10, D-01219 Dresden
E-Mail: IfflaenderL@dzsf.bund.de