Risikobewertung für vernetzte kritische Infrastrukturen

Stefan Schauer[1] · Sandra König[1] · Stefan Rass[2]
Thomas Grafenauer[2] · Jasmin Wachter[2] · Thomas Schaberreiter[3]
Gerald Quirchmayr[3] · Simon Poledna[4] · Martin Latzenhofer[1]
Romana Stollnberger[1] · Klaus Steinnocher[1]

[1]Austrian Institute of Technology
Center for Digital Safety & Security
{sandra.koenig | martin.latzenhofer | stefan.schauer | klaus.steinnocher
romana.stollnberger}@ait.ac.at

[2]Alpen-Adria-Universität Klagenfurt
Institut für Angewandte Informatik
{stefan.rass | thomas.grafenauer | jasmin.wachter}@aau.at

[3]Universität Wien
Fakultät für Informatik
{thomas.schaberreither | gerald.quirchmayr}@univie.ac.at

[4]avedos GRC GmbH
simon.poledna@avedos.com

Zusammenfassung

Dieser Beitrag stellt ein System zur Identifikation und Bewertung potenzieller Kaskadeneffekte innerhalb eines Netzwerks von kritischen Infrastrukturen vor. Bei dem Ansatz handelt es sich um ein hybrides Simulationsmodell, das einerseits statische Daten über die kritischen Infrastrukturobjekte konsistent abbildet und andererseits ermöglicht, dynamische Daten (wie den aktuellen Status der Infrastrukturen im Netzwerk) auf Basis von Perkolationstheorie und Markov-Ketten zu verarbeiten. Die statischen Daten fließen dabei in eine Gap-Analyse, um potentielle Lücken in der Umsetzung von Sicherheitsmaßnahmen zu identifizieren, während durch die dynamische Komponente Abhängigkeiten zwischen verschiedenen Infrastrukturen bei der Analyse berücksichtigt werden. So können mögliche Konsequenzen bestimmter Szenarien, etwa wenn eine Infrastruktur ihre Kapazität reduzieren muss oder komplett ausfällt, durch Simulationen ermittelt werden. Das System ermöglicht durch diesen hybriden Ansatz eine ganzheitliche Risikobetrachtung, die durch strukturierte Aufbereitung der Ergebnisse sowie graphische Darstellung der dynamischen Ausbreitung von Kaskadeneffekten im Netzwerk eine umfassende Risikoanalyse der kritischen Infrastrukturen bietet. Auf diese Weise können nicht nur die Risiko- und Sicherheitsverantwortlichen einer Infrastruktur die Folgen eines Vorfalls an einem beliebigen Punkt im Netz tiefergehender analysieren, sondern auch staatliche Behörden, die mit dem Schutz der kritischen Infrastrukturen betraut sind, sich auf einen potentiellen Krisenfall vorbereiten.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 313-322.

1 Einleitung

Im Allgemeinen werden als kritische Infrastrukturen jene Anlagen oder Systeme (oder Teile davon) bezeichnet, die für die Aufrechterhaltung wesentlicher gesellschaftlicher Funktionen verantwortlich sind und deren Störung oder Ausfall erhebliche Auswirkungen auf das wirtschaftliche und soziale Wohlergehen der Bevölkerung haben würde [Euro08]. Kritische Infrastrukturen sind daher von signifikanter Bedeutung für die Sicherstellung zentraler gesellschaftlicher Abläufe, wie die Versorgung mit lebensnotwendigen Gütern und Dienstleistungen. Sie sind in diversen Bereichen zu finden und umfassen sowohl die grundlegenden Versorgungsnetzwerke (Strom, Gas, Wasser), als auch Informations- und Kommunikationsnetzwerke und reichen bis hin zu intermodalen Systemen mit komplexen Verflechtungen und hoher gesellschaftlicher Bedeutung (wie etwa medizinische Versorgung oder Transportnetzwerke). Durch die stetig wachsende Anzahl immer komplexerer Verbindungen zwischen den einzelnen kritischen Infrastrukturen steigt auch der Grad der gegenseitigen Abhängigkeiten, woraus sich i.A. ein gegen Störungen sensibles Gesamtsystem ergibt [RiPK01].

Aufgrund dieser stark verflochtenen Zusammenhänge und Abhängigkeiten ist deutlich zu sehen, dass eine Beeinträchtigung oder gar der Totalausfall einer kritischen Infrastruktur nicht nur diese Infrastruktur alleine betrifft, sondern potentiell auch Auswirkungen auf eine Reihe anderer kritischer Infrastrukturen sowie auf das wirtschaftliche und soziale Wohlergehen der Bevölkerung haben kann. Allein für den Bereich der Energiewirtschaft und Elektrizitätsversorgung in Österreich zeigten dies die beiden Studien BlackÖ.1 [ReSc11] und BlackÖ.2 [RSBM15], in denen unterschiedliche Szenarien eines lokalen und nationalen Stromausfalls untersucht wurden. Darüber hinaus haben real eingetretene Zwischenfälle gezeigt, wie weitläufig und markant sich diese Beeinträchtigungen gestalten können. So waren etwa 2012 in Indien 600 Millionen Menschen von einem Stromausfall betroffen [Pidd12, SVAB12]. Im Jahr 2005 hatte die Abschaltung zweier Versorgungsleitungen und die unzureichende Dokumentation der Kapazitätsleistung der verbliebenen Leitung deren Überlastung zur Folge und legte daraufhin den gesamten Bahnverkehr in der Schweiz für mehrere Stunden lahm [Schw05, Schw14]. Das zwölfstündige Blackout in Italien im Jahr 2003 wurde durch den Ausfall zweier neuralgischer Versorgungsleitungen aus Frankreich und der Schweiz verursacht und resultierte in einem finanziellen Schaden von ca. 1,182 Milliarden Euro [ScRe14].

Ein zentraler Ansatzpunkt, um solch einer Beeinträchtigung oder einem Totalausfall entgegen zu wirken, ist der Einsatz einer umfassenden Sicherheitsarchitektur sowie eines Risikomanagementsystems. Derartige Systeme sind bei den einzelnen kritischen Infrastrukturbetreibern oft bereits im Einsatz, betrachten aber meist nur die individuellen Bedrohungen. Abhängigkeiten zu anderen Infrastrukturen werden häufig nur am Rande in eine Bewertung mit aufgenommen oder bleiben komplett unbeachtet. Erste Ansätze zur Modellierung und Simulation von derartigen Abhängigkeiten zwischen kritischen Infrastrukturen sind in [Rina04] beschrieben. Das in diesem Beitrag präsentierte CERBERUS-System stellt einen neuen Ansatz dar, der insbesondere die Identifikation und Bewertung von Kaskadeneffekten innerhalb eines Netzwerks von untereinander abhängigen kritischen Infrastrukturen unterstützen soll. Hierfür werden stochastische Modelle (vor allem Markov-Ketten) verwendet, welche die potenziellen Folgen der Interdependenzen zwischen verschiedenen Infrastrukturen beschreiben. Die Auswirkungen einer Kapazitätsreduktion oder eines Totalausfalls einer Infrastruktur werden auf Basis dieses Modells über eine fixe Zeitspanne simuliert.

Die daraus gewonnenen Erkenntnisse können in einem späteren Stadium mit Informationen über bereits umgesetzten Sicherheitsmaßnahmen – sofern solche Informationen vorliegen – kombiniert und in eine Risikokennzahl überführt werden. Durch eine strukturierte Aufbereitung der Simulationsergebnisse und eine graphische Darstellung der dynamischen Ausbreitung von Kaskadeneffekten können die Resultate zielgerecht kommuniziert werden.

Der hier vorgestellte Ansatz wurde im Zuge des Forschungsprojekts CERBERUS (Cross Sectoral Risk Management for Object Protection of Critical Infrastructures) entwickelt, welches durch die Österreichische Forschungsförderungsgesellschaft (FFG) im Rahmen des KIRAS-Programms gefördert wird. Neben den wissenschaftlichen und wirtschaftlichen Partnern sind in CERBERUS sowohl Ministerien, die mit dem Schutz kritischer Infrastrukturen in Österreich betraut sind, als auch eine Reihe kritischer Infrastrukturen als End User stark involviert. CERBERUS richtet sich einerseits an die Betreiber kritischer Infrastrukturen, denen die Ergebnisse wichtige Aufschlüsse über die Auswirkung von Versorgungsengpässen anderer kritischer Infrastrukturen geben können, wodurch die Planung von präventiven Maßnahmen unterstützt wird. Andererseits zählen auch die staatlichen Behörden und Blaulichtorganisationen, welche mit dem Schutz und der Unterstützung kritischer Infrastrukturen betraut sind, zu den potentiellen Nutzern, da die Informationen aus dem CERBERUS-System ihnen helfen können, potenzielle Schwachpunkte zu erkennen und damit ihre Leistungen im Krisenfall anzupassen und zu verbessern.

2 Systemüberblick

Das CERBERUS-System integriert mehrere Komponenten, welche die unterschiedlichen Hauptaufgaben des Systems übernehmen (siehe Abbildung 1). Hierzu gehören die Datenbereinigung und die Modellierung, jeweils eine separate Komponente für die statische und die dynamische Risikoanalyse (zu der ebenfalls die Simulationskomponente zählt) sowie die Ergebnisauswertung und die Visualisierung. Die Datenhaltung erfolgt über eine zentrale Datenbank. Die Resultate der Analyse sind einerseits schriftliche Reports, welche die Ergebnisse der Analyse zusammenfassen und erklären, sowie andererseits eine visuelle Darstellung der Ergebnisse inklusive Verortung. Im Folgenden werden die Funktionen der einzelnen Komponenten sowie deren Zusammenspiel kurz erklärt.

Das CERBEURS-System baut auf Informationen über kritische Infrastrukturen auf, welche separat und unabhängig gesammelt wurden. Dies kann zum Beispiel durch staatliche Behörden erfolgen, die in engem Kontakt zu den Infrastrukturen stehen und diese in sicherheitsrelevanten Fragen unterstützen. Die dabei erhobenen, potentiell unterschiedlichen subjektiven Experteneinschätzungen werden sofern möglich zu einem Konsens zusammengeführt und etwaige Unsicherheiten werden während der Datenbereinigung reduziert.

Das CERBERUS-Modell kann entsprechend der Datengrundlage individuell instanziiert und adaptiert werden. Dabei gilt grundsätzlich, dass mehr Daten zu einem präziseren Modell führen, welches die Abhängigkeiten detaillierter abbilden kann. In der Modellierung werden aus den vorhandenen Daten die benötigten Modellparameter geschätzt, welche ihrerseits in die anschließende Simulation einfließen.

In der statischen Risikoanalyse werden die grundlegenden Charakteristika der kritischen Infrastruktur zusammengefasst indem diese in einzelne Teilobjekte (Assets) zerlegt wird. Für die jeweiligen Assets werden Risikobewertungen auf Basis von Expertenwissen durchgeführt.

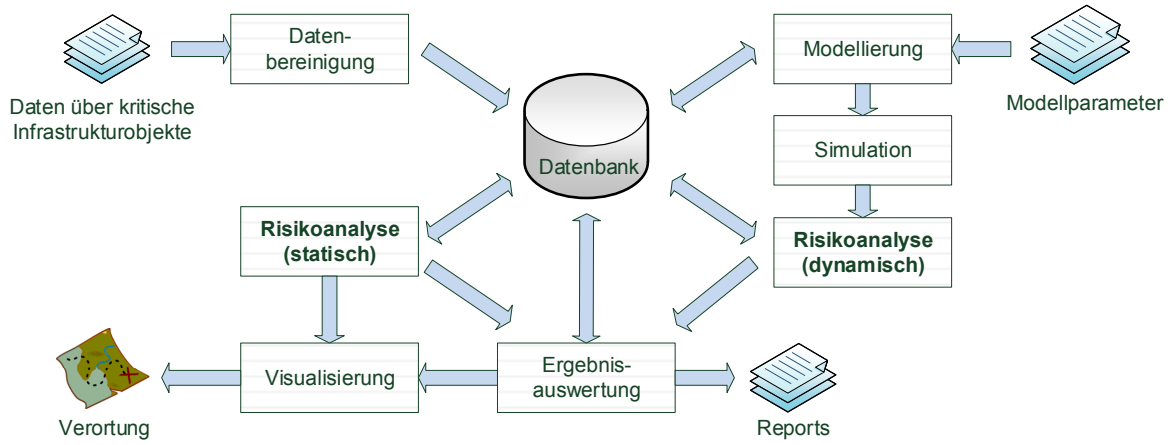

Abb. 1: Schematische Darstellung der CERBERUS-Systemarchitektur

Die Datenerfassung und Datenverarbeitung wird vom GRC (Governance, Risk and Compliance) Softwaretool risk2value unterstützt.

In der dynamischen Risikoanalyse werden die Auswirkungen eines Vorfalls, der zu einem Teil- oder Totalausfall einer kritischen Infrastruktur führen kann, auf die abhängigen kritischen Infrastrukturen simuliert. Hierbei basiert die Simulation auf dem oben angesprochenen CERBERUS-Modell, welches die Statusübergänge einer kritischen Infrastruktur durch stochastische Prozesse beschreibt. Implementiert wird die Simulation im Framework OMNeT++, dass die Ergebnisse an risk2value weiterleitet.

Zur Visualisierung der Ergebnisse wird eine „virtuelle“ Stadt konstruiert, in der die Kaskadeneffekte Schritt für Schritt gezeigt werden können. Diese virtuelle Stadt soll möglichst realitätsnah sein und trotzdem keinerlei Rückschlüsse auf die im Projekt betrachteten Use Cases zulassen. Neben der visuellen Darstellung soll auch eine schriftliche Ergebnisauswertung die Resultate der Analyse verständlicher machen.

Im Folgenden werden das statische Risikomodell, das dynamische Risikomodell und die Aufbereitung der Ergebnisse detaillierter beschrieben, da diese das Herzstück des CERBERUS-Systems bilden.

3 Statisches Risikomodell

Das statische Risikomodell im CERBERUS System baut im Allgemeinen auf dem Prinzip der Gap-Analyse auf. Dabei werden die bestehenden Maßnahmen und Controls, die innerhalb einer kritischen Infrastruktur bereits implementiert sind, den potentiellen Gefährdungen gegenübergestellt und es wird analysiert, inwiefern die Maßnahmen auf die Gefährdungen wirken. Das statische Risikomodell baut auf detaillierten Informationen über die einzelnen kritischen Infrastrukturen im Netzwerk auf und beschreibt ihren inneren Aufbau. Hierfür wird jede kritische Infrastruktur als Asset dargestellt, welches alle nötigen Informationen beinhaltet. Über einen Risikokatalog werden die potentiellen Gefährdungen abgebildet und mit den Assets in Verbindung gebracht. Parallel sind in einem Control-Katalog die möglichen Maßnahmen gesammelt, welche ebenfalls den Assets zugeordnet werden können.

Im Zuge einer Risikobewertung werden für jede Infrastruktur sowohl die relevanten Gefährdungen als auch die umgesetzten Maßnahmen identifiziert. Für jede Control wird ein Reifegrad

angegeben, der die Wirksamkeit des Controls gegenüber einer Gefährdung beschreibt und somit die Auswirkungen beeinflusst. Je höher der Reifegrad, desto geringer der Schaden, der durch eine Gefährdung verursacht wird. Im Gegensatz zu klassischen Ansätzen, in denen ein Schaden oft anhand monetärer Werte angegeben wird, erfolgt die Bewertung der Auswirkungen im CERBERUS-Modell über vier Indikatoren: Mensch, Wirtschaft, Gesellschaft und Umwelt. Somit können die Auswirkungen eines Ausfalls einer Infrastruktur im Kontext diese vier Bereiche separat abgeschätzt werden. Das CERBERUS-Modell erlaubt es ebenfalls, die Auswirkung einer Gefährdung auf eine Infrastruktur für drei unterschiedliche Zeithorizonte (kurz-, mittel- und langfristig) zu bewerten. Hierbei kann für jede Infrastruktur individuell festgelegt werden, welche Zeitspanne (in Sekunden, Stunden, Tagen, etc.) als kurz-, mittel- und langfristig angesehen wird.

Das statische Risikomodell ist im Tool risk2value umgesetzt; es werden darin alle Daten erfasst und die Risikobewertungen durchgeführt. Zusätzlich ermöglicht es risk2value auch, die Ergebnisse aus dem dynamischen Modell (siehe Abschnitt 4 im Anschluss) direkt zu integrieren. Somit können die Ergebnisse aus den statischen Risikobewertungen sowie den Simulationen des dynamischen Modells gemeinsam abgelegt werden und für die weitere Verarbeitung (z.B. Visualisierung und Reporting, siehe Abschnitt 5) aufbereitet werden.

Im Zuge des Projekts wird davon ausgegangen, dass die benötigten Informationen über die kritischen Infrastrukturen bereits vorhanden sind, etwa aus bestehenden Analysen, oder erhoben werden können, etwa durch Befragungen bei den Infrastrukturbetreibern. So werden im Projekt Datenblätter der Ministerien als Basis für das statische Modell verwendet (jedoch ohne die konkreten Daten der Infrastrukturen zu verwenden). Hierbei ist natürlich klar, dass es durch die subjektiven Experteneinschätzungen zu Einschränkungen für das Modell kommen kann (siehe Abschnitt 6 für Details).

4 Dynamisches Risikomodell

Das dynamische Risikomodell baut auf den Abhängigkeiten zwischen kritischen Infrastrukturen auf, die im statischen Modell beschreiben sind. Diese Abhängigkeiten können auf verschiedene Arten dargestellt werden, z.B. mittels einer Ontologie [EFKW06]. Im CERBERUS Risikomodell wird ein graphentheoretischer Ansatz verfolgt, bei dem die Infrastrukturen durch Knoten und die Abhängigkeiten zwischen ihnen durch gerichtete Kanten dargestellt werden. Eine derartige Verwendung eines Abhängigkeitsgraphen als Basis für die Risikoanalyse ist nicht neu und ist bereits im Hierarchical Holographic Modelling (HHM) [Haim81] oder bei Rinaldi [RiPK01, DuPM06] zu finden. Eine Besonderheit im CERBERUS-Modell [KöRa17] ist jedoch, dass der aktuelle Grad der Beeinträchtigung eines jeden Knotens durch einen von mehreren Zuständen repräsentiert werden kann. Um das Modell den real vorhandenen Unwägbarkeiten und Unsicherheiten anzupassen, werden Zustandsübergänge durch Zufallsvariablen beschrieben. Dies ermöglicht die Berücksichtigung von nicht exakt vorhersehbaren Auswirkungen eines Vorfalls auf das gesamte Netzwerk der kritischen Infrastrukturen. Stochastische Prozesse wurden bereits in ähnlichen Ansätzen in der Literatur eingesetzt, um die Ausbreitung von Beeinträchtigungen in einem Netzwerk zu beschreiben (etwa in [SvWo07], [WaST12] oder [RaHa16]), die Verwendung unterschiedlicher Zustände ist in diesem Kontext jedoch neu. Die Besonderheit des CERBERUS-Modells ist hierbei die Balance zwischen Komplexität und Ausdrucksstärke des Modells: so wird durch den vorgeschlagenen Ansatz vermieden, eine ggf. exponentielle Anzahl von Parametern im Modell zu haben (wie dies etwa bei Bayes'schen Netzen geschehen könnte). Gleichermaßen erlaubt das Modell die Beschreibung von stochastischen

und deterministischen Abhängigkeiten, und erweitert hierdurch die Möglichkeiten alternativer Ansätze wie etwa System Dynamics.

Die Idee des CERBERUS-Modells wird in Abbildung 2 illustriert. Die verschiedenen Zustände, in denen sich die kritische Infrastruktur X befinden kann, werden durch Teilknoten mit verschiedener Färbung dargestellt (obere Gruppe von Knoten). Im konkreten Fall wird ein Ampelsystem zur Darstellung des Zustandes verwendet („grün“ = „alles OK“, „gelb“ = „teilweise Beeinträchtigung“, „rot“ = „Totalausfall“). Jeder Inputknoten befindet sich ebenfalls in einem dieser vordefinierten Zustände. Tritt bei einem Inputknoten ein Problem auf (sein Zustand ändert sich z.B. auf „gelb“ oder „rot“) so kann dies Auswirkungen auf die kritische Infrastruktur haben. Wie bereits angesprochen sind die Folgen nur schwer vorhersehbar und werden daher im Modell durch eine Zufallsvariable beschrieben. Somit ändert die kritische Infrastruktur ihren Zustand mit einer gewissen Wahrscheinlichkeit. Diese stochastische Abhängigkeit wird durch eine Markov-Kette modelliert, welche für jeden Zustand eines Inputknotens eine Wahrscheinlichkeitsverteilung über die Zustände der abhängigen Infrastruktur angibt. Hierbei sind aufgrund multipler Abhängigkeiten gleichzeitig verschiedene Zustände möglich. Beispielsweise kann ein Problem beim Stromversorger zu einer teilweisen Beeinträchtigung der Infrastruktur führen (Status „gelb“), da eine Notstromversorgung verfügbar ist; ein gleichzeitig auftretendes Problem beim Wasserlieferanten kann aber einen Totalausfall (Status „rot“) zur Folge haben. In diesem Fall wird nach dem Maximumprinzip aggregiert und der schlimmste Zustand an die nächste abhängige Infrastruktur weitergemeldet.

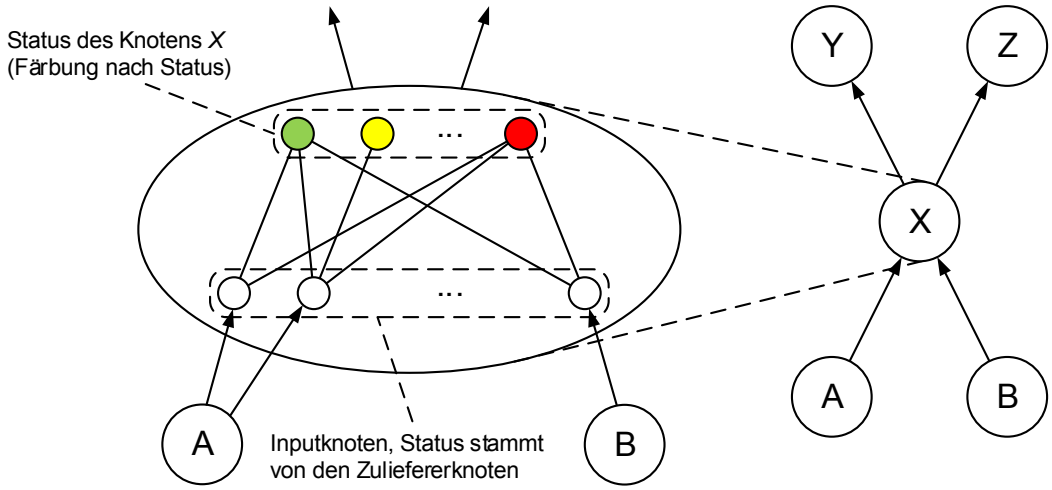

Abb. 2: Schematische Darstellung des CERBERUS Modells

Die Analyse der Auswirkungen einer teilweisen Beeinträchtigung oder eines Totalausfalls einer Infrastruktur auf das Gesamtnetzwerk wird mit Hilfe einer stochastischen Simulation durchgeführt. Hierfür wird das diskrete, ereignisgesteuerte System OMNeT++ eingesetzt, mit dem der Informationsfluss zwischen den Knoten (bei CERBERUS entspricht dies der Auswirkung eines Vorfalls durch die modellierte Abhängigkeit) mit geringem Aufwand zu implementieren ist. Zudem können die unterschiedlichen Dynamiken im CERBERUS-Modell, etwa deterministische und nichtdeterministische sowie zeitliche Einflüsse (zum Beispiel zusätzliche Folgen bei längerem Andauern von Ausfällen), einfach abgebildet werden.

Eine Simulation wird durch ein bestimmtes Ereignis initiiert, welches vom Benutzer ausgewählt wird und eine oder mehrere Infrastrukturen betrifft. Daraufhin wechseln die abhängigen

Infrastrukturen von ihrem Ausgangszustand (Status „grün“) in einen beeinträchtigten Zustand (Status „gelb“ oder „rot“). Dieser Zustandsübergang ist durch die oben angesprochene Wahrscheinlichkeitsverteilung bestimmt, welche im System durch eine Übergangsmatrix für jede Kante im Abhängigkeitsgraphen dargestellt ist. Zudem wird die Übergangswahrscheinlichkeit auch für die drei Zeiträume (kurz-, mittel- und langfristig) definiert. Somit können sich die Werte der Übergangsmatrix während der Laufzeit der Simulation verändern, wodurch die reale Entwicklung besser dargestellt wird (so hat etwa ein kurzfristiger Stromausfall kaum Auswirkungen, während ein langfristiger Ausfall eine Infrastruktur stark beeinträchtigen kann). Zusätzlich können Redundanzen wie Notstromaggregate oder andere Notfallmaßnahmen direkt in der Simulation abgebildet werden.

5 Auswertung und Darstellung

Eine Form der Ergebnisdarstellung im CERBERUS-System ist eine geographische Visualisierung der simulierten Auswirkungen, etwa die durch einen Stromausfall betroffene Region. Der hierbei räumliche Kontext der simulierten Auswirkungen ist ein unverzichtbarer Bestandteil für die Bewertung. Durch die Verortung werden einerseits die Abhängigkeiten der einzelnen Komponenten, andererseits die Vernetzung untereinander klar aufgezeigt. Ein wesentlicher Aspekt, der u.a. durch geographisch gestützte Analysen ausgewertet werden kann, ist die Abschätzung der Auswirkungen von Schadensereignissen, z.B. wie viele Personen von einem Ereignis betroffen sind.

Um Bezüge zur Realität zu vermeiden, wurde im Projekt bewusst eine virtuelle Stadt in einem Geo-Informationssystem (GIS) aufgebaut, bei der die Funktionalitäten im Vordergrund stehen und die nicht mit einer realen Stadt in Verbindung gebracht werden kann, obgleich reale Städte als Vorlage für die Modellstadt dienten. Im Allgemeinen bietet das System aber jegliche Möglichkeiten, die Infrastrukturen entsprechend ihrer realen Gegebenheiten zu verorten.

Abb. 3: Simulationsergebnis der Ausbreitung der Folgen eines Ausfalls der Wasserversorgung

Zusätzlich zu der visuellen Darstellung der Ergebnisse bietet das CERBERUS-System auch Berichte an. Diese sind auf unterschiedliche Management-Ebenen zugeschnitten, wodurch die Informationen für unterschiedliche Empfänger-Gruppen aufbereitet werden können. Mit Hilfe dieser Berichte kann zum Beispiel eine Liste der größten Gefährdungen für die betrachteten

Infrastrukturen erstellt, die neuralgischen Punkte im Netzwerk aufgeschlüsselt oder eine umfassende Risikoeinschätzung für eine einzelne kritische Infrastruktur erzeugt werden. Auf Basis dieser Berichte können sowohl Vorschläge zur Verbesserung des Schutzes für einzelne Infrastrukturen (z.B. Erhöhung des Reifegrads spezifischer Maßnahmen) als auch mögliche Einsatzpläne für Assistenzleistungen (z.B. durch die Ministerien) erarbeitet werden.

6 Einsatzbereiche und Einschränkungen

Für das beschriebene CERBERUS-System gibt es zwei Hauptanwendungsbereiche. Zum einen ist das System für nationale Behörden gedacht, die einen Überblick über die verschiedenen kritischen Infrastrukturen in einer bestimmten Region (z.B. einer Stadt oder einem Bundesland) haben. Dabei wird davon ausgegangen, dass diese Behörde entweder über explizite Informationen über die Abhängigkeiten zwischen den Infrastrukturen verfügt, z.B. aus früheren Studien, oder sich mit Experten der Infrastrukturen in Verbindung setzt, um die relevanten Informationen zu erhalten. In Österreich stellt das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) eine derartige Behörde dar, welche die Betreiber kritischer Infrastrukturen bei der Verbesserung ihres Risiko- und Sicherheitsmanagements unterstützt. In diesem Kontext ist es für das BVT wichtig, Vorfälle im Netzwerk der kritischen Infrastrukturen zu modellieren und deren Folgen für das gesamte Netzwerk zu simulieren.

Daraus können neuralgische Punkte identifiziert werden und kann mit Vorschlägen zur Verbesserung von Sicherheitsmaßnahmen bei den Infrastrukturen präventiv eingreifen.

Zum anderen kann das CERBERUS-System auch von den Betreibern großer kritischer Infrastrukturen eingesetzt werden, die sich einen Überblick über die Zusammenhänge zwischen verschiedenen Teilen ihrer Organisation (z.B. Niederlassungen, Produktionslinien, interne Dienstleistungen usw.) und über die Abhängigkeiten von ihren Lieferanten verschaffen wollen. Bei einem derartigen internen Gebrauch würden weitere Details zu den internen Prozessen, der Systemdynamik und den daraus resultierenden Abhängigkeiten zur Verfügung stehen, die für das CERBERUS-Modell mehr Daten liefern. Somit kann das CERBERUS-System hier wesentlich genauere Aussagen zu wichtigen Prozessen und Leistungen innerhalb der kritischen Infrastruktur und potentiellen Schwachstellen liefern. In einem idealtypischen Umfeld könnten die Daten aus dem internen CERBERUS-System bei einer kritischen Infrastruktur so aufbereitet werden, dass sie direkt in die Analysen der nationalen Behörde einfließen können, wodurch automatisch ein höherer Detailgrad der Informationen gewährleistet werden kann.

Aus beiden Anwendungsbereichen ist eine markante Einschränkung des CERBERUS-Systems direkt ersichtlich: Der Ansatz ist stark datengetrieben und erfordert detaillierte Informationen über die einzelnen Infrastrukturen und deren Abhängigkeiten untereinander sowie über die Folgen bestimmter Ereignisse, genauer gesagt Aussagen über den Schweregrad der Beeinträchtigung einer Infrastruktur bei Ausfällen von Versorgungsstrukturen. Zudem muss die Wahrscheinlichkeitsmatrix, welche die Zustandsübergänge für eine Infrastruktur beschreibt, durch einen oder mehrere Experten geschätzt werden (wofür im Umfeld des Systems geeignete statistische Verfahren entwickelt wurden). Dieses subjektive Element der Modellbildung kann u.U. in der Praxis problematisch sein, ist aber im Allgemeinen nicht nur auf das CERBERUS Modell beschränkt. Die Experten, welche die Informationen innerhalb der einer kritischen Infrastruktur bereitstellen, verfügen möglicherweise nicht genügend Erfahrung oder haben keinen vollständigen Überblick über einen Bereich. Dadurch könnten unvollständige oder fehlerhafte

Datensätze in das System eingebracht werden, was die Genauigkeit der Ergebnisse beeinträchtigt. Im Zuge des Projekts wurde jedoch erkannt, dass eine systematische Auseinandersetzung von ExpertInnen mit den für CERBERUS relevanten Fragestellungen (speziell in Bezug auf die Abhängigkeiten zwischen kritischen Infrastrukturen und deren potentiellen Auswirkungen) wertvolle Informationen liefert und zur Steigerung der Awareness bei den kritischen Infrastrukturen beiträgt. Eine weitere Problematik im Zusammenhang mit den Expertenbefragungen stellt die Sensibilität der benötigten Informationen dar. Hier ist es oft der Fall, dass die Experten nur teilweise oder gar nicht bereit sind, diese an externe Stellen (z.B. nationale Behörden) weiterzugeben. Dies mag zwar im Kontext der Sicherheit begründet sein, beeinträchtigt jedoch die Möglichkeiten der Analyse im CERBERUS-System sowie dessen Ergebnisse.

7 Conclusio

Kritische Infrastrukturen stellen das Rückgrat der meisten Versorgungsstrukturen in der heutigen Gesellschaft dar. Zwischenfälle innerhalb dieser Infrastrukturen, die zu einer Beeinträchtigung oder gar zu einem Ausfall führen können, haben daher weitgehende Auswirkungen. Deshalb ist ein strukturiertes Risikomanagement in diesem Bereich von zentraler Bedeutung.

In diesem Beitrag wurde das CERBERUS-System vorgestellt, welches die Modellierung und Bewertung der Folgen von Kaskadeneffekten in einem Netzwerk kritischer Infrastrukturen unterstützt. Dabei baut das System auf einem mathematischen Modell auf, mit dem Änderungen des Betriebszustandes einer Infrastruktur dargestellt und deren Folgen für den Gesamtverbund simuliert werden können. Die Ergebnisse weisen auf neuralgische Punkte im Zusammenspiel kritischer Infrastrukturen hin, wodurch die Planung von präventiven Maßnahmen sowohl innerhalb der kritischen Infrastrukturen als auch durch die verantwortlichen Regierungsorganisationen unterstützt wird.

Danksagung

Dieser Beitrag wurde durch das FFG/KIRAS Projekt „CERBERUS – Cross Sectoral Risk Management for Object Protection of Critical Infrastructures" (Projekt-Nr. 854766) finanziert.

Literatur

[DuPM06] D. Dudenhoeffer, M.R. Permann; M. Manic: CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. In: Proceedings of the 2006 Winter Simulation Conference. Monterey, USA, 2006, S. 478–485

[EFKW06] A. Ekelhart, S. Fenz, M.D. Klemen, E. Weippl: Security Ontology: Simulating Threats to Corporate Assets. In: A. Bagchi, V. Atluri, (Hrsg.); Information Systems Security. Bd. 4332. Berlin, Heidelberg, S. 249–259, 2006

[Euro08] European Commission: COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In: Official Journal of the European Union (2008), Nr. L345, S. 75–82

[Haim81] Y. Haimes: Hierarchical Holographic Modeling. In: IEEE Transactions on Systems, Man, and Cybernetics Bd. 11 (1981), Nr. 9, S. 606–617

[KöRa17] S. König, S. Rass: Stochastic Dependencies Between Critical Infrastructures. In: SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, IARIA, Ed., 2017, pp. 93–98, ISBN 978-1-61208-582-1, S. 106–110

[Pidd12] H. Pidd: India blackouts leave 700 million without power. URL https://www.theguardian.com/world/2012/jul/31/india-blackout-electricity-power-cuts. abgerufen am 2018-03-21.

[RaHa16] M. Rahnamay-Naeini, M.M. Hayat: Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach. In: IEEE Transactions on Smart Grid Bd. 7 (2016), Nr. 4, S. 1997–2006

[ReSc11] J. Reichl, M. Schmidthaler: Blackouts in Österreich (BlackÖ.1) – Endbericht. Linz, Österreich, 2011.

[Rina04] S. M. Rinaldi: Modeling and simulating critical infrastructures and their interdependencies, in 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the, Big Island, HI, USA, 8 pp, 2004.

[RiPK01] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly: Identifying, understanding, and analyzing critical infrastructure interdependencies. In: IEEE Control Systems Bd. 21 (2001), Nr. 6, S. 11–25

[RSBM15] J. Reichl, M. Schmidthaler, K. de Bruyn, G. Muggenhumer, L. Rebhandl, F. Frank, P. Mayr: Blackoutprävention und -intervention - Endbericht. Linz, Österreich, 2015

[Schw05] Schweizer Bundesbahnen SBB: Nationaler Stromausfall: netzweiter Stromunterbruch auf dem Bahnnetz. https://www.sbb.ch/de/meta/news.html/2005/6/26822.

[Schw14] Schweizer Radio und Fernsehen SRF: Der Blackout 2005 – ein schwarzer Tag für die SBB – News – SRF. URL https://www.srf.ch/news/schweiz/der-blackout-2005-ein-schwarzer-tag-fuer-die-sbb.

[ScRe14] M. Schmidthaler, J. Reichl: Economic Valuation of Electricity Supply Security: Ad-hoc Cost Assessment Tool for Power Outages. In: ELECTRA (2014), Nr. 276, S. 10–15

[SVAB12] S.C. Srivasta, A. Velayutham, K.K. Agrawal, A.S. Bakshi: Report of the Enquiry Committee on Grid Disturbance in Northern Region on 30th July 2012 and in Norther, Eastern and Noth-Eastern Region on 31st July 2012. New Dehli, India: Ministry of Power, Government of India, 2012

[SvWo07] N. Svendsen, S.D. Wolthusen: Connectivity models of interdependency in mixed-type critical infrastructure networks. In: Information Security Technical Report Bd. 12 (2007), Nr. 1, S. 44–55

[WaST12] Z. Wang, A. Scaglione, R.J. Thomas: A Markov-Transition Model for Cascading Failures in Power Grids. In: 2012 45th Hawaii International Conference on System Sciences, 2012, S. 2115–2124