Risikobeurteilung in der IT-Sicherheit Kritischer Infrastrukturen
– Eine Analyse der Risikobeurteilung im Förderschwerpunkt ITS|KRITIS –

Themengebiet: Management von Informationssicherheit – Risiko-Management: Herausforderungen und Lösungen

Gliederung

Einleitung und Motivation

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) bezeichnet jene Organisationen oder Einrichtungen, welche eine wichtige Bedeutung für das staatliche Gemeinwesen ausüben und bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden, als Kritische Infrastrukturen (KRITIS). Da die Störung einer KRITIS weitreichende Folgen mit sich bringt, müssen Maßnahmen ergriffen werden um die Funktionsfähigkeit und damit einhergehend die grundlegende Versorgung der Bevölkerung gewährleisten zu können.

Die Risikobeurteilung in der IT-Sicherheit Kritischer Infrastrukturen bildet dabei ein besonders interessantes und relevantes Thema. Denn die Kosten für die Absicherung gegenüber einer Vielfalt von aktuellen hin zu zukünftigen Bedrohungen sind groß, die potentiellen Schadenssummen sind hoch und der Schaden trifft die Allgemeinheit und nicht ausschließlich die Kritische Infrastruktur. Gleichzeitig fehlen bei kleinen und mittleren Betreibern aber Personal und Ressourcen um existierende Risikobeurteilungsmethoden in der Praxis umzusetzen. Dabei soll gerade die Risikobeurteilung die Brücke zwischen der Analyse und der strategischen Planung von Risiken in einer Organisation schlagen.

Kontext

Das Bundesministerium für Bildung und Forschung (BMBF) fördert, um die IT-Sicherheit von KRITIS voranzutreiben und zu stärken, den Förderschwerpunkt IT-Sicherheit für Kritische Infrastrukturen, ITS|KRITIS. Adressiert werden in dem Förderprogramm nicht nur die großen Betreiber Kritischer Infrastrukturen, sondern insbesondere die kleinen und mittleren Unternehmen (KMU)[Vernetzte IT-Sicherheit Kritischer Infrastrukturen, VeSiKi]. Um die Verbesserung der IT-Sicherheit voran zu bringen, müssen u. a. die Angriffspotentiale – die Bedrohungen und Schwachstellen – der KRITIS-Unternehmen identifiziert und die Risiken bewertet werden. Hierfür werden, laut Vernetzte IT-Sicherheit Kritischer Infrastrukturen, VeSiKi, bereits etablierte, Risikobeurteilungsmethoden verwendet oder neue Vorgehensweisen erforscht. Der Förderschwerpunkt ITS|KRITIS umfasst 12 Forschungsprojekte mit dem Projekt VeSiKi als Begleitforschungsprojekt. VeSiKi behandelt querschnittliche Themen wie z. B. diese projektübergreifende Analyse der Methoden der Risikoanalyse in Kooperation mit den Verbundprojekten. Ein Verbundprojekt das sich beispielsweise mit den potentiell anwendbaren Risikobeurteilungsmethoden von KRITIS-Betreibern auseinander setzt ist das Projekt MoSaIK (Modellbasierte Sicherheitsanalyse von IKT-basierten Kritischen Infrastrukturen).

Ziele des Beitrags

Die Ziele des Beitrags stützten sich auf die Beantwortung folgender Fragen:

1. Welche Risikobeurteilungsmethoden gibt es um die IT-Sicherheit zu untersuchen?
2. Was sind die Bedürfnisse und Herausforderungen der Risikobeurteilung für KRITIS-Betreiber?
3. Welche Risikobeurteilungsmethoden werden in den Projekten verwendet bzw. erforscht? Welchen Nutzen haben diese Methoden für KRITIS?

Normen, Standards und Methoden des Risikomanagements

ISO 31000 – Risikomanagement

Mit dem Standard ISO 31000 wurde eine einheitliche Definition für die Begriffe rund um das Risikomanagement und dessen Prozesselemente festgelegt. Ziel des Standards ist es, für alle Formen des Risikos anwendbar zu sein, sowie Konsistenz und Sicherheit im Risikomanagement zu realisieren. Aus diesem Grund wurden neben dem Glossar auch Leistungskriterien, ein Framework und ein Prozess definiert, nach welchen ein Unternehmen effizientes und nachhaltiges Risikomanagement realisieren kann. Der Standard ist von allen öffentlichen, privaten und gemeinschaftlichen Unternehmen, Vereinigungen, Gruppen oder Individuen anwendbar.[Purdy,2010][Brühwiler, 2008]

Das Risikomanagement-Framework folgt dem Plan-Do-Check-Act Zyklus. Der iterative Ablauf des Frameworks erlaubt es, dass die Integration des Risikomanagements in einem Unternehmen eine kontinuierliche Verbesserung vorweisen kann. Die Durchführungsphase behandelt die Ausführung des Risikomanagement-Prozesses. Dieser Prozess besteht aus fünf Elementen deren Abfolge nicht sequentiell verläuft, sondern die Elemente können mehrfach iteriert werden. Die Bündelung von Risikoidentifikation, -analyse und -bewertung bildet die Risikobeurteilung auf Basis derer erst die Risikobewältigung ins Auge gefasst werden kann. Zusätzlich gelten der Austausch sowie die ständige Kontrolle der Risiken als wesentliche Prozesselemente. Der Zusammenhang zwischen dem Framework, dem Prozess und den einzelnen Prozesselementen ist Abbildung 1 zu entnehmen.[Purdy,2010][Brühwiler, 2008]

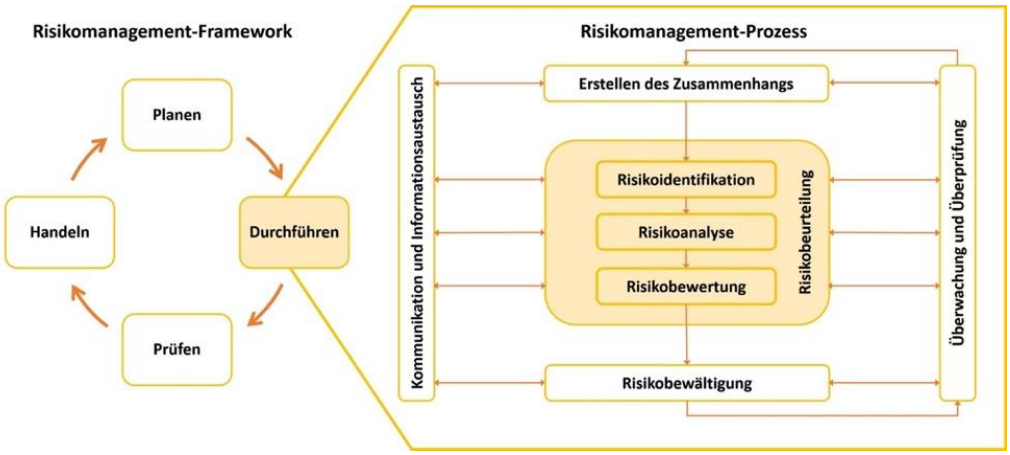

Abbildung 1: Risikomanagement-Framework und Risikomanagement-Prozess nach ISO 31000. Grafik adaptiert von *Brühwiler [2008]*, *Purdy [2010]*.

Risikobeurteilungsmethoden - ISO/IEC 27001 und verwandte Methoden

Ein etablierter Standard ist beispielsweise die Norm ISO/IEC 27001, welche die Realisierung eines Informationssicherheitsmanagementsystems (ISMS) vorsieht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für die Etablierung und Aufrechterhaltung eines ISMS die IT-Grundschutz Methode ausgearbeitet - mehrere Standards und Kataloge sind Inhalt dieser Methode, um ein angemessenes Sicherheitsniveau gewährleisten zu können. ISIS12 ist eine Vorgehensweise entwickelt vom Bayerischen IT-Sicherheitscluster e. V., abgeleitet von dem ISO/IEC 27001 und dem IT-Grundschutz und speziell auf KMUs angepasst, um deren Bedürfnissen nachkommen zu können. Die strategische Bewertung von Risiken sowie eine Planungstechnik um IT-Sicherheit langfristig garantieren zu können bietet vgl. CERT der amerikanische OCTAVE-Ansatz in seinen drei Ausprägungen an. Als Software as a Service werden auch kostenpflichtige Vorgehensmodelle angeboten. Hierzu gehört laut ENISA, beispielsweise RiskSafe Assessment von Squared Limited aus England.

Fazit - Anwendbarkeit von generischen Risikobeurteilungsmethoden

Bereits vorhandene, allgemein gehaltene Beurteilungskriterien zur Schaffung von IT-Sicherheit können zwar nicht mit branchenspezifischen Kriterien auftrumpfen, allerdings sind Methoden vorhanden, die den Einsatz in KMUs ermöglichen und Mindeststandards für die IT-Sicherheit festsetzten. Zu unterscheiden ist bei der Zuordnung von potentiell anwendbaren Methoden in KRITIS-Unternehmen aber, ob die am schnellsten ausgeschöpften Mittel vom Faktor Mensch oder vom Faktor Kapital erzeugt werden. Der organisatorische Gesichtspunkt von ISMS sollte durch den Risikomanagementprozess nach ISO 31000, jedenfalls mit möglichst wenig Ressourceneinsatz, realisierbar sein.

Die Alternativen zur Verwendung von neu entwickelten oder angepassten Risikobeurteilungsmethoden würden OCTAVE-S und ISIS12 für KRITIS mit eingeschränktem Personal und Kapital darstellen. Diese Ansätze wurden für KMUs entwickelt und können von wenigen Mitarbeitern des Unternehmens in kurzer

Zeit durchgeführt werden. Allerdings werden bei diesen Methoden die KRITIS relevanten Bedürfnisse, Herausforderungen sowie gesetzlichen Vorgaben des IT-Sicherheitsgesetztes nicht berücksichtigt. Beispielsweise bietet ISIS12 lediglich eine statische Sichtweise der Bedrohungen, wodurch eine unvollständige Abdeckung der Risiken gegeben ist. Für die KMU unter den Betreibern Kritischer Infrastrukturen ist die Berücksichtigung genannter Faktoren allerdings essentiell. Hier setzt nun die Analyse der Forschung in den Forschungsprojekten des Förderschwerpunkts ITSlKRITIS an. Einige Fragen die daher im nächsten Kapitel des Beitrages untersucht werden sind: „Welchen besonderen Herausforderungen sehen sich die Betreiber Kritischer Infrastrukturen in der Anwendung von Risikomanagement ausgesetzt und welchen nehmen sich die erforschten oder verwendeten Risikoanalysemethoden der Forschungsprojekte an?“, „Wie gehen die Methoden auf branchenspezifische Merkmale ein?“ und „Wie gehen sie mit den limitierten Faktoren Mensch und Kapital um?“.

Methoden der Risikobeurteilung im Förderschwerpunkt ITSlKRITIS

Die in diesem Kapitel herausgegriffen Projekte führen u. a. in ihrer Forschungstätigkeit eine Risikobeurteilung durch oder forschen an einer eigenen, neuen Risikobeurteilungsmethode. Die angewandten oder neu erarbeiteten Methoden und Verfahren werden festgehalten, der Kontext der Risikobeurteilung erfasst und die Ziele der jeweiligen Projekte beschrieben.

Der Ansatz von MosaIK

Das Ziel des Projekts MoSaIK ist die Entwicklung einer Methode sowie von Werkzeugen zu ihrer Anwendung für die effiziente Risikoanalyse und Bewertung des Sicherheitsniveaus Kritischer Infrastrukturen in den Sektoren Energie, Information und Telekommunikation, Wasser, Staat und Verwaltung. Dabei soll der Ressourcenaufwand für den Betreiber minimiert und die Aktualität und Qualität der Bewertung des Sicherheitsniveaus im Vergleich zum derzeitigen Stand deutlich verbessert bzw. eine Bewertung überhaupt erst ermöglicht werden. Aus diesem Grund wurden zunächst die Herausforderungen und Bedürfnisse der Betreiber Kritischer Infrastrukturen an die Vorgehensweisen erhoben. Bei je einem KRITIS-Betreiber wurde eine Methode basierend auf dem IT-Grundschutz bzw. Angriffsbäumen (Attack Trees) durchgeführt und die Erfahrungen dokumentiert. Durch diese Erfahrungen wird eine neue modellbasierte Risikobeurteilungsmethode erforscht. Die Komplexität der Modellierung wird dabei vorwiegend vom Aufbau der Infrastruktur und der späteren Nutzbarkeit durch die KMUs geprägt. Die Methode entsteht mit dem Blick nach innen auf die etablierten Vorgehensweisen und Technologie in den Unternehmen, wodurch die Bedürfnisse, Herausforderungen von KRITIS-Betreibern berücksichtigt werden. Der Einsatz von Werkzeugen und die Erhebung von Messdaten mittels Sensoren soll die Betreiber bei der Durchführung der Methode unterstützen und den Aufwand für die Risikobeurteilung verringern, sowie die Sicherheitsbewertung auf tatsächlichen Daten abstützen.

Der Ansatz von AQUA-IT-Lab

Dieses Verbundprojekt nimmt sich dem KRITIS-Sektor Wasser an. Ziel ist es die IT-Sicherheit durch einen Schnelltest und einem mit Komponenten von Wasserversorgern ausgestattetem Labor analysieren und bewerten zu können. Der Schnelltest setzt sich aus einer angepassten Business Impact Analyse (BIA) und einer Bewertung des IT-Betriebs zusammen. Während die Bewertung des IT-Betriebs die Robustheit adressiert, fokussiert die BIA auf die Resilienz des Unternehmens. Aus beiden Analysen werden Handlungsempfehlungen gewonnen, welche das Sicherheitslevel des Unternehmens möglichst ressourcenschonend verbessern. Der Schnelltest bietet dabei eine sehr personal- und kapitalschonende Variante um eine Risikobeurteilung der unternehmensweiten IT-Sicherheit vorzunehmen. Eine vertiefte Analyse, z.B. in Form eines Penetrations- oder Wiederanlauftests, kann an den Schnelltest anschließend im Labor durchgeführt werden. Hierzu werden ausgewählte unternehmensspezifische Komponenten (Steuerungen, Firewalls, SCADA-Systeme) entweder physisch genutzt oder virtualisiert getestet. Über die Simulatoren ist zudem eine Untersuchung des menschlichen Faktors in puncto Angriffserkennung, -eindämmung sowie Wiederanlauf möglich.

Der Ansatz von PREVENT

PREVENT (Management-Software für präventives Krisen- und Risiko-Management für Rechenzentren systemrelevanter Banken) entwickelt Methoden und Werkzeuge für ein systematisches Risiko- und Compliance-Management, um auf Basis aufeinander aufbauender Risikomodelle situationsgerechte Risikolagebilder für den operationalen Betrieb einer Bank zu berechnen. Vorrangiges Ziel ist es, Risiken, die ihren Ursprung in den technischen Domänen (IT-Sicherheit, Rechenzentrumsbetrieb) haben, auf die Geschäftsprozesse einer Bank abbilden zu können und so ihre Auswirkungen im operationalen Umfeld der Bank bewertbar zu machen. Voraussetzung für ein solches durchgängige Risiko- und Compliance-Management ist die einheitliche Modellierung der IT-Infrastruktur, der Geschäftsprozesse und der jeweiligen Bedrohungsszenarien. In diesem Kontext entwickelt das Projekt innovative Ansätze zur modularen Risikomodellierung, die es erlauben, die sicherheitskritischen Abhängigkeiten zwischen IT-

Infrastruktur, IT-Betrieb und Geschäftsprozessen zu formalisieren, wodurch der Prozess der Risikoberechnung und -aggregation automatisierbar wird. In Kombination mit echtzeitfähigen Risikoindikatoren lassen sich so kontinuierlich Risikolagebilder erstellen, die als situationsgerechte Entscheidungsgrundlage dem Management zur Verfügung stehen. Ergänzend zu den Werkzeugen und Methoden wird ein Prozess für die Umsetzung von Risiko- und IT-Sicherheitsmanagement in Banken bzw. dessen Rechenzentrum definiert, der sich an dem Risikomanagementprozess nach ISO 31000 orientiert. Methoden, Werkzeuge und Prozess ergänzen sich zu einem Framework, mit dem die Finanz- und Versicherungsbranche ein strategisches Werkzeug für ein effizientes IT Risikomanagement an die Hand gegeben werden kann. Banken wie auch die Betreiber eines Bankenrechenzentrums werden so im Falle einer Bedrohung in die Lage versetzt, proaktiv Gegenmaßnahmen zu initiieren.

Konklusion

Die Verbundprojekte des Förderschwerpunktes ITSIKRITIS beschäftigen sich mit der Reduzierung von IT-Sicherheitsproblemen in den KRITIS-Sektoren, durch die Erforschung von neuen IT-Sicherheitslösungen. In diesem Rahmen werden in Forschungsprojekten Risikobeurteilungsmethoden erarbeitet oder bereits bestehende Methoden adaptiert, wodurch auf das entsprechende Anwendungsgebiet zugeschnittene und branchenspezifische Beurteilungsverfahren angeboten werden können.

Die Langversion des Beitrags

Die Langversion dieses Papiers wird vertieft auf die Normen, Standards und Methoden des Risikomanagements, die Anwendbarkeit von generischen Risikobeurteilungsmethoden und die Risikobeurteilungsmethoden der Verbundprojekte im Förderschwerpunkt ITSIKRITIS eingehen. Zudem werden die erhobenen Bedürfnisse und Herausforderungen der KRITIS-Betreiber, welche das Fundament für die erforschten oder adaptieren Methoden bilden, vorgestellt.

Acknowledgements

Die Verbundprojekte des Förderschwerpunktes ITSIKRITIS danken dem BMBF.

Literaturverzeichnis

Bayerischer IT-Sicherheitscluster e. V. ISIS12-Informations-SIcherheitsmanagementSystem in 12 Schritten. URL https://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html. Letzter Zugriff: 16.08.2016.

Brühwiler, B. (2008). Neue Standards im Risikomanagement. Management und Qualität-Das Magazin für integrierte Managementsysteme, 5(2008):26–27. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Kritische Infrastrukturen. URL http://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html . Letzter Zugriff: 17.06.2016.

Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz. URL https://www.bsi.bund.de/cln_174/DE/Themen/ITGrundschutz/itgrundschutz_node.html. Letzter Zugriff: 16.08.2016.

CERT. OCTAVE. URL http://www.cert.org/resilience/products-services/octave/. Letzter Zugriff: 16.08.2016.

ENISA. RiskSafe Assessment. URL https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_risksafe-assessment. Letzter Zugriff: 16.08.2016.

Purdy, G. (2010). ISO 31000: 2009—setting a new standard for risk management. Risk analysis, 30(6):881–886.

Vernetzte IT-Sicherheit Kritischer Infrastrukturen, VeSiKi. Förderschwerpunkt IT-Sicherheit für Kritische Infrastrukturen. URL https://www.itskritis.de/. Letzter Zugriff: 23.06.2016.