Florian Skopik
Tímea Páhi
Maria Leitner *Hrsg.*

Cyber Situational Awareness in Public-Private-Partnerships

Organisationsübergreifende Cyber-Sicherheitsvorfälle effektiv bewältigen

Springer Vieweg

Cyber Situational Awareness in Public-Private-Partnerships

Florian Skopik · Tímea Páhi · Maria Leitner
Hrsg.

Cyber Situational Awareness in Public-Private-Partnerships

Organisationsübergreifende Cyber-Sicherheitsvorfälle effektiv bewältigen

Springer Vieweg

Hrsg.
Florian Skopik
Center for Digital Safety & Security
AIT Austrian Institute of Technology
Wien
Österreich

Maria Leitner
Center for Digital Safety & Security
AIT Austrian Institute of Technology
Wien
Österreich

Tímea Páhi
Center for Digital Safety & Security
AIT Austrian Institute of Technology
Wien
Österreich

ISBN 978-3-662-56083-9 ISBN 978-3-662-56084-6 (eBook)
https://doi.org/10.1007/978-3-662-56084-6

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Geleitwort des BMI

„One of the main cyber-risks is to think they don't exist." (Stephane Nappo); Die Staaten und die postindustriellen Gesellschaften des 21. Jahrhunderts sind in einem stetig steigenden Ausmaß von den Leistungen und Diensten der modernen Informationstechnik abhängig. Informationstechnik durchdringt zunehmend auch – und vor allem – Bereiche, die für das Funktionieren des Staates und die Sicherstellung der Daseinsvorsorge der Bevölkerung unverzichtbar geworden sind. Erfolgreiche Angriffe auf diesbezügliche Systeme können signifikante Auswirkungen auf Staat, Wirtschaft, Wissenschaft und Gesellschaft haben.

Gleichzeitig sind im Bereich der Netz- und Informationssicherheit besorgniserregende Tendenzen zu beobachten. Hochentwickelte Schadsoftwareprodukte dringen in vermeintlich sichere staatliche Netze ein, Verschlüsselungssoftware legt hunderttausende Systeme, darunter das britische Gesundheitssystem, lahm und Myriaden von billig produzierten, potenziell unsicheren Internet-of-Things-Geräten überschwemmen den Markt. Diese und ähnliche Herausforderungen können nur dann erfolgreich bewältigt werden, wenn Staat und Gesellschaft ein hohes Maß an Resilienz aufbauen und aufrechterhalten können.

Die europäische Union hat diese Herausforderungen erkannt und mit einer Richtlinie zur Erhöhung des Sicherheitsniveaus von Netz- und Informationssystemen in der Union einen ersten wichtigen Schritt gesetzt. Diese Richtlinie wird in der ersten Jahreshälfte 2018 durch das österreichische Netz- und Informationssystemsicherheitsgesetz (NISG) umgesetzt. Dieses sieht Maßnahmen vor, um Cyber-Sicherheit zu gewährleisten und die Resilienz zu steigern. Dazu gehören, neben der Schaffung einer Cyber-Sicherheitsstrategie und der Etablierung einer eigenständigen Behörde für Netz- und Informationssicherheit, auch eine Reihe von Anforderungen an die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste.

Das Cyber Security Center (CSC) im Bundesministerium für Inneres wird mit dem In-Kraft-Treten des NISG die Aufgaben der operativen NIS-Behörde wahrnehmen. Dies umfasst im Wesentlichen den Betrieb einer Melde-Sammelstelle für sicherheitsrelevante Vorfälle und die Koordination von verpflichtenden Sicherheitsaudits bei betroffenen Unternehmen. Gleichzeitig fungiert das CSC als Schnittstelle zu vergleichbaren Einrichtungen in den europäischen Partnerstaaten. Die operative NIS-Behörde weist in diesem Zusammenhang eine besondere Stellung innerhalb der österreichischen Cyber-Sicherheitsstruktur

auf. Während betroffene Unternehmen nur den jeweils eigenen Bereich kennen und sektorspezifische Computer-Notfallteams lediglich den eigenen Sektor überblicken, nimmt das CSC einen österreichweiten, sektorübergreifenden Blickwinkel ein. Dies ermöglicht die Erstellung eines gesamtstaatlichen Lagebildes, das Grundlage für gegebenenfalls zu treffende Maßnahmen ist.

Doch weder die operative NIS-Behörde, noch die anderen staatlichen Gremien im Bereich der Cyber-Sicherheit sind alleine in der Lage, eine hohe Resilienz aufzubauen und aufrecht zu erhalten. Dazu bedarf es einer gemeinsamen Anstrengung aller im Bereich der Cyber-Sicherheit tätigen, staatlichen und privaten Stakeholder. Vertrauen, Kooperation und Informationsaustausch zwischen all diesen Einrichtungen werden der Schlüssel zu einer erfolgreichen Bewältigung dieser Anforderungen sein. Österreich ist auf einem guten Weg.

DI Philipp Blauensteiner
Leiter des Cyber Security Centers
Bundesministerium für Inneres
Österreich

Geleitwort des BMLV

Als „Cyber-Koordinator des Bundesministeriums für Landesverteidigung“ und Kommandant des „Kommandos Führungsunterstützung & Cyber Defence (KdoFüU&CD)“ bin ich dem Ersuchen, ein Geleitwort zu diesem hochaktuellen und praxisbezogenem Buch zu verfassen, sehr gerne nachgekommen. Dies umso mehr, als zwischen dem Österreichischen Bundesheer (ÖBH) und dem Austrian Institute of Technology (AIT) eine intensive Kooperation im Rahmen der Plattform KSÖ sowie diverser Forschungsprojekte, wie es beispielsweise das im Buch dargestellte Forschungsprojekt **Cyber Incident Situational Awareness (CISA)** ist, besteht.

Die Verfasser sprechen mit ihrem Buch ein hochaktuelles Thema an. Ein Thema, dass wegen seiner Signifikanz nicht nur für Forscher und Wissenschaftler, sondern auch für facheinschlägig interessierte Mitarbeiter von Behörden, Dienststellen im öffentlichen wie auch von Unternehmen des privaten Sektors, von höchstem Interesse sein muss.

Die Cyber-Attacken auf die RUAG 2015 in der Schweiz, oder der Ende 2017 erkannte Angriff einer Hackergruppe auf den Informationsverbund Berlin – Bonn (IVBB), verdeutlichen die Gefahren aus dem Cyberraum, der sich unsere IKT-Infrastruktur trotz großer Sicherheitsanstrengungen ausgesetzt sieht. Es geht in diesem Cyberraum gleichermaßen um innerstaatliche Bedrohungen, wie auch um grenzüberschreitende Cyber-Angriffe aus einem über die virtuellen Staatsgrenzen hinausreichenden Raum. Zur Feststellung und Analyse von Bedrohungen ist ein klares und umfassendes Lagebild eine „conditio sine qua non“. Nur so können zeitgerecht klare, nachvollziehbare, lageangepasste und rechtlich haltbare Entscheidungen getroffen werden. Dies gilt für Cyber Security, Cyber Crime wie auch für uns im Cyber Defence-Bereich in gleichem Maße.

Aufgrund dieser Erkenntnis hat Österreich im Rahmen der Umsetzung der Netz- und Informationssicherheitsrichtlinie der EU in Form des NIS-Gesetzes (derzeit im Entwurf vorliegend) sowie der konsequenten Umsetzung der EU Datenschutzgrundverordnung (DSGVO) sowohl für die kritische Infrastruktur als auch die nationalen Behörden die Grundlagen für ein entsprechendes Sicherheitsniveau nach „lege artis“ geschaffen. Gleichsam wurde selbige als Teil der gesamtstaatlichen Sensorik verpflichtet.

Das Ziel des Forschungsprojektes CISA war es, aus den durch die Sensorik bereitgestellten Informationen ein Lagebild zu generieren. Dieses soll ebenenadäquat Informationen in Bezug auf Cyber-Angriffe auf überwachte Systeme bereitstellen. Die Bearbeitung

des Projektes erfolgte in Kooperation zwischen AIT und einer Vielzahl von Unternehmen aus dem privaten und öffentlichen Bereich, nicht zuletzt unserem Bundeministerium für Landesverteidigung, welches gerade infragen der Lagebildgenerierung und faktenbasierter Entscheidungsfindungsprozesse eine besondere Expertise aufweist.

Es sind Forschungsprojekte wie CISA, die besonders geeignet sind, Cyber Awareness ebenenübergreifend und gesamtstaatlich zu schaffen, um so den Herausforderungen in der Cyber-Domäne in all ihrer Hybridität als ein „Whole of Nation" entgegenzutreten.

Mit dem vorliegenden Buch spannen die Autoren in sehr übersichtlicher Art und Weise den Bogen von der Notwendigkeit eines Situationsbewusstseins und der Erstellung von Cyber-Lagebildern sowie dem organisationsübergreifenden Austausch sicherheitsrelevanter Informationen als Grundlage für Cyber-Lagebilder bis hin zur Thematik von nationalen Strukturen und Prozessen zur Erstellung von Cyber-Lagebildern, den Informations- und Meldepflichten sowie dem Datenschutz in „Public Private Partnerships".

Die bisherigen Maßnahmen sind wichtige und richtige Schritte, um die dringend notwendige nationale Fähigkeitsentwicklung voranzutreiben – sie ein substanzieller Teil eines umfassenden Ansatzes zur Verbesserung der Resilienz unseres Staates gegenüber Cyber-Bedrohungen zu betrachten. Bedrohungen, denen wir uns in bewährter Art und Weise im breiten kooperativen Ansatz stellen: Behörden, Wissenschaft, Industrie und Wirtschaft gemeinsam – für Österreich.

In diesem Sinne wünsche ich allen Leserinnen und Lesern viel Freude und vor allem nachhaltigen Erkenntnisgewinn beim Studium dieses Buchs.

Generalmajor
Ing. Mag. Hermann KAPONIG
Österreichisches Bundesheer
Kommando Führungsunterstützung & Cyber Defence (KdoFüU&CD)

Geleitwort des BKA

Die Gewährleistung eines hohen Maßes an Sicherheit von Netz- und Informationssystemen auf nationaler und internationaler Ebene ist eine der obersten Prioritäten Österreichs und eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft. So ist das Funktionieren kritischer Infrastrukturen heute in hohem Ausmaß von verschiedenen Technologien und deren Zusammenspiel abhängig. Sie sind zu einer „Hauptschlagader" von Wirtschaft und Gesellschaft geworden, Ausfälle können daher entsprechend schwerwiegende Folgen zeitigen.

Die vielen positiven Ausprägungen und Entwicklungen der Digitalisierung laufen einher mit einer zunehmenden Gefahrenlage, die sich aus dem Cyber Raum ergibt. Diese Schattenseite der fortschreitenden Digitalisierung ist von ständig wandelnden Bedrohungen gekennzeichnet und entwickelt sich in einem hohen Tempo weiter. Eine steigende Komplexität und Interdependenz der eingesetzten Technologien schafft immer wieder neue Angriffspotenziale für Kriminelle, wobei Angreifer nicht aufhören werden, das Internet permanent weiter für kriminellen Zwecke zu missbrauchen.

Der Staat darf in diesem Zusammenhang niemals nachlassen, mit der Wirtschaft und Forschung zusammen die Veränderungsprozesse, die sich aus der zunehmenden Digitalisierung ergeben, im Interesse der Bürgerinnen und Bürger zu bewerten, aktiv zu gestalten und zeitgerechte Rahmenbedingungen zu schaffen. Dabei nimmt die Gewährleitung der Sicherheit eine zentrale Stellung ein. Um der äußerst komplexen Bedrohungslage und den Herausforderungen im Cyber Bereich entgegenzutreten, gibt es eine wachsende Anzahl politischer Programme und Strategien auf europäischer und nationaler Ebene. Wichtige Punkte sind auf europäischer Ebene insbesondere die NIS-Richtlinie und die Datenschutz-Grundverordnung. Auf nationaler Ebene sind die Österreichische Strategie für Cyber Sicherheit (ÖSCS), das Netz- und Informationssystemsicherheitsgesetz und das österreichische Programm zum Schutz kritischer Infrastrukturen (APCIP) essenziell.

Als sehr positive Entwicklung sei zudem die vom Bundeskanzleramt als Public-private-Partnership ins Leben gerufene „Cyber Sicherheit Plattform" (CSP) genannt, die sich als die zentrale Plattform Österreichs für die Kooperation zwischen dem privaten und öffentlichen Sektor in Sachen Cyber Sicherheit und dem Schutz kritischer Infrastrukturen etabliert hat. Sie hat sich durch das Engagement der Teilnehmerinnen und Teilnehmer nicht nur zu der Plattform für den Informationsaustausch zu aktuellen Fragen der Cyber

Sicherheit entwickelt, sondern sogar zu einem Impulsgeber, zu einem Think Tank für künftige Herausforderungen.

Die derzeit wohl wichtigste Aufgabe in Österreich ist die Umsetzung der NIS-Richtlinie durch das Netz- und Informationssystemsicherheitsgesetz. Mit einer von allen Seiten akzeptierten legistischen Grundlage und den Umsetzungen der dafür notwendigen Einrichtungen und Prozesse werden die nächsten Schritte in Richtung eines gesamtstaatlichen Ansatzes für die Cyber Sicherheit in Österreich unternommen. Mit der Umsetzung der NIS-Richtlinie wird in Österreich ein nationaler Rahmen mit entsprechenden Organisations- und Koordinierungsstrukturen für Cyber Sicherheit eingerichtet. Die Erstellung eines gesamtheitlichen Lagebildes für Österreich, welches einen wesentlichen Beitrag für die Cyber Sicherheit leisten wird, soll in diesen Organisations- und Koordinierungsstrukturen stattfinden.

Diesbezüglich ist hervorzuheben, dass der Sicherheitsforschung im Nachgehen der Frage, wie Cyber Sicherheit gesamtstaatlich effizient und wirkungsvoll gestaltet werden kann, hohe Bedeutung zukommt. So stellen insbesondere KIRAS Forschungsprojekte einen wichtigen Teil des Diskurses zu Sicherheit in Österreich dar. Projekte wie CISA sowie weitere aktuelle Forschungsprojekte sind ein Musterbeispiel dafür, wie das Zusammenwirken privater und öffentlicher Stakeholder gesamtstaatliche Ansätze schaffen kann, indem die Inhalte der KIRAS Projekte laufend mit staatlichen Bedarfsträgern diskutiert und abgeglichen werden. So finden die Ergebnisse Einzug in die staatlichen Planungsinstrumente und leisten damit einen unschätzbaren Beitrag in der Gestaltung eines widerstandsfähigen Österreich.

Nach Umsetzung der NIS-Richtlinie wird es um eine schrittweise intelligente Verbesserung der österreichischen Cyber Sicherheitsarchitektur gehen, bei welcher wissenschaftliche Projekte und Beiträge, wie zum Beispiel in Form dieses Buches, weiterhin eine gesamtstaatlich wichtige Rolle einnehmen werden.

DI Franz Vock
Cyber Security Koordinator
Bundeskanzleramt Österreich

Vorwort der Herausgeber

Advanced Persistent Threats und State-sponsored Hacks stellen neue Formen der Bedrohung für Organisationen dar, deren Geschäfte maßgeblich über das Internet abgewickelt werden. Aber auch „low profile"-Angriffe, welche sich vorgefertigter Tools und Schadsoftware bedienen, werden immer ausgefeilter – denn auch die Angriffsflächen moderner hochkomplexer IKT Infrastrukturen wachsen von Jahr zu Jahr. Das Kompromittieren von Webseiten, Attackieren von Diensten oder Ausspionieren vertraulicher Firmeninformationen steht bei diesen Angriffen im Mittelpunkt. Die Motivation dazu ist oft vielfältig geprägt und umspannt von der Erlangung wirtschaftlicher Vorteile bis hin zur Schädigung aus politischen oder religiösen Motiven mannigfaltige Facetten. Je wichtiger das Funktionieren digitaler Dienste für unsere Gesellschaft wird, desto eher gelangen diese Dienste auch ins Visier von Wirtschaftskriminellen, Spionen, Terroristen und staatsfeindlichen Gruppierungen. Um diesen Bedrohungen angemessen zu begegnen, haben viele Staaten umfangreiche nationale Cyber-Sicherheitsstrategien erarbeitet und umgesetzt. Waren bis vor kurzem überwiegend privatrechtlich geführte Computer Emergency Response Teams (CERTs bzw. CSIRTs) alleinige Mittel, um organisationsübergreifend für Sicherheit zu sorgen, haben Staaten nun bereits sehr intensiv damit begonnen, ihre Rolle beim Schutz nationaler kritischer Infrastrukturen und essenzieller Dienste vor Cyber-Bedrohungen einzunehmen. Cyber Security Centers und Cyber Defense Centers werden von staatlichen Institutionen zunehmend genutzt, um anfänglich genannten Bedrohungen angemessen zu begegnen. Eine der Hauptaktivitäten ist dabei die enge Vernetzung aller Beteiligten, v.a. auch bestehender CERTs bzw. CSIRTs, und der rege Informationsaustausch über aktuelle Bedrohungen, sowie der – bis zu einem gewissen Grad verpflichtende – Informationsaustausch über Sicherheitsvorfälle.

Die Europäische Union hat mit der Erlassung der NIS-Richtlinie (Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union) und der daraufhin in den Mitgliedstaaten begonnenen Umsetzung in nationales Recht einen wichtigen Grundstein für die Etablierung der zur Gewährleistung der Cyber-Sicherheit erforderlichen Strukturen geschaffen. Ein wichtiger Meilenstein dabei ist die Einrichtung sog. NIS-Behörden. Gleichzeitig bringt aber dieser wichtige Schritt eine ganze Reihe neuer Herausforderungen mit sich – nicht nur für wenige, sondern für alle Unternehmen, die entweder kritische Infrastrukturen betreiben

oder aber digitale Dienste bereitstellen. Naturgemäß gibt es, wie bei allen weitreichenden Veränderungen der Rahmenbedingungen, Unsicherheiten in Bezug auf die Umsetzung der Richtlinie und folglich Realisierung der zuvor genannten NIS-Behörden zum Informationsaustausch. Während ihre Rollen grob in der NIS-Richtlinie umrissen sind, ist noch weitgehend unklar, wie weit die Kompetenzen im Detail gehen sollen und v.a. wie die Ausgestaltung ihrer Arbeit im Alltag aussehen wird. Die Schnittstellen zwischen Organisationen und staatlichen Einrichtungen, die Art der ausgetauschten Informationen, die dafür erforderlichen Prozesse auf Seiten der Organisationen, aber auch des Staates werden derzeit breit diskutiert.

Durch den regen Austausch sicherheitsrelevanter Informationen zwischen Unternehmen und dem Staat sollen dabei Cyber-Lagebilder auf nationaler Ebene entstehen, um die Erkennung, Analyse und Bewältigung von Cyber-Angriffen zu unterstützen. Während die Umsetzung dieser Vision im Großen und Ganzen intuitiv erscheint, ist die konkrete Ausgestaltung dieser Vernetzung noch weitgehend offen. In diesem Kontext ist auch die verschärfte Datenschutzproblematik durch Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) zu sehen. Die daraus resultierenden Spannungen aufgrund des für die Gewährleistung der Sicherheit erforderlichen Informationsaustauschs zwischen Organisationen einerseits und des Datenschutzes von potenziell personenbezogenen Daten andererseits sollen im vorliegenden Buch näher beleuchtet werden.

Dieses Buch behandelt den Themenkomplex des Situationsbewusstseins in Public-Private Partnerships (PPP) und richtet sich an eine breite Leserschaft: Personen der öffentlichen Verwaltung und der Industrie, die mit Aufgaben im Sicherheitsmanagement betraut sind, sowie alle Leserinnen und Leser, die generell am Thema Cyber-Situationsbewusstsein interessiert sind. Das Buch kann von Dozentinnen und Dozenten im Bereich Cyber-Sicherheit und Public Administration an Universitäten und Hochschulen, sowie Studentinnen und Studenten genutzt werden.

Das breite Themenfeld, an dem Cyber-Situationsbewusstsein anknüpft, spiegelt sich auch im Inhalt des Buches wider.

- Kap. 1 befasst sich mit dem Aufbau und der Nutzung von Cyber-Situationsbewusstsein und wie dies auf nationaler Ebene mit Cyber-Sicherheitsstrategien umgesetzt werden kann. Ein weiterer Aspekt ist die Umsetzung von Cyber-Situationsbewusstsein in nationalen Cyber-Lagezentren und die Verwendung von Cyber-Lagebildern.
- Kap. 2 beleuchtet den organisationsübergreifenden Informationsaustausch zu Cyber-Sicherheitsvorfällen zwischen Cyber-Lagezentren und Stakeholdern. Es beschreibt wie Erkennung und Abwehr von Angriffen durch Informationsaustausch maßgeblich verbessert werden können.
- Nationale Strukturen und Prozesse zur Erstellung von Cyber-Lagebildern werden in Kap. 3 beschrieben. Dabei werden der Informationsfluss und die Management-Prozesse zwischen Cyber-Lagezentren und anderen Stakeholdern, wie zum Beispiel Meldeprozesse im Rahmen der NIS-Richtlinie, beschrieben.

- Mit rechtlichen Informations- und Meldepflichten in PPPs befasst sich Kap. 4. Insbesondere werden Meldepflichten in Bezug auf die NIS-Richtlinie, Datenschutzrecht und Telekommunikationsrecht analysiert.
- Kap. 5 beleuchtet den Datenschutz in PPPs. Meldepflichten und -prozesse können in den Datenverarbeitungen und Datenübermittlungen auch personenbezogene Daten enthalten und daher ist die Frage des Datenschutzes auch innerhalb von Cyber-Lagezentren zu stellen.
- In Kap. 6 werden mögliche Informations- und Datenquellen für Cyber-Lagebilder beschrieben. Zusätzlich werden Kriterien zur Bewertung von Informations- und Datenquellen definiert, um die Qualität der Informationen in Cyber-Lagebildern beurteilen zu können.
- Kap. 7 beschreibt Informationsanalysekonzepte zur Erstellung von Cyber-Lagebildern in PPPs. Das Konzept beschreibt eine Architektur, die eine Aggregation aus multiplen Datenquellen und die Datenaufbereitung für Lagebilder in Cyber-Lagezentren unterstützt und den gesamten Datenlebenszyklus berücksichtigt.
- Die Evaluierung von Cyber-Situationsbewusstsein im praktischen Einsatz wird in Kap. 8 anhand einer Planspielübung gezeigt. Eine Übung ermöglicht künftigen Operateuren in Lagezentren, in simulierten Situationen Cyber-Situationsbewusstsein zu bilden und eine Lagebeurteilung vorzunehmen.

Diese Übersicht zeigt, dass die Herstellung von Cyber-Situationsbewusstsein viele Aspekte beinhaltet und dieses Buch einen Beitrag zur Forschung und Entwicklung in diesem Bereich leistet.

Wien, April 2018

Florian Skopik
Timea Pahi
Maria Leitner

Inhaltsverzeichnis

Über die Herausgeber

Dr. Dr. Florian Skopik, CISSP, CISM, CCNP-S leitet das Sicherheitsforschungsprogramm am AIT Austrian Institute of Technology, wo er gemeinsam mit seinem 40-köpfigen Team an nationalen und internationalen Forschungsprojekten in den Bereichen Schutz kritischer Infrastrukturen, Anomalieerkennung in Rechnernetzen, Threat Intelligence, Risikomanagement und Kryptographie arbeitet.

Bevor er zu AIT kam, war er von 2007 bis 2011 an der Technischen Universität Wien als wissenschaftlicher Mitarbeiter und Postdoktorand tätig, wo er an einer Reihe internationaler Forschungsprojekte zu Web-basierten Collaboration Systems beteiligt war. In dieser Zeit promovierte er auch in Informatik (Dr. techn.) und Sozial- und Wirtschaftswissenschaften (Dr. rer.soc.oec). Er verbrachte mehrere Monate als Expert Advisor bei IBM Research India in Bangalore. Er veröffentlichte mehr als 100 wissenschaftliche Konferenzbeiträge und Zeitschriftenartikel, sowie mehrere Bücher, und ist Mitglied verschiedener Konferenzprogrammkomitees und Standardisierungsgruppen wie ETSI TC Cyber und OASIS CTI. Er hält außerdem etliche branchenrelevante Sicherheitszertifikate, darunter Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), CCNP Security und ISO27001 Information Security Manager, und ist registrierter Subject Matter Expert der ENISA für die Themen „*new ICTs and emerging application areas*“ und „*Critical Information Infrastructure Protection (CIIP) and CSIRTs cooperation*“.

Florian Skopik ist IEEE Senior Member, Mitglied der Association for Computing Machinery (ACM), Member of the International Information System Security Certification Consortium (ISC)², und Member of the International Society of Automation (ISA).

Timea Pahi, BSc, BA ist Junior Scientist im Sicherheitsforschungsprogramm des Centers for Digital Safety & Security am AIT Austrian Institute of Technology. Timea ist Ingenieurin für IT-Sicherheit und hat ihren zweiten Abschluss in Sicherheits- und Verteidigungsstudien. Sie arbeitet derzeit an mehreren Forschungsprojekten und Publikationen, die sich auf nationale Cybersicherheit, Cyber-Situationsbewusstsein, Cyber-Lagebilderstellung, Analyse von professionellen Cyber-Angriffen und deren Taktiken, Techniken und Verfahren (TTPs) konzentrieren. Ihre aktuellen Forschungsinteressen umfassen Threat Intelligence, Penetration Testing und die die Erstellung von realistischen Angriffssimulationen (sog. Cyber Security Übungen in Cyber Ranges) sowohl auf Organisationsebene als auch auf staatlicher Ebene.

© by Johannes Zinner

Dr. Maria Leitner ist Scientist in der Forschungsgruppe Cyber Security im Center for Digital Safety & Security am AIT Austrian Institute of Technology. Dr. Leitner koordiniert und arbeitet in nationalen und internationalen Forschungsprojekten im Bereich Situationsbewusstsein, Schutz von kritischen Infrastrukturen und Identitätsmanagement. Im Bereich Situationsbewusstsein beschäftigt sie sich mit der Gestaltung von Cyber Lagebildern, Cyber Security Übungen und deren technischer Umsetzung in Cyber Ranges, d. h. in simulierten komplexen IKT-Infrastrukturen. Dr. Leitner ist unter anderem in der Arbeitsgruppe 5 „Education, training, awareness, exercise“ in der European Cyber Security Organisation (ECSO) und der Cyber Sicherheit Plattform Austria tätig. Sie ist Mitglied bei ACM sowie IEEE und hat über 25 referierte Journal-, Konferenz- und Workshopartikel veröffentlicht.

Das Konzept von Situationsbewusstsein und Cyber-Lagebildern

1

Maria Leitner, Timea Pahi und Florian Skopik

Zusammenfassung

Situationsbewusstsein beschäftigt sich mit der Wahrnehmung und dem Verstehen einer Situation sowie der Prognose dieser. Dieses Situationsbewusstsein wird auch im Cyber Raum immer wichtiger, um die aktuelle Lage einschätzen und bewerten zu können. Oftmals wird dies als Cyber-Situationsbewusstsein bezeichnet. Dieses Kapitel beschreibt umfassende Aspekte zur Herstellung von Cyber-Situationsbewusstsein und zeigt, dass nicht nur technische Aufgaben, sondern auch organisatorische Voraussetzungen zur Herstellung benötigt werden. Als Grundlage werden wissenschaftliche Modelle zur Herstellung von Cyber-Situationsbewusstsein analysiert und verglichen. Dies zeigt wie erste kognitive Modelle in technische Modelle adaptiert wurden, um Menschen immer mehr bei der Verarbeitung von Informationen zur Erkennung der Lage zu unterstützen. Darauf aufbauend werden Cyber-Sicherheitsstrategien beschrieben, die zur Umsetzung von Situationsbewusstsein auf nationaler Ebene beitragen können. Cyber-Sicherheitsstrategien umfassen häufig die Umsetzung von Cyber-Lagezentren. Dazu werden übliche Aufgaben und Verantwortlichkeiten von Lagezentren sowie der Austausch mit Stakeholdern definiert. Cyber-Lagezentren nutzen diverse Cyber-Lagebilder, um gesammelte Informationen über Situationen über definierte Zeiträume nachvollziehbar darzustellen. Sie sind daher ein wichtiges Hilfsmittel zur Bewertung von Situationen und Herstellung von Cyber-Situationsbewusstsein.

M. Leitner (✉) · T. Pahi · F. Skopik
Center for Digital Safety & Security, AIT Austrian Institute of Technology, Wien, Österreich
e-mail: maria.leitner@ait.ac.at; timea.pahi@ait.ac.at; florian.skopik@ait.ac.at

F. Skopik et al. (Hrsg.), *Cyber Situational Awareness in Public-Private-Partnerships*,
https://doi.org/10.1007/978-3-662-56084-6_1

1.1 Einleitung

Situationsbewusstsein, d. h. sich der aktuellen Lage bewusst zu sein, ist ein immer wichtiger werdendes Instrument in den Informations- und Kommunikationstechnologien (IKT) geworden. Oftmals wird Cyber-Situationsbewusstsein auf das Bewusstsein der Lage in der Cyber-Domäne angewendet. Individuen, nationale und internationale Organisationen sowie Nationen benötigen Cyber-Situationsbewusstsein. Zum Beispiel können Organisationen ein umfangreiches Lagebild über den aktuellen Stand der eigenen IKT Infrastruktur kennen und ob es Cyber-Vorfälle oder -Ereignisse derzeit in der Infrastruktur gibt. Auf staatlicher Ebene geht es bei Cyber-Situationsbewusstsein jedoch eher z. B. um den Ausfall kritischer Services für Bürgerinnen und Bürger und wie Informationsaustausch bei stärkeren Cyber-Vorfällen mit diversen Stakeholdern erleichtert werden kann. Dieses Kapitel zielt darauf ab einen umfassenden Überblick über Situationsbewusstsein zu geben, insbesondere dessen Ursprung und wie Situationsbewusstsein im Bereich der Informationssicherheit und Cyber-Sicherheit angewandt werden kann.

Abschn. 1.2 beschäftigt sich mit dem Hintergrund und der Definition von Situationsbewusstsein. Weiterführend beschreibt Abschn. 1.3 den aktuellen Stand der Technik anhand einer Auflistung relevanter Situationsbewusstseinsmodelle, die kognitive und technische Ansätze verfolgen.

Zur Sicherung der Cyber-Landschaft wird eine internationale Koordination als auch Kooperation insbesondere aufgrund der hohen Vernetzung der Stakeholder, Strukturen und IT-Landschaften immer wichtiger. Konventionelle Strategien benötigen eine globale Sichtweise zur Stabilisierung und Sicherung der Cyber-Landschaft. Dieser Paradigmenwechsel spiegelt sich auch eindeutig in den nationalen und internationalen Cyber-Sicherheitsstrategien der letzten zehn Jahre wider. Das Abschn. 1.4 behandelt daher Beispiele nationaler Cyber Security Strategien in Deutschland, Österreich und der Schweiz.

Ein gemeinsamer Nenner aller Strategien für Cyber-Sicherheit ist die empfohlene Realisierung von Kompetenzzentren, z. B. als Cyber-Lagezentren, Computer Emergency Response Teams (CERT) oder Computer Security Incident Response Teams (CSIRT), auf nationaler Ebene. Ein nationales Cyber-Lagezentrum soll als vertrauenswürdiger Dritter agieren und zum Beispiel den Informationsaustausch zwischen öffentlichen und privaten Organisationen koordinieren. Im Abschn. 1.5 werden Merkmale und mögliche Aufgaben von Cyber-Lagezentren beschrieben und Beispiele von existierenden nationalen Cyber-Lagezentren gebracht.

In Abschn. 1.6 wird der Lagebildbegriff erörtert. Abhängig vom Zweck und der Nutzung eines Lagebildes kann es verschiedene Eigenschaften aufweisen, z. B. Lagebilder der Flugüberwachung, der IKT Infrastruktur oder der Cyber-Vorfälle. Diese verschiedenen Aspekte werden unter dem Begriff der Dimensionen zusammengefasst und analysiert. Zusätzlich werden auch Beispiele für Lagebilder beschrieben. Abschn. 1.7 fasst die wichtigsten Ergebnisse zusammen.

1.2 Situationsbewusstsein

Im Bereich Cyber-Sicherheit spielt Situationsbewusstsein (*situational awareness*[1] in Englisch, abgekürzt SA) eine immer wichtigere Rolle für Organisationen und Staaten. Es existieren bereits viele Definitionen zu Situationsbewusstsein (siehe Tab. 1.1) und bis zum Jahr 1995 sind alle in der Tabelle angeführten Definitionen militärischen Ursprungs.

Tab. 1.1 Definitionen zu Situationsbewusstsein

Jahr	Auszug	Quelle
1987	„*Situation awareness is knowledge of current and near-term disposition of both friendly and enemy forces within a volume of airspace.*“	Hamilton 1987
1988	„*The authors distinguish four SA dimensions from a collection of definitions: where, what, when, and who. Where refers to spatial awareness, what characterizes identity awareness, who is associated with responsibility or automation awareness, and when signifies temporal awareness.*“	Harwood et al. 1988
1991	„*Situational awareness is principally (though not exclusively) cognitive, enriched by experience*“	Hartman und Secrist 1991
1992	„*SA is a pilot's (or aircrew's) continuous perception of self and aircraft in relation to the dynamic environment of flight, threats, and mission, and the ability to forecast, then execute tasks based on that perception. It is problem solving in a three-dimensional spatial relationship complicated by the fourth dimension of time compression, where there are too few givens and too many variables.*“	Carroll 1992
	„*Situation Awareness refers to the ability to rapidly bring to consciousness those characteristics that evolve during a flight.*“ „*Notice that the ‚evolve' part of this definition excludes other information, like declarative and procedural knowledge, that may be rapidly brought to mind. Notice too that ‚the ability to bring' allows SA to refer to things that may not at that moment be in consciousness (or working memory, if you choose). But you have to be able to grab them when you need them.*“	Wickens 1992

[1] Die beiden Begriffe „situation awareness“ und „situational awareness“ werden in diesem Dokument gleichwertig behandelt. Oftmals wird in älteren Publikationen von „situation awareness“ gesprochen, jedoch wird in aktuelleren Publikationen oft „situational awareness“ referenziert.

Tab. 1.1 (Fortsetzung)

Jahr	Auszug	Quelle
	„*Although situation awareness contributes to good performance, it is not synonymous with it. It is possible to have good SA and still not be a good pilot because of poor motor skills, co-ordination or attitude problems. Conversely, under automated flight conditions it is possible to have good performance with minimal SA.*“	Tenney et al. 1992
	„*One's ability to remain aware of everything that is happening at the same time and to integrate that sense of awareness into what one is doing at the moment.*“	Haines und Flateau 1992
1995	*SA is* „*an abstraction that exists within our minds, describing phenomena* that *we observe in humans performing work in a rich and usually dynamic environment.*“	Billings 1995
	„*SA provides ‚the primary basis for subsequent decision making and performance in the operation of complex, dynamic systems …' At its lowest level the operator* needs *to perceive relevant information (in the environment, system, self, etc.), next integrate the data in conjunction with task goals, and, at its highest level, predict future events and system states based on this understanding.*“ „*… the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.*“	Endsley 1995
	„*SA requires an* operator *to ‚quickly detect, integrate and interpret data gathered from the environment.*“	Green et al. 1995
	„*Situation awareness is adaptive, externally-directed consciousness that has as* its *products knowledge about a dynamic task environment and directed action within that environment.*“	Smith und Hancock 1995
1997	„*SA means that a human appropriately responds to important informational cues. This definition contains four key elements: (1) humans, (2) important informational cues, (3) behavioral cues, and (4) appropriateness of the responses. Important informational cues refer to environmental stimuli that are mentally processed by the human.*“	Dalrymple und Schiflett 1997
1998	„*SA is ‚the pilot's internal model of the world around him at any point in time.' It is derived from the aircraft instrumentation, the out-the-window view, and his or her senses. Individual capabilities, training, experience, objectives, and the ability to respond to task workload moderate the quality of the operator's SA.*“	Endsley 1998

Der Grund dafür war das wachsende Interesse am Verhalten der Piloten während Luftschlachten. Es wurde unter anderem untersucht wie Piloten ihre und die gegnerische Lage erkennen und die Umgebung wahrnehmen. Eine häufig verwendete Definition von

Situationsbewusstsein stammt aus dem Jahre 1995 von Endsley (1995). Nach Endsley wird Situationsbewusstsein folgendermaßen aufgebaut: (1) Die Objekte in der Umgebung werden wahrgenommen. (2) Ihre Bedeutung wird verstanden. (3) Die Veränderungen in der Umgebung und der zukünftige Zustand der Objekte werden zutreffend für eine ausreichende Zeitspanne vorhergesagt. Die detaillierte Beschreibung dieses dreistufigen Prozesses erfolgt in Abschn. 1.3.1. Die folgende Tabelle fasst eine Auswahl an Definitionen zu Situationsbewusstsein von 1987 bis 1998 zusammen.

Die Definitionen in Tab. 1.1 zeigen, dass das Konzept von Situationsbewusstsein sowohl in zivilen als auch in militärischen Bereichen verwendet wird. Die anfänglichen Definitionen fokussieren auf menschlichen Aspekten in verschiedenen Krisensituationen. Sie beschreiben Situationsbewusstsein als kognitive Wahrnehmung und Wissensvermittlung. Definitionen bis zum Jahr 1995 sehen Situationsbewusstsein primär als den aktuellen, kognitiven Kenntnisstand und dem Verstehen der sich ständig verändernden Bedrohungslandschaft. Das Herstellen von Situationsbewusstsein und dessen Bewertung dient als Grundlage zur Entscheidungsfindung. Das bedeutet, dass die Entscheidungsfindung auf Situationsbewusstsein aufbaut (siehe z. B. das Modell von Endsley im Abschn. 1.3.1). In der Literatur versuchen Entscheidungsträger (z. B. Piloten) die Lage/Situation zu verstehen und zu bewerten (d. h. Situationsbewusstsein aufzubauen), um dann zu entscheiden welche Maßnahmen gesetzt werden sollten.

Der Begriff Cyber-Situationsbewusstsein (*cyber situational awareness*, abgekürzt CSA) transportiert diese Grundgedanken in die Cyber-Domäne. Beispielsweise wird nach Bahşi und Maennel (2015) dieser Begriff als Netzwerküberwachung, Informationsaustausch, Korrelation von Sicherheitsevents und high-level Sicherheitsberichte interpretiert.

Basierend auf dieser Begriffsdefinition beschreibt der nächste Abschnitt Modelle, die zum Aufbau von Situationsbewusstsein herangezogen werden können.

1.3 Modelle zur Etablierung von Situationsbewusstsein

Dieser Abschnitt beschreibt die theoretischen Modelle zum Aufbau von Situationsbewusstsein, die in einer Recherche (siehe Pahi et al. 2017a) ermittelt wurden. Viele davon beziehen sich auf das Situation Awareness Model in (Endsley 1995). In weiterer Folge wird jedes Modell kurz beschrieben.

1.3.1 OODA Loop (1976)

Der Observe-Orient-Decide-Act (OODA) Loop ist ein Informationskonzept aus dem militärischen Bereich und wurde vom Air Force Pilot John Boyd (1976) entwickelt (siehe Abb. 1.1). Cyber-Verteidigung wird mit OODA als ein ganzheitlicher Prozess mit verschiedenen Phasen in der Entscheidungsfindung dargestellt (Klein et al. 2011).

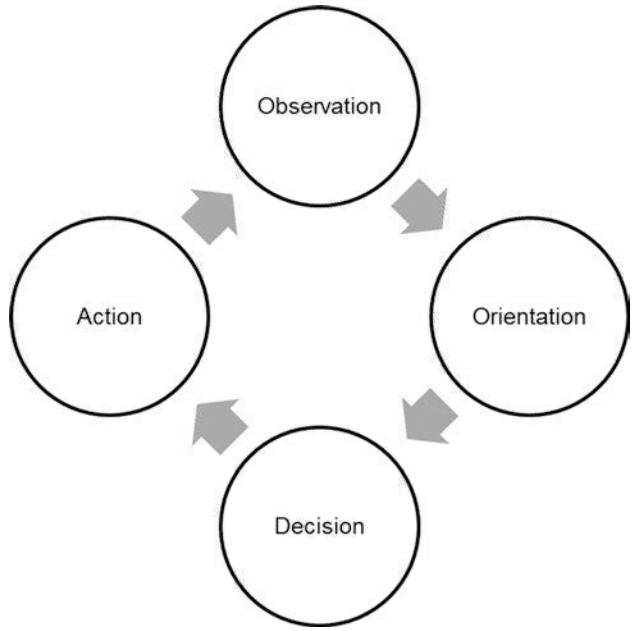

Abb. 1.1 OODA Loop. (Eigene Darstellung durch die Autoren, siehe Leitner et al. (2017) nach Boyd (1976))

Das Modell versucht die Handlungen und Verhaltensweise einer Entität, wie z. B. eines Piloten, einer Truppe, eines Staates oder einer Organisation, in einer fremden Umgebung abstrakt abzubilden.

Boyd zerlegte den ablaufenden Entscheidungsprozess in vier größere Teile:

1. Die Beobachtung (*Observation*) ist eine Art von Informationssammlung. Es umfasst die Sammlung von Informationen über Organisationen und ihrer Umgebung.
2. Die Orientierung (*Orientation*) ist eine Art von Monitoring der Umgebung. Es bezieht sich auf die Berechnung von relevanten Indikatoren, Vorhersagen zu machen und Warnungen an Entscheidungsträger zu geben.
3. Die Entscheidungsfindung (*Decision making)* wird von der Phase der Orientierung unterstützt, um schnellere Reaktionszeiten zu ermöglichen bzw. weniger Ressourcen aufzuwenden.
4. In der Durchführungsphase (*Act*) werden in der vorherigen Phase getroffene Entscheidungen mit Maßnahmen umgesetzt.

Durch das Handeln verändert sich die Situation und der OODA-Loop beginnt von vorne. Jede Entscheidung führt zu neuen Konsequenzen, die wieder als Entscheidungsgrundlage dienen (Althaus 2002). Laut Dierke et al. wiederholt sich der Entscheidungszirkel endlos, d. h. jede Entscheidung beginnt von neuem mit einer intensiven Beobachtungsphase, dem Sammeln von Daten und Fakten (Dierke und Houben 2013). Aktuellere und

umfassendere Informationen führen zu einem besseren Situationsbewusstsein und zu einer höheren Erfolgssicherheit. Es gab noch Weiterentwicklungen des OODA-Loops (z. B. Brehmer 2005).

1.3.2 JDL Data Fusion Model (1980)

Das häufig verwendete Joint Directories of Laboratory (JDL) Data Fusion Model unterscheidet mehrere Stufen der Verarbeitung und Verdichtung von Information in unterschiedlich komplexen Räumen (Kokar und Kim 1993). Das JDL-Modell bestand ursprünglich aus 4 Stufen (White 1988): L0 – Source Pre-Processing L1- Object Assessment, L2 – Situation Assessment und L3 – Impact Assessment. Weitere Stufen wurden nachträglich ergänzt (Steinberg et al. 1998), so wie zum Beispiel die Stufe L4 – Fusion Process Refinement.

Ein Beispiel dieser Erweiterung wird in Abb. 1.2 dargestellt, wobei die Reihenfolge der Ebenen den Abstraktionsgrad darstellt und keine zeitliche Abfolge festlegt (Llinas et al. 2004). Nach der Vorverarbeitung der Sensordaten gehört zur Objekterkennung auf Ebene 1 die Registrierung der Daten in einem Koordinatensystem, die Assoziation der Erkennungen, die zeitliche Verfolgung der Objekte und gegebenenfalls ihre Klassifikation. Aus der erhaltenen Umgebungsbeschreibung kann in Ebene 2 die Situation erkannt werden, aus der sich in Ebene 3 Gefahren ableiten lassen. Ebene 4 repräsentiert die übergeordnete Ablaufsteuerung zur Prozessoptimierung. Die letzte Ebene deckt die kognitive Verbesserung ab.

Es gibt weitere Variationen des JDL Modells. Zum Beispiel wird im Modell von Dasarathy (1997) die Fusion hinsichtlich der Verarbeitung auf und zwischen den Abstraktionsebenen der Daten, Merkmale und Entscheidungen beschrieben (Tischler 2014). Ein weiteres Beispiel ist (Giacobe 2010), der das JDL-Modell unter dem Aspekt der Cyber-Sicherheit erweitert. Der Autor beschreibt wie die Techniken der Datenfusion SA innerhalb von Netzwerken schärfen und verbessern können. Sein Modell berücksichtigt die menschlichen und kognitiven Kapazitäten und unterstützt die Cyber Security Analysten. Giacobe (2010) erweitert das ursprüngliche Modell mit einer fünften Ebene, die eine Schnittstelle zwischen einem Analysten und dem Datenfusionssystem bildet.

1.3.3 Situation Awareness Model (1995)

Der Begriff „*Situation Awareness*“ aus dem Modell von (Endsley 1995) wird häufig referenziert, die genaue Definition lautet: „*Situational Awareness is the perception of the elements in the environment within a span of time and space, the comprehension of their meaning and the projection of their status in the near future*“ (Endsley 1995).

Endsley versteht SA als Teil der Informationsverarbeitung und integriert darin Wahrnehmung, Aufmerksamkeit und Gedächtnis. Der Kerngedanke des Modells ist unter

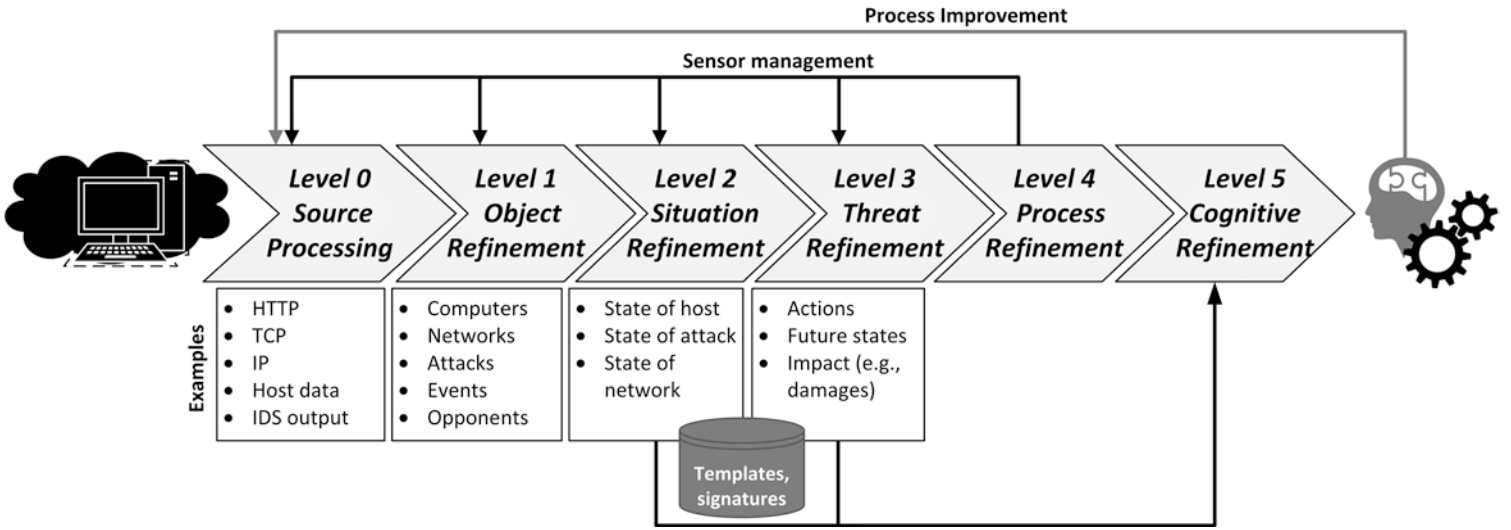

Abb. 1.2 JDL-Model. (Eigene Darstellung durch die Autoren, siehe Leitner et al. (2017) nach Hall and McMullen (2004))

anderem, dass SA eine durch die Kapazität von Aufmerksamkeit und Arbeitsgedächtnis begrenzte Ressource ist. SA unterliegt dem Einfluss von Zielen und Erwartungen der Person, die die Aufmerksamkeit, die Wahrnehmung und Interpretation der Information steuert (Badke-Schaub et al. 2008). Ausgehend von der Definition werden drei Ebenen (siehe Abb. 1.3) im Situational Awareness Model (SAM) unterschieden:

- **Ebene 1 – Wahrnehmung von Elementen einer aktuellen Situation** (*Perception of elements in current situation*): Diese Ebene beinhaltet die Wahrnehmung der Lage, sowie die Merkmale und die Dynamik der relevanten Situationselemente.
- **Ebene 2 – Verstehen der Bedeutung der aktuellen Situation** (*Comprehension of current situation*): Diese Ebene beschreibt das Verstehen der Bedeutung der Situationselemente zu einem ganzheitlichen Bild.
- **Ebene 3 – Prognose der künftigen Lage** (*Projection of future status*): Auf dieser Ebene werden Veränderungen in der Umgebung und die künftigen Lagen (z. B. von Elementen) für eine bestimmte Zeitspanne prognostiziert.

Abb. 1.3 zeigt den Zusammenhang zwischen den drei Ebenen des Situationsbewusstseins und den Zusammenhang zwischen Situationsbewusstsein (*situation awareness*),

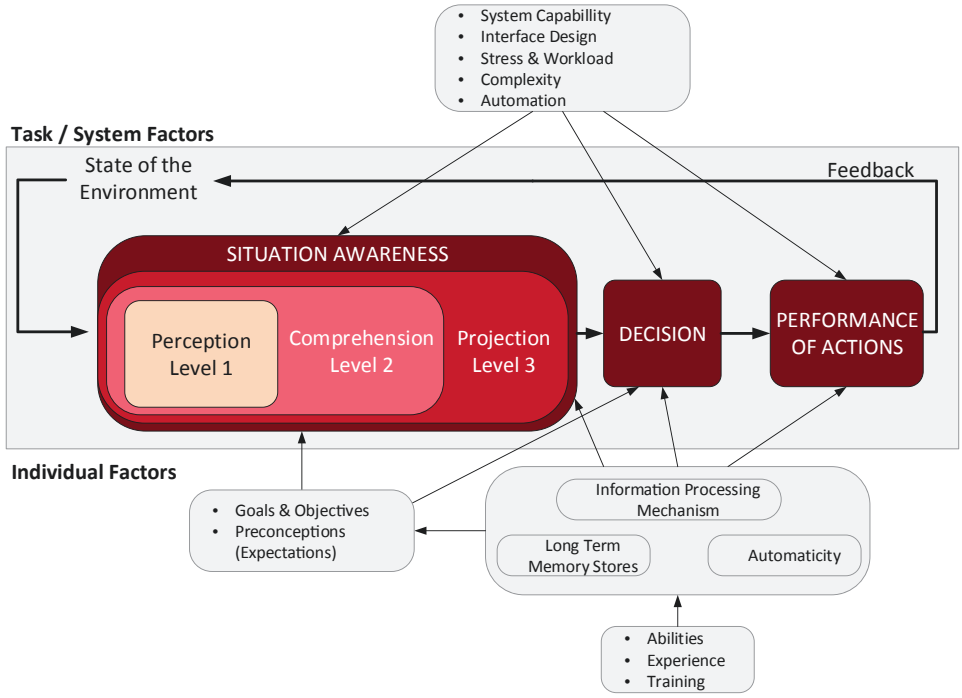

Abb. 1.3 Situation Awareness Model. (Eigene Darstellung durch die Autoren, siehe Leitner et al. (2017) nach Endsley (1995))