Xpert.press

Helmut Leopold
Thomas Bleier
Florian Skopik (Hrsg.)

Cyber Attack Information System

Erfahrungen und Erkenntnisse aus der IKT-Sicherheitsforschung

Springer Vieweg

Xpert.press

Helmut Leopold
Thomas Bleier
Florian Skopik (Hrsg.)

Cyber Attack Information System

Erfahrungen und Erkenntnisse aus der IKT-Sicherheitsforschung

Springer Vieweg

Die Reihe **Xpert.press** vermittelt Professionals in den Bereichen Softwareentwicklung, Internettechnologie und IT-Management aktuell und kompetent relevantes Fachwissen über Technologien und Produkte zur Entwicklung und Anwendung moderner Informationstechnologien.

Helmut Leopold · Thomas Bleier · Florian Skopik
Herausgeber

Cyber Attack Information System

Erfahrungen und Erkenntnisse aus der IKT-Sicherheitsforschung

Springer Vieweg

Herausgeber

Helmut Leopold, Thomas Bleier und Florian Skopik
AIT Austrian Institute of Technology GmbH
Wien, Österreich

Das Forschungsprojekt "CAIS Cyber Attack Information System" wurde im Österreichischen Sicherheitsforschungs-Förderprogramm KIRAS – eine Initiative des Bundesministeriums für Verkehr, Innovation und Technologie (bmvit) - gefördert.

ISSN 1439-5428
ISBN 978-3-662-44305-7 ISBN 978-3-662-44306-4 (eBook)
DOI 10.1007/978-3-662-44306-4

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

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer Vieweg ist Teil der Fachverlagsgruppe Springer Science+Business Media
(www.springer.com)

Vorwort der Herausgeber

In unserer jüngsten Geschichte haben sich die Informations- und Kommunikationstechnologien (IKT) zur zentralen Lebensader für sämtliche Wirtschaftsbranchen und alle Lebensbereiche entwickelt. Als allgegenwärtige Querschnittstechnologie ermöglichen sie viele, heute irreversibel im Gang befindliche Entwicklungen als Antwort auf viele unserer wichtigen Zukunftsfragen. Sie sind der Motor unserer umfassend kollaborativ arbeitenden und vernetzten Erkenntnisgesellschaft mit einer darauf aufbauenden Innovationsökonomie. Damit garantieren wir unsere internationale Wettbewerbsfähigkeit, unseren Wohlstand und unseren gesellschaftlichen Fortschritt.

Die IKT Infrastrukturen haben jedoch heute eine enorme Funktionsvielfalt und ein hohes Maß an Komplexität erreicht, so dass Verfügbarkeit und vor allem auch Sicherheitsaspekte nicht mehr im vollen Umfang von einzelnen Unternehmen oder auch von einzelnen staatlichen Organisationen alleine beherrscht werden können. Und die IKT haben gleichzeitig in vielfacher Verschränkung mit anderen Schlüsseltechnologien ein hohes Niveau an multipler gesellschaftlicher Abhängigkeit erreicht, für deren Bewältigung wir erst neue Antworten finden müssen. Mit anderen Worten: Die IKT sind neben dem Energienetz unsere kritischste Infrastruktur. Als Enabler für moderne Stromnetze, telemedizinische Einrichtungen, vernetzte Verkehrsleitsysteme, eGovernment-Dienstleistungen, neue Produktionsprozesse oder auch für den einfachen Zugang zu unseren Informationsdatenbanken, sind sie in vielfacher Hinsicht zu einem Sicherheitsrisiko für das Funktionieren des Staates als Ganzes geworden.

Dies ist umso mehr eine Herausforderung, als sich auch die Gefahrenlage im Cyber-Space über die letzten Jahre mit der gleichen rasanten Geschwindigkeit potenzierte, wie neue Services und Tools unser Internet bereicherten und nachhaltig veränderten. Vor dem Hintergrund immer raffinierterer und technologisch ausgereifterer Angriffsarsenale für Cyber-Kriminalität, Cyber-Krieg und Cyber-Spionage ist jedes fortschrittliche Land angehalten, in einer Art Wettrüsten und im permanenten Wettlauf mit potentiellen Angreifern geeignete Gegenstrategien zur Sicherung und Erhaltung seiner kritischen Infrastrukturen zu entwickeln und umzusetzen.

Sicherheit ist dabei ein sehr vielschichtiges Phänomen, dem vielschichtige Bedrohungen gegenüber stehen. Die modernen Staaten in Europa haben mit ihren Systemen der Gewaltenteilung und der Etablierung von Zuständigkeiten für gesellschaftliche Teilbereiche

über Jahrzehnte jeweils eigene, auf ihre spezifischen Bedürfnisse zugeschnittene, Sicherheitskonzepte entwickelt. Die Regierung als auch die unterschiedlichen Sicherheitsorganisationen und Organe, vom Militär über die Polizei bis hin zu zivilen Schutzeinrichtungen, entwickeln ihre Einsatzstrategien auf Basis spezifischer gesetzlicher Ermächtigungen und benötigen daher für ihre Domänen unterschiedliche Lagebilder als oberste Entscheidungsgrundlage für die politische Führung des Landes, für militärische Generalstäbe oder für die Führungskader der öffentlichen Sicherheit.

Die IKT als kritische Infrastruktur und die heutigen Cyber-Bedrohungen bringen jedoch eine neue Dimension ins Spiel. Eine wirksame Verteidigung und effiziente Gegenmaßnahmen gegen Angriffe können wegen der Komplexität der IKT nur durch das Zusammenwirken aller Kräfte entwickelt werden. Es braucht ein gemeinsames Werkzeug, damit für alle Sicherheitsaufgaben die entsprechend notwendigen Informationen für effektive Lagebilder bereitgestellt werden können.

Im Zuge einer prinzipiellen Innovationsstrategie organisiert Österreich durch das Bundesministerium für Verkehr, Innovation und Technologie (bmvit) ein explizites Sicherheitsforschungsförderprogramm – KIRAS, welches wissenschaftliche Kompetenzen mit industriellen Fähigkeiten und den Anforderungen der Sicherheitsorganisationen als Bedarfsträger in Projekten vereint, damit neueste Technologien als Problemlösung für unterschiedliche Fragestellungen zur Verfügung stehen und gesellschaftliche, soziale und kulturelle Aspekte (GSK Aspekte)[1] als inhärenter Bestandteil jeder Entwicklung mitberücksichtigt werden.

Diese Rahmenbedingung und die besondere Cyber-Sicherheitsproblematik markierten den Ausgangspunkt für die Konzeption eines eigenen Projektes zur Entwicklung eines „Cyber Attack Information Systems (CAIS)“. Mit diesem nationalen Projekt sollen die im Lande vorhandenen Expertisen gebündelt werden, um effektive Gegenmaßnahmen für zukünftige Bedrohungen im Cyber-Sicherheitsbereich zu entwickeln aber auch der Grundstein gelegt werden, um Österreich international in diesem Technologiebereich führend zu positionieren.

Durch das gemeinsame Verständnis, dass Bedrohungen am effektivsten mit umfangreichen Lageinformationen begegnet werden kann, die auf einem gemeinsamen, domänenübergreifenden Informationssystem beruhen, konnten alle relevanten Stakeholder der nationalen Sicherheit in das Projekt eingebunden werden. Dies erlaubte die Zusammenstellung eines schlagkräftigen Konsortiums mit wichtigen für die Sicherheit zuständigen österreichischen Regierungsstellen – Bundeskanzleramt (BKA), Bundesministerium für Landesverteidigung und Sport (BMLVS) und Bundesministerium für Inneres (BM.I) – , starken Industriepartnern und mit innovativen Forschungseinrichtungen, mit dem die Entwicklung eines „Cyber-Attack Information Systems (CAIS)“ in Angriff genommen werden konnte.

Im Grunde geht es bei CAIS um die Antizipation zukünftiger Cyber-Risiken und von aufkommenden Bedrohungen und um die Entwicklung neuer Tools und Werkzeuge für die

[1] GSK Aspekte … geistes-, sozial und kulturwissenschaftliche Aspekte.

frühzeitige Entdeckung von Angriffen durch das Erkennen von Anomalien in technischen Systemen sowie um die Abschätzung von deren Auswirkungen, also zusammengefasst, um eine verbesserte Situationswahrnehmung der nationalen IKT Sicherheit in Echtzeit.

Darauf aufbauend geht es im Projekt um die Erarbeitung einer Plattform für den vertrauensvollen und strukturierten Austausch von sicherheitsrelevanten Informationen und Frühwarnungen von Bedrohungen zwischen allen Sicherheitsstellen und damit um die Optimierung präventiver Möglichkeiten und rascherer reaktiver Maßnahmen im Falle von Cyber-Attacken. Die zwischen 2011 und 2013 im KIRAS-Projekt CAIS erarbeiteten technischen Lösungen stellen damit eine Umsetzung von Elementen der österreichischen Cyber-Strategie (ÖSCS) dar und bildeten die Grundlage für einen europäisch relevanten Forschungsschwerpunkt, der wesentlich von Österreich mitgestaltet wird.

Im Projekt CAIS wurden die grundsätzlichen Strukturen für Lagebildprozesse, für ein Cyber-Abwehrzentrum, für Angriffserkennung und Auswirkungssimulation untersucht. Wesentliche Erkenntnisse des Projektes sind nun auch die Grundlage für eine neu gestartete Projektinitiative, welche sich auf die „Trusted Information Sharing“ Thematik fokussiert. Im ebenfalls vom nationalen Sicherheitsforschungsprogramm KIRAS geförderten neuen Projekt „Cyber Incident Information Sharing (CIIS)“, 2013–2015, wird die in CAIS begonnene Arbeit weitergeführt und vertieft. In gleichem Maße diente das nationale CAIS Projekt als gute Ausgangslage um sich in weiterführenden europäischen Forschungsinitiativen in diesem Bereich erfolgreich zu positionieren.

Das vorliegende Buch berichtet über die im Projekt erzielten Ergebnisse zur Stärkung der Widerstandfähigkeit kritischer Infrastrukturen gegenüber zukünftigen Cyber-Angriffen und gibt Empfehlungen für den Aufbau eines Cyber-Lagezentrums in Österreich. Die folgenden Seiten geben Interessierten nicht nur Einblick in diese hoch komplexe und brandaktuelle Materie, von der wir alle betroffen sind, sondern zeigt auch vorbildlich, welche Erfolge bei einem harmonisierten Vorgehen und durch Bündelung mehrerer Expertisen und Kernkompetenzen in Österreich möglich sind.

Helmut Leopold
Thomas Bleier
Florian Skopik

Inhaltsverzeichnis

1 Einleitung zum Cyber Attack Information System 1
Helmut Leopold, Florian Skopik, Thomas Bleier, Josef Schröfl, Mike Fandler, Roland Ledinger und Timo Mischitz
1.1 Kommunikationsnetze als grundlegende Lebensadern unserer modernen Gesellschaft 1
1.2 IKT als kritische Infrastruktur 4
1.3 Das Bedrohungspotential verändert sich 5
1.3.1 Technologietrends 5
1.3.2 Neue Angriffsszenarien 6
1.4 Neue Gegenmaßnahmen werden notwendig 7
1.4.1 Nationale Cyber-Strategien in Österreich 8
1.4.2 Zusammenarbeit der Stakeholder 9
1.5 Ansatz: CAIS – Cyber Attack Information System 9
1.5.1 Das Projektkonsortium 10
1.5.2 Projektergebnisse 11

2 Cyber-Angriffsszenarien und wirtschaftliche Auswirkungen 13
Alexander Klimburg und Philipp Mirtl
2.1 Einleitung 13
2.2 Wirtschaftliche Modellierung eines großräumigen Cyber-Ausfalls 16
2.2.1 Der Internetbeitrag zum Bruttoinlandsprodukt (BIP) 16
2.2.2 Der Internetbeitrag zum BIP in Vergleichsländern 17
2.2.3 Der Internetbeitrag zum BIP in den USA und Österreich 20
2.2.4 Volkswirtschaftliche Bedeutung eines Internetausfalls 28
2.3 Erstellung der Bedrohungsanalysen 32
2.3.1 Matrix-Zeilen: Ebenen der Cyber-Kriegsführung 34
2.3.2 Matrix-Spalten: Formen von Cyber-Angriffen 35
2.3.3 Miniszenarien 36
2.3.4 Bewertung aus unterschiedlichen Perspektiven 37
2.3.5 Auswahl der Interviewpartner 39

2.4 Erarbeitung der Cyber-Angriffsszenarien 40
2.4.1 Miniszenarien („Vignetten“ im Detail) 40
2.4.2 Auswertung der Umfrage: „Aus Sicht der eigenen Organisation“ 48
2.4.3 Auswertung der Umfrage: „Aus Sicht eines Cyber-Lagezentrum“ 51

3 Cyber Attack Information System: Gesamtansatz 53
Florian Skopik, Thomas Bleier und Roman Fiedler
3.1 Einleitung 53
3.2 Situationsbewusstsein für Incident-Response 54
3.3 CAIS Stakeholder-Verantwortlichkeiten 56
3.3.1 Zuständigkeiten von Einzel-Organisationen 57
3.3.2 Zuständigkeiten des Nationalen Lagezentrums 57
3.4 Eine Architektur für ein Cyber Attack Information System 59
3.4.1 CAIS Architektur – Organisationsebene 60
3.4.2 CAIS Architektur – Nationale Ebene 60
3.4.3 Rollen, Interaktionen und Informationsaustausch 61
3.5 Anwendung des CAIS-Ansatzes 64
3.5.1 Schutzmechanismen gegen Cyber-Angriffe 64
3.5.2 Agile und Gemeinschaftliche Anomalieerkennung 65

4 Modellierung und Simulation kritischer IKT-Infrastrukturen und deren Abhängigkeiten 71
Simon Tjoa und Marlies Rybnicek
4.1 Einleitung 71
4.2 Anforderungen 73
4.3 Ansatz zur Modellierung und Simulation von Cyber-Abhängigkeiten kritischer Infrastrukturen 76
4.3.1 Beispielszenario „Distributed Denial of Service (DDoS)“ 84
4.3.2 Prototypische Implementierung 86
4.4 Ergebnisse, Schlussfolgerungen und Ausblick 87

5 Erkennen von Anomalien und Angriffsmustern 89
Roman Fiedler, Florian Skopik, Thomas Mandl und Kurt Einzinger
5.1 Einleitung 89
5.2 CAIS-Ansatz zur Erkennung von Cyber-Angriffen 91
5.2.1 Fundamentaler Ansatz 92
5.2.2 Anomalieerkennung – Ansätze aus der Bioinformatik 92
5.3 Beschreibung des Anomalieerkennungsalgorithmus 94
5.3.1 Basismodell und grundlegende Definitionen 94
5.3.2 Festlegen von Suchmustern zur Log-Zeilen Vektorisierung 96
5.3.3 Ereignisklassifizierung 96
5.3.4 Evaluierung von Hypothesen und System-Modell Aktualisierung 97

5.4 Architektur der Analysesoftware . . . 98
5.4.1 Log File Management . . . 99
5.4.2 Anomalieerkennung . . . 100
5.4.3 Berichtswesen und Konfiguration . . . 102
5.5 Anomalieerkennung: Detailszenario . . . 102
5.5.1 Ein realistischer Anwendungsfall . . . 102
5.5.2 Diskussion des Szenarios . . . 106
5.6 Bewertung des Konzepts bzgl. Datenschutzaspekten . . . 111
5.6.1 Datenquellen . . . 111
5.6.2 Datenarten . . . 112
5.6.3 Auftraggeber oder Dienstleister . . . 114
5.6.4 Ziel der Verwendung der Daten . . . 115
5.6.5 Datenschutzrechtlichen Verpflichtungen für CAIS . . . 115
5.6.6 Datensicherungsmaßnahmen . . . 116

6 Evaluierung von CAIS im praktischen Einsatz . . . 119
Herwig Köck, Martin Krumböck, Walter Ebner, Thomas Mandl, Roman Fiedler, Florian Skopik und Otmar Lendl
6.1 Einleitung . . . 119
6.2 Struktur realer Abläufe und Systeme . . . 120
6.2.1 Netzwerkaufbau . . . 120
6.2.2 Logmanagement . . . 121
6.2.3 Konfigurations-Management . . . 124
6.2.4 Disaster Recovery . . . 127
6.3 Integration der CAIS Werkzeuge in reale Infrastrukturen . . . 128
6.3.1 Anomalieerkennung . . . 128
6.3.2 Modellierungs- und Simulationstool . . . 129
6.4 Schnittstellen zu kommerziellen Werkzeugen . . . 132
6.4.1 APT Malware und automatische Analysesysteme . . . 132
6.4.2 Nutzen von automatischen Analysesystemen für CAIS . . . 133
6.4.3 Mögliche Integration in CAIS . . . 135
6.5 Pilotstudie: CAIS Anwendung in der Praxis . . . 137
6.5.1 Organisationseinbindung in CAIS . . . 138
6.5.2 Ablauf im Falle eines Angriffs . . . 142
6.5.3 Lagebildverteilung und Unterstützung . . . 145

7 Datenschutzleitlinie für Forschungsprojekte . . . 149
Kurt Einzinger
7.1 Einleitung . . . 149
7.2 Ziel der Datenschutzleitlinien . . . 150
7.3 Geltungsbereich der Datenschutzleitlinien . . . 151
7.3.1 Geltungsbereich . . . 151

7.3.2 Was sind personenbezogene Daten? . . . 151
7.3.3 Über die rechtliche Natur von IP-Adressen . . . 152
7.3.4 NAT – Network Address Translation . . . 153
7.3.5 Die Behandlung nur indirekt personenbezogener Daten . . . 155
7.3.6 Vorratsdaten nach dem Telekommunikationsgesetz (TKG) . . . 157
7.3.7 Nationale Datenschutzbehörden . . . 160
7.4 Privacy By Design (eingebauter Datenschutz) . . . 162
7.4.1 Einbau des Datenschutzes bei der Konzeption eines Systems . . . 162
7.4.2 Frühzeitige Klärung datenschutzrechtlicher Fragen . . . 163
7.4.3 Folgenabschätzung . . . 164
7.4.4 Einsatz einer „privatsphärenfreundlichen“ Technologie . . . 165
7.4.5 Zweckbestimmung des Systems . . . 165
7.5 Datenverwendungen in der Forschung . . . 166
7.5.1 Zulässigkeit der Verwendung von Daten . . . 166
7.5.2 Entscheidung über Verwendung personenbezogener Daten . . . 167
7.5.3 Wissenschaftliche Forschung und Statistik im DSG 2000 . . . 168
7.5.4 Genehmigung durch die Datenschutzbehörde (DSB) . . . 169
7.5.5 Meldepflicht nach § 17 DSG 2000 (DVR) . . . 169
7.6 Datensicherheit, Datensicherheitsmaßnahmen . . . 170
7.6.1 Gesetzlich vorgeschriebene Datensicherheitsmaßnahmen . . . 170
7.6.2 Meldungspflichten bei Sicherheitsvorkommnissen . . . 172
7.6.3 Wie lange sind die Daten aufzubewahren? . . . 174
7.6.4 Wem sollte Zugriff auf die personenbezogenen Daten gewährt werden? . . . 174
7.6.5 Schulungen in datenschutzrechtlichen Fragen . . . 175
7.6.6 Vertraulichkeit . . . 175
7.7 Übermittlung und Weitergabe von Daten . . . 176
7.7.1 Allgemeiner Rahmen . . . 176
7.7.2 Register der Übermittlung und Weitergabe von Daten . . . 176
7.7.3 Ausgliederung der Verarbeitung . . . 177
7.8 Gewährleistung und Nachweis guter Verwaltungspraxis . . . 178
7.8.1 Datenverwendungsstrategie . . . 178
7.8.2 Datenschutzaudit . . . 179

8 Empfehlung an die Politik und Ausblick . . . 181
Alexander Klimburg, Philipp Mirtl und Kurt Einzinger
8.1 Der sicherheitspolitische Rahmen des Nationalen Cyber-Lagezentrums . 181
8.1.1 Aufgaben und Kategorien von „National Cybersecurity Centers“ (NCC) . . . 184
8.1.2 Lagebilderstellung, Berichte und Sensoren . . . 185
8.1.3 Anforderungen der Europäischen Union . . . 193
8.1.4 Vorschlag zu einem möglichen „Austrian Cyber Center“ . . . 194

8.1.5 Entwicklung eines Anomaly Detection-gestützten Netzwerks . . 198
8.2 Datenschutzrechtliche Aspekte 201
8.2.1 Allgemeines 201
8.2.2 Änderungen im österreichischen Datenschutzregime 203
8.2.3 Änderungen in der EU-Datenschutzgrundverordnung 204
8.2.4 Network and Information Security (NIS) Directive 206

Einleitung zum Cyber Attack Information System

1

Helmut Leopold, Florian Skopik, Thomas Bleier, Josef Schröfl,
Mike Fandler, Roland Ledinger und Timo Mischitz

1.1 Kommunikationsnetze als grundlegende Lebensadern unserer modernen Gesellschaft

Die globalen Veränderungen im neuen Jahrtausend bringen ganz neue Anforderungen für unsere Gesellschaft mit sich. Die Lösung großer gesellschaftlicher Fragestellungen wie Energie, Sicherheit, Gesundheitsversorgung im Kontext der demographischen Veränderung der Gesellschaft oder Verkehrsmanagement in Großstädten ist wesentlich von IT Innovationen bestimmt. eGovernment, eHealth, eMobility, eEnergy, eEnvironment oder auch smart city, smart building, car2car oder car2infrastructure communication sind oft verwendete Schlagwörter um diese zukünftigen intelligenten oder smarten Systeme zu beschreiben. Solche smarten Anwendungsbereiche die durch einen weitreichenden Einsatz von Informations- und Kommunikationstechnologien (IKT) entstehen sind vielfältig:[1]

- Die Vernetzung unserer Fahrzeuge und Einsatz von intelligenter Sensorik für moderne Verkehrssysteme.[2] Einerseits fährt das Fahrzeug immer mehr autonom, erhöht die

Helmut Leopold ✉ · Florian Skopik · Thomas Bleier
AIT Austrian Institute of Technology GmbH,, Wien, Österreich
e-mail: florian.skopik@ait.ac.at

Josef Schröfl
Österreichisches Bundesministerium für Landesverteidigung und Sport, Wien, Österreich

Mike Fandler
Österreichisches Bundesministerium für Inneres, Wien, Österreich

Roland Ledinger · Timo Mischitz
Österreichisches Bundeskanzleramt, Wien, Österreich

[1] Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think, John Murray Publishers, 2013.

[2] Thomas R. Köhler, Dirk Wollschläger, Die digitale Transformation des Automobils – 5 Megatrends verändern die Branche, Media Manufaktur, 2014 (ISBN: 978-3-9814661-9-5).

H. Leopold et al. (Hrsg.), *Cyber Attack Information System*, Xpert.press,
DOI 10.1007/978-3-662-44306-4_1