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

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

Sicherheit, informiert und unterhält und andererseits werden neue Verkehrsmanagementmethoden möglich. Durch eine intelligente Vernetzung der Automobile wird z. B. eine erhebliche Reduktion des CO_2-Ausstoßes erwartet.[3]

- Durch eine intelligent gesteuerte Energieproduktion (erneuerbare Energien) und Energieverteilung (smart grid) bis hin zu einem Energiemanagement zu Hause (smart home) entstehen neue Systemarchitekturen, welche die Umstellung von fossilen auf erneuerbare Energieträger ermöglichen und den Energieendverbrauch senken.[4]
- Durch eine neue Vernetzung zwischen Patient, Arzt und Betreuer werden neue Formen der medizinischen Versorgung als auch der Vorbeugung und des Lifestylemanagements ermöglicht. „Closed loop healthcare" Telemedizinsysteme erlauben neue Behandlungs- und Betreuungsansätze für Volkskrankheiten wie Diabetes[5], Herzschwäche und Übergewicht aber auch für neue Formen der Betreuung von pflegebedürftigen Menschen, welche für alle Stakeholder Vorteile generieren (Patient, Arzt, Gesundheitssystem). Ambient Assisted Living (AAL)[6] oder Enhanced Living Environments (ELE) sind neue Konzepte die diesen Trend beschreiben.[7]
- Eine Vernetzung von Produktionssystemen führt zu „Industrie 4.0" Konzepten: Produktionssysteme werden miteinander vernetzt um Produktionsprozesse zeitlich und räumlich verteilt auch über Firmengrenzen hinweg effizienter zu gestalten. Sensoren werden zur Qualitätskontrolle in Echtzeit eingesetzt, oder auch direkt mit Endverbrauchern vernetzt um den Produktionsprozess zu optimieren. Schlussendlich geht es um eine direkte Vernetzung der Endverbraucher mit den Produktionsprozessen um eine neue Flexibilität zu schaffen, die die Variantenvielfalt und die Qualität der Produkte wesentlich erhöht.[8]
- Immer mehr Bürgerdienste und Interaktionen zwischen öffentlicher Hand und Bürgern werden über elektronische Wege realisiert. eGovernment Dienste sind zu einem bestimmenden Element der Produktivitätssteigerung eines Wirtschaftsstandortes geworden.

[3] eCoMove Initiative, http://www.ecomove-project.eu/, letzter Zugriff: 1. November 2014.
[4] Farhangi, Hassan. „The path of the smart grid." Power and Energy Magazine, IEEE 8.1 (2010): 18–28.
[5] G. Schreier, H. Eckmann, D. Hayn, K. Kreiner, P. Kastner, N. Lovell: „Web versus App – compliance of patients in a telehealth diabetes management programme using two different technologies"; Journal of Telemedicine and Telecare, 18 (2012), S. 476–480.
[6] Mario Drobics, Angelika Dohr, Helmut Leopold, Harald Orlamünder, Standardized Communication in ICT for AAL and eHealth, 5. Deutscher AAL-Kongress 24.–25.01.2012, Berlin (Tagungsband), VDE Verlag GmbH, Berlin.
[7] ICT COST Action IC1303 AAPELE – Algorithms, Architectures and Platforms for Enhanced Living Environments, http://www.cost.eu/COST_Actions/ict/Actions/IC1303, letzter Zugriff: 1. November 2014.
[8] Siehe z. B. die Initiative der deutschen Bundesregierung: http://www.bmbf.de/de/9072.php bzw. http://www.produktion.de/automatisierung/industrie-4-0-smarte-produkte-und-fabriken-revolutionieren-die-industrie/ oder auch die 2014 gestartete Österreichische Initiative http://www.alpbach.org/de/vortrag/industrie-4-0-die-naechste-industrielle-revolution/, letzter Zugriff: 1. November 2014.

Österreich hat in diesem Bereich z. B. seit Jahren eine besondere Vorreiterrolle übernommen[9] und nimmt seit 2006 den ersten Platz des eGovernment Rankings der Europäischen Kommission ein (Capgemini Benchmark) ein und seit 2011 hat Österreich bei den eGovernment-Diensten die höchsten Benutzerzahlen als auch die höchsten Akzeptanzwerte (eGovernment Monitor der Initiative D21[10]).[11]

Diese Vernetzung von physischen Systemen durch IKT wird oft auch als Machine-2-Machine (M2M) Kommunikation bezeichnet. Um die enge Vernetzung IKT-basierter, bis dato auch autonom agierender elektronischer Systeme mit der physikalischen Welt zu beschreiben, werden solche Systeme auch als Cyber Physical Systems (CPS) bezeichnet.[12]

Dieser Trend bringt eine neue Dynamik der Systementwicklung und weitreichende Konsequenzen für Systemdesign und Anwendungsbereiche mit sich. Aber unabhängig von diesen Entwicklungstrends sind bereits heute grundlegende Geschäftsprozesse unserer Unternehmen aber auch jegliche Form von Privatkommunikation schon lange von der verfügbaren globalen Vernetzung durch Breitbandkommunikationsnetze und IT Plattformen abhängig. Egal ob im persönlichen Umfeld, in kleinen Firmen, internationalen Unternehmen oder im Behördenbereich, die Einbindung von elektronischen Technologien in Kommunikations-, Produktions- und Entscheidungsprozesse aber auch die die private Alltagskommunikation ist in den letzten Jahren massiv erfolgt. Unsere Jugend, auch als

[9] Z.B. war Österreich das erste Land das in den 80er Jahren ein digitales Grundbuchregister (eGrundbuch) und ein eFirmenbuch realisierte; es war in der EU das erste Land das 1997 mit help.gv.at und FinanzOnline zwei elektronische Bürgerservice Portale für Services der öffentlichen Hand auf den Markt brachte. Beide Dienste wurden u. a. mit dem eEurope Award und Speyer Award ausgezeichnet; ebenfalls bereits 1997 wurde ein elektronisches Rechtsinformationssystem (RIS) realisiert; seit 1997 werden alle Gesetze als auch der Gesetzeswerdungsprozess offiziell und authentisch elektronisch im Internet publiziert; diese Pionierarbeit wurde mit dem UN Public Service Award ausgezeichnet; 2003 wurde das erste behördenübergreifendes Dokumentenmanagement (ELAK) und zentrales Melderegister implementiert; weiters war Österreich das erste EU Land, das bereits 2004 ein eGovernment Gesetz (2004) veröffentlichte, und es war das erste Land, das eine Bundesweite elektronische Infrastruktur für eHealth-Dienste implementierte (ELGA). Darüber hinaus hat Österreich beim Einsatz von modernsten Telemedizinanwendungen für die mobile Versorgung von chronisch kranken Menschen wie Diabetes und Herzschwäche durch international beispielgebende Initiativen wie der Gesundheitsdialog Diabetes von der Versicherung für Eisenbahn und Bergbau (VAEB) (siehe http://www.ait.ac.at/et-award2011, letzter Zugriff: 1. November 2014), als auch die geplante Einführung einer Telemedizinregelversorgung für Patienten mit Herzschwäche im Land Tirol (siehe Pressemeldung 12.2014, http://www.tirol.gv.at/meldungen/meldung/artikel/herzmobil-tirol/; letzter Zugriff: 1. November 2014). 2011 wurde das OpenGovernmentDataPortal veröffentlicht, welches mit dem UN Public Service Award ausgezeichnet wurde und dann von anderen Ländern übernommen wurde (D, CH, EU). 2012 wurde die Volkszählung als reine Registerzählung durchgeführt.

[10] http://www.egovernment-monitor.de/die-studie/2014.html, Initiative D21, letzter Zugriff: 1. November 2014.

[11] eGovernment ABC, 2014, www.digitales.oesterreich.gv.at, letzter Zugriff: 1. November 2014.

[12] „Towards a thriving data-driven economy“, Special theme: Cyber-Physical Systems, ECRIM News, Number 97, April 2014.

„digital natives“ bezeichnet, weil sie mit diesen neuen Gewohnheiten aufgewachsen ist, hat ihr Verhalten bereits auf den Cyber-Space abgestimmt und ihr kollektives Kommunikationsverhalten verändert.[13]

Wirtschaft, Verwaltung aber auch die Gesellschaft als solches sind in engster Weise mit dieser Technologie verbunden. Wir alle verlassen uns somit in zunehmendem Maße auf moderne Informations- und Kommunikationstechnologien und sind schlussendlich mit einer beträchtlichen Abhängigkeit von diesen Technologien konfrontiert. Die potentiellen Auswirkungen dieser Abhängigkeiten sind mittlerweile enorm. Der Ausfall von Energienetzen, des Bankensystems, der Versorgung der Bevölkerung mit lebenswichtigen Produkten oder der Staatsverwaltung, kann enorme wirtschaftliche Schäden bewirken bzw. ganze Staaten massiv beeinträchtigen.[14]

1.2 IKT als kritische Infrastruktur

Das Funktionieren unserer modernen Gesellschaft ist somit sehr stark von der ständigen Verfügbarkeit unserer IKT Infrastrukturen abhängig. IKT Infrastrukturen sind eine unverzichtbare Basis für die Modernisierung fast aller unserer Lebensbereiche geworden und müssen daher neben dem Stromnetz als die wesentliche kritische Infrastruktur unserer Gesellschaft eingestuft werden.

Kritische Infrastrukturen sind Systeme die eine überragende Bedeutung für die Aufrechterhaltung zentraler gesellschaftlicher Funktionen haben. Dazu gehören Energienetze, Wasserversorgung, Lebensmittel, Gesundheitseinrichtungen, der Finanz- und Transportsektor, Forschungs- und Ausbildungseinrichtungen, Medien und Kultur (z. B. Rundfunk und Fernsehen) aber auch die Schwerindustrie, die chemische, die Raumfahrt- und die Nuklearindustrie, sowie alle politischen Institutionen, welche die Regierbarkeit eines Landes in seiner Gesamtheit sicherstellen wie Justiz, Exekutive und Militär und die dafür verantwortlichen Stellen (Gerichte, Ministerien, Landesregierungen, Städte etc.) und schlussendlich auch klassische Kommunikationsinfrastrukturen wie Telefonnetze.[15] Diesen Infrastrukturen ist gemeinsam, dass ihre Störung oder Zerstörung schwerwiegende Auswirkungen auf die Sicherheit und die Wirtschaft eines Landes, die Gesundheit und das soziale Wohl der Bevölkerung und das Funktionieren des Gemeinwesens Staat als Ganzes haben.

[13] Allison Cerra, Christina James, Identity Shift: Where Identity Meets Technology in the Networked-Community Age, Wiley, November 2011, ISBN: 978-1-118-18113-3.

[14] Blackouts in Österreich Teil I – Analyse der Schadenskosten, Betroffenenstruktur und Wahrscheinlichkeiten großflächiger Stromausfälle: http://energyefficiency.at/web/projekte/blacko.html, KIRAS Sicherheitsforschung, letzter Zugriff: 1. November 2014.

[15] Vgl. Green Paper on a European programme for critical infrastructure protection, European Commission, COM/2005/0576, November 2005, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576, letzter Zugriff: 1. November 2014.

Nachdem all diese Infrastrukturen bereits wesentlich auf IT Anwendungen aufbauen und zunehmend durch IKT umfassend vernetzt werden, erfahren diese Anwendungsgebiete auch eine neue Abhängigkeit von IT-Plattformen und IKT Infrastrukturen, was dazu führt, dass digitale IKT-Netze aber auch herkömmliche Internetzugänge als grundlegende kritische Infrastrukturen betrachtet werden müssen.[16]

In letzter Zeit hat dieser Aspekt an Aufmerksamkeit gewonnen, nicht zuletzt durch öffentlich gewordene Vorfälle, wie etwa die Cyber-Angriffe auf Estland 2007[17], oder den Stuxnet-Virus-Angriff 2010 auf die Iranischen Atomkraftwerke[18] oder auch eine Reihe von weiteren Angriffen[19, 20] gegen kritische Infrastrukturen wie Red October, Miniduke, TeamSpy, APT1. All diese Attacken, als auch jüngste Cyber-Angriffe auf Sony Pictures und Banken in Europa und USA, demonstrieren die besonderen Gefahren für unsere Cyber Physical Systems eindrucksvoll.

1.3 Das Bedrohungspotential verändert sich

Zwei sich wechselseitig beeinflussende globale Trends führen nun zu neuen Bedrohungspotentialen die auch besondere Gegenmaßnahmen verlangen:

1.3.1 Technologietrends

Ökonomische Zwänge der Systembetreiber bringen eine zunehmende Vernetzung der Systeme mit sich. Technische Systeme, die früher isoliert funktioniert haben, werden miteinander vernetzt um Überwachungsaufgaben und Fernwartungsprozesse zu vereinfachen. Über solche wirtschaftliche Gesichtspunkte hinaus kommt es durch die Logik einer raschen wirtschaftlichen Innovationsentwicklung zu einem Trend der Verwendung von offenen Systemarchitekturen, zum Einsatz von Commercial Off The Shelf (COTS) Technologien und standardisierten Schnittstellen. Durch diese technischen Trends werden implizit neue Schwachstellen in den Systemen generiert und gleichzeitig ist es wesentlich einfacher durch breit vorhandene Technologiekenntnisse neue Angriffsmethoden zu entwickeln.

[16] Vgl. Bleier, Thomas: An Analysis of ICT Influence Factors on Critical Infrastructure Security, Master Thesis, 2011 und Lewis, Ted G.: Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, John Wiley & Sons, 2006.
[17] Gaycken, Sandro: Cyberwar – Das Internet als Kriegsschauplatz. Open Source Press, 2011.
[18] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. Security & Privacy, IEEE, 9(3), 49–51.
[19] http://www.russia-direct.org/content/most-dangerous-cyberweapons-2013, and http://resources.infosecinstitute.com/teamspy-miniduke-red-october-and-flame-analyzing-principal-cyber-espionage-campaigns/, letzter Zugriff: 1. November 2014.
[20] http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat, letzter Zugriff: 1. November 2014.

Die entstehenden Cyber Physical Systems werden zunehmend komplexer. Einerseits werden die Funktionen der einzelnen Systeme immer ausgereifter und zudem kommt durch die Vernetzung eine neue Dimension dazu, welche ein Gesamtsystemverständnis immer schwieriger macht. Man spricht auch von komplexen „System of Systems".

Durch diese Entwicklungen werden nun auch die Abhängigkeiten zwischen den einzelnen Komponenten aber auch Systemen verstärkt, welche bei Fehlfunktionen und Störungen viel leichter zu Kettenreaktionen führen können und somit wesentlich rascher größere Konsequenzen nach sich ziehen.[21]

1.3.2 Neue Angriffsszenarien

Das Ausmaß und die Professionalität der Bedrohungen haben sich in den letzten Jahren wesentlich verändert. Während zu Beginn das Interesse an der Technik im Vordergrund stand und die ersten Viren ohne kommerzielle Interessen entwickelt wurden, hat in den letzten Jahren wirtschaftliches Interesse als Motivation eine führende Rolle eingenommen. Die Bedrohung geht nicht mehr von einzelnen, isoliert arbeitenden Hackern aus, sondern von organisierten Strukturen mit beträchtlichen Investitionen in entsprechende Angriffe.[22, 23]

Zudem gilt es zu beachten, dass diese Bedrohungen in ihrem Ausmaß ein junges Phänomen sind. Ein Virenschutzprogramm muss heute an die 240 Mio. verschiedene Malware-Signaturen erkennen.[24] Jeden Tag kommen ca. 160.000 neue Malware-Signaturen dazu[25] (alle 2,5 Sekunden taucht eine neue Bedrohung auf[26]). Diese massive Entwicklung hat sich erst in den letzten Jahren zu diesem Ausmaß ausgewachsen und stellt die Industrie aber auch die Gesellschaft vor neue Herausforderungen im Umgang mit der Cyber-Domäne.

Durch das immer breiter werdende vorhandene Technologie Know-how und durch den großen Aufwand, den Angreifer bei ihren Cyber-Attacken betreiben, werden die Angriffsmethoden zudem immer ausgefeilter und auch komplizierter. Bei sog. „Advanced Persistent Threats (APTs)" werden unterschiedlichste Angriffsansätze geschickt miteinander kombiniert, um Schutzmechanismen auszuhebeln. Typischerweise werden bei solchen Angriffsverfahren zeitlich und räumlich verteilt unterschiedliche Methoden zum Einsatz gebracht, wobei die einzelnen Attacken oft unverdächtig sind und damit oft in den betrof-

[21] Rinaldi, S.M. (2004), Modeling and simulating critical infrastructures and their interdependencies, IEEE HICS.
[22] Yar, Majid. Cybercrime and society. Sage, 2013.
[23] Bradbury, Danny: Digging up the hacking underground. Infosecurity, 7 2010, No. 5, 14–17, http://www.infosecurity-magazine.com/view/13117/digging-up-the-hacking-underground/i, ISSN 1754-4548, letzter Zugriff: 1. November 2014.
[24] http://www.av-test.org/de/statistiken/malware/, letzter Zugriff: 1. November 2014.
[25] http://www.scmagazineuk.com/160000-new-malware-samples-arriving-every-day/article/349235/, letzter Zugriff: 1. November 2014.
[26] http://www.trendmicro.de/media/ds/anti-malware-nss-labs-datasheet-de.pdf, letzter Zugriff: 1. November 2014.

fenen Systemen von den herkömmlichen Schutzmechanismen lange unentdeckt bleiben. Solche kombinierten Angriffsstrategien wie z. B. die Verknüpfung von Social Engineering mit dem Einsatz von Phishing SW und gezielter Malware, welche in Teilen in ein System geschleust und erst viel später aktiviert werden, führen zu komplexen und sehr spezifischen Angriffsmustern, welche mit herkömmlichen Verteidigungsstrategien sehr schwer zu bekämpfen sind.

Auch wenn es eine Menge an verschiedenen Bedrohungsszenarien und Motivationen gibt, sind die Angriffsstrategien und verwendete Technologie oft ähnlich. Grundsätzlich gilt es zu attestieren, dass Cyber-Angriffe üblicherweise sehr spät erkannt werden können, sehr schwer zurück verfolgbar sind und oft auch nicht isoliert betrachtet werden können.

Zusammenfassend muss somit festgestellt werden, dass wir mit einer grundlegenden Problematik konfrontiert sind. Zum einen werden die Cyber-Angriffe immer raffinierter und intelligenter und zum anderen führt der steigende Grad der Vernetzung von Systemen und durch die eingesetzte IT zu immer komplexeren Systemen was eine sinkende Kenntnis über das Gesamtsystem unweigerlich mit sich bringt. Wenn die Sicherheit unserer zukünftigen Kommunikationsnetze und dem Internet nicht sichergestellt werden kann, wird dies auch zu einem massiven negativen Effekt auf die Innovationsleistung in vielen Anwendungsbereichen führen.[27]

Unabhängig davon ob die Motivation der Angriffe auf unsere kritische IKT Infrastruktur kriminell, wirtschaftlich oder militärisch ist, die Angriffsszenarien haben sich massiv verändert und werden immer aufwendiger gestaltet, was entsprechende Gegenmaßnahmen zunehmend schwieriger macht.

1.4 Neue Gegenmaßnahmen werden notwendig

Um der besonderen Bedrohung als auch der enormen Komplexität Rechnung zu tragen, sind neue Methoden und Technologien erforderlich, die nur durch eine gemeinsame Anstrengung aller Akteure erreicht werden kann, um erfolgreiche nationale Gegenstrategien zu entwickeln, damit die kritischen IKT Infrastrukturen des Landes für die großen gesellschaftlichen Aufgabenstellungen verfügbar sind.

[27] Helmut Leopold, Thomas Bleier, Safety & Security in Future Networks Will Need a New Internet Science, PIK - Praxis der Informationsverarbeitung und Kommunikation, Band 36, Heft 3, Seiten 191–197, ISSN (Online) 1865–8342, ISSN (Print) 0930–5157, DOI: 10.1515/pik-2013-0021, August 2013.

1.4.1 Nationale Cyber-Strategien in Österreich

In diesem bisher beschriebenen Kontext wurden in vielen Ländern aber auch in Organisationen wie der NATO Cyber-Strategien entwickelt.[28] Deutschland hat 2009 eine nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie[29]) veröffentlicht, und die EU beschloss am 12. Juni 2012 eine Resolution zum Schutz kritischer Informationsinfrastrukturen in Europa.[30]

Auch In Österreich wurde unter Koordination des Bundeskanzleramtes (BKA) in Zusammenarbeit mit dem Bundesministerium für Inneres (BM.I), dem Bundesministerium für Landesverteidigung und Sport (BMLVS) sowie dem Bundesministerium für Europa, Integration und Äußeres (BMEIA) im Rahmen einer intensiven Zusammenarbeit aller Stakeholder eine Österreichische Strategie für Cyber Sicherheit (ÖSCS) ausgearbeitet[31] und von der Bundesregierung am 20. März 2013 beschlossen. Die Strategie für Cyber-Sicherheit ist ein wesentlicher Bestandteil des von der Bundesregierung am 2. April 2008 beschlossenen Masterplanes zum Schutz kritischer Infrastrukturen – Austrian Programme for Critical Infrastructure Protection (APCIP).[32, 33]

Die ÖSCS ist ein umfassendes und proaktives Konzept zum Schutz des Cyber-Raums und der Menschen im virtuellen Raum. Sie verbessert Sicherheit und Widerstandskraft der österreichischen Infrastrukturen und Leistungen im Cyber-Raum. Es werden sieben Handlungsfelder und dazugehörige Maßnahmen festgelegt, die eine operative Umsetzung ermöglichen. Für einige der darin festgelegten Maßnahmen, wie beispielsweise die „Schaffung einer Struktur zur Koordination auf der operativen Ebene", stellt das CAIS Projekt direkt verwendbare Ergebnisse bereit, die als Basis für eine operative Umsetzung dienen können.[34]

---

[28] Vgl. Brunner, Elgin M./Suter, Manuel: International CIIP Handbook 2008/2009. Center for Security Studies, ETH Zurich, 2008, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=91952, letzter Zugriff: 1. November 2014.

[29] http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf, letzter Zugriff: 1. November 2014.

[30] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167, letzter Zugriff: 1. November 2014.

[31] https://www.bka.gv.at/DocView.axd?CobId=50748, letzter Zugriff: 1. November 2014.

[32] Die Maßnahmen des APCIP Masterplanes sollen das Risikomanagement, das Bussines Continuity Management und das Sicherheitsmanagement bei jenen Unternehmen und Organisationen stärken, die eine strategische Bedeutung für Österreich haben. Neben den organisatorischen und rechtlichen Risiken, den Marktrisiken, den Natur- und den technischen Gefahren wird empfohlen auch die internationalen Gefahren, die auch die Cyber-Risiken umfassen, intensiv zu bearbeiten.

[33] http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf, letzter Zugriff: 1. November 2014.

[34] H. Habermayer, J. Schröfl, Genese und wesentliche Inhalte der Österreichischen Strategie für Cyber-Sicherheit, S+F, (32. Jg.) 1/2014.

1.4.2 Zusammenarbeit der Stakeholder

Um den neuen Bedrohungen erfolgreich begegnen zu können, ist eine enge Zusammenarbeit zwischen allen Akteuren notwendig. Technologiehersteller, Netzbetreiber, Service-Anbieter, Industrie-Vereinigungen und verschiedene Stakeholder der öffentlichen Hand müssen gemeinsam Systeme entwickeln um Angriffe frühzeitig erkennen zu können und einen Informationsaustausch sicher zu stellen um rasch effektive Gegenmaßnahmen entwickeln zu können.

Um effiziente Abwehrmaßnahmen ausarbeiten zu können, ist es erforderlich, einen Überblick über die aktuelle Bedrohungslage zu bekommen, um Ausmaß und Auswirkungen besser einschätzen zu können und entsprechende Gegenstrategien konzipieren zu können.

In den letzten Jahren haben sich zwar bereits sehr erfolgreich nationale Computer-Emergency-Response Teams (CERTs) gebildet. Primäre Aufgabe dieser Institutionen ist die Verteilung von Informationen an die Betreiber kritischer Infrastrukturen, um sie über bereits bekannte Schwachstellen zu informieren. Ein wesentlicher nächster Schritt ist die Etablierung eines bidirektionalen Informationsflusses (auch direkt zwischen unterschiedlichen Betreibern kritischer Infrastrukturen), welcher derzeit noch nicht ausreichend ausgeprägt ist. Zur effektiven Abwehr von Angriffen müssen nicht nur bereits erkannte Attacken zeitnah weitergemeldet werden, sondern auch im Vorfeld von Attacken erkannte Anomalien kommuniziert werden, die für sich genommen möglicherweise noch harmlos sind, aber bereits auf drohende Angriffe hinweisen können.

In diesem Sinne empfiehlt die 2013 veröffentlichte europäische „Network and Information Security (NIS) Richtlinie“[35] den Aufbau nationaler Cyber-Lagezentren, welche nicht nur den Sicherheitsstatus der nationalen Infrastruktur erfassen, sondern auch koordinierte Aufgaben bei der Prävention und auch Abwehr von Angriffen übernehmen. Für eine solche Aufgabe ist es unbedingt notwendig geeignete Mechanismen und Prozesse für den Austausch von Informationen zu etablieren.

1.5 Ansatz: CAIS – Cyber Attack Information System

Um nun der neuen Bedrohungslage Rechnung zu tragen und neue Werkzeuge und Methoden für zukünftige Anforderungen zu entwickeln, wurde in Österreich eine spezielle Initiative gestartet, um im engen Schulterschluss zwischen den öffentlichen Bedarfsträgern BMLVS, BM.I und BKA und der Wissenschaft, Forschung und Industrie neue Lösungsansätze zu entwickeln. So wurde das Projekt „CAIS – Cyber Attack Information System“ unter der Federführung des AIT Austrian Institute of Technology konzipiert welches im

[35] Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union; http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and, 07/02/2013, letzter Zugriff: 1. November 2014.