Fraunhofer IOSB

visIT

[Privacy by Design und IT-Sicherheit]

www.iosb.fraunhofer.de

ISSN 1616-8240

Fraunhofer IOSB

Impressum

***vis*IT** erscheint etwa vier mal pro Jahr und informiert über ausgewählte Forschungsthemen des Fraunhofer IOSB. Für die Bestellung von Einzelheften, ein kostenloses ***vis*IT**-Abo sowie für Adressänderungen und Abbestellungen schicken Sie bitte eine E-Mail an publikationen@iosb.fraunhofer.de

Herausgeber
Prof. Dr.-Ing. habil. Jürgen Beyerer

Redaktion
Ulrich Pontes

Layout
Ellen Simon

Druck
Kraft Premium GmbH
76275 Ettlingen

Anschrift der Redaktion
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
Fraunhoferstr. 1
76131 Karlsruhe
Telefon +49 721 6091-300
Fax +49 721 6091-413
presse@iosb.fraunhofer.de

Ein Institut der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V. München

19. Jahrgang
ISSN 1616-8240

Bildquellen

Seite 4: GUIDE_BMBF_Projektbild_VOLLVERSION_Fotolia_162241958_L

Seite 5: Depositphotos_11035116

Alle anderen Abblildungen:
© Fraunhofer IOSB

INHALT

Gastbeiträge

Themen

Editorial

Liebe Freunde des Fraunhofer IOSB,

schon der Titel dieser Ausgabe umfasst mit den Begriffen ***Privacy by Design*** und ***IT-Sicherheit*** zwei Begriffe, die momentan in aller Munde sind, aber keinesfalls eindeutig verstanden werden. Für uns bedeuten sie, dass wir unsere Systeme technisch derart gestalten, dass der Schutz sensibler Daten bereits beim Entwurf einer Technologie beachtet wird. Dies umfasst im Falle von Privacy by Design die Gewährleistung des Datenschutzes betroffener Personen, im Falle von IT-Sicherheit die Vertraulichkeit, Integrität und die Verfügbarkeit von Informationen und Systemen, welche im digitalen Zeitalter ein hohes Gut darstellen.

Damit steht diese Ausgabe unter einem Motto, das brennender fast nicht sein könnte. Folgt man den Medien, scheint es fast so, als wäre jetzt die absolut letzte Chance, das Thema Datenschutz und IT-Sicherheit zu bearbeiten und die eigene Firma in ihrer Existenz zu schützen. So waren Anfang Mai die Zeitungen voller Warnungen vor der Europäischen Datenschutzgrundverordnung (DSGVO) und der damit einhergehenden Abmahnwelle. Die Furcht vor hohen Bußgeldern – die DSGVO sieht Strafen von bis zu vier Prozent des weltweiten Jahresumsatzes einer Firma als Obergrenze für vorsätzliche oder grob fahrlässige Verstöße gegen den Datenschutz vor – wurde durch entsprechende Beiträge der Medien geschürt. Fast täglich wird in den Medien darüber berichtet, dass Hacker Angriffe auf Daten von Firmen und auch von Staaten verüben. So beziffert das IT-Sicherheitsunternehmen Symantec für Deutschland den direkten finanziellen Schaden durch Internetkriminalität auf 16,4 Milliarden Euro.

Obwohl wir es als Forscher schätzen, wenn die Sensibilität für dieses wichtige Thema steigt, sehen wir in der vorherrschenden Kommunikation wenig konstruktive Diskussionsansätze, wie das Problem tatsächlich zu lösen ist. Auch wenn man heute vermutlich nicht mehr mit Gewissheit sagen kann, von wem der Ausspruch »Sicherheit ist kein Zustand, sondern ein Prozess« eigentlich stammt, stimmt er mehr denn je. Mit kurzfristigen Einzelaktionen können die Herausforderungen IT-Sicherheit und Datenschutz nicht bewältigt werden. Es braucht methodische Arbeit, um das eigene Schutzniveau dauerhaft und nachhaltig zu erhöhen.

Da Datenschutz und IT-Sicherheit klassische Querschnittsthemen sind und der Bedarf daran in nahezu allen Domänen – vom Auskunftssystem bis hin zur kritischen Infrastruktur – zu finden ist, hoffen wir, dass in unserer Themenauswahl auch für Sie etwas dabei ist und wünschen Ihnen eine anregende Lektüre.

Karlsruhe, im Dezember 2018

Prof. Dr.-Ing. habil. Jürgen Beyerer Dr. Elisabeth Peinsipp-Byma Dr.-Ing. Thomas Usländer

Prof. Dr.-Ing. habil. Jürgen Beyerer
Institutsleiter

Dr. rer. nat. **Elisabeth Peinsipp-Byma**
Abteilungsleiterin Interaktive Analyse und Diagnose (IAD)

Dr.-Ing. Thomas Usländer
Abteilungsleiter Informationsmanagement und Leittechnik (ILT)

Gastbeitrag

ADRESSATEN DER DATENSCHUTZRECHTLICHEN VERANTWORTUNG IN DER FORSCHUNG

In Forschungsprojekten ist zu Beginn die datenschutzrechtliche Verantwortung festzulegen. Aufgabe des Verantwortlichen ist es, sicherzustellen, dass die Verarbeitung personenbezogener Daten den Anforderungen der Datenschutzgrundverordnung der Europäischen Union (DSGVO) entspricht. Es sind geeignete technische und organisatorische Maßnahmen zu treffen, um die Rechte und Freiheiten natürlicher Personen zu wahren (Art. 24 DSGVO). Da die Nutzung personenbezogener Daten (Bild, Name, Kennnummer, Standort, Verhalten etc.) einen Eingriff in das Persönlichkeitsrecht bedeutet, ist z. B. eine Einwilligung des Betroffenen zu der vorgesehenen Datenverarbeitung für einen bestimmten Zweck erforderlich.

WER IST DATENSCHUTZRECHTLICH VERANTWORTLICH?

»Verantwortlicher« ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen **über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet** (…) (Art. 4 Nr. 7 DSGVO). In einem Forschungskonsortium kommen alle Verbundpartner als Träger der datenschutzrechtlichen Verantwortung infrage. Mit dem Projektantrag und dem Kooperationsvertrag haben die Projektbeteiligten ihren Forschungszweck festgelegt. Sie sind daher gemeinsam für die Datenverarbeitung verantwortlich, vgl. Art. 26 DSGVO.

WIE WIRD DIE VERANTWORTUNG FESTGELEGT?

Die für die Datenverarbeitung gemeinsam Verantwortlichen legen in einer **Vereinbarung** in transparenter Form fest, wer von ihnen welche Verpflichtung nach der Datenschutzgrundverordnung der Europäischen Union erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Personen betrifft (Auskunft, Berichtigung, Löschung etc.) und wer welchen Informationspflichten gem. Art. 13 und 14 DSGVO nachkommt. Bei der Verantwortungszuweisung können die einzelnen Arbeitspakete (Projektaufgaben, Experimente etc.) berücksichtigt werden. So kann festgelegt werden, dass jeder Projektpartner die datenschutzrechtliche Verantwortung für die eigenen Arbeitspakete trägt.

KONTAKT

Prof. Dr. jur. Brunhilde Steckler

Fachhochschule Bielefeld
Fachbereich Wirtschaft und Gesundheit Interaktion 1

33619 Bielefeld

brunhilde.steckler@fh-bielefeld.de
www.fh-bielefeld.de

Gastbeitrag

IT-SICHERHEIT: EINE KOMPLEXE UND LANGFRISTIGE HERAUS-FORDERUNG

Mit der fortschreitenden Digitalisierung aller Industriezweige gewinnt auch das Thema IT-Sicherheit verstärkt an Bedeutung. Der in diesem Zuge vielfach gehegte Wunsch nach vollständig sicheren IT-Systemen ist zwar nachvollziehbar – in der Praxis mit komplexen IT-Landschaften und unter Einbeziehung des Faktors Mensch jedoch fernab jeglicher Realität. Folglich ist IT-Sicherheit in der Praxis primär eine (Risiko-)Managementaufgabe, die u. a. die Identifikation und Bewertung von Risiken und darauf aufbauend die Ergreifung von (ökonomisch sinnvollen) Schutzmaßnahmen umfasst.

Aus technischer Sicht sehen wir uns hier mit vielfältigen Herausforderungen konfrontiert. Vor allem der aktuell vorherrschende Drang, reflexartig vormals isolierte eingebettete Systeme mit dem Internet zu verbinden (Stichwort Internet of Things, kurz IoT), erhöht deren Angriffsfläche signifikant und sollte bezüglich der Sinnhaftigkeit in vielen Fällen zumindest kritisch hinterfragt werden.

Ohne Frage bietet die Digitalisierung einmalige Chancen und sollte angesichts rasanter technologischer Entwicklungen keinesfalls verschlafen werden. Wer von den Vorteilen der Digitalisierung profitieren möchte, muss jedoch als Grundvoraussetzung bereit sein, die damit einhergehenden IT-Sicherheitsrisiken zu erkennen und geeignete Schutzmaßnahmen zu ergreifen.

Aus Sicht der Forschung existieren hier bereits zahlreiche Lösungen. Am Kompetenzzentrum IT-Sicherheit des FZI machen wir jedoch immer wieder die Erfahrung, dass insbesondere KMU angesichts der hohen Komplexität der Thematik bei der Umsetzung in die Praxis Unterstützung benötigen. Insbesondere der Blockchain-Hype zeigt zudem, dass viele Unternehmen bei der technologischen Bewertung von komplexen Lösungen im Bereich der IT-Sicherheit an ihre Grenzen stoßen.

Auch für die Zukunft zeichnen sich für das Thema IT-Sicherheit spannende Entwicklungen ab: So bietet z. B. das Thema KI das Potenzial, Angriffe und Schwachstellen zunehmend automatisiert zu erkennen, erfordert aber zugleich die Entwicklung neuer Methoden zur Absicherung solcher selbstlernenden Systeme vor Manipulation.

KONTAKT

PD Dr.-Ing. Ingmar Baumgart

Leiter Kompetenzzentrum
IT-Sicherheit
Forschungszentrum Informatik FZI

76131 Karlsruhe
Telefon +49 721 9654-355
baumgart@fzi.de
www.fzi.de

IT-SICHERHEIT FÜR INDUSTRIELLE ZUSTANDSÜBERWACHUNGS-SYSTEME

KONTAKT

Felix Specht M.Sc.

Digitale Infrastruktur (DIS)
Fraunhofer IOSB-INA Lemgo

Telefon +49 5261 942 90-44
felix.specht@iosb-ina.fraunhofer.de
www.fraunhofer-owl.de

KONTAKT

Jens Otto M.Sc.

Digitale Infrastruktur (DIS)
Fraunhofer IOSB-INA Lemgo

Telefon +49 5261 942 90-44
jens.otto@iosb-ina.fraunhofer.de
www.fraunhofer-owl.de

Cyber-physische Produktionssysteme (CPPS) bestehen aus Hardware- und Software-Komponenten und kontrollieren physikalische Produktionsprozesse. Ein Hauptmerkmal von CPPS ist die Fähigkeit sich an geänderte Produktionsziele, wie neue Produktvarianten oder Produktionsmodule, anzupassen. Abbildung 1a) zeigt ein modulares CPPS. Jedes Produktionsmodul stellt eine Fähigkeit zur Verfügung, z. B. Transportieren, Abfüllen, Entladen oder Erhitzen.

Condition Monitoring Systeme (Zustandsüberwachungssysteme, kurz CMS) werden eingesetzt, um Fehler in CPPS zu erkennen, z. B. den Ausfall eines Transportmoduls oder eines Heißluftmoduls. Dazu werden beispielsweise Prozessdaten wie Motorsignale oder Temperaturwerte eines Produktionsmoduls mit maschinellen Lernverfahren analysiert. Deep Neural Networks (tiefe neuronale Netze, kurz DNN) sind maschinelle Lernverfahren, welche mit Prozessdaten trainiert werden können. Somit lernen DNN einen physikalischen Prozess als mathematisches Modell abzubilden.

Bei der Verwendung von DNN gibt es jedoch ein Problem. Es kann nicht mit absoluter Sicherheit bestimmt werden, ob alle möglichen Fehler im CPPS erkannt werden können. Dies liegt daran, dass die zum Training verwendeten Prozessdaten nicht alle möglichen Systemzustände enthalten. Insbesondere wird das Problem deutlich durch sogenannte Adversarial Examples. Dabei handelt es sich um speziell berechnete Prozessdaten, die es ermöglichen ein

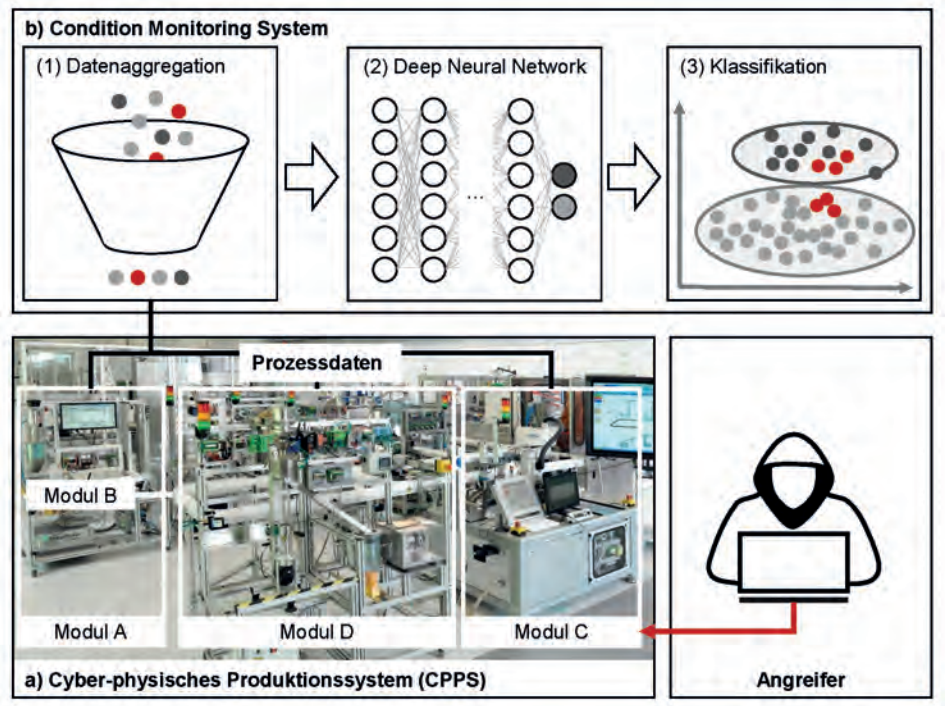


Abbildung 1: Im cyber-physischen Produktionssystem (a) kann ein Angriff mit Adversarial Examples gegen das Condition Monitoring System (b) zu unerkannten Störfällen führen.

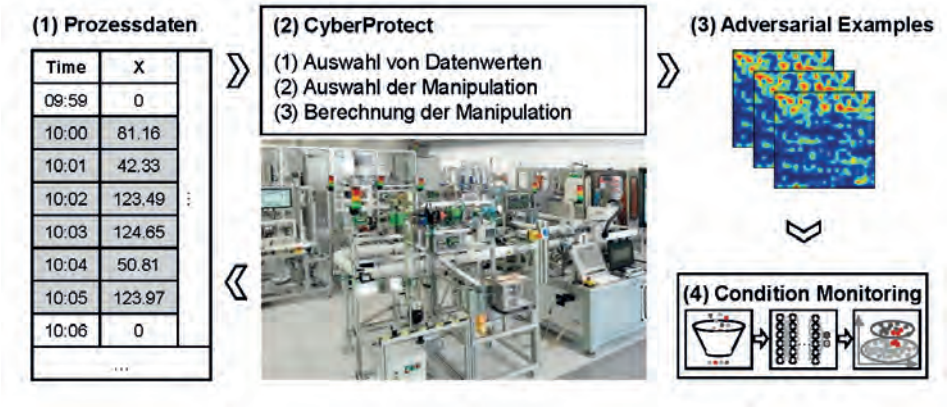


Abbildung 2: Die grundlegende Idee des CyberProtect-Lösungsansatzes.

CMS zu stören. Hacker können Adversarial Examples verwenden, um unbemerkt vom CMS Prozessdaten zu manipulieren (Abb. 1). Durch die Manipulation der Prozessdaten können Produktionssysteme gestört oder beschädigt werden, z. B. kann ein manipuliertes Heißluftmodul zu einem Brand in der Fabrik führen.

Die Literatur beschreibt Adversarial Examples als manipulierte Eingaben mit der Fähigkeit, ein DNN zu täuschen, sodass das DNN die Eingabe falsch kategorisiert. Dabei sind Adversarial Examples nahezu identisch im Vergleich zu nicht manipulierten Eingaben. DNN werden unter anderem in autonomen Fahrzeugen zur Auswertung von Kamerabildern eingesetzt. In diesem Zusammenhang sind Adversarial Examples beispielsweise manipulierte Bilder, die dazu führen, dass ein DNN ein Stoppschild fälschlicherweise als Vorfahrtsschild erkennt. Dies kann zu Sach- und Personenschäden führen.

Sicherheitsforscher am Fraunhofer IOSB-INA in Lemgo haben einen Lösungsansatz entwickelt, um CMS vor Angriffen mit Adversarial Examples zu schützen. Die Softwarelösung CyberProtect berechnet Adversarial Examples und verwendet diese, um DNN-basierte CMS abzusichern (Abb. 2). Für die Berechnung von Adversarial Examples wird ein trainiertes DNN benötigt. Zunächst wird ein DNN mit zuvor aufgezeichneten Prozessdaten eines CPPS trainiert. Die Prozessdaten beinhalten sowohl fehlerhafte als auch nicht fehlerhafte Produktionsdurchläufe. Anschließend werden Adversarial Examples berechnet, indem mithilfe des trainierten DNN spezielle Prozessdatenwerte ausgewählt und manipuliert werden. Das DNN wird nun mit den Prozessdaten und den berechneten Adversarial Examples neu trainiert. Dadurch bildet das DNN nicht nur den physikalischen Prozess ab, sondern auch Prozessdaten, die zu einer falschen Erkennung durch das CMS führen können. Das Ergebnis ist ein DNN, das vor Manipulation durch Adversarial Examples geschützt ist.

Der Einsatz von CyberProtect hat zwei Vorteile:

- DNN in CMS können bezüglich ihrer Fähigkeit zur Fehlererkennung bewertet werden, indem sie durch Adversarial Examples getestet werden.
- DNN können vor Manipulation durch Adversarial Examples geschützt und CMS somit verbessert werden.

Zukünftige Arbeiten befassen sich mit einem generalisierten Lösungsansatz, um DNN nicht nur gegen bekannte, sondern auch gegen unbekannte Adversarial Examples zu schützen.

Literatur:

[1] F. Specht; J. Otto; O. Niggemann; B. Hammer: Generation of Adversarial Examples to Prevent Misclassification of Deep Neural Network based Condition Monitoring Systems for Cyber-Physical Production Systems. In Proc. of 16th IEEE International Conference on Industrial Informatics (INDIN), 2018.

[2] J. Otto; B. Vogel-Heuser; O. Niggemann: Automatic parameter estimation for reusable software components of modular and reconfigurable cyber-physical production systems in the domain of discrete manufacturing. IEEE Transactions on Industrial Informatics, 14(1):275–282, 2018.

[3] C. Szegedy; W. Zaremba; I. Sutskever; J. Bruna; D. Erhan; I. Goodfellow; R. Fergus: Intriguing properties of neural networks. In Proc. of the 2nd International Conference on Learning Representations (ICLR), Banff, Canada, 2014.

[4] I. Goodfellow; J. Shlens; C. Szegedy: Explaining and harnessing adversarial examples. In Proc. of the 3rd International Conference on Learning Representations (ICLR), San Diego, USA, 2015.

[5] J. Otto; B. Vogel-Heuser; O. Niggemann: Online parameter estimation for cyber-physical production systems based on mixed integer nonlinear programming, process mining and black-box optimization techniques. at - Automatisierungstechnik 66.4 (2018): 331-343.

SECURITY-TESTING FÜR INDUSTRIELLE AUTOMATISIERUNGS-KOMPONENTEN

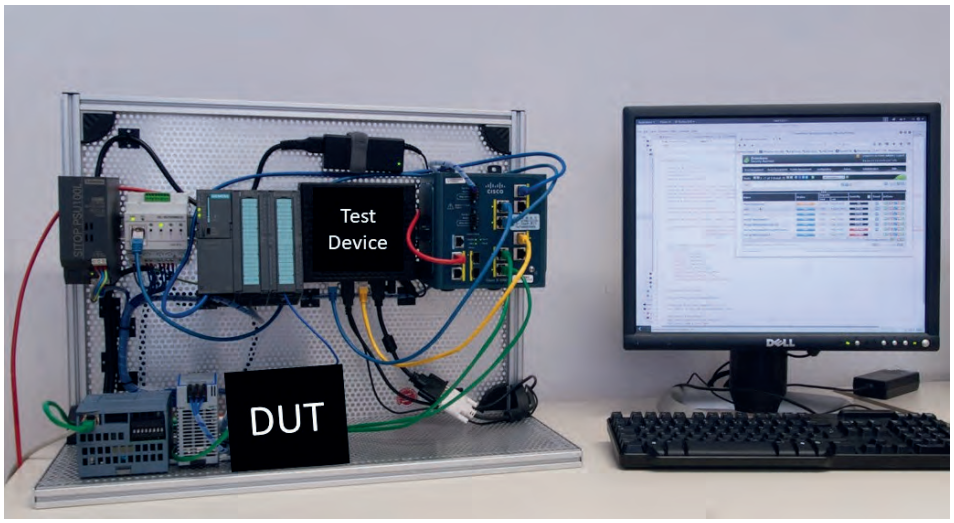


Abbildung 2: Aufbau von ISuTest zur Untersuchung von Automatisierungskomponenten.

Maschinen und Geräte im industriellen Umfeld werden verbreitet durch Automatisierungskomponenten gesteuert und überwacht. Diese kommunizieren auf verschiedenen Ebenen. Zum einen stellen sie Echtzeitfunktionalitäten in ihrer Kommunikation mit den Maschinen und Geräten bereit. Zum anderen werden sie im Zuge von *Industrie 4.0* und dem *Industrial Internet of Things* (IIoT) immer stärker mit lokalen Netzen oder auch mit dem Internet verbunden. Beispielsweise bieten einige Automatisierungskomponenten Webanwendungen an, auf die über das Netzwerk zugegriffen werden kann. Diese Webanwendungen können unter anderem zur Konfiguration und Statusabfrage dienen.

AUTOMATISIERUNGSKOMPONENTEN ALS ANGRIFFSZIEL

Durch die erhöhte Vernetzung und das Angebot weiterer Zugriffspunkte auf die Automatisierungskomponenten können diese leichter zum Ziel von Angreifern werden. Da die Automatisierungskomponenten zentrale Bestandteile der Produktion sind, kann ein Angriff auf sie weitreichende Folgen haben. So können Sachschäden, Reputationsverlust oder auch Personenschäden die Folge sein.

SECURITY-TESTING

Um Angriffe zu vermeiden, müssen Schwachstellen in Automatisierungskomponenten erkannt und möglichst früh ausgebessert werden. Die Überprüfung, ob Schwachstellen vorliegen (sogenanntes Security-Testing), sollte schon früh in den Entwicklungsprozess einer Automatisierungskomponente eingebunden werden.

Der generelle Ablauf eines solchen Security-Testings ist in Abbildung 1 dargestellt. Ein Test-Device führt hierbei die Tests zur Überprüfung des zu untersuchenden Systems aus. Dafür sendet das Test-Device über einen

KONTAKT
Anne Borcherding

Informationsmanagement und Leittechnik (ILT)
Fraunhofer IOSB

Telefon +49 721 6091-311
anne.borcherding@iosb.fraunhofer.de
www.iosb.fraunhofer.de/ILT

Kommunikationskanal verschiedene Eingaben an das Device under Test (DUT). Dessen Ausgaben werden wiederum vom Test-Device ausgewertet (Monitoring). Entsprechen die Ausgaben des Device under Test nicht den erwarteten Werten, liegt wahrscheinlich eine Schwachstelle vor. Bei Automatisierungskomponenten können diese zu vergleichenden Ausgaben vielfältig sein. Hierunter fallen beispielsweise elektrische oder magnetische Ausgaben, aber auch Ausgaben über Lichtsignale oder Ethernet.

Besonders effizient ist automatisiertes Security-Testing, bei welchem der Entwickler selbst kaum eingreifen muss. Im Bereich der Office-IT existieren hierfür bereits entsprechende Werkzeuge und Frameworks. Aufgrund der Vielzahl an Schnittstellen und Standards bei industriellen Komponenten gestaltet sich dies für Automatisierungskomponenten schwieriger.

Am Fraunhofer IOSB wurde daher das Security-Testing-Framework ISuTest entworfen und in einem Prototyp umgesetzt [1]. ISuTest ermöglicht automatisiertes Security-Testing von Automatisierungskomponenten und bezieht dabei verschiedene Schnittstellen der Automatisierungskomponenten in die Untersuchungen ein.

Ein Beispielaufbau von ISuTest ist in Abbildung 2 dargestellt. Auf der linken Seite ist eine Testumgebung mit verschiedenen Automatisierungskomponenten und zusätzlicher Infrastruktur, beispielsweise für die Stromversorgung und die Kommunikation mit dem Test-Device, aufgebaut. Über die Tastatur und den Bildschirm kann ein Entwickler neue Security-Tests definieren, ausführen lassen und die Ergebnisse auswerten. ISuTest wurde durch zwei Erweiterungen in seinem Funktionsangebot ergänzt. Zum einen wurde eine Fuzzing-Komponente eingebunden [2]. Diese variiert gewisse Eingaben an das Device under Test unter Verwendung verschiedener Heuristiken. Diese Eingaben können weitere Schwachstellen aufdecken.

WEBSERVER-SECURITY

Zusätzlich zu der Erweiterung um eine Fuzzing-Komponente wurden verschiedene bestehende Verwundbarkeitsscanner für traditionelle Webanwendungen in ISuTest integriert. Diese Verwundbarkeitsscanner führen Security-Tests gegen Webanwendungen aus, unabhängig davon, ob diese auf einem klassischen Webserver oder auf einer Automatisierungskomponente laufen. Durch die Integration der Verwundbarkeitsscanner in ISuTest werden diese Verwundbarkeitsscanner um das Monitoring anderer Ausgabekanäle erweitert. So ist es möglich herauszufinden, wie sich Angriffe auf die Webanwendung auf andere Schnittstellen auswirken.

Durch diese Integration konnten bereits einige neue Schwachstellen auf realen Automatisierungskomponenten gefunden werden. Dabei war es insbesondere möglich, durch einen Angriff auf die Webanwendung andere Schnittstellen der Automatisierungskomponenten zu treffen.

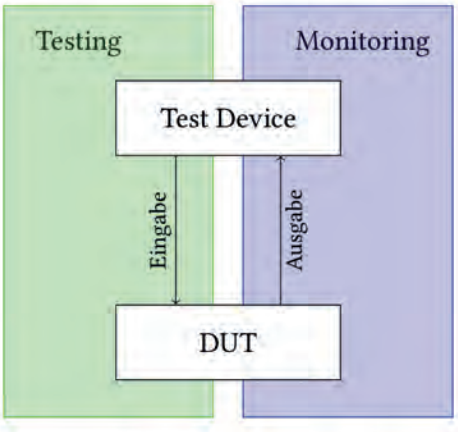


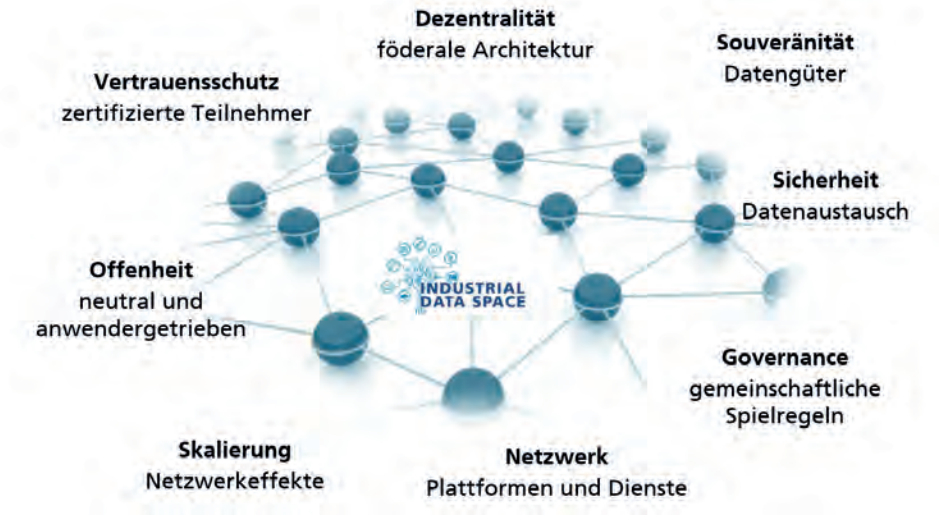
Abbildung 1: Genereller Ablauf eines Security-Tests.

Literatur:

[1] Steffen Pfrang, David Meier, and Valentin Kautz: Towards a Modular Security Testing Framework for Industrial Automation and Control Systems: ISuTest. In: Proceedings of the 22nd IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2017. Limassol, Cyprus, 2017.

[2] Steffen Pfrang et al.: Advancing Protocol Fuzzing for Industrial Automation and Control Systems. In: Proceedings of the 4th International Conference on Information Systems Security and Privacy - Volume 1: ForSE, INSTICC. SciTePress, 2018, pp. 570–580.

DATENSOUVERÄNITÄT DURCH DATENRÄUME



Leistungsmerkmale des Industrial Data Space.

In einer zunehmend vernetzten Welt bilden Daten bzw. deren Austausch die Grundlage innovativer Geschäftsmodelle. Das Konzept der Datenräume (von engl. Data Spaces) verfolgt das Ziel, Daten für derartige Geschäftsmodelle unkompliziert verfügbar, auffindbar und nutzbar zu machen. Hierzu werden Beschreibungen von Daten in einer gemeinsamen Sprache (Informationsmodell) erstellt und auf einem Datenmarktplatz veröffentlicht. Die Daten selbst bleiben bis zu ihrem Abruf in der Hoheit der Organisation und werden auch erst bei Bedarf in die von abrufenden Anwendungen benötigten Formate oder Strukturen konvertiert. Ebenso können über den Datenmarktplatz Applikationen ausgetauscht werden, die Auswertefunktionen für bestimmte Daten bereitstellen. Ein Datenraum ist somit ein dezentrales Peer-to-Peer-Netzwerk, in welchem Daten bzw. Datenanalysebedarfe mit entsprechenden Auswertedienstleistern zusammenfinden.

Der Industrial Data Space (https://www.fraunhofer.de/de/forschung/fraunhofer-initiativen/industrial-data-space.html) ist ein solcher virtueller Datenraum, der den sicheren Austausch und die einfache Verknüpfung von Daten in Geschäftsökosystemen auf Basis von Standards und mithilfe gemeinschaftlicher Governance-Modelle unterstützt. Um gemeinsame Anforderungen zu erheben und gemeinsame Standards zu etablieren, organisieren sich die beteiligten Fraunhofer-Institute mit Unternehmen in einem Verein, der International Data Spaces Association (https://www.international-dataspaces.org/).

Für Unternehmen sind Daten nur dann wertvoll, wenn sie auch verarbeitet werden können. Gleichzeitig muss eine umfassende und gemeinhin akzeptierte neue Umgangspraxis mit der Verwertung und Nutzung von Daten verankert werden, die in der Praxis teils durch Verträge und teils durch tech-

KONTAKT

Dr.-Ing. Pascal Birnstill

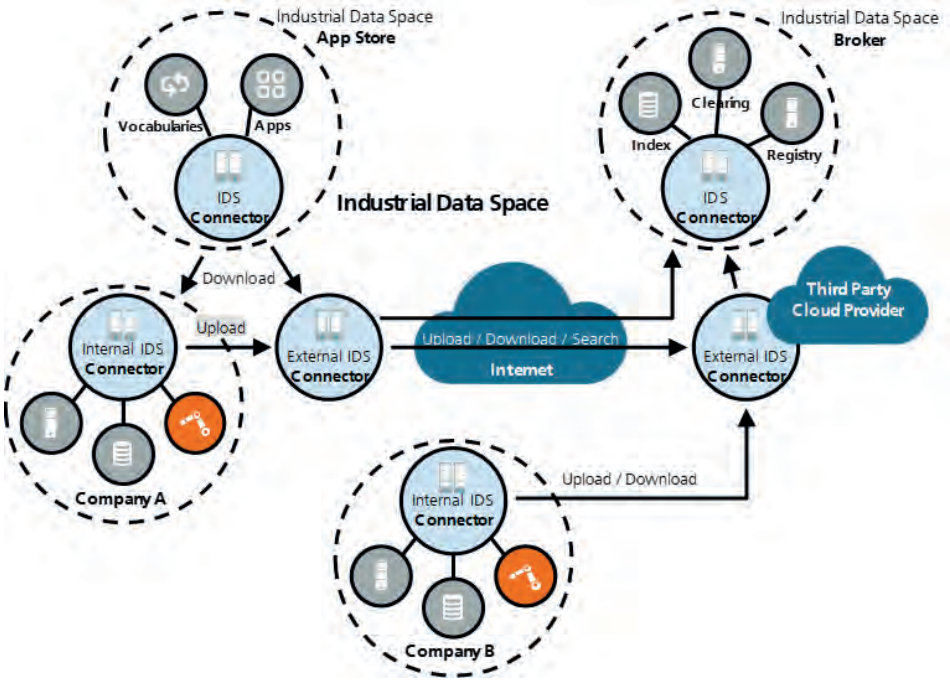
Interaktive Analyse und Diagnose
Fraunhofer IOSB

Telefon +49 721 6091-612
pascal.birnstill@iosb.fraunhofer.de
www.iosb.fraunhofer.de/IAD

nische Mechanismen wie etwa Nutzungskontrolle durchgesetzt werden muss. Der Datenbereitsteller – also das Unternehmen – legt in der Datenbeschreibung selbst fest, zu welchen Bedingungen und Zwecken ein bereitgestellter Datensatz genutzt werden darf. Die Daten werden nur dann ausgetauscht, wenn sie von vertrauenswürdigen Partnern mittels Konnektoren angefragt werden, die über hinreichende Mechanismen zur Gewährleistung von Datensicherheit und Datensouveränität verfügen. Um diese Überprüfung zu ermöglichen, bietet der Industrial Data Space Zertifizierungskriterien sowie eine Authentifizierungs- und Attestierungsinfrastruktur an. Teilnehmende Organisationen können somit die Vertrauenswürdigkeit ihrer Konnektoren zertifizieren lassen und zu jeder Zeit überprüfbar machen.

Im Ergebnis können Partner einer Wertschöpfungskette in gegenseitigem Einverständnis gemeinsam auf bestimmte Daten zugreifen, um jeweils oder gemeinsam damit etwas Neues anzufangen, neue Geschäftsmodelle zu entwickeln, ihre eigenen Prozesse effizienter zu gestalten oder anderweitig zusätzliche Wertschöpfungsprozesse zu initiieren.

Das Fraunhofer IOSB trägt zur Sicherheitsarchitektur des Industrial Data Space bei, insbesondere bei den Themen Data-Provenance-Tracking, Nutzungskontrolle und Attestierung von Komponenten. Data-Provenance-Tracking verfolgt die Flüsse von Daten über Systemgrenzen hinweg und macht sie nachvollziehbar. Hierdurch können Nutzungskontrolltechnologien unterstützt werden, welche die Nutzung von Daten in Übereinstimmung mit vereinbarten Richtlinien technisch durchsetzen. Nutzungskontrolle erlaubt es einem Datenbereitsteller, vorab Richtlinien für die Nutzung seiner Daten zu spezifizieren, für deren Einhaltung der Datennutzer über entsprechende technische Mechanismen verfügen muss. Beispiele für solche Richtlinien sind: »Daten dürfen nur für 24 Stunden gespeichert werden« oder »Daten dürfen nur in anonymisierter Form weitergegeben werden«. Entsprechende Mechanismen stellt der Industrial Data Space im sogenannten Trusted-Connector bereit (https://industrial-data-space.github.io/trusted-connector-documentation/docs/dev_core/).
Damit der Datenbereitsteller sich auf die Wirksamkeit der Mechanismen verlassen kann, wird die Integrität eines Trusted-Connectors attestiert, sodass mögliche Manipulationen erkannt werden können. Durch dieses Zusammenwirken von Sicherheitsmechanismen behält der Datenbereitsteller die Souveränität über seine Daten auch noch nach dem Austausch, da er sich auf die Einhaltung der geforderten Richtlinien verlassen kann.



Architektur des Industrial Data Space.

DAS LERNLABOR CYBERSICHERHEIT

KONTAKT

Dipl.-Ing. Steffen Nicolai

Energie (NRG)
Fraunhofer IOSB Ilmenau

Telefon +49 3677 461-112
steffen.nicolai@iosb-ast.fraunhofer.de
www.iosb.fraunhofer.de/AST

KONTAKT

Prof. Dr.-Ing. Jörg Lässig

Energie (NRG)
Fraunhofer IOSB Ilmenau,
Außenstelle Görlitz

Telefon +49 3581 7925-354
joerg.laessig@iosb-ast.fraunhofer.de
www.iosb.fraunhofer.de/AST

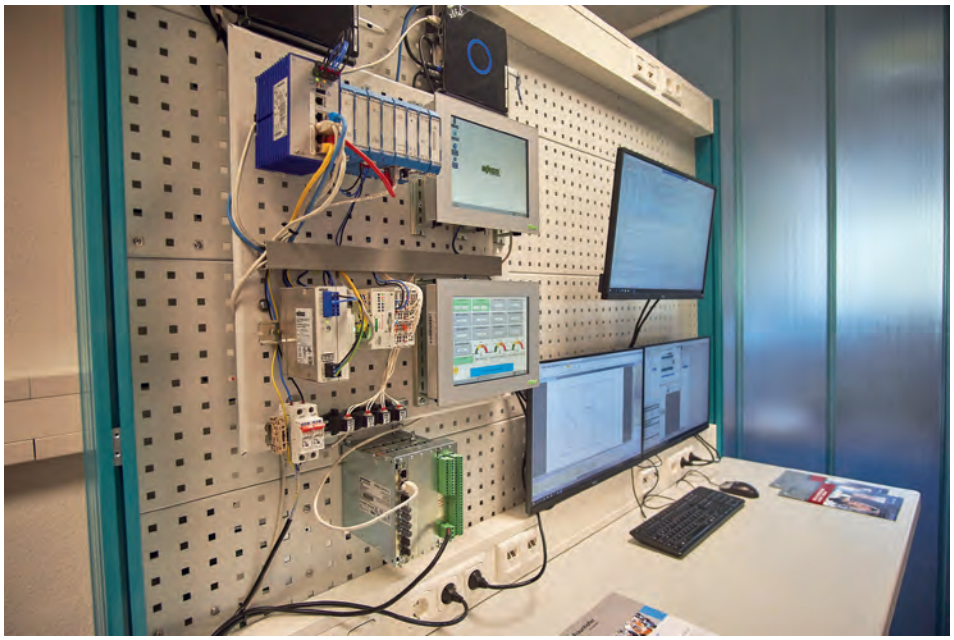
Die fortschreitende Automatisierung, Digitalisierung und Vernetzung führt zu deutlich gestiegenen Anforderungen an die Betreiber von Energie- und Wasserversorgungsnetzen. Dies umfasst neben der gebräuchlichen Automatisierungs- und Fernwirktechnik auch immer mehr die gesamte IKT-Unternehmensinfrastruktur. Um beide Bereiche in einem ganzheitlichen Forschungs- und Schulungspaket abdecken zu können, haben der Standort Ilmenau mit dem Schwerpunkt Energiesysteme sowie die Außenstelle Görlitz mit dem Schwerpunkt IT-Systeme beide Kompetenzen in dem vom BMBF geförderten »Lernlabor Cybersicherheit Energie- und Wasserversorgung« (LLCS) gebündelt. Dies umfasst neben den Forschungsaktivitäten (z. B. Security by Design, Security by Default, Resilience by Design) auch zwei Lernlabore sowie ein umfassendes und auf die unternehmensspezifischen Bedürfnisse zugeschnittenes Schulungsportfolio.

FORSCHUNG

Das komplexe Forschungsthema Cybersicherheit betrifft sowohl energiesystemische Fragestellungen (Energieverteilnetze, Energiesystemführung, energiewirtschaftliche Prozesse, Identifikation von Cyberattacken, Gefährdungs-, Risiko- und Schwachstellenanalyse) als auch die Betrachtung der zugehörigen IKT-Systeme, IKT-Infrastruktur sowie IKT-Schnittstellen. Hier spielen beispielsweise Bedrohungs- und Angriffsszenarien, Penetrationstests oder die Integrität, Sicherheit und Vertraulichkeit als Kernziele der Informationssicherheit eine wichtige Rolle. Weitere Untersuchungen beziehen sich auf die sichere Kommunikation in Versorgungsinfrastrukturen, die Anomalie-Erkennung sowie die Robustheit und Resilienz von Energienetzen.

LABORINFRASTRUKTUR

Im Rahmen des LLCS wurde am Standort Ilmenau eine umfangreiche Demonstrator-



Ein Teil des Labordemonstrators mit zentralem SCADA-System in Ilmenau.

ENERGIE- UND WASSERVERSORGUNG

Plattform aufgebaut, die eine umfassende Nachbildung der Automatisierung der Leit- sowie der Feldebene in der elektrischen Energieversorgung erlaubt. Ziel der Plattform ist es, eine realitätsnahe Schulungsumgebung zu schaffen, um komplexe Zusammenhänge und das Zusammenspiel energietechnischer Prozesse mit den IKT-Komponenten von Fernwirk- und Leitsystemarchitekturen logisch und nachvollziehbar darstellen zu können. Der aktuelle Aufbau bildet einen Ausschnitt eines vollautomatisierten Umspannwerks mit unterschiedlichen Betriebsmitteln und Automatisierungskomponenten ab. Die installierten Komponenten sind an ein zentrales SCADA-System gekoppelt, sodass eine reale Umgebung für die installierte Fernwirktechnik gegeben ist. Für die Kommunikation der Komponenten wurden Protokolle verwendet, die den aktuellen Stand der Technik darstellen, aber die Möglichkeit bieten, zukünftige Entwicklungen zu integrieren. Die Datenbasis für das SCADA-System bildet eine hoch performante Echtzeitumgebung zur Netzberechnung, die es ermöglicht, komplexe elektrische Systeme zu simulieren. Über einen Power-Hardware-in-the-Loop (kurz PHIL) Versuchsstand können Betriebsmittel sowohl in das energetische Teilsystem als auch in die Simulation und das SCADA-System integriert werden. Somit ist es möglich, IT-Angriffe auf unterschiedlichste Betriebsmittel und komplette Versorgungsstrukturen während des Betriebs zu untersuchen.

Neben dem stationären Laboraufbau wurde am Standort Görlitz ein mobiler Demonstrator entwickelt. Der Aufbau bildet ein eigenständiges Szenario aus der Feldebene des Energiesektors ab und zeichnet sich durch eine kompakte, transportable Bauweise aus. Er besitzt neben aktuellen Automatisierungskomponenten der Energieversorgung

Mobiler Demonstrator des Lernlabors.

auch die Möglichkeit, Datenströme unterschiedlicher Protokolle zu monitoren und zu visualisieren. Damit können systematisch Angriffsszenarien entwickelt und praktisch erprobt werden. Auch die drei wesentlichen Schutzziele der Informationssicherheit (Integrität, Sicherheit und Vertraulichkeit) können in unterschiedlichen Ausprägungen berücksichtigt werden. Mithilfe integrierter Sicherheitskomponenten (verschiedene Firewalls) können abschließend die passenden Verteidigungsstrategien entwickelt werden. Der mobile Demonstrator dient in der Anwendung zum einen als flexibles Schulungsinstrument (z. B. für In-House-Schulungen), aber auch als Highlight-Exponat für diverse Veranstaltungen und Messen.

SCHULUNGEN

Das umfassende Cybersicherheits-Know-how sowohl auf Ebene der technischen Automatisierungs- und Systemtechnologie als auch im Bereich der IKT wird in einem umfangreichen Schulungsangebot der Fraunhofer Academy auf dem Bildungsmarkt angeboten. Zu den vielfältigen, auf die Kundenbedürfnisse zugeschnittenen Inhalte gehören unter anderem:

- Aktuelle Gesetzeslage
- Angriffsbeispiele und Angriffsablauf
- IT-Sicherheitsmanagement
- Security Awareness
- Mitarbeitersensibilisierung
- Standardisierungen (ISO 2700x, BSI IT-Grundschutz, VDE 3473)
- IT-Sicherheitsmanagement-Tools
- Vorbereitung und Ablauf von Zertifizierungen
- Vergleich von IT-Sicherheitsmanagement-werkzeugen
- Praktische Angriffs- und Fallbeispiele

Darüber hinaus sind In-House-Schulungen sowie Kooperationen mit externen Schulungsanbietern möglich. Zusätzlich ergeben sich unabhängige und individuell zugeschnittene FuE-Dienstleistungen rund um das Thema IT-Sicherheit für Firmen, kommunale und öffentliche Einrichtungen und im Umfeld der Energie- und Wasserversorgung. Diese umfassen:

- Konzepte und Analysen von energietechnischen Infrastrukturen
- Risikobewertung im Rahmen von Informations-Sicherheits-Management-System (ISMS)
- Erarbeitung von Konzepten für die Ausgestaltung von ISMS bei Energieversorgern.

QR-Code zu den Schulungen.

PRIVACY INSIGHT

Abbildung 1: Die Startansicht der Auskunftsplattform Privacy Insight.

MOTIVATION

Die wachsende Komplexität moderner Informationssysteme erschwert die Nachvollziehbarkeit der Speicherung und Verarbeitung personenbezogener Daten. Der einzelne Bürger ist den Systemen quasi ausgeliefert. Das Datenschutzrecht versucht dem entgegenzuwirken. Transparenz, das Recht zu wissen, wer was wann und bei welcher Gelegenheit über einen weiß, ist ein fundamentales Grundrecht. In der Europäischen Datenschutz-Grundverordnung (DSGVO) ist dieses Recht in Artikel 15 verankert.

Es ist allerdings nicht ausreichend, dem Betroffenen mit unübersichtlichen Datenbergen zu überfrachten. Ausufernde Informationen in Textform können und wollen die meisten Betroffenen nicht lesen. Die DSGVO legt in Artikel 12 fest, dass Informationen an den Betroffenen verständlich und leicht zugänglich sein müssen. Nur durch eine knappe und übersichtliche Darstellung der Informationen in einem abgestuften Modell wird das Verständnis des Betroffenen gefördert.

Durch eine Auskunft muss dem Betroffenen zudem die Wahrnehmung seiner Interventionsrechte auf Löschung, Sperrung und Berichtigung gewährleistet werden.

ANSATZ

Die am Fraunhofer IOSB entwickelte Auskunftsplattform Privacy Insight bietet Betroffenen einen grafischen, interaktiven Zugang zu allen erforderlichen Informationen über die Datenverarbeitung. Zum Einstieg wird eine knappe Übersicht gezeigt. Bei Interesse erlaubt die Plattform ein stufenweises Eintauchen in weitere Informationen.

Privacy Insight ist eine Webanwendung. Sie besteht von oben nach unten aus den drei Teilen Navigationsleiste, Visualisierung des Informationsflusses (Herkunft-Empfänger-Ketten) und Statusleiste (Abbildung 1). Nach Anmeldung über die vorgelagerte Anmeldemaske wird der Informationsfluss zunächst mit minimalen Details angezeigt. Am linken Fensterrand sind alle Datenquellen, am

KONTAKT

Dr.-Ing. Erik Krempel

Interaktive Analyse und Diagnose
Fraunhofer IOSB

Telefon +49 721 6091-292
erik.krempel@iosb.fraunhofer.de
www.iosb.fraunhofer.de/IAD

Abbildung 2: Auskunft über die Datenverarbeitung in der Abteilung Kundenbetreuung.

rechten Rand alle Senken dargestellt. Die verantwortliche Stelle wird als ein Knoten in der Fenstermitte repräsentiert.

FUNKTIONSWEISE

Links neben den Quellen und rechts neben den Senken befinden sich jeweils Icons für alle erhobenen beziehungsweise übermittelten personenbezogenen Daten. Die Icons sind abhängig von der Datenkategorie gestaltet. Dies soll das Wiederfinden bestimmter personenbezogener Daten erleichtern. Bei der Auswahl eines Datums wird der Fluss dieses Datums hervorgehoben. Wird die Detailsicht für ein Datum geöffnet, ergibt sich dort die Möglichkeit das Datum einzusehen, zu exportieren, zu berichtigen, zu sperren oder zu löschen.

Wie oben erwähnt sind in der Informationsflussvisualisierung zu Beginn nur die Erhebung und Übermittlung personenbezogener Daten dargestellt. Durch Anwählen des Knotens öffnet sich die nächste Ebene in der Hierarchie, beispielsweise eine Sicht auf die einzelnen Abteilungen und die Informationsflüsse zwischen ihnen. Von besonderem Interesse für den Betroffenen sind Informationsflüsse zu Auftragsdatenverarbeitern, also externen Firmen, die die eigenen Daten im Auftrag verarbeiten. Diese Flüsse werden im Provenance-Graphen gesondert hervorgehoben.

Für jeden Knoten ist es möglich, ein Kontextmenü aufzurufen, um die in den entsprechenden Bereichen verarbeiteten oder gespeicherten Daten, gemeinsam mit dem jeweiligen Zweck der Verwendung, einzusehen (Abbildung 2). Kleine Icons machen deutlich, was mit den Daten im jeweiligen Knoten geschieht.

Die Navigationsleiste bietet Interaktionsmöglichkeiten, die sich nicht direkt auf einzelne Elemente des Informationsflusses beziehen. Die Möglichkeit im Rahmen des Rechts auf Datenübertragbarkeit, die gesamte Auskunft in einem maschinenlesbaren Format (JSON) zu exportieren, findet sich ebenfalls dort. Die Statusleiste bietet kontextsensitive Zusatzinformationen und dient der farblich codierten Darstellung des gewährleisteten Datenschutzniveaus.

NÄCHSTE SCHRITTE

Das Fraunhofer IOSB stellt mit Privacy Insight eine Lösung vor, die es Unternehmen erlaubt, ihre Auskunftsverfahren weit über das übliche Maß hinaus zu automatisieren. Damit werden nicht nur Mitarbeiter in der Kundenbetreuung entlastet, sondern man grenzt sich durch den hohen Komfort und das Datenschutzniveau von seinen Mitbewerbern ab.

Nach der Entwicklung eines Prototyps sind wir nun auf der Suche nach interessierten Partnern, die als erstes Privacy Insight für ihr Unternehmen testen wollen.

Literatur:

Christoph Bier; Kay Kühne and Jürgen Beyerer: Privacy Insight: The Next Generation Privacy Dashboard in: S. Schiffner; J. Serna; D. Ikonomou; K. Rannenberg (Editors): Privacy Technologies and Policy 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016, Proceedings.

Karlsruhe

Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung IOSB
Fraunhoferstraße 1
76131 Karlsruhe
Telefon +49 721 6091-0
Fax +49 721 6091-413
info@iosb.fraunhofer.de
www.iosb.fraunhofer.de

Ettlingen

Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung IOSB
Gutleuthausstraße 1
76275 Ettlingen
Telefon +49 7243 992-0
Fax +49 7243 992-299
www.iosb.fraunhofer.de

Ilmenau

Fraunhofer IOSB, Institutsteil für
angewandte Systemtechnik AST
Am Vogelherd 50
98693 Ilmenau
Telefon +49 3677 4610
Fax +49 3677 461-100
info@iosb-ast.fraunhofer.de
www.iosb-ast.fraunhofer.de

Görlitz

Fraunhofer IOSB, Institutsteil für
angewandte Systemtechnik AST
Außenstelle Görlitz,
Abteilung Energie
Brückenstraße 1
02826 Görlitz
Telefon +49 3581 7925354
joerg.laessig@iosb-ast.fraunhofer.de

Lemgo

Fraunhofer IOSB, Institutsteil
für industrielle Automation INA
Langenbruch 6
32657 Lemgo
Telefon +49 5261 94290-22
Fax +49 5261 94290-90
juergen.jasperneite@iosb-ina.fraunhofer.de
www.iosb-ina.fraunhofer.de

Beijing

Representative for Production and
Information Technologies
Unit 0610, Landmark Tower II
8 North Dongsanhuan Road
Chaoyang District
100004 Beijing, PR China
Telefon +86 10 6590 0621
Fax +86 10 6590 0619
muh@fraunhofer.com.cn