Fraunhofer

TRENDS FÜR CYBERSICHERHEIT

INHALT

6 »Oft mangelt es am Bewusstsein«
Doppelinterview mit Prof. Claudia Eckert und Prof. Michael Waidner

10 Cybersicherheit in der Produktion: Sicher vernetzt

12 Automotive Security: Sicher unterwegs

14 Sicherheit für kritische Infrastrukturen

16 Digitale Services – Was ist mit Sicherheit und Datensouveränität?

18 Sicherheit leicht gemacht
Interview mit Prof. Matthew Smith

20 Lernlabor Cybersicherheit:
Die Sicherheitsexperten von morgen

23 Kurzmeldungen

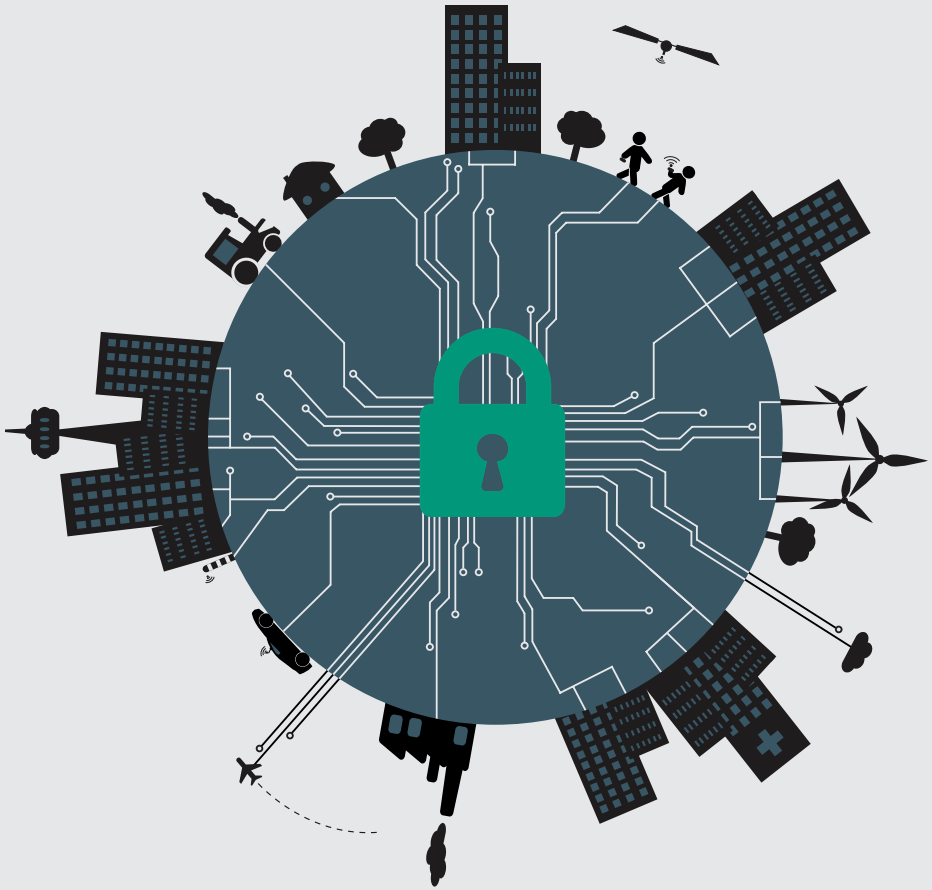
SICHER IN DIE DIGITALE ZUKUNFT

Cybersicherheit ist ein Grundpfeiler der Digitalisierung. Ohne Vertrauen in die Sicherheit neuer Technologien wird die digitale Transformation nicht gelingen. Allein 2015 verzeichnete das Bundeskriminalamt 45 000 Fälle von Cyberkriminalität mit einem Gesamtschaden von 40,5 Millionen Euro. Die Dunkelziffer liegt um ein Vielfaches höher. Gleichzeitig steigt das wirtschaftliche Potenzial durch Digitalisierung. Durch höhere Gewinne und weniger gebundenes Kapital errechneten Experten einen zusätzlichen Wertbeitrag von 420 Milliarden Euro allein in Westeuropa bis 2035.

Chancen und Risiken liegen in der digitalen Welt eng beieinander. Wer online ist, ist angreifbar. Je komplexer die Strukturen, desto verletzlicher sind sie. Es ist Aufgabe der Cybersicherheitsforschung, die Risiken zu minimieren, um die Chancen besser nutzen zu können. Fraunhofer-Institute forschen in vielen sicherheitsrelevanten Bereichen – sei es an kritischen Infrastrukturen, Industrie 4.0, vernetzter Mobilität oder Internetsicherheit generell. In diesem Heft finden Sie nur einen kleinen Ausschnitt des großen Spektrums.

Besonders am Herzen liegt mir zudem das Thema Aus- und Weiterbildung, denn mit der fortschreitenden Digitalisierung werden wir in den nächsten Jahren sehr viel mehr Sicherheitsspezialisten benötigen. Dabei ist schon jetzt ein besorgniserregender Mangel an Fachkräften zu beobachten. Der rasante Wettlauf mit den Cyberpiraten und die Entwicklung neuer, sicherer Technologien erfordern gut geschulte Experten, die immer auf dem neuesten Wissensstand sind und gleichzeitig kreative, neue Wege gehen. Deshalb hat die Fraunhofer Academy gemeinsam mit Fraunhofer-Instituten und Fachhochschulen ein beispielloses Bildungsprogramm für Cybersicherheit ins Leben gerufen.

Prof. Dr. Reimund Neugebauer



»Sicher ist, dass nichts sicher ist. Selbst das nicht.«
Joachim Ringelnatz, deutscher Schriftsteller

»Zu argumentieren, man mache sich nichts aus Datenschutz, weil man nichts zu verbergen habe, ist wie zu sagen, man mache sich nichts aus Redefreiheit, weil man nichts zu sagen habe.«
Edward Snowdon, Whistleblower

»Passwörter sind wie Unterwäsche. Du darfst sie keinen sehen lassen, musst sie regelmäßig wechseln und solltest sie nicht mit Fremden tauschen.«
Chris Pirillo, Technik-Blogger

»Der Computer wurde zur Lösung von Problemen erfunden, die es früher nicht gab.«
Bill Gates, Microsoft-Mitbegründer

»Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, wird am Ende beides verlieren.«
Benjamin Franklin, Erfinder und US-Staatsmann

Prof. Claudia Eckert

Prof. Michael Waidner

»OFT MANGELT ES AM BEWUSSTSEIN«

Ein Interview mit Prof. Claudia Eckert vom Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC und Prof. Michael Waidner vom Fraunhofer-Institut für Sichere Informationstechnologie SIT zu Herausforderungen, Chancen und Initiativen in punkto Cybersicherheit.

Vor einigen Jahren sah man die Cloud eher skeptisch. Heute scheint kaum noch jemand Bedenken zu haben. Gehen wir heute sorgloser mit unseren Daten um?

Eckert: Auch heute noch haben viele Cloud-Kunden Bedenken, die meist aus einem gefühlten Kontrollverlust resultieren – insbesondere im Mittelstand. Für Unternehmen geht es um die Einhaltung gesetzlicher Vorgaben, aber auch um den Schutz von Geschäftsgeheimnissen und Kundendaten. Deshalb gibt es durchaus ein gestiegenes Sicherheitsbewusstsein. Die Cloud-Anbieter versuchen zunehmend durch Transparenzmaßnahmen oder auch Zertifizierungen Vertrauen zu schaffen. Aufgabe der Sicherheitsforschung ist es, die Anbieter als neutraler Partner durch Technologien und Maßnahmen zu unterstützen. Denn eine professionell gemanagte Cloud-Infrastruktur ist gerade für kleine und mittlere Unternehmen in der Regel deutlich sicherer als eine in Eigenregie betriebene lokale Lösung.

Waidner: Auch wir sehen, dass Unternehmen sehr genau prüfen, welche Art von Cloud sie nutzen, welche Daten sie dort speichern und wie sicher der Service ist. Doch wer heute als Unternehmen erfolgreich sein will, der kommt an Cloud Computing nicht vorbei. Fraunhofer entwickelt deshalb zum einen ergänzende Lösungen wie OmniCloud, mit denen Unternehmen ihre Daten sicher und günstig in der Cloud speichern können. Zum anderen arbeiten wir an Verfahren zur automatisierten Analyse von Cloud-Diensten. Damit können Anbieter nachweisen, dass ihre Dienste gesetzliche oder kundenspezifische Anforderungen erfüllen.

Frau Eckert, Ihr Institut ist vor allem auf integrierte Sicherheit spezialisiert. Mit welchen Herausforderungen kommen Unternehmen zu Ihnen?

Eckert: Die größten Herausforderungen entstehen gerade im Bereich Automotive Security mit den rasanten Entwicklungen hin zum autonomen Fahren, aber auch bei der industriellen Sicherheit und in der vernetzten Gesundheitsversorgung – wie bei personalisierter Medizin oder vernetzten Medizingeräten. Die digitale Transformation führt in diesen Bereichen zu einem hohen Bedarf an maßgeschneiderten, eingebetteten Sicherheitslösungen. Klassische Lösungen sind hierfür häufig nicht geeignet, da sie oft zu aufwändig oder nicht echtzeitfähig sind oder nicht skalieren. Daneben wollen Unternehmen zunehmend Methoden und Werkzeuge für die Entwicklung sicherer Systemlösungen, um beispielsweise Risikoeinschätzungen einheitlich durchzuführen, sie nachvollziehbar und über Unternehmensgrenzen hinweg vergleichbar zu machen.

Herr Waidner, Ihr Institut führt regelmäßig Bedrohungsanalysen und Sicherheitstests durch. Was sind die häufigsten Sicherheitslücken?

Waidner: Die häufigsten Angriffe sind automatisierte Attacken, bei denen Angreifer massenhaft bekannte Sicherheitslücken von Servern oder Webanwendungen ausnutzen. Die Mehrzahl dieser Angriffe ließe sich mit geringem Aufwand abwehren, würden Unternehmen bekannte Prozesse und Technologien zur Absicherung einsetzen. Doch oft mangelt es etwa am Bewusstsein, sind die Sicherheitslösungen umständlich in der Handhabung oder der Aufwand und Betrieb sind

für kleine Firmen und Mittelständler zu kostspielig. Gleichzeitig wächst aber die Gefahr durch gezielte, hochprofessionelle Angriffe im Rahmen von Wirtschafts- oder Industriespionage. Um solche Advanced Persistant Threats zu erkennen und zu vereiteln, müssen Unternehmen moderne Sicherheitslösungen einsetzen: Werkzeuge, mit denen man Konfigurationen automatisiert testen und optimieren kann oder Management- und Monitoring-Tools, um auch fortgeschrittene Angriffe in der Unternehmens-IT zu erkennen.

Frau Eckert, in München entstand in diesem Jahr das Leistungszentrum für sichere vernetzte Systeme. Was sind die Forschungsschwerpunkte?

Eckert: Die wesentlichen Forschungssäulen des Leistungszentrums sind intelligente Sensorik, taktile Vernetzung, Datenanalyse und -verarbeitung sowie Integrierte Sicherheit. Das werden die Themen der Zukunft sein und wir möchten hier konkrete Lösungen für spezifische Anwendungen, wie der vernetzten Mobilität, dem Gesundheitswesen und Industrie 4.0 zur Einsatzreife bringen. Diese werden ein wichtiger Beitrag für die weltweite Roadmap für das Internet der Dinge sein. Wir möchten wesentliche Standards zur sicheren Vernetzung von Systemen gestalten und grundlegende Konzepte zur Konstruktion sicherer Cyber-Physischer Systeme erforschen und etablieren.

Herr Waidner, in Darmstadt gibt es gleich zwei Leistungs- beziehungsweise Kompetenzzentren. Woran forschen sie?

Waidner: Seit 2015 erforschen im »Center for Research in Security« (CRISP) über 450 Mitarbeitende, wie sich die Sicherheit komplexer und heterogener IT-basierter Systeme ganzheitlich beurteilen und nachweislich verbessern lässt. Mit dem neuen Fraunhofer-Leistungszentrum »Sicherheit und Datenschutz in der digitalen Welt« unterstützt die Fraunhofer-Gesellschaft CRISP und verschafft Unternehmen schnelleren Zugang zu neuesten Forschungsergebnissen in dem Bereich.

So können Firmen frühzeitig Sicherheit und Datenschutz in ihren Entwicklungen und Anwendungen berücksichtigen. Hier kooperieren wir eng mit den Hochschulen und der regionalen Industrie. Darmstadt ist somit eines der weltweit größten Forschungszentren für Cybersicherheit.

Bei Sicherheitslösungen scheinen US-amerikanische Unternehmen derzeit die Nase vorn zu haben. In welchen Bereichen punktet Deutschland?

Eckert: Da muss ich widersprechen. Die US-Amerikaner sind uns zwar bei Consumer-Lösungen und Software voraus, aber bei eingebetteter Software und besonders eingebetteter und hardware-basierter Sicherheit liegt Deutschland vorne. »Security made in Germany« ist eine starke Marke. Wir haben in Deutschland viele Forschungszentren, die international in der ersten Liga spielen. Die Sicherheit bei Industrie 4.0 und bei Automotive wird auch in Zukunft sehr stark durch deutsche Lösungen geprägt sein. Denn wir haben sowohl die Anwendungs- als auch die Technologie- und Ingenieurskompetenz, um nachhaltig sichere Lösungen zu bauen. Mit Forschungsstrukturen wie der Fraunhofer-Gesellschaft verfügen wir zudem über die richtigen Instrumente, um innovative Forschungsergebnisse im engen Schulterschluss mit der Industrie bedarfsgerecht zu entwickeln und zur Anwendungsreife zu bringen.

Waidner: Die Vermarktungsmöglichkeiten von Sicherheitslösungen sind in den USA sicher besser, der Forschungsstandort Deutschland ist aber absolut konkurrenzfähig. Wir haben exzellente Universitäten, und die Welt beneidet uns um unsere außeruniversitären Forschungsgesellschaften. Nehmen Sie zum Beispiel Israel, wo das Fraunhofer SIT seit letztem Jahr gemeinsam mit der Hebrew Univerity of Jerusalem ein Projektzentrum für Cybersicherheit aufbaut. Die Kombination von exzellenter und zugleich anwendungsorientierter Forschung, für die die Fraunhofer-Gesellschaft steht, existiert dort nicht. Deutsche Kompetenz in Cybersicherheit ist also selbst in der Cybernation Israel gefragt.

CYBERSICHERHEIT IN DER PRODUKTION: SICHER VERNETZT

Industrie 4.0 lebt von der Vernetzung von Maschinen und Daten – nicht nur innerhalb der Unternehmen, sondern auch über deren Grenzen hinweg. Um die eigenen Produktionsdaten vor Schäden durch Hackerangriffe zu schützen, erforschen Fraunhofer-Experten wirksame Lösungen.

Produktionsanlagen waren bislang kaum an das Internet angebunden und somit vor Cyberangriffen geschützt. Im Zuge von Industrie 4.0 ändert sich das: Die Maschinen kommunizieren miteinander oder auch mit ihrem Hersteller außerhalb des Unternehmens, die Netze werden weiter geöffnet. Die Kehrseite: Pro Jahr entsteht allein der Industrie ein Schaden von mehr als 22 Milliarden Euro durch Datendiebstahl, Spionage und Sabotage, ermittelte der Branchenverband Bitkom 2016.

Forscher arbeiten an Lösungen, um vernetzte Industrieanlagen effektiv vor Cyberangriffen und Spionage zu schützen. Im »Nationalen Referenzprojekt für IT-Sicherheit in der Industrie 4.0«, kurz IUNO, ziehen 21 Partner an einem Strang – darunter drei Fraunhofer-Institute sowie Bosch, Siemens oder Volkswagen. »Wir entwickeln eine Toolbox mit IT-Technologien, mit der sich Mittelständler fit machen können für Industrie 4.0«, erläutert Dr. Thorsten Henkel, Wissenschaftler am Fraunhofer SIT. Sie soll unter anderem vor Diebstahl geistigen Eigentums und vor Raubkopien schützen. Verkauft ein Unternehmen beispielsweise die Konstruktionsdaten einer Bremsscheibe, sollen für den Käufer nur die Produktionszahlen möglich sein, für die er bezahlt hat. Eine weitere Herausforderung liegt darin, den Daten erzeugenden Maschinen Identitäten zu verleihen – als eine Art »Person« mit Anspruch auf Datenschutz. Doch was, wenn die Maschine durch den Einsatz neuer Bauteile verändert wird? Bei welchen Eingriffen bleibt die Identität der Maschine erhalten, bei welchen nicht?

Cyberangriffe simulieren

Angriffe auf Produktionsnetze können drastische Auswirkungen bis hin zu kompletten Ausfällen haben. Forscher am Fraunhofer-Institut für Optik, Systemtechnik und Bildauswertung IOSB haben die Möglichkeit, in einem IT-Sicherheitslabor für Produktions- und Automatisierungstechnik potenzielle Cyberangriffe nachzustellen, zu analysieren und so neue Strategien und geeignete Abwehrmaßnahmen zu entwickeln. In dem Labor können die Wissenschaftler die gesamte komplexe IT-Infrastruktur einer Fabrik nachbilden, samt Büronetz sowie den Netzen zur Produktionsplanung, -überwachung und -steuerung.

Nicht nur Cyberangriffe sind eine Herausforderung, die neue Lösungen erfordert, auch die Datensouveränität. Wie können Unternehmen untereinander Daten austauschen, ohne dabei Geschäftsgeheimnisse zu offenbaren und ohne die Kontrolle über diese Daten zu verlieren? Hierfür hat die Fraunhofer-Gesellschaft die Initiative Industrial Data Space ins Leben gerufen, ein »Network of Trusted Data«, in dem Unternehmen ihre Daten souverän und sicher vernetzen können.

Studie zur Sicherheit für Industrie 4.0

Wie es um rechtliche, organisatorische und technische Aspekte in punkto »IT-Sicherheit für die Industrie 4.0« steht, haben die Forscher mehrerer Fraunhofer-Institute gemeinsam mit weiteren Partnern für die gleichnamige Studie des Bundesministeriums für Wirtschaft und Energie BMWi analysiert. Zentrale Empfehlungen sind etwa die Einführung von Mindeststandards für IT-Sicherheit sowie deren rechtliche Regulierung, die Nutzung digitaler Identitäten und zertifizierter Produkte in digitalen Wertschöpfungsnetzen sowie die Schaffung von Konzepten für eine integrierte Betrachtung von Safety- und Security-Aspekten.

http://s.fhg.de/cybersecurity

AUTOMOTIVE SECURITY: SICHER UNTERWEGS

Ob selbstfahrende Autos, Elektromobilität oder Car2X-Kommunikation – die Digitalisierung eröffnet uns eine neue Dimension der Mobilität. Sie birgt immense Chancen, aber auch ungeahnte Risiken für Fahrzeuge und Verkehrsteilnehmer. Deshalb sind diese Zukunftsszenarien ohne ausreichende Cybersicherheit und Datenschutz nicht realisierbar.

Die Datenströme moderner Autos sind heute umfangreicher als die eines Flugzeugs. Nicht nur die Technik, auch der Fahrer hinterlässt Datenspuren: Denn neben Bewegungs- und Geschwindigkeitsprofilen werden auch so persönliche Daten wie Sitzeinstellungen oder Schaltverhalten aufgezeichnet. Informationen über Fahrzeug und Fahrer ermöglichen zwar zahlreiche neue Anwendungen für Hersteller und Dienstleister. Datenschützer sehen das Ganze allerdings skeptisch: Denn bislang hat der Fahrer keine Kenntnis und keinen Einfluss darauf, welche Daten er preisgibt. Dies wollen Forscher vom Fraunhofer SIT im Projekt »Selbstdatenschutz im vernetzten Fahrzeug – SeDaFa« nun gemeinsam mit Partnern aus Forschung, Bund und Industrie ändern. »Das Ziel liegt einerseits in der Transparenz, welche Daten überhaupt erhoben werden, andererseits in der Datenhoheit des Fahrers. Er soll selbst entscheiden und kontrollieren können, welche Daten er wem freigibt«, erläutert Prof. Christoph Krauß, Projektkoordinator und Abteilungsleiter am Fraunhofer SIT. Der Datenfluss soll also nicht komplett unterbunden, sondern vielmehr datenschutzfreundlich gestaltet werden. Dafür aggregieren die Forscher zum Beispiel Daten in einer Gruppe von Fahrzeugen – so ist nicht zuzuordnen, von welchem Fahrzeug einzelne Informationen stammen –, verschicken sie unter einem Pseudonym oder leiten sie anonym weiter. »Die Hauptaufgabe liegt in der Risikobewertung für die Nutzer. Hier gibt es noch so gut wie keine Grundlagen. Die Frage ist: Wie können wir die Daten so aufbereiten, dass der Nutzer das Risiko der Weitergabe einschätzen kann?«, sagt Krauß. Denn dies ist nicht immer offensichtlich: So lässt sich aus dem scheinbar unkritischen Geschwindigkeitsprofil durch das Hinterlegen von Graphen, Kurven und Ampeln auf das Bewegungsprofil schließen. Nutzerstudien sollen nun zeigen, wie man den Fahrern solche Datenschutzrisiken am besten verdeutlichen kann. Anschließend wollen die Forscher einen Demonstrator entwickeln, der sich wiederum in Nutzerstudien bewähren soll.

Hackerschutz im Auto der Zukunft

Mit zunehmender Vernetzung der Fahrzeug-IT mit dem Internet wachsen auch die Risiken von Hackerangriffen. Selbstfahrende Fahrzeuge etwa werden nur akzeptiert, wenn zum Beispiel das Kartenmaterial, mit dem sie navigieren, vor Manipulationen geschützt ist. Gleich in mehreren EU-Projekten entwickeln Fraunhofer-Forscher deshalb durchgängige und einheitliche IT-Sicherheitskonzepte für die Car2X-Kommunikation, um die Authentizität, Integrität und Vertraulichkeit beim Austausch von sensiblen Daten sicherzustellen.

Elektroautos sicher betanken

Elektroautos bringen weitere Sicherheitsrisiken mit sich: Wie kann man gewährleisten, dass niemand sein Auto auf Kosten anderer auflädt? Wie lässt sich vermeiden, dass sich aufgrund der Ladevorgänge Bewegungsprofile erstellen lassen? Solchen Fragen rund um das sichere Laden und Abrechnen widmen sich SIT-Forscher im Projekt DELTA unter anderem mit der RWE-Tochter innogy. Die Partner entwickeln die Prototypen eines Lade-Controllers im Auto sowie einer Ladesäule. Dabei sichern sie sowohl die Säule mit integriertem Smart-Meter als auch die Datenübertragung zwischen Fahrzeug, Ladesäule und Backendsystemen ab. So wird auch das Laden von Elektroautos in punkto Datenschutz sicherer.

http://s.fhg.de/AutomotiveSecurity

SICHERHEIT FÜR KRITISCHE INFRASTRUKTUREN

Energie, Wasser, medizinische Versorgung – legen Cyberangriffe solche Infrastrukturen lahm, sind die Ausmaße enorm. Doch gerade für kleinere Versorgerunternehmen ist es oftmals schwer, sich und damit das gesamte System adäquat zu schützen. Vor allem für diese Zielgruppe vereinfachen Fraunhofer-Forscher Schutz und Risikobewertung.

Unbedacht hat man den Anhang der E-Mail geöffnet. Nun geht nichts mehr, man hat sich einen Computer-Virus eingehandelt. Was beim Privatmann für Frust und Ärger sorgt, erreicht bei kritischen Infrastrukturen ein anderes Ausmaß. Ein Angriff könnte schlimmstenfalls die komplette Wasserversorgung, das Energie- oder Telekommunikationsnetz lahmlegen und somit die nationale Sicherheit bedrohen. Die Bundesregierung räumt der Abwehr von Cyberangriffen gegen kritische Infrastrukturen daher oberste Priorität ein. Nicht ohne Grund: Schon längst sind sie Ziel von Angreifern aus unterschiedlichen Richtungen geworden.

Die Herausforderung: Im Zuge der Energiewende sind die Anlagen nicht nur direkt miteinander, sondern zunehmend auch über das Internet verbunden. Was energiepolitisch viel Sinn macht, bedeutet aus Sicht der Cybersicherheit große Herausforderungen und verlangt leistungsstarke Sicherheitslösungen. Für die Verantwortlichen in den Betreiberanlagen heißt das: Sie müssen die IT-Sicherheit jederzeit auf dem neusten Stand und flächendeckend aufrechterhalten – und zwar nicht für eine zentralisierte Struktur, sondern für zahlreiche heterogene, regionale Unternehmen. Doch gerade für sie ist es oft schwierig, die Sicherheit zu gewährleisten.

Sicherheitsniveau bewerten

Zunächst gilt es, die Sicherheitslücken aufzuspüren. Wo sind Einfallstore für Angreifer? Welche Lücken müsste man stopfen? Das Bundesamt für Sicherheit in der Informationstechnik BSI gibt eine standardisierte Beurteilung – eine Art umfassender Fragenkatalog – vor, um Risiken zu identifizieren. Allerdings ist diese zu komplex für kleinere Unternehmen. Forscher des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit AISEC arbeiten daher im Projekt MOSAIK daran, diese Bewertung zu verschlanken: »Wir vereinfachen das Experten-zentrierte Verfahren des BSI auf ein einfacheres Vorgehen, welches auch Fachanwender durchführen können.«, sagt Dr. Jörn Eichler, Abteilungsleiter am Fraunhofer AISEC. »Indem wir das Wissen von Experten strukturiert bereitstellen, müssen viele Fragen nicht mehr gestellt werden.« Hat ein Mitarbeiter etwa eingegeben, dass eine Telefonanlage einen Datenzugang bereitstellt, lassen sich durch die Methode vorbewertete Bedrohungen systematisch identifizieren. Ein Werkzeug hilft dabei, das Verfahren einfach anzuwenden. Die Wissenschaftler entwickeln dafür ein modellbasiertes Baukastensystem: Ausgangspunkt sind branchen- und technologiespezifische Vorlagen, die Fachanwender eigenständig an das eigene Unternehmen anpassen können.

Mögliche Schutzkonzepte

Ähnlich wie bei der Risikobewertung ist es auch beim Schutz: Für kleinere Unternehmen ist Menge und Wirkung möglicher Maßnahmen kaum zu überblicken. Welches Konzept bietet den besten Schutz bei auftretenden Bedrohungen? Auch hier arbeiten die Forscher an einer Lösung. »Die Methode unterstützt auch eine schablonengestützte Auswahl passender Maßnahmen«, erläutert Eichler. Langfristig soll es dann sogar möglich sein, vorab verschiedene Maßnahmen durchzuspielen und zu testen, wie hilfreich sie jeweils gegen die konkret ermittelten Bedrohungen sind, ohne den laufenden Betrieb zu stören.

http://s.fhg.de/KRITIS

DIGITALE SERVICES – WAS IST MIT SICHERHEIT UND DATENSOUVERÄNITÄT?

Seien es Suchmaschinen oder Online-Shops: Datenbasierte digitale und überall verfügbare Services erleichtern den Alltag. Aber wie ist es um die Sicherheit von Diensten, Schutz von Daten sowie letztlich auch Vermögenswerten und Identitäten bestellt?

Mal schnell was im Internet nachschauen oder in den Online-Shops stöbern ist eine feine Sache. Doch: Digitale Dienste sammeln Daten über Personen und Unternehmen, verarbeiten sie teilweise in nicht transparenter Weise und geben sie weiter. So entstehen mitunter detaillierte Profile von Nutzern. »Daten sind zum vierten Produktionsfaktor geworden«, sagt Michael Ochs, Geschäftsfeldmanager am Fraunhofer-Institut für Experimentelles Software Engineering IESE. »Schutz der Privatsphäre, Identität und geistigem Eigentum sowie Vertrauen in die Services werden zu einer wesentlichen Fragestellung bei der Nutzung digitaler Dienste.«

Be white? Be black?

Will man bestimmte Dienste nutzen, so geht das meist nicht, ohne die Geschäftsbedingungen zu akzeptieren. Ganz oder gar nicht. Das heißt aber auch: Man hat keinen Einfluss darauf, wer wann was mit den persönlichen Daten machen kann (be white). Möchte jemand nicht so transparent werden, bleibt nur, diese Dienste nicht zu nutzen (be black). Einerseits stärkt der Gesetzgeber in Regularien wie der EU-Datenschutzgrundverordnung (EU-DSGVO) die Rechte der Nutzer und erhöht die Transparenz. Andererseits gilt: Firmen müssen Daten für innovative Geschäftsmodelle nutzen können und sich gegen Gefahren aus dem Cyberspace absichern.

Technologische Verfahren wie Datennutzungskontrolle und Biometrie können dabei helfen, beide Welten zusammenzuführen und damit eine Balance zwischen Nutzen und Missbrauchsrisiken herzustellen.

Be gray – and be secure!

Fraunhofer-Forscher ermöglichen nun eine dritte – und vor allem sicherere – Option: Be gray and be secure. Mit der Technologie IND2UCE vom Fraunhofer IESE bestimmen die Nutzer allein, ob sie ihre Daten teilen wollen und wenn ja in welcher Form. Wenn noch dazu etwa biometrische Verfahren den Zugriff auf die Daten absichern, wie das Fraunhofer-Institut für Graphische Datenverarbeitung IDG es ermöglicht, steht einer sichereren Nutzung von digitalen Diensten nichts mehr im Wege. Der Clou bei diesen Verfahren: Ein oder auch mehrere Merkmale des Nutzers werden zur Authentifizierung und Identifikation eingesetzt. Damit lassen sich sensible und persönliche Daten oder geistiges Eigentum von Unternehmen stärker schützen als beispielsweise mit der reinen Verwendung von Passwörtern. Darüber hinaus können die Nutzer der Dienste durch die Datennutzungskontrolle direkt und einfach steuern, wie Dienstleister und Dritte ihre Daten verarbeiten dürfen.

Erste prototypische Anwendungen der Technologien laufen bereits in verschiedenen Bereichen: So schützen sie im Finanzwesen die persönlichen Kundendaten, verhindern bei Cloud- und Hosting-Diensten, dass die Daten außerhalb der rechtlich erlaubten geografischen Bereiche abgelegt werden und vermeiden, dass Applikationen von Wettbewerbern auf der gleichen virtuellen Maschine ausgeführt werden. Weitere Dienste, bei denen die Nutzer die Souveränität über ihre Daten dank der neuen Technologie in der Hand behalten, stehen kurz vor der Markteinführung. Von der EARTO (European Association of Research and Technology Organisations) wurde die Technologie IND2UCE mit dem Innovation Prize ausgezeichnet.

http://s.fhg.de/datennutzungskontrolle

Prof. Matthew Smith

SICHERHEIT LEICHT GEMACHT

IT-Schutz funktioniert nur dann zuverlässig, wenn er sich am Menschen orientiert. Denn meist hat dieser weder Lust noch Zeit, sich durch unverständliche Informationen zu wühlen – und vertraut darauf, dass schon nichts passieren wird. Prof. Matthew Smith arbeitet mit seinem Team am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE daran, IT-Sicherheit anwendbarer zu machen.

Prof. Smith, wie wollen Sie IT-Sicherheit einfacher gestalten?
Sicherheitstechnologien werden in der Praxis häufig fehlerhaft bedient oder gleich ganz umgangen. Ein Großteil der Sicherheitsforschung beschränkt sich dabei auf die technologische Seite – wenn der Mensch Fehler bei der Anwendung macht, dann war der Mensch nicht gut genug. Wir verfolgen mit »Usable Security« den entgegengesetzten Ansatz: Macht der Mensch Fehler, war die Technologie nicht gut genug. Bei uns steht also der Mensch im Mittelpunkt.

Wie gehen Sie dabei konkret vor?
Im ersten Schritt wollen wir herausfinden, wo die Probleme liegen. Dazu holen wir Menschen in unser Labor und beobachten, wie sie Sicherheitstechnologien anwenden. Welche Probleme haben die Nutzer damit? Wo tauchen Fragen auf? Diese Stolperfallen beheben wir und nehmen der Technologie ihre Komplexität. Auch spezielle Wünsche der Nutzer setzen wir um. In einem letzten Schritt testen wir unsere Entwicklung in einer Studie.

Wie profitiert der Nutzer davon?
Nehmen wir zum Beispiel Apps auf dem Smartphone. Sie können zum Teil auf Adressbuch und Bilder zugreifen, den Aufenthaltsort des Geräts bestimmen und ähnliches. Üblicherweise haben die Nutzer nicht im Blick, welche Daten für die App freigeschaltet werden. Und wollen sie es doch herausfinden, sind die Informationen so komplex, dass sie schnell wieder aufgeben. Wir haben für Android ein System entwickelt, das den Nutzern konkrete Hinweise gibt – etwa »Diese App kann auf deine Bilder zugreifen und sie löschen«. Eine Untersuchung zeigte: Nutzer, die unsere Lösung verwenden, installieren deutlich häufiger sichere Apps als eine Vergleichsgruppe ohne unsere Technologie. Sprich: Die Anwender können besser einschätzen, welche Apps auf welche Daten zugreifen und können entsprechend reagieren. Zudem sinken die Risiken für eine Fehlbedienung.

Woran forschen sie momentan?
Während die klassische »Usable Security«-Forschung den Anwender im Blick hat, konzentrieren wir uns seit einiger Zeit auf die Experten. Schließlich sind sie ja auch Menschen – nur sind ihre Fehler deutlich gravierender als die der Nutzer. Dieser Ansatz trägt viele Früchte. Ein Beispiel: Entwickler von Apps schützen die Kommunikation ihrer Anwendungen durch Verschlüsselung gegen Angriffe. Aber bei fast jeder fünften App war dieser Schutz unzureichend. Angreifer hätten also Kreditkartennummern oder Bankdaten der Anwender abgreifen können. In einer Studie mit den App-Entwicklern haben wir die Ursachen der Fehlerquellen aufgedeckt und eine entsprechende Lösung erarbeitet: Sie vereinfacht den Entwicklungsprozess deutlich, die gängigen Fehler in der Programmierung treten nicht mehr auf.

Wann kommt Ihre Technologie auf den Markt?
Google hat unseren Ansatz jetzt in Android-N integriert. Auch Studien mit Experten, die sich auf Schadsoftware konzentrieren, zeigen: Die Nutzbarkeit – sowohl für User als auch für Experten – ist ein unglaublich wichtiges Thema. »Usable Security« kann vieles leisten, weil sie den Menschen als gleichwertigen Partner betrachtet.

LERNLABOR CYBERSICHERHEIT: DIE SICHERHEITSEXPERTEN VON MORGEN

Gut ausgebildete IT-Sicherheitsfachleute sind hierzulande rar gesät. Um im Wettlauf mit den Cyberkriminellen nicht ins Hintertreffen zu geraten, müssen Fach- und Führungskräfte ihnen in Kenntnissen und Fähigkeiten stets einen Schritt voraus sein. Mit einem modularen, berufsbegleitenden Weiterbildungskonzept wollen Fraunhofer-Institute und Fachhochschulen den Mangel an Weiterbildungsangeboten beheben.

Weiterbildung in der IT-Sicherheit ist eine Aufgabe von nationalem Interesse: Hohe finanzielle Verluste, Versorgungsengpässe oder Störungen der öffentlichen Sicherheit können die Folgen von Cyberattacken auf kritische Infrastrukturen und Industrieanlagen sein. Das Bedrohungspotenzial wächst mit zunehmender Vernetzung und Digitalisierung.

Der Weiterbildungsbedarf ist enorm: Bereits 2014 sahen laut IHK-Unternehmensbarometer 61 Prozent der Betriebe in punkto Sicherheit der IT-Infrastruktur einen vordringlichen Qualifizierungsbedarf. Doch boten 2015 nur fünf von 64 großen Universitäten, in denen Informatik gelehrt wird, einen Studiengang für IT- und Cybersicherheit an. Damit nicht genug: Nach einer Studie von Frost & Sullivan werden bis 2020 weltweit 1,5 Millionen Fachkräfte im Sicherheitssektor fehlen.

Kooperationsmodell mit Fachhochschulen

Die Fraunhofer-Gesellschaft und ausgewählte Fachhochschulen reagieren auf diesen Mangel und haben ein modulares Weiterbildungskonzept für Cybersicherheit entwickelt: Dafür wurde der Kooperationsverbund Lernlabor Cybersicherheit geschaffen, der in den nächsten Jahren mit jeweils sechs Millionen Euro vom Bundesministerium für Forschung und Bildung gefördert wird.

Das Verbundkonzept sorgt dafür, dass neueste oder absehbare Forschungserkenntnisse schnell in die Lehrangebote einfließen. In modernen Labors, in denen sich reale Bedrohungsszenarien nachstellen lassen, können sich Teilnehmer praxisnah in folgenden Themenfeldern qualifizieren:

- Industrielle Produktion/Industrie 4.0
- Kritische Infrastrukturen/Anwendungsfall Energie- und Wasserinfrastrukturen
- Hochsicherheit und Emergency Response
- Internetsicherheit und IT-Forensik
- Softwarequalität/Produktzertifizierung
- Embedded Systems, Mobile Security und Internet of Things

Kompakte Veranstaltungsformate erlauben eine berufsbegleitende Qualifikation und flexibel kombinierbare Module vermitteln IT-Sicherheit für unterschiedliche Berufsrollen. Die Fraunhofer Academy entwickelt dabei bedarfsorientiert das Angebot und sorgt für ein durchgängiges Qualitätsmanagement.

Die Industrie befürwortet die Initiative, wie Thomas Tschersich, Senior Vice President Group Security Service bei der Deutschen Telekom AG, sagt: »Besonders das Angebot berufsbegleitender kleinerer Weiterbildungsmodule, in denen Personen sehr transferorientiert und kompakt in aktuellen Themen und der Anwendung aktueller Werkzeuge geschult werden, begrüßen wir sehr.«

http://www.cybersicherheit.fraunhofer.de

CRISP
Center for Research
in Security and Privacy

SECURITY AT LARGE

Bislang betrachteten Cybersicherheitsforscher meist isolierte Systeme überschaubarer Größe. Der Forschungsschwerpunkt des vom Bund und dem Land Hessen geförderten Center for Research in Security and Privacy (CRISP) in Darmstadt liegt hingegen darauf, wie sich große, reale Systeme wie etwa das Internet, Industrie 4.0 oder intelligente Energienetze absichern lassen. Unter dem Stichwort »Security at Large« bündelt das Center die Kompetenzen der Technischen Universität und der Hochschule Darmstadt, des Fraunhofer-Instituts für Sichere Informationstechnologie SIT und des Fraunhofer-Instituts für Graphische Datenverarbeitung IGD. Die Forscher untersuchen das Zusammenspiel von Komponenten, testen Gesamtsysteme und entwickeln umfassende Sicherheitslösungen.

http://s.fhg.de/CRISP

SICHER BEZAHLEN

Der illegale Handel mit Kreditkartendaten blüht und Betrüger sind erfinderisch in der Wahl ihrer Mittel. Ob Trojaner im Kartenlesegerät oder gehackte Online-Accounts, die Betrugsmuster ändern sich schnell. Die Software »MINTify rule« unterstützt Banken dabei, Kreditkartenbetrug zu erkennen und stoppt verdächtige Abbuchungen nach bestimmten Regeln. Entwickelt haben die Software die Forscher des Fraunhofer-Instituts für Intelligente Analyse- und Informationssysteme IAIS in Sankt Augustin gemeinsam mit Partnern des Unternehmens Paymint. Das System muss möglichst schnell Millionen Datensätze der Kreditinstitute durchlaufen. Dies dauerte anfangs noch bis zu einer halben Stunde. Dank selbstlernender Algorithmen erkennt die Software innerhalb weniger Minuten ein Betrugsmuster und stoppt den Zahlungsvorgang.

http://s.fhg.de/kreditkartenbetrug

Mehr Informationen:
www.fraunhofer.de/cybersicherheit

Kontakt
Fraunhofer-Gesellschaft e.V.
Kommunikation
Hansastraße 27c
80686 München
http://s.fhg.de/pressekontakt

Impressum
Fraunhofer-Gesellschaft e.V.
Kommunikation
Hansastraße 27c
80686 München

Konzept: Mandy Kühn
Redaktion: Klaudia Kunze (V.i.S.d.P.),
Janine van Ackeren, Mandy Kühn,
Tanja Schmutzer
Bilder und Umsetzung: Larissa Hummel

Bildquellen
Cover, Seite 15, 16, 22: Shutterstock
Seite 3: Ines Escherich/Fraunhofer
Seite 4: Fraunhofer AISEC
Seite 7: links: Andreas Heddergott/TU Muenchen
rechts: Fraunhofer SIT
Seite 8: iStockphoto
Seite 11: Sven Doering/Agentur Focus/Fraunhofer
Seite 13: PantherMedia/Cindy Fischer
Seite 19: Fraunhofer FKIE
Seite 20: Fraunhofer IOSB
Seite 21: Matthias Heyde/Fraunhofer FOKUS

© Fraunhofer-Gesellschaft 2016