idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Karlsruher Institut für Technologie
Monika Landgraf

05.02.2019
http://idw-online.de/de/news710087

Forschungs- / Wissenstransfer, Kooperationen
Gesellschaft, Informationstechnik
überregional

Roadmap zur Cybersicherheitsforschung

Wie den digitalen Bedrohungen auf europäischer Ebene künftig besser begegnet werden kann, haben unter der Koordination des BMBF-Verbundprojektes secUnity 30 namhafte europäische IT-Sicherheitsexperten in der secUnity-Roadmap niedergelegt, darunter Forscherinnen und Forscher des Karlsruher Instituts für Technologie (KIT). Am heutigen Dienstag, 5. Februar, stellen die Wissenschaftlerinnen und Wissenschaftler von secUnity die Roadmap in Brüssel vor und übergeben sie offiziell an die Europäische Agentur für Netzwerk und Informationssicherheit ENISA.

Übermittlung von Nachrichten, Verkehr, Industrieproduktion, Forschung, Verwaltung – nahezu kein Bereich kommt mehr ohne moderne Informations- und Kommunikationstechnologien aus. Gleichzeitig nimmt die Zahl der Cyberangriffe, die bekannt werden, stetig zu. Solche Attacken auf die digitale Infrastruktur durch Kriminelle oder staatliche Organisationen bedrohen den Wohlstand und die Sicherheit unserer Gesellschaften, am Ende sogar Freiheit und Demokratie. Bei einer Abendveranstaltung in der Vertretung des Landes Hessen bei der Europäischen Union in Brüssel werden secUnity-Wissenschaftler mit Vertretern des Europäischen Parlaments und der Europäischen Kommission über „Zivile Cybersicherheitsforschung für digitale Souveränität“ diskutieren und im Anschluss offiziell die secUnity-Roadmap veröffentlichen und an die Europäische Agentur für Netzwerk und Informationssicherheit übergeben.

„Das Gefahrenpotenzial, das Cyberattacken für hochentwickelte Länder entfalten können, kann man nicht hoch genug einschätzen“, warnt Professor Jörn Müller-Quade, Sprecher des Kompetenzzentrums für IT-Sicherheit KASTEL am KIT. In secUnity arbeiten IT-Sicherheitsexperten aus ganz Deutschland zusammen. Beteiligt sind, neben den drei nationalen Kompetenzzentren KASTEL, CRISP und CISPA, Spezialisten der TU Darmstadt, der Ruhr-Universität Bochum und der Fraunhofer-Institute für Angewandte und Integrierte Sicherheit AISEC und für Sichere Informationstechnologie SIT.

Cybersicherheitsexperten bemängeln schon lange, dass Firmen, öffentliche Einrichtungen und Institutionen nicht ausreichend auf digitale Bedrohungen vorbereitet seien. Im Gegenteil: Durch die fortschreitende Vernetzung, die sich durch digitale Trends wie Industrie 4.0, Smart Home oder selbstfahrende Autos noch potenzieren wird, würden die Angriffsflächen für Cyberkriminelle immer größer. In der jetzt vorgelegten Roadmap, die das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Verbundprojekt secUnity initiiert hat, haben die über 30 europäischen Autoren zukünftige Herausforderungen und Lösungswege identifiziert. Zum Beispiel werden die Sicherheit eingebetteter Systeme, Maschinelles Lernen, die Problematik der fehlenden Awareness und das Phänomen von Fake News untersucht und Vorschläge für mehr Sicherheit erarbeitet.

Sehr kritisch sehen die Experten die Verwendung von Hardwarelösungen, die oft ohne IT-Sicherheitsüberprüfung verwendet werden. Dies gefährde die digitale Souveränität Europas. „Eine Möglichkeit diese Situation zu verbessern, wären hier europäische Prüfinstitute, um die Technik unabhängig zu analysieren“, so Professor Michael Waidner, Direktor des Nationalen Forschungszentrums für angewandte Cybersicherheit CRISP und des Fraunhofer-Instituts SIT in Darmstadt. Zudem könnten Open-Source-Software- und Hardwarelösungen transparent in der EU entwickelt werden.

Da aber auch in Zukunft noch weiterhin eine Vielzahl von preiswerten jedoch unsicheren Hard- und Softwarekomponenten verbaut und genutzt wird, reichen Ansätze zur Entwicklung vertrauenswürdiger europäischer Lösungen nicht aus, um vernetzte Systeme wirksam zu schützen. Am Beispiel Smart Home führt Professorin Claudia Eckert, Direktorin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit AISEC in München aus: „Wir brauchen Lösungen, um die Risiken solcher Komponenten zu minimieren und die Systeme resilient zu betreiben. Kameras, Türöffner, die Heizungssteuerung – jedes Heimautomatisierungsgerät ist ein mögliches Einfallstor für große Netz-Attacken. Sichere Gateways für die Verbindung unsicherer Komponenten können beispielsweise dafür sorgen, dass keine sensitive Information die Heimumgebung verlässt und keine Zugriffe von außen auf Steuerungskomponenten möglich sind.“ Resilienz trotz unkalkulierbarer Komponenten – dies muss natürlich insbesondere für kritische Infrastrukturen wie Gesundheits- und Energieversorgung, aber auch für Behörden und Unternehmen sichergestellt werden.

Auch die weltweit stark vorangetriebene Entwicklung von Quantencomputern berge Gefahren. Jörn Müller-Quade warnt: „Es ist zwar bislang noch nicht gelungen, einen hinreichend großen Quantencomputer zu bauen, um die Sicherheit aktueller kryptographischer Verfahren zu gefährden, aber dies könnte sich schnell ändern. Der derzeitige Fortschritt in der Quantentechnologie ist so groß, dass wir heute schon Vorsorge treffen müssen. Wir müssen unsere komplexen vernetzten Systeme auf zukunftssichere, noch weiter zu erforschende Verschlüsselungsverfahren umstellen.”

Methoden der Künstlichen Intelligenz viele neue Anwendungsfälle, sie bringen aber auch gravierende Risiken für die IT-Sicherheit mit sich: Maschinelle Lernprozesse können durch gezielte Manipulationen während der Lernphase und auch im Betrieb einfach angegriffen werden. „Bevor diese Technologien in kritischen Bereichen oder zur Verbesserung der Lebensqualität eingesetzt werden können, muss das Vertrauen in diese Verfahren und in deren Zuverlässigkeit auf ein wissenschaftliches Fundament gesetzt werden“, fordert Professor Thorsten Holz von der Ruhr-Universität Bochum.

Auch werfen neue Möglichkeiten der Informationsgesellschaft wie etwa intelligente Stromnetze, die den Alltag komfortabler machen und beim Energiesparen helfen, rechtliche und ganz besonders datenschutzrechtliche Fragen auf: „Angesichts der fundamentalen Risiken, die durch die Digitalisierung ganzer Industriezweige und auch kritischer Infrastrukturen wie die Strom- oder Energieversorgung für die Versorgungssicherheit entstehen, brauchen wir dringend einen europäisch harmonisierten Rechtsrahmen für IT-Sicherheit", sagt Dr. Oliver Raabe vom Zentrum für Angewandte Rechtswissenschaft (ZAR) des KIT. Die rechtlichen Maßstäbe, welche Risiken akzeptabel sind und welche Schutzmaßnahmen den Unternehmen zugemutet werden könnten, müssten erst noch entwickelt werden. Ebenso Maßgaben für die Sicherung von Qualität und Unverfälschbarkeit der großen Datenbestände (Big Data).

Zudem müssen die Bürgerinnen und Bürger selbst, die zunehmend komplexe Kommunikationssysteme nutzen, beim Schutz ihrer Privatsphäre und IT-Sicherheit unterstützt werden. „Ziel der Forschung ist daher zum Beispiel, Methoden für einen Privacy Advisor zu entwickeln. Diese sollen beim Hochladen von Bildern oder Nachrichten ins Netz die Risiken einschätzen und unter Berücksichtigung bisheriger Posts aufzeigen, wie viel zusätzliche private Information durch die Veröffentlichung preisgegeben wird. Dies würde die Bürger dabei unterstützen, sich souverän in sozialen Netzwerken zu bewegen“, kündigt Professor Michael Backes, Gründungsdirektor des CISPA Helmholtz-Zentrums für Informationssicherheit, an.

Angesichts dieser immer größer werdenden Datenbestände, ergeben sich für viele Unternehmen neue Möglichkeiten für Innovationen, aber auch die Gefahr eine scheinbar sichere Marktposition im digitalen Zeitalter zu verlieren. „Daten sind nicht per se das Öl des 21. Jahrhunderts. Sie bekommen erst dann einen Wert, wenn Geschäftsmodelle entwickelt werden, die sie wertvoll machen – und Wertvolles hat besonderen Schutz und Sicherheit verdient“, erklärt Peter Buxmann, CRISP-Wissenschaftler und Professor für Wirtschaftsinformatik sowie Leiter des Gründungszentrums HIGHEST an der TU Darmstadt. Bürgerinnen und Bürger müssen sich des Wertes und Schutzbedarfs ihrer Daten bewusst werden, während Transparenz bei der Nutzung und Weiterverarbeitung von Daten sowie faire Preismodelle von Anbietern umgesetzt werden müssen. „Politisch sollten wir uns deswegen eher weg vom Prinzip der Datensparsamkeit in Richtung Datensouveränität bewegen und faire Geschäftsmodelle fördern und fordern“, so Buxmann.

„Um all diesen Herausforderungen zu begegnen, braucht die zivile Cybersicherheit ein interdisziplinäres Netzwerk von Experten der zivilen Cybersicherheitsforschung auf EU-Ebene“, fasst secUnity-Sprecher Jörn Müller-Quade zusammen.

Weitere Informationen im Internet unter: https://it-security-map.eu/de/startseite/

Weiterer Pressekontakt: Margarete Lehné, stellv. Pressesprecherin, Tel.: +49 721 608-21157, Fax: +49 721 608-43658, margarete.lehne@kit.edu

Als „Die Forschungsuniversität in der Helmholtz-Gemeinschaft“ schafft und vermittelt das KIT Wissen für Gesellschaft und Umwelt. Ziel ist es, zu den globalen Herausforderungen maßgebliche Beiträge in den Feldern Energie, Mobilität und Information zu leisten. Dazu arbeiten rund 9 300 Mitarbeiterinnen und Mitarbeiter auf einer breiten disziplinären Basis in Natur-, Ingenieur-, Wirtschafts- sowie Geistes- und Sozialwissenschaften zusammen. Seine 25 100 Studierenden bereitet das KIT durch ein forschungsorientiertes universitäres Studium auf verantwortungsvolle Aufgaben in Gesellschaft, Wirtschaft und Wissenschaft vor. Die Innovationstätigkeit am KIT schlägt die Brücke zwischen Erkenntnis und Anwendung zum gesellschaftlichen Nutzen, wirtschaftlichen Wohlstand und Erhalt unserer natürlichen Lebensgrundlagen.

Originalpublikation:

https://www.kit.edu/kit/pi_2019_015_roadmap-zur-cybersicherheitsforschung.php

Anhang Roadmap zur Cybersicherheitsforschung http://idw-online.de/de/attachment70896