

## Roadmap zur Cybersicherheitsforschung: Verbundprojekt secUnity stellt Empfehlungen in Brüssel vor

06.02.2019 | Internationalisierung Deutschlands, Bi-/Multilaterales

<https://it-security-map.eu/de/startseite/>

Wie den digitalen Bedrohungen auf europäischer Ebene künftig besser begegnet werden kann, haben unter der Koordination des BMBF-Verbundprojektes secUnity 30 europäische IT-Sicherheitsexpertinnen und -experten in der secUnity-Roadmap niedergelegt. Am 5. Februar stellten die Wissenschaftlerinnen und Wissenschaftler die Roadmap in Brüssel vor und übergaben sie offiziell an die Europäische Agentur für Netzwerk und Informationssicherheit ENISA.

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 Autorinnen und 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 gesehen wird die Verwendung von Hardwarelösungen, die oft ohne IT-Sicherheitsüberprüfung verwendet werden. *„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.

Auch die weltweit stark vorangetriebene Entwicklung von Quantencomputern berge Gefahren und Methoden der Künstlichen Intelligenz brächten gravierende Risiken für die IT-Sicherheit mit sich. Weiterhin werfen neue Möglichkeiten der Informationsgesellschaft, wie etwa intelligente Stromnetze, rechtliche und ganz besonders datenschutzrechtliche Fragen auf. 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“*, kündigt Professor Michael Backes, Gründungsdirektor des Helmholtz-Zentrums für Informationssicherheit (CISPA), an.

*„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.

Quelle: Karlsruher Institut für Technologie

Redaktion: 06.02.2019 von Miguel Krux, VDI Technologiezentrum GmbH

Länder / Organisationen: EU

Themen: Information u. Kommunikation, Sicherheitsforschung

[Zurück](#)

---

Weitere Informationen