

PRESSEMITTEILUNG

7. November 2022

Autarkie in Germany: asvin.io unterstützt neue Cybersicherheits-Initiative des Bundes

Deutschland investiert 30 Millionen Euro in die Entwicklung innovativer Systeme für Cybersicherheit.

Halle (Saale)/Stuttgart, 07.11.2022 - Die asvin GmbH, Spezialist für sichere Software-Lieferketten, erhält mit seinem Konsortium „MANTRA“ Forschungsaufträge von der Agentur für Innovation in der Cybersicherheit (Cyberagentur). asvin leitet damit eines von insgesamt sechs Konsortien, die für die Startphase des mit insgesamt 30 Millionen Euro dotierten Forschungsvorhabens ausgewählt wurden. Ziel des Projekts ist die Entwicklung neuer Systeme für operative Cybersicherheit nach Vorbild des „Cybertsecurity Mesh“, um die Resilienz von Behörden und Kritischer Infrastruktur zu erhöhen.

Mirko Ross, Gründer und Geschäftsführer der asvin GmbH, hebt die sicherheitspolitische Bedeutung der Initiative hervor: „Mit MANTRA haben wir die hervorragende Möglichkeit, die Souveränität der Bundesrepublik im Bereich Cybersicherheit zu erhöhen. Ähnlich wie in den USA oder in Israel wird jetzt die technologische Cybersicherheitskompetenz in Deutschland deutlich ausgebaut. MANTRA schafft hierfür eine Cybersicherheitslösung für kritische Infrastrukturen ‚made in Germany‘, und zwar für Deutschland und Europa gleichermaßen.“

Das von asvin geleitete Konsortium MANTRA hat sich mit seinem KI- und DLT-basierten F&E-Ansatz gegen 13 Mitbewerber durchgesetzt. Am 7. November 2022 wurden jetzt in Halle (Saale) die Verträge von Prof. Dr. Christian Hummert, Forschungsdirektor, und Daniel Mayer, kaufmännischer Direktor der Cyberagentur unterzeichnet. Gegenstand der Forschung sind „Existenzbedrohende Risiken aus dem Cyber- und Informationsraum und Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien“.

Automation der Cyber-Abwehr steht im Vordergrund

MANTRA realisiert ein sicheres und resilientes Framework zum Echtzeit-Austausch von Cyber-Angriffsmustern und deren Risiko-Management. Der neuartige, auf Graphen-Modellen basierende Ansatz bietet erhebliche Vorteile im Cybersicherheitsmanagement, insbesondere bei der Automatisierung und Priorisierung von Schutzmaßnahmen, aber auch bei der Risikominimierung und während der aktiven Abwehr von Cyberangriffen. Die MANTRA Projektpartner verfügen über ein umfangreiches Ökosystem an Behörden, Verbänden, Industrieunternehmen, Mittelstand, Forschungseinrichtungen und Startups. Neben der asvin GmbH sind dies Allianz, BDI, BSI, CAS AG, Volkswagen, Fraunhofer AISEC, OTH Regensburg, KIT, MIT und Fraunhofer IAO.

Reduktion von sechs auf drei Konsortien in den nächsten Projektphasen

Die erste Projektphase des bislang größten Cybersicherheits-Forschungsvorhabens in Deutschland ist auf sechs Monate angelegt. Bis Ende Mai 2023 werden die Forschungsverbände ihre bisher eingereichten Projektideen weiter ausarbeiten. „Wir waren sehr erfreut, dass sich sehr viele Unternehmen und Institutionen für unsere Ausschreibung interessierten“, betonte Prof. Dr. Hummert, und führte weiter aus: „Die Qualität der Bewerbungen war außergewöhnlich hoch. Für die Jury waren also hervorragende Bedingungen gegeben, um die sechs Forschungsverbände aus dem Pool auszuwählen.“ Daniel Mayer ergänzte dazu: „Das Auftragsvolumen von 30 Millionen Euro stellt letztlich hohe Erwartungen an die Forschungsverbände im Wettbewerb um die besten Ergebnisse.“ In den kommenden Jahren werden die Forschungsprojekte untereinander mit verschiedenen Ansätzen um die innovativste Forschungsidee konkurrieren. Die Anzahl der Teilnehmer wird sich dabei im Laufe des Verfahrens stufenweise reduzieren. Die Evaluation der Angebote besorgte eine Fachjury aus Mitgliedern der Cyberagentur sowie Vertretern der gesamtgesellschaftlichen Sicherheitsvorsorge.

(3.816 Zeichen)

Über asvin: Die Stuttgarter asvin GmbH entwickelt mit derzeit 20 Mitarbeiter:innen umfassende Lösungen für KI und Software Supply Chain Security. Diese gewährleisten die Sicherheit und korrekte Herkunft von Software in IoT-Umgebungen über ihren gesamten Lebenszyklus. Entlang von Daten-Lieferketten entsteht damit eine durchgängige Vertrauensschicht, welche die Resilienz im Internet der Dinge (IoT) gegenüber Cyberangriffen maßgeblich erhöht.

Kontakt für die Presse

Konrad Buck, asvin GmbH
Mobil: +49 151 4653 9192
E-Mail: k.buck@asvin.io

Download-Material zum aktuellen Presseartikel:

[asvin Logo \(svg\)](#)

[Bildmaterial](#)

[Logo Cyberagentur](#)

[Artikel in reiner Textform \(*.txt\)](#)