FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN

Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz

Aufruf zur Einreichung von Anträgen (2024-01)

gemäß der „Förderrichtlinie Cybersicherheitsforschung in Hessen“ des Hessischen Ministeriums des Innern, für Sicherheit und Heimatschutz

1. **Allgemeines**
   Eine Zuwendung auf Basis der o. g. Richtlinie ist im Rahmen dieses Aufrufs nur möglich für Forschungsvorhaben, die Fragestellungen innerhalb eines der unter Nr. 5 genannten Themengebiete behandeln.

   Dieser Aufruf wurde am 23.01.2024 veröffentlicht. Ab diesem Zeitpunkt können auf Basis der Richtlinie Antragsskizzen eingereicht werden.

2. **Ablauf des Verfahrens**
   Die Antragstellung erfolgt gemäß Nr. 7 der Förderrichtlinie. In einem ersten Schritt wird eine Antragsskizze eingereicht. Sofern dem Zuwendungsgeber bereits diesbezügliche Skizzen vorliegen, kann dieser Schritt entfallen. In einem zweiten Schritt erfolgt nach Aufforderung durch den Zuwendungsgeber die Einreichung des Projektantrags.
   Es wird empfohlen, vor Einreichung einer Antragsskizze mit dem Zuwendungsgeber Kontakt aufzunehmen, um die Eignung des geplanten Forschungsvorhabens zu beraten.

3. **Fristen zur Einreichung von Antragskizzen und zur Antragsstellung**
   Die Antragsskizze muss spätestens drei Wochen nach Veröffentlichung dieses Aufrufs beim Zuwendungsgeber eingegangen sein. Der Zuwendungsgeber ist bestrebt, den Antragsteller innerhalb von vier Wochen nach Ende dieser Frist zur Abgabe eines Projektantrags aufzufordern. Sollte das Projekt nicht förderungsfähig sein, so informiert der Zuwendungsgeber den Antragsteller darüber.

   Der Projektantrag muss nach erfolgter Aufforderung innerhalb von sechs Wochen eingereicht werden.

   Sowohl Antragsskizze als auch Projektantrag müssen von einer vertretungsberechtigten Person des Antragstellers unterschrieben und schriftlich an folgende Stelle gerichtet sein:

Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz
Referat VII 4 Innovationsmanagement Cybersicherheit
Friedrich-Ebert-Allee 12
65185 Wiesbaden

Beide Dokumente sind zusätzlich elektronisch an den Zuwendungsgeber (E-Mail-Funktionspostfach: RefLtgVII4@innen.hessen.de) zu senden. Das Datum des Poststempels gilt als fristwahrend.

4. Maximale Fördersumme

Für das Forschungsvorhaben dieses Aufrufs werden maximal 350.000 € als Zuwendung bewilligt. In begründeten Ausnahmefällen (bspw. bei Gemeinschaftsanträgen) kann davon abgewichen werden.

5. Thematischer Rahmen (Themengebiet)

Die Zuwendung zielt stets auf die wissenschaftliche Erforschung von Fragen der Cybersicherheit im Kontext der öffentlichen Verwaltung in Hessen in definierten Themengebieten. Das Forschungsvorhaben muss Teile des skizzierten Forschungsbedarfs abdecken und in seiner Zielstellung den Stand der Forschung übertreffen.

Eine Zuwendung im Rahmen dieses Aufrufs ist nur möglich für ein Forschungsvorhaben, das Fragestellungen innerhalb des folgenden Themengebiets behandelt:

„Autonome Cyberresilienz-Agenten zur Abwehr von Cyberangriffen“

IT-Systeme (z.B. Kommunikationsanlagen, Endgeräte, Server etc.) im KRITIS-Bereich (z.B. Katastrophenschutz, Feuerwehr, Rettungsdienste, Polizei oder Verwaltung) müssen insbesondere in Krisen- und Notfällen, z.B. ausgelöst durch Angriffe auf die Digitaltechnik, verfügbar bleiben. Andernfalls hätte dies weitreichende Folgen für die Bevölkerung. Damit diese Systeme auch im Krisenfall sicher weiter funktionieren bzw. deren Funktionen schnell wiederhergestellt werden können, ist das Ziel des Forschungsprojektes die Entwicklung von autonomen und intelligenten Cyber-Resilienz-Agenten, die im zentralen Betrieb wesentliche Cyber-Resilienz-Aufgaben mit Funktionen wie Schutz, Überwachung, Notlauf- bzw. Wiederherstellungsmodi teilautonom bzw. autonom unterstützen und durchführen. Es soll eine Konzeption für eine Proof-of-Concept Implementierung und Auswertung eines ersten Cyberresilienz Agenten in realitätsnahem Umfeld und Einsatz entwickelt werden. Dabei soll bei den Konzepten ein besonderer Fokus auf Gegebenheiten, Anforderungen und zukünftigen Bedarfen einer Anwendungsdomäne (z. B. Systeme zur Kommunikation, Koordination oder Verwaltung) liegen. Es soll ein Proof-of-Concept System mit Demonstratoren für die jeweiligen Funktionen entwickelt werden. Die Implementierung soll kontinuierlich angepasst und erprobt werden, um rasch Einfluss auf die Ausprägung von Cyberresilienz in zukünftigen Systemen nehmen zu können. Es sollen im speziellen sichere Laufzeitumgebungen für Agenten auf Zielgeräten oder in Netzwerken, dezentrale/lokale Angriffserkennung und -abwehr, die Aufrechterhaltung von Kernfunktionen sowie die autonome und vertrauenswürdige Systemwiederherstellung untersucht werden.

6. Maximale Projektlaufzeit

Die Forschungsvorhaben sollen eine dem Forschungsgegenstand (Bedarf, Methodik und Ziel) angemessene Laufzeit haben. Dabei soll eine Laufzeit von 12 Monaten als Richtwert dienen; 24 Monate dürfen nicht überschritten werden.