FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN

Hessisches Ministerium des Innern und für Sport

Aufruf zur Einreichung von Anträgen (2021-02)

gemäß der „Förderrichtlinie Cybersicherheitsforschung in Hessen“ des Hessischen Ministeriums des Innern und für Sport

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 05.04.2021 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 und für Sport
   Referat VII 4 Innovationsmanagement Cybersicherheit
   Friedrich-Ebert-Allee 12
   65185 Wiesbaden

Beide Dokumente sind zusätzlich elektronisch an den Zuwendungsgeber (E-Mail-Funktionspostfach: RefLtgVII4@hmdis.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:

„Organic Computing“: Internet of Things (IoT) Anwendung eines KDNA/KHS-Systems für Drohnen

Das IT-Forschungsumfeld des „Organic Computing“ nutzt Konzepte aus der Biologie, um bspw. Fähigkeiten zur Selbstorganisation, Selbstanpassung, Selbstheilung und Selbstschutz auf technische Informationssysteme zu übertragen. Hierdurch sollen hochrobuste und resiliente Systeme ermöglicht werden. Eine Anwendung dieser Prinzipien zur Verbesserung der Cybersicherheit in „Internet of Things (IoT) Systemen“ für Flugdrohnen soll im Rahmen dieses Förderaufrufs erforscht werden, um Angriffe auf künstlichen DNA-Systems (KDNA) und künstlichen Hormonsystems (KHS) zu erkennen, abzuwehren und sie proaktiv zu verhindern.

Auf dieser Basis sollen (a) eine Machbarkeits-, (b) eine Umsetzungsstudie und (c) mindestens zwei flugfähige Drohnen als Demonstratoren entwickelt werden. Mittels KDNA und KHS sollen die Prozessoren und Sensoren von Drohnen als IoT-Knoten intelligent miteinander und mit der IoT-Infrastruktur an einer Bodenstation vernetzt werden und so zu einer „organischen IT-Einheit“ werden.

Das geplante Forschungsvorhaben im Bereich Cybersicherheit für organische IoT-Systeme soll eine „Immunisierung des Systems“ mit dem KHS gegenüber Angriffen und Manipulationen vorsehen. Die Absicherung des Drohnen-KDNA-Systems könnte hierbei in zwei Dimensionen erfolgen.

In einer ersten Dimension könnten IoT-Knoten erforscht werden, die zu einer festen Gruppe gehören und untereinander bekannt, bzw. „vertraut“ sind, bspw. in einer Überwachungsaufgabe.
In einer zweiten Dimension könnten demgegenüber IoT-Knoten betrachtet werden, die außerhalb der ersten Gruppe stehen, aber mit ihr kooperieren, bspw. ergänzende, unterstützende Drohnen, die dynamisch bei Bedarf angefordert werden (bspw. bei plötz-

licher Änderung oder Erweiterung der Überwachungsaufgabe), zusätzlich dazu Steuerungsrechner, welche die Daten der Drohnen auswerten oder anderweitigen Zugriff auf die Drohnen haben.

In dieser zweiten Dimension ist die Erforschung einer sog. „Immunbarriere“ gewünscht, bspw. in Form einer Hormonfirewall, die eine Fremd-/Eigenerkennung von künstlichen Hormonen durch Prüfung von Absender und Empfänger durchführt und somit eine Gefahr klassifizieren kann.

Die Fremd- und Eigenerkennung soll dynamisch durch Methoden der künstlichen Intelligenz, wie neuronale Netze, ergänzt werden, um variable Angriffsvektoren zu erkennen, zu klassifizieren und proaktiv abzuwehren. Demzufolge sollen mögliche Gegenmaßnahmen erforscht werden, wie bspw. durch diese Hormonfirewall der jeweilige Absender isoliert bzw. der bösartige Absender identifiziert und ignoriert werden kann.

Das Forschungsvorhaben soll auf fachlicher und operativer Ebene durch die hessische Polizei begleitet 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.