

Aufruf zur Einreichung von Anträgen **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 05.10.2020 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 Antragsskizzen 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: RefLtqVII4@hmdis.hessen.de) zu senden. Das Datum des Poststempels gilt als fristwährend.

4. Maximale Fördersumme

Pro Forschungsvorhaben dieses Aufrufs werden maximal 300.000 € als Zuwendung bewilligt. In begründeten Ausnahmefällen (bspw. bei Gemeinschaftsanträgen) kann davon abgewichen werden.

5. Thematischer Rahmen (Themengebiete)

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 Forschungsvorhaben, die Fragestellungen innerhalb eines der folgenden Themengebiete behandeln:

5.1. Optimierung von organisationsübergreifenden Cybersicherheitsprozessen

In der modernen und immer stärker digitalisierten Verwaltung bestehen auf verschiedenen Ebenen, wie etwa der Landesebene oder der Ebene von Städten und Kommunen, Bedarfe zur Implementierung von Cybersicherheitsprozessen. Durch einen ebenen- und damit auch organisationsübergreifenden Ansatz sollen solche Prozesse effektiver und effizienter umgesetzt und implementiert werden.

Das Hessen CyberCompetenceCenter (Hessen3C) ist die zentrale Kompetenzstelle zur Zusammenarbeit staatlicher Behörden für Cybersicherheit in Hessen. Es hat die Aufgabe, die Sicherheit in der Informationstechnik des Landes zu erhöhen, cyberspezifische Gefahren abzuwehren, die Effizienz der Bekämpfung der Cyberkriminalität zu erhöhen, Synergien zu schaffen und hessische Verwaltungen, Unternehmen sowie Bürgerinnen und Bürger zu beraten.

Es ist angedacht, zunächst die Kooperationsstrukturen von Hessen3C und damit die Schnittstellen zu den Kommunen im Hinblick auf Hebung von Nutzungspotenzialen für Cybersicherheitsprozesse zu optimieren. Die Forschungszielsetzung des hiermit aufgerufenen Projekts sollte demnach auf vier Schwerpunkten basieren:

1. Analyse des Status quo hinsichtlich kooperativer Strukturen für Cybersicherheitsprozesse,
2. der Entwicklung von Maßnahmen und Verbesserungen,
3. der Einführung dieser und
4. deren Evaluation, u.a. als Blaupause im Hinblick auf weitere Städte, kleinere Kommunen und Gemeinden.

Die Ergebnisse daraus sollen im Hinblick auf deren Verwertung einerseits zur Verbesserung der organisationsübergreifenden Cybersicherheitsprozesse und

daraus folgend zur Unterstützung der Sicherheitsniveaus innerhalb der Städte und Kommunen beitragen. Diese Unterstützungen sollen zunächst mit einer größeren Kommune, bspw. der Digitalstadt Darmstadt, erarbeitet werden, um dann als Blaupause für weitere Städte und Kommunen dienen zu können.

Innerhalb des Hessen3C koordiniert und unterstützt auf Landesebene das CERT (Computer Emergency Response Team) die Bearbeitung von Sicherheitsvorfällen im Zusammenhang mit der Nutzung von Informationstechnik. Der o.g. Forschungsbereich soll sich konkret auf die Kooperationsstrukturen von Hessen3C beziehen, also bspw. auf die Landes-CERT-Meldungen. Diese gehen aktuell unidirektional, d.h. ohne produktive Rückkopplung, an Kommunen und kleine und mittelständische Unternehmen (KMU). In Zusammenarbeit mit Hessen3C sollen optimierte, innovative und ggf. bidirektionale Schwachstellen-/CERT-Prozesse o.ä. entwickelt und nach deren Pilotierung evaluiert werden. Es wird eine enge Zusammenarbeit zwischen dem Hessen3C und dem Zuwendungsempfänger angestrebt, um eine möglichst passgenaue Forschung und nutzbringende Implementierung, bzw. Evaluation in diesem Bereich zu ermöglichen.

5.2. Awareness-Training: KI-Chatbots

Um die Wirkungsweisen von Awareness-Trainings zu erforschen und zu unterstützen und damit eine weitere Optimierung der zielgruppenspezifischen Sensibilisierung zu erreichen, soll in diesem Forschungsvorhaben der Einsatz von KI-Chatbots erforscht werden. Ein KI-Chatbot ist ein intelligentes, sprach- bzw. textbasiertes Dialogsystem, welches das Chatten mit einer Künstlichen Intelligenz erlaubt. Von der aktuellen Corona-Pandemie ausgehend, sind solche KI-Chatbots unabhängig nutzbar, da sie vermehrt auch über digitale Angebote o.ä. einsetzbar sind und nicht zwangsläufig einen Präsenzbetrieb erfordern.

Als Lern- und Schulungsszenario könnte ein gemischter Ansatz (engl. Blended Learning) angenommen werden. Der KI-Chatbot soll als zusätzliches E-Learning-Werkzeug in Kombination mit einer Präsenz- oder Onlineschulung eingesetzt werden, um die Fragen von Nutzerinnen und Nutzern zu beantworten und ggf. auch um das (Vor-)Wissen zu erfragen und dann zu vertiefen. Dabei soll schwerpunktmäßig die allgemeine Sicherheitsbasis und Awareness der Mitarbeiterinnen und Mitarbeitern in ihrem täglichen Arbeitsumfeld fokussiert werden.

In diesem Forschungsvorhaben soll untersucht werden, wie das Grundlagenwissen zum Thema IT-Awareness und Cybersicherheit durch die Verwendung eines KI-Chatbots zielgruppenspezifisch gesteigert werden kann. Zielgruppen sind dabei insbesondere Anwenderinnen und Anwender ohne detaillierte Kenntnisse bzgl. Informationssicherheit, Führungskräfte und IT-Administratoren. Es soll dabei eine Machbarkeitsstudie, ein Umsetzungskonzept einschließlich der beispielhaften Umsetzung sowie ein Prototyp bzw. Demonstrator erarbeitet werden.

Ziel des Forschungsvorhabens ist es, die Wirksamkeit eines KI-Chatbots bei der Sensibilisierung der Mitarbeiterinnen und Mitarbeiter der hessischen Landesverwaltung und des Innenressorts zielgruppenspezifisch zu ermitteln. Der

KI-Chatbot soll dabei an ausgewählten Fokusgruppen getestet und optimiert werden.

5.3. Erforschung und Entwicklung automatisierter Erkennungs- und Klassifikationsverfahren von „Fake News“ und „Hate Speech“ in Zusammenarbeit mit der Meldestelle Hasskommentare des Hessen3C

Ein Ziel der Meldestelle Hasskommentare bei Hessen3C ist es, u.a. Hasskommentare und extremistische Internetinhalte möglichst schnell zu erfassen und diese an die entsprechende Stelle weiterzuleiten.

Im Forschungsvorhaben sollen automatisierte Verfahren zur Erkennung und Klassifikation von falschen Behauptungen (Fake News) und Hasskommentaren (Hate Speech) im Internet erforscht und in enger Zusammenarbeit mit der Meldestelle Hasskommentare des Hessen3C entwickelt werden.

Die entwickelten Verfahren sollen eine automatisierte Vor-Klassifikation von Meinungsäußerungen als (a) gerechtfertigt, (b) diskriminierend/beleidigend und (c) strafrechtlich relevant ermöglichen, welche die Klassifikation durch Expertinnen und Experten unterstützen soll. Weiterhin sollen die Verfahren eine automatische Vor-Klassifizierung von Nachrichten als (a) seriös, (b) teilweise gefälscht, (c) gefälscht und (d) gefährlich ermöglichen. Es wird eine enge Zusammenarbeit zwischen der Meldestelle Hasskommentare und dem Zuwendungsempfänger angestrebt, um eine möglichst passgenaue Forschung und Entwicklung in diesem Bereich zu ermöglichen.

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.