Bekanntmachung des nicht-förmlichen Interessenbekundungsverfahrens zu einer geplanten Beauftragung zur Forschung und Entwicklung von Fähigkeiten im Hinblick auf existenzbedrohende Risiken aus dem Cyber- und Informationsraum für Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien

28. September 2021

Auftraggeber
Agentur für Innovation in der Cybersicherheit GmbH
Willy-Brandt-Straße 87
06110 Halle (Saale)

Berater
FPS Fritze Wicke Seelig Partnerschaftsgesellschaft von Rechtsanwälten mbB
Eschersheimer Landstraße 25-27
60322 Frankfurt am Main

1. Hintergrund und Ziel

„Frau Müller ist nicht unbedingt überrascht von der Warnmeldung. Ihr Teammitglied Kassandra hatte schon vorhergesagt, dass es im Bereich der Energiesicherheit in dieser Woche verstärkt zu Angriffen kommen wird. Und jetzt hat ihr Teammitglied Oskar tatsächlich einen Eingriff in ein Untersystem identifiziert. Eine erste Analyse hat ergeben, dass der Angreifer an der Identifikation von Kundendaten interessiert ist. Eine eher harmlose Attacke; trotzdem besteht innerhalb des Darknets in letzter Zeit ein vermehrtes Interesse an diesen Informationen. Der Warnhinweis an Frau Müller erhält zusätzlich die Information, dass Michael und Anna sich bereits um das Problem gekümmert haben. Der infizierte Bereich wurde aus dem System entkoppelt und die Kundendaten verfälscht; dadurch glaubt der Angreifer noch immer, dass das Virus nicht bemerkt wurde, was für die schon eingeleitete Identifikation des Angreifers wichtig ist. Zusätzlich haben Anna und Michael den „point of vulnerability“ bereits identifiziert und gepatcht. Dies geschah binnen 5 Minuten, nachdem Oskar gewarnt hat. Derzeit arbeiten Anna und Michael weiter an der Identifikation von ähnlichen Angriffsmöglichkeiten in anderen Systemen und patchen etwaige Schwachstellen.

Frau Müller würde ihr Team ja gerne loben, aber das geht nicht. Denn ihre Teammitglieder sind KI-gestützte Programme. Kassandra analysiert auf Basis von empirischen Daten, kriminologischen Erkenntnissen und technischen Entwicklungen die Wahrscheinlichkeit, welche Systeme in Zukunft vermehrt attackiert werden. Diese Daten übergibt „sie“ an die drei anderen Systeme Oskar, Anna und Michael. Oskar ist darauf programmiert, Systeme nach möglichen Angreifern zu durchsuchen. Anna und Michael, Nachfolgersysteme der beiden Programme, die gemeinsam den ersten Platz in der deutschen CyberChallenge gewonnen haben, stehen ständig im Wettstreit, sich gegenseitig anzugreifen und ihre eigenen Systeme zu patchen, falls ein „point of vulnerability“ identifiziert wurde. Mittlerweile hat Frau Müller

von Herrn Schmidt, ihrem menschlichen Kollegen aus der Gruppe Digitale Forensik, die Nachricht erhalten, dass der Angreifer identifiziert werden konnte."

Das oben dargestellte Szenario ist derzeit noch eine Zukunftsvision dazu, wie digitale Systeme – insbesondere im Hochsicherheitsbereich – in Zukunft geschützt werden können. Die Cyberagentur plant, entsprechende Forschung zu beauftragen und damit erste Schritte in die Zukunft zu beschreiten. Denn das umrissene Problem ist akut: Im Zuge der Corona-Pandemie und damit einhergehender Verlagerung der Arbeit in das Homeoffice mit stärkerer digitaler Vernetzung der Mitarbeiter – auch im Bereich der inneren und äußeren Sicherheit – ist die Bedrohung durch Cyberattacken noch größer geworden. Besondere Ziele sind Behörden, Kritische Infrastrukturen, Technologieunternehmen und der Einzelhandel. Aufgrund dieser steigenden Gefahr für die nationale Sicherheit aus dem Cyber- und Informationsraum, besteht ein dringender Bedarf an besseren Methoden und Werkzeugen, um ein hohes Cybersicherheitsniveau für die Bundesrepublik Deutschland zu gewährleisten.

2. Gegenstand der geplanten Beauftragung

Die Agentur für Innovation in der Cybersicherheit plant die Beauftragung von einem wagnisbehafteten zukunftsweisenden Forschungs- und Entwicklungsprojekt im Bereich der Cybersicherheit. Ziel ist die Entwicklung neuer Fähigkeiten für die operative Cybersicherheit, die Behörden im Bereich der inneren und äußeren Sicherheit in Deutschland auf zukünftige Bedrohungen im digitalen Raum vorbereiten. Diese Fähigkeiten konzentrieren sich auf vier Probleme bzw. Fragen innerhalb der Säulen Prävention, Detektion, Reaktion und Repression der operativen Cybersicherheit:

a) Transparenz zum Niveau der Cybersicherheit von Systemen, Netzwerken und Nutzern

Hintergrund: Eine fundierte Einschätzung des Sicherheitsniveaus von Systemen und Systemverbünden ist für verschiedene Szenarien im Kontext der Gewährleistung innerer und äußerer Sicherheit von hoher Relevanz. Sei es bei der Einschätzung der Sicherheit von Regierungsnetzen, von eigenen Waffensystemen oder Internet-of-Things-Systemen (IoT). In all diesen Szenarien ist die Kenntnis bzw. Bewertung des Sicherheitsniveaus die Basis, um angemessene und auf das jeweilige System abgestimmte Entscheidungen hinsichtlich des Schutzes und der Verwendung der Systeme treffen zu können.

Fragestellungen: Wie ist es möglich, auf technischer Ebene den Sicherheitszustand von Systemen und Systemverbünden im Einsatzbereich der inneren und äußeren Sicherheit zu bestimmen und zu bewerten? Wie lassen sich die Einzelelemente eines Systems testen (z.B. Firmware, Netzwerk, Applikationen) und lassen sich die Einzelergebnisse geeignet kombinieren, um eine Gesamtbewertung des Sicherheitszustands abzuleiten?

b) Zeitnahe Detektion und Abwehr von Cyberangriffen

Hintergrund: Derzeit dauert es i.d.R. immer noch mindestens mehrere Monate, bis Angreifer in infiltrierten Systemen gefunden werden. In dieser Zeit können nicht nur sensible Daten abfließen, sondern Angreifer auch ihre Spuren verwischen. Entsprechend erschwert werden etwa Spionageabwehr und Strafverfolgung. Somit ergibt sich eine ständige Unklarheit über die Gewährleistung der Informationssicherheit. Die sich daraus ergebende Gefährdung der Verfügbarkeit, Vertraulichkeit und Integrität der Informationen kann insbesondere im Umfeld

Kritischer Infrastrukturen und behördlicher Anwendungen die Handlungs- und Funktionsfähigkeit im Gesamten bedrohen.

Fragestellungen: Wie gelingt es, Cyberangriffe, etwa auf Regierungsnetze, Waffensysteme etc., schneller und zuverlässiger – automatisiert – zu erkennen? Wie lassen sich Einzelevents zu diesem Zweck präziser korrelieren, die Zahl an Meldungen von Erkennungssystemen ohne Qualitätsverlust reduzieren, große Datenmengen effizient verarbeiten, annotieren und anreichern, sowie Prozess- und Protokollwissen effizient modellieren und nutzbar machen?

c) Eindeutige, unabstreitbare Attribution von Cyberangriffen

Hintergrund: Die Attribution von Cyberangriffen ist die notwendige Basis, um auf einen Angriff so reagieren zu können, dass dieser abgewehrt, die ausgenutzten Schwachstellen geschlossen, die Quelle identifiziert und unschädlich gemacht werden können. Somit ist die eindeutige, unabstreitbare Attribution von Cyberangriffen ein Kernbedarf aller mit der Gewährleistung der inneren und äußeren Sicherheit beauftragten Entitäten; sei es im Bereich der kriminalpolizeilichen Organisationen zur Bekämpfung von Cyberkriminalität, bei Nachrichtendiensten im Zusammenhang mit Cyberspionage oder im Umfeld von militärischen Operationen im Kontext von Cyberwarfare.

Fragestellungen: Wie belastbar ist die Attribution von Cyberangriffen auf Basis aktuell zur Verfügung stehender Indikatoren? Wie lässt sich diese Belastbarkeit messbar machen? Welche Eigenschaften müssen bessere Indikatoren aufweisen und wie lassen sich solche Indikatoren erschließen?

d) Minimierung ausnutzbarer Schwachstellen von Systemen und Netzwerken

Hintergrund: Cyberangriffe stellen eine Bedrohung für die innere und äußere Sicherheit dar. Schwachstellen sind entsprechende Einfallstore für Cyberangriffe. Gelingt es, die Zahl ausnutzbarer Schwachstellen und die Zeit für ihre Ausnutzung zu minimieren, steigt der Aufwand für Angreifer und damit auch das Cybersicherheitsniveau. Speziell der sichere Betrieb von Systemen und Infrastrukturen würde davon enorm profitieren. Im Kontext der Behörden und Organisatoren mit Sicherheitsaufgaben (BOS) besteht beispielsweise Bedarf zur Absicherung des IVBB, von Telekommunikationsinfrastrukturen und Einsatznetzen.

Fragestellungen: Wie lassen sich Schwachstellen in besonders sicherheitssensiblen Systemen automatisiert finden und schließen? Wie lässt sich eine Vollautomatisierung erreichen? Wie lassen sich statische und dynamische Analyseansätze kombinieren und welche Systemabdeckung lässt sich damit erreichen?

3. Ziel und Inhalt des Interessenbekundungsverfahrens

a) Potentieller Teilnehmerkreis

Die Interessenbekundung dient insbesondere dazu, dass die Cyberagentur einen Überblick über Anzahl und Art der Zielgruppe gewinnt. Interessierte potentielle Teilnehmer aus verschiedensten Institutionen, wie z.B. Universitäten, außeruniversitäre Forschungseinrichtungen, KMUs, Start-ups werden daher aufgerufen, sich durch Abgabe einer Ideenskizze am Interessenbekundungsverfahren zu beteiligen.

Aufgrund der hohen Komplexität des Auftrags erachtet die Cyberagentur die Gründung von Konsortien mit breiter Expertise als zielführend. Das Interessenbekundungsverfahren soll auch dazu dienen, dass sich für das spätere Verfahren geeignete Konsortien zusammenfinden können. An dem Interessenbekundungsverfahren selbst können die Teilnehmer entweder einzeln oder schon als Konsortium teilnehmen. Falls (noch) kein Konsortium gebildet wird, wird gebeten, in der Ideenskizze anzugeben, ob eine Teilnahme am späteren Verfahren als Einzelbewerber oder als Konsortium angedacht ist und wie viele Partner wahrscheinlich benötigt werden.

b) Intellectual Property Rights

Die Cyberagentur ist gehalten, sich 100% der IP der Produkte, die in dem zu beauftragenden Projekt entwickelt werden, zu sichern, es sei denn, wirtschaftliche oder rechtliche Aspekte verhindern dies. Sollte letzteres für interessierte Teilnehmer zutreffen, wird gebeten, dies im Rahmen der Ideenskizze darzulegen und zu begründen.

c) Volumen und Laufzeit des Projekts

Die Cyberagentur geht davon aus, dass ein Projektvolumen von maximal 15 Millionen Euro für eine holistische Betrachtung und Erarbeitung der vier Säulen erforderlich ist. Dabei ist es erwünscht, dass Projekte alle vier Säulen bearbeiten. Falls ein Teilnehmer nicht alle vier Säulen bearbeiten kann, wird gebeten, dies in der Ideenskizze wissenschaftlich zu begründen.

Geplant ist eine Laufzeit von 60 Monaten. Falls eine andere Laufzeit als zielführender erachtet wird, wird um Begründung gebeten.

d) Technische Expertise

Im Rahmen des sich anschließenden Verfahrens müssen die Bewerber die technischen Fähigkeiten im Bereich Fähigkeitsentwicklung mit Bezug zur Cybersicherheit aufweisen. Um einen besseren Marktüberblick zu gewinnen, bitten wir um Beantwortung folgender Frage in der Ideenskizze:

Frage: In welchen Projekten haben Sie im Bereich Cybersecurity in den letzten fünf Jahren geforscht?

Nachweis: Liste von Projekten mit kurzer Beschreibung des Projekts, Tätigkeiten des Auftragnehmers sowie komplettem finanziellen Projektvolumen und Anteil des Auftragnehmers.

e) Management Expertise

Für das sich anschließende Verfahren müssen die Bewerber die notwendigen Fähigkeiten besitzen, um ein großes, komplexes Forschungsprojekt zu leiten. Um einen besseren Marktüberblick zu gewinnen, bitten wir um Beantwortung folgender Frage in der Ideenskizze:

Frage: In welchen Projekten in den letzten fünf Jahren haben Sie Projektleitungsaufgaben übernommen?

Nachweis: Kurze Beschreibung des Projekts sowie des finanziellen Projektvolumens und der Anzahl der Unterauftragnehmer/Konsortialpartner. CV des Projektleiters.

f) Identifizierung möglicher weiterer Handlungsfelder

Es ist ausdrücklich erwünscht, dass Teilnehmer in der Ideenskizze auf weitere (nicht beschriebene, fehlende) Handlungsfelder hinweisen. Durch diese zusätzliche Erschließung darf sich keine Verschlechterung der beschriebenen erforderlichen Handlungsfelder ergeben.

g) Inhalt Ideenskizze

Die Ideenskizze soll im PDF-Format eingereicht werden und sollte einen Umfang von 15 DIN-A4-Seiten inklusive des Deckblattes nicht überschreiten (Schriftart Arial, Schriftgröße 11, einfacher Zeilenabstand, Rand mindestens 2 cm). Unterstützende Dokumente (wie CVs) sind exklusive.

Die Ideenskizze sollte folgender Gliederung folgen:

- Deckblatt mit Kontaktdaten (Name, Adresse, Telefon, E-Mail-Adresse) des interessierten Teilnehmers / Konsortium und eines Ansprechpartners;
- Executive Summary;
- Beschreibung des Vorhabens:
    - Kurzbeschreibung, die die oben beschriebenen Themen und Fragestellungen adressiert;
    - Darstellung des Innovationsgrads und Zukunftsfähigkeit des Projekts;
    - Beschreibung Methodik und wissenschaftlicher Ansätze;
    - Impact auf die Forschungslandschaft und Fähigkeitsentwicklung;
    - Zeitplanung, erforderliches Budget.

4. Frist zur Teilnahme am nichtförmlichen Interessensbekundungsverfahren

Interessierte Teilnehmer können bis zum Stichtag

12. November 2021, 14.00 Uhr

ihre Ideenskizzen elektronisch einreichen an: HSK-Ideenskizze@cyberagentur.de. Entstehende Kosten sind nicht erstattungsfähig. Des Weiteren begründet das Verfahren keinerlei gegenseitige Verpflichtungen.

Nach Ende des Verfahrens erhalten Interessenten detaillierte Informationen zum weiteren Vorgehen. Insbesondere werden dann die vertraglichen und vergaberechtlichen Inhalte abschließend bestimmt und das Verfahren ggf. zur Beauftragung eröffnet. Weitere Hintergrund- und aktuelle Informationen können ggf. auf der Internetseite http://www.cyberagentur.de abgerufen werden.

Fragen zum Interessenbekundungsverfahren können ausschließlich über die oben genannte E-Mail-Adresse gestellt werden. Es wird gebeten, Fragen bis spätestens 5. November 2021 zu stellen, um eine rechtzeitige Beantwortung zu gewährleisten. Aus Gründen der

Gleichbehandlung werden alle Fragen und Antworten anonymisiert allen Teilnehmern auf folgender Website zur Verfügung gestellt: www.cyberagentur.de/hsk-ideenskizze.

Darüber hinaus sind mündliche Abstimmungen und ergänzende Auskünfte durch die Cyberagentur nicht möglich.