Bundesanzeiger
Herausgegeben vom
Bundesministerium der Justiz
www.bundesanzeiger.de

Bekanntmachung
Veröffentlicht am Freitag, 23. September 2022
BAnz AT 23.09.2022 B1

Bundesministerium für Wirtschaft und Klimaschutz

Förderbekanntmachung IT-Sicherheit in der Wirtschaft – Transferstelle Cybersicherheit und Fokusprojekte

Vom 15. September 2022

1 Zuwendungszweck, Förderziele, Rechtsgrundlagen

1.1 Zuwendungszweck

Die Cybersicherheitsstrategie 2021 der Bundesregierung bewertet die IT- und Cybersicherheit als gesamtgesellschaftliche Aufgabe, die auch von mittelständischen Unternehmen wahrzunehmen ist. Auch der Koalitionsvertrag für die 20. Legislaturperiode greift Digitalisierung und IT-Sicherheit im Mittelstand auf: Kleine und mittlere Unternehmen (KMU) sollen bei der Digitalisierung durch unkomplizierte Förderung gestärkt und die Unterstützung für IT-Sicherheit ausgebaut werden.[1] Sichere und damit nachhaltige Digitalisierung des Mittelstands kann nur mit adäquater IT- und Cybersicherheit gelingen.

IT- und Cybersicherheit ist eine zentrale Voraussetzung für die erfolgreiche und nachhaltige Implementierung digitaler Technologien und Anwendungen.[2] Die Entwicklung digitaler Geschäftsmodelle und -prozesse erfordert auch ausgeprägte unternehmerische IT- und Cybersicherheit. Vor allem im Mittelstand stehen wachsende Anforderungen an die IT- und Cybersicherheit begrenzten Ressourcen, unzureichender Fachkenntnis und geringer Investitionsbereitschaft gegenüber.[3] Die Corona-Pandemie hat im Mittelstand einen Digitalisierungsschub ausgelöst. Die IT- und Cybersicherheit hat sich indes nicht in gleichem Maße entwickelt. Damit hat die Pandemie die Sicherheitslücke bei KMU und Handwerksbetrieben vergrößert. Mittelständler hinsichtlich der Gefahren der digitalen Welt zu sensibilisieren, sie zu informieren und zu Lösungsmöglichkeiten zu befähigen, hat damit nochmals an Bedeutung gewonnen. In seinem Bericht zur Lage der IT-Sicherheit in Deutschland bewertet das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Gefährdungslage der IT-Sicherheit in vielen Bereichen als hoch.[4] Auch perspektivisch wird sich die Bedrohungslage für Unternehmen weiter verschärfen. So berichtet das Bundeskriminalamt in seinem Bundeslagebild Cybercrime 2021 von einer kontinuierlichen Dynamik der Bedrohungslage.[5] Cyberkriminalität entwickelt sich arbeitsteilig, wodurch Angriffe ausgefeilter, individueller und einfacher umsetzbar werden („cybercrime-as-a-service“).

Während in der Vergangenheit überwiegend größere Unternehmen Opfer von Cyberangriffen wurden, berichten gegenwärtig verstärkt mittelständische Unternehmen von IT-Sicherheitsvorfällen: Deutlich mehr als die Hälfte der Mittelständler hat bereits einen Cyberangriff erlebt bzw. darauf reagiert.[6] Zudem nehmen Lieferkettenangriffe stark zu, mit denen Hacker Mittelständler als schwächstes Glied einer Lieferkette attackieren und über sie besser geschützte Unternehmen angreifen. Besonders kritisch ist hierbei, dass insbesondere kleinere Unternehmen ihr individuelles Risiko tendenziell stärker unterschätzen, was in der Konsequenz dazu führt, dass erforderliche Schutzmaßnahmen gar nicht, zu spät oder nicht umfangreich genug eingeführt werden. Sensibilisierung, Information und weitere Ausprägungen der Befähigung sind besonders herausfordernd, weil Erfolge in der IT- und Cybersicherheit in der Regel

[1] Koalitionsvertrag 2021-2025, S. 19.
[2] VDE (2016), Digitalisierung 2020, Frankfurt am Main.
[3] Köhler et al. (2021), IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland, Berlin.
[4] BSI (2021), Die Lage der IT-Sicherheit in Deutschland 2021, Bonn.
[5] BKA (2022), Bundeslagebild Cybercrime, Wiesbaden.
[6] Dreißigacker et al. (2021), Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020, KfN-Forschungsbericht Nr. 162, Hannover (S. 52).

nicht sichtbar sind, sodass Investitionen in Präventionsmaßnahmen gescheut werden.[7] Dies betrifft insbesondere Mittelständler, die zwar abstrakt von der Gefährdungslage wissen, diese Kenntnis indes nicht in unternehmerisches Handeln überführen.

Mit der Transferstelle IT-Sicherheit im Mittelstand hat das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) im Jahr 2020 im Rahmen der Initiative IT-Sicherheit in der Wirtschaft ein Unterstützungsangebot für mittelständische Betriebe geschaffen.[8] Die Transferstelle IT-Sicherheit im Mittelstand sensibilisiert, informiert und befähigt KMU und Handwerk für IT- und Cybersicherheit und übernimmt eine Lotsenfunktion, damit sich Mittelständler in der Angebotsvielfalt verschiedenster Cybersicherheitslösungen zurechtfinden. Daneben vernetzt sie sich mit anderen Akteuren der IT- und Cybersicherheit, anderen Initiativen und Multiplikatoren, um gemeinsam die Awareness für IT-Sicherheit in der Zielgruppe KMU zu steigern und die Umsetzung von IT-Sicherheitsmaßnahmen in KMU zu begünstigen. Dieses Angebot wird durch themenspezifische Einzel- und Verbundprojekte ergänzt.

Die sich dynamisch entwickelnde Gefährdungslage, die durch die Pandemie vergrößerte Sicherheitslücke und die beschriebene Ausgangslage der bestehenden Förderung für IT- und Cybersicherheit im Mittelstand zeigen, dass auch nach dem Auslaufen der Förderung der aktuellen Transferstelle IT-Sicherheit im Mittelstand ab dem dritten Quartal 2023 ein bedarfsgerechtes Förderangebot für IT- und Cybersicherheit im Mittelstand erforderlich ist. KMU und Handwerksbetriebe müssen weiterhin und verstärkt mit innovativen und aufsuchenden Formaten dabei unterstützt werden, ihr Cybersicherheitsniveau zu erhöhen und ihr Unternehmen gegen die Risiken der digitalen Welt zu schützen. Nur so können sie auch künftig wettbewerbsfähig sein.

Diese Förderbekanntmachung ist die Grundlage, eine neu akzentuierte Transferstelle Cybersicherheit sowie Fokusprojekte zu fördern, die die aktuellen Herausforderungen der IT- und Cybersicherheit im Mittelstand adressieren.

1.2.1 Förderziele

Ziele der Förderung der Initiative IT-Sicherheit in der Wirtschaft sind:

- Sichere digitale Transformation im Mittelstand,
- Erhöhung des IT- und Cybersicherheitsniveaus im Mittelstand,
- Wissen in KMU, Handwerksbetrieben und Start-ups über die Gefahren der digitalen Welt im Allgemeinen und für das eigene Unternehmen im Besonderen erhöhen,
- Wissen in KMU, Handwerksbetrieben und Start-ups über Handlungsmöglichkeiten in allen Teilbereichen der Cybersicherheit – Prävention, Detektion und Reaktion – erhöhen,
- Handlungskompetenz in allen Teilbereichen der Cybersicherheit in KMU, Handwerksbetrieben und Start-ups erhöhen,
- Entwicklung und Durchführung innovativer aufsuchender Formate, mit denen das Thema IT- und Cybersicherheit auch in Betriebe getragen werden kann, die bisher nur schwer zu erreichen waren,
- Den Einsatz sicherer digitaler Prozesse, digitaler Technologien und digitaler Geschäftsmodelle und damit auch die Wettbewerbs- und Innovationsfähigkeit des Mittelstands erhöhen,
- Transferstrukturen mit anderen Akteuren der IT- und Cybersicherheit etablieren,
- Technologische, organisatorische und arbeitsgestaltende Kompetenzen der IT- und Cybersicherheit erhöhen, Sicherheit von und Vertrauen in (Anbieter/Anwender) IKT-Systeme inkl. Hard- und Software erhöhen.

Die Transferstelle Cybersicherheit wird auf den Arbeiten der bisherigen Transferstelle IT-Sicherheit im Mittelstand aufbauen und den dortigen Fokus auf Prävention insbesondere um die Elemente Detektion und Reaktion erweitern. Zudem sollen Start-ups bei der IT- und Cybersicherheit verstärkt adressiert werden. Durch ein ausgeprägtes eigenes IT-Sicherheits-Know-how soll es der Transferstelle Cybersicherheit noch besser gelingen, komplexe Themen und Zusammenhänge der IT- und Cybersicherheit für den Mittelstand anschaulich aufzubereiten und zu transferieren.

Die Fokusprojekte sind Einzel- und Verbundprojekte, die sich einzelnen bzw. spezifischen Fragestellungen widmen und konkrete, rasch anwendbare bzw. nutzbare Ergebnisse für KMU und Handwerk (einschließlich Start-ups) erarbeiten.

Die Transferstelle Cybersicherheit soll mit den noch laufenden Einzel- und Verbundprojekten der alten Förderbekanntmachung und den neuen Fokusprojekten dieser Förderbekanntmachung sowie insbesondere mit dem Netzwerk der Mittelstand-Digital Zentren, den Europäischen Digitalen Innovationszentren (European Digital Innovation Hubs – EDIHs) und dem Nationalen Koordinierungszentrum für Cybersicherheit (NKCS) Synergien heben.

1.2.2 Rechtsgrundlagen

Projekte können nach Maßgabe dieser Förderbekanntmachung, der §§ 23, 44 der Bundeshaushaltsordnung, der Allgemeinen Verwaltungsvorschriften zu den §§ 23, 44 BHO und der Allgemeinen Nebenbestimmungen für Zuwendungen auf Ausgaben- bzw. Kostenbasis durch Zuwendungen gefördert werden.

Soweit die Förderung nach Maßgabe der Nummern 2.1.1 und 2.2.2 des Unionsrahmens für staatliche Beihilfen für Forschung, Entwicklung und Innovation – FuEuI-Unionsrahmen (ABl. C 198 vom 27.6.2014, S. 1) erfolgt und die Zuwendungsempfänger die Voraussetzungen einer Einrichtung für Forschung und Wissenstransfer im Sinn von Num-

[7] Köhler et al. (2021), IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland, Berlin.
[8] BAnz AT 31.12.2018 B2

mer 1.3 Doppelbuchstabe ee des FuEuI-Unionsrahmen erfüllen, stellt die Zuwendung keine Beihilfe im Sinne des Artikel 107 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) dar. Insoweit werden ausschließlich Wissenstransfermaßnahmen gefördert, die gemäß Nummer 2.1.1 des Unionsrahmens für staatliche Beihilfen für FuEuI-Unionsrahmen (ABl. C 198 vom 27.6.2014, S. 1) als nichtwirtschaftliche Tätigkeiten der Zuwendungsempfänger einzustufen sind.

Falls diese Voraussetzungen nicht erfüllt sind und eine wirtschaftliche Tätigkeit gegeben ist, erfolgt die Förderung auf der Grundlage der Verordnung (EU) Nr. 1407/2013 der Kommission vom 18. Dezember 2013 über die Anwendung der Artikel 107 und 108 des Vertrags über die Arbeitsweise der Europäischen Union auf De-minimis-Beihilfen (ABl. L 352 vom 24.12.2013, S. 1). Der Gesamtbetrag der einem Unternehmen von einem Mitgliedstaat gewährten De-minimis-Beihilfen darf innerhalb eines fließenden Zeitraums von drei Steuerjahren den Betrag von 200 000 Euro nicht überschreiten. Dem Antrag ist eine Erklärung in schriftlicher oder elektronischer Form beizufügen, in der der Antragsteller alle anderen ihm in den beiden vorangegangenen sowie im laufenden Steuerjahr gewährten De-minimis-Beihilfen angibt (De-minimis-Erklärung). In den in Artikel 1 Absatz 1 der Verordnung (EU) Nr. 1407/2013 genannten Ausnahmefällen ist eine Förderung ausgeschlossen.

Der Antragsteller muss sich im Antrag auf Förderung damit einverstanden erklären, dass

- sämtliche mit dem Antrag oder im weiteren Verfahren beim Projektträger eingereichten Unterlagen auch dem BMWK zur Verfügung stehen,
- die Förderung auf Grundlage von § 44 BHO in Verbindung mit der Verwaltungsvorschrift Nummer 9.1 und 9.2 zu § 44 BHO in einem zentralen System des Bundes erfasst wird (Zuwendungsdatenbank),
- alle im Zusammenhang mit der Förderung bekannt gewordenen Daten und Nachweise
  - vom Projektträger, dem BMWK oder einer von einem der beiden beauftragten Stelle auf Datenträger gespeichert werden können,
  - zum Zweck der Erfolgskontrolle gemäß der Verwaltungsvorschrift nach § 7 BHO weiterverarbeitet werden können,
  - von BMWK an zur Vertraulichkeit verpflichtete, mit einer Evaluation beauftragte Dritte weitergegeben und dort weiterverarbeitet werden können,
  - für Zwecke der Bearbeitung und Kontrolle der Anträge, der Statistik, Monitoring, wissenschaftliche Fragestellungen, Verknüpfung mit amtlichen Daten, Evaluation und der Erfolgskontrolle des Förderprogramms verwendet und ausgewertet werden,
- die anonymisierten bzw. aggregierten Auswertungsergebnisse veröffentlicht und an den Bundestag und an Einrichtungen des Bundes und der Europäischen Union weitergeleitet werden können.

Die Informationen werden ausschließlich für die vorgenannten Zwecke verwendet, vertraulich behandelt und so anonymisiert veröffentlicht, dass ein Rückschluss auf einzelne Personen, Unternehmen oder Einrichtungen nicht möglich ist.

Ein Rechtsanspruch auf Gewährung einer Zuwendung besteht nicht. Der Zuwendungsgeber entscheidet nach pflichtgemäßem Ermessen im Rahmen der verfügbaren Haushaltsmittel.

Für die Bewilligung, Auszahlung und Abrechnung der Zuwendung sowie für den Nachweis nach und die Prüfung der Verwendung und die gegebenenfalls erforderliche Aufhebung des Zuwendungsbescheids und die Rückforderung der gewährten Zuwendung gelten die §§ 48 bis 49a des Verwaltungsverfahrensgesetzes, die §§ 23, 44 BHO und die hierzu erlassene Verwaltungsvorschrift. Der Bundesrechnungshof ist gemäß den §§ 91, 100 BHO zur Prüfung berechtigt.

2 Gegenstand, Aufgaben und Randbedingungen der Förderung

2.1 Gegenstand der Förderung

Das BMWK beabsichtigt die Förderung einer Transferstelle Cybersicherheit, die den Kern der Initiative IT-Sicherheit in der Wirtschaft ausmacht. Die Transferstelle soll ergänzt werden um Fokusprojekte, in welchen bedarfsgerecht und gezielt Lösungen für relevante und übergreifende Problemstellungen von KMU einschl. Start-ups und Handwerk im Schwerpunkt IT- und Cybersicherheit erarbeitet werden.

2.2 Aufgaben

1. Die Transferstelle Cybersicherheit erfüllt folgende Aufgaben:

   a) Die Transferstelle Cybersicherheit nutzt, erarbeitet und verbreitet praxisorientierte Informations- und Unterstützungsangebote durch Wissenstransfer für den Wissens- und Kompetenzaufbau in KMU und Handwerk einschließlich Start-ups. Die Transferstelle berät dabei nicht einzelfallbezogen, sondern transferiert anwendungsorientiertes Wissen praxisorientiert und passgenau. Die mehrstufige Transferarbeit (von Basisangeboten bis hin zur Vermittlung von Spezialkompetenzen) berücksichtigt den individuellen Reifegrad der IT- und Cybersicherheit der adressierten Unternehmen. Zugleich werden alle relevanten Dimensionen der Informationssicherheit („Organisation“, „Technik“ und „Mensch“) sowie die Phasen „Prävention“, „Detektion“ und „Reaktion“ einbezogen. Die anerkannten Schutzziele der Informationssicherheit Vertraulichkeit, Integrität, Verfügbarkeit sowie Authentizität werden berücksichtigt und adressiert.

Die Transferstelle Cybersicherheit entwickelt und nutzt innovative aufsuchende Formate, mit denen auch die Unternehmen erreicht werden, die bisher nicht oder nur unzureichend für IT- und Cybersicherheit sensibilisiert, informiert und befähigt werden konnten und deshalb über ein regelmäßig hohes Schutzdefizit verfügen. Im Angebotsportfolio der Transferstelle Cybersicherheit werden Angebote Dritter, insbesondere Angebote des Netzwerks der Mittelstand-Digital Zentren, berücksichtigt. Die Transferstelle nimmt eine Bündelungs- und Lotsenfunktion wahr: Sie ist zentrale Anlaufstelle und stellt existierende zielgruppenspezifische Unterstützungsangebote Dritter (insbesondere aus Initiativen von Bund und Ländern) anwenderfreundlich und übersichtlich dar. Die Angebote und Inhalte der Transferstelle sind adressatengerecht gestaltet, indem sie eine möglichst hohe Praxisorientierung aufweisen. KMU, Handwerksbetriebe und Start-ups werden mit präventiven, detektierenden und reaktiven Maßnahmen (d. h. Reaktion im Fall eines Cyberangriffs) vertraut gemacht.

Die Transferstelle Cybersicherheit greift die Produkte der bisherigen Transferstelle IT-Sicherheit im Mittelstand (insbesondere Sec-O-Mat, Internetseite und App) auf, nutzt diese weiter und entwickelt sie kontinuierlich fort. Bestehende Netzwerke und Kooperationen werden ebenfalls übernommen und weiterentwickelt.

Diese transferorientierten Produkte sollen eigenständig, aber auch in Kooperation mit öffentlichen Institutionen oder Verwaltungen, Multiplikatoren wie Verbänden, Kammern oder Wirtschaftsförderungseinrichtungen umgesetzt werden. Kooperationen sorgen für den Ausbau regionaler und bundesweiter Unterstützungs- und Transfernetzwerke. Sofern verfügbar, sollten bestehende Infrastrukturen (z. B. bei regionalen Kooperationspartnern) genutzt werden.

Die Transferstelle berücksichtigt aktuelle Entwicklungen und Bedrohungen bei allen Formaten, ohne jedoch tagesaktuelle Entwicklungen aufzunehmen, wie sie typischerweise von Cyber Emergency Response Teams (CERT) wahrgenommen werden.

b) Innovative Angebote befähigen durch Wissenstransfer Führungskräfte sowie Beschäftigte, damit sie Entscheidungen zur IT- und Cybersicherheit eigenständig bewerten können. Dabei kommen aufsuchende und Online-Formate zur Anwendung, die ausgeprägten Praxisbezug aufweisen. Es können eigene Angebote durch die Transferstelle Cybersicherheit entwickelt oder Angebote Dritter für den Transfer aufbereitet bzw. genutzt werden. Synergien mit Fokusprojekten der Initiative IT-Sicherheit in der Wirtschaft sollen erschlossen werden.

c) Zielgruppenorientierte Öffentlichkeitsarbeit flankiert alle Maßnahmen der Transferstelle und greift unternehmensnahe Positivbeispiele auf, die andere Unternehmerinnen und Unternehmer ansprechen und zum Nachahmen anregen. Die Öffentlichkeitsarbeit soll Anlaufstelle und Lotse sein, indem sie einen einfachen Zugriff auf Angebote, Anlaufstellen und Kontaktpersonen ermöglicht, den Suchaufwand für Unternehmen reduziert und auf Förder- und Unterstützungsmöglichkeiten (Bund, Länder, Multiplikatoren etc.) hinweist. Mit einer Projektinternetseite soll bundesweite Strahlkraft entwickelt werden. Zudem engagiert sich die Transferstelle bei relevanten Fachmessen. Darüber hinaus plant und realisiert sie öffentlichkeitswirksame Auftritte, auch in Kooperation mit Dritten, wie insbesondere ausgewählten Mittelstand-Digital Zentren, und nutzt aktiv die sozialen Medien. Neben den projektspezifischen Kommunikationszielen werden auch die Ziele der Initiative IT-Sicherheit in der Wirtschaft aktiv verfolgt. Dies erfolgt beispielweise durch die Berücksichtigung und Verbreitung von Projektergebnissen aus den bisherigen Projekten der Initiative. Hierbei handelt es sich um anwendungsbezogene Tools, digitale Lerneinheiten, Demonstrationsbeispiele und Materialien für KMU, die entsprechende Sichtbarkeit in der Zielgruppe erfahren sollen. In gemeinsamen Abstimmungstreffen mit diesen Projekten werden Synergien und Potenziale aufgezeigt. Dabei übernimmt die Transferstelle eine koordinierende und leitende Funktion.

d) Die Transferstelle vernetzt sich mit relevanten Akteuren der IT- und Cybersicherheit (z. B. aus Forschung, Vereinen, Verbänden, Fördergebern und Gebietskörperschaften) und fördert den Austausch untereinander. Synergien mit dem Nationalen Koordinierungszentrum für Cybersicherheit (NKCS) und der durch das NKCS aufzubauenden nationalen Cybersicherheitscommunity sollen erschlossen werden. Die Vernetzung soll insbesondere dazu dienen, Strukturen zu schaffen, die auch nach einem Ende der Förderung Bestand haben und mittelständische Unternehmen verstetigt unterstützen.

e) Aktuelle Bedrohungen, neue Entwicklungen und aktuelle Themen werden laufend in einem prägnanten mittelstandsspezifischen holistischen „Lagebild Cybersicherheit im Mittelstand“ erfasst und bei den Angeboten und Maßnahmen der Transferstelle aufgegriffen. Die Projektbeteiligten beobachten dazu laufend das wissenschaftliche und wirtschaftliche Umfeld sowie die Entwicklung der Gefährdungslage für den Mittelstand, um aktuelle Herausforderungen von KMU im Bereich IT-Sicherheit zu identifizieren. Erkenntnisse werden in regelmäßigen Abständen (beispielsweise zweimal pro Jahr) in geeigneter Form für den Mittelstand aufbereitet und veröffentlicht. Berücksichtigt werden insbesondere Publikationen des BSI und weiterer Dritter. Dopplungen sind zu vermeiden. Eine tagesaktuelle Beobachtung ist nicht vorgesehen, aber Trends und die Grundlinien aktueller Entwicklungen sollen mittelstandsgerecht abgebildet, mit eigenen Formaten zu Sensibilisierung, Information und Befähigung verknüpft und praxisgerecht kommuniziert und transferiert werden.

Das Projekt wirkt darauf hin, dass die Arbeit der Transferstelle Cybersicherheit nach dem Auslaufen der Förderung weitergeführt und der Nutzen für den Mittelstand verstetigt werden kann (Verwertung und Anschlussfähigkeit).

2. Die Fokusprojekte erfüllen folgende Aufgaben:

Die Fokusprojekte sind Einzel- oder Verbundprojekte, die für mittelstandsspezifische Probleme Lösungen erarbeiten. Dadurch soll das IT-Sicherheitsniveau von KMU, Handwerk (einschließlich Start-ups) nachhaltig erhöht werden. Fokusprojekte sind ausgeprägt mittelstands- und praxisorientiert und zur direkten Nutzung durch die Ziel-

gruppen bestimmt. Die Projektpartner sollen über ein gutes Verständnis der konkreten Bedarfe des Mittelstandes verfügen, sodass keine Bedarfsanalysen, Studien o. Ä. erforderlich sind. Alle Fokusprojekte enthalten geeignete Transferformate, die die Ergebnisse in die Breite tragen und so hohe Wirkungen und eine große Reichweite erzielen.

Die Fokusprojekte haben regelmäßig insbesondere folgende Merkmale:

- Schnelle Erarbeitung erster Ergebnisse und Beginn des Transfers innerhalb von sechs Monaten,
- Kurze Entwicklungszyklen und – soweit möglich – iterative Weiterentwicklung, agile Projektsteuerung,
- Praxiskooperationen mit Mittelständlern oder andere geeignete und innovative Transferformate,
- Eigenständige Öffentlichkeitsarbeit, um die Lösungen bei den Zielgruppen zu verbreiten. Mit ÖA-Strukturen von Mittelstand-Digital und der Transferstelle Cybersicherheit soll kooperiert werden,
- Projektergebnisse sollen gut und praxisnah verwertbar und – soweit möglich – hinsichtlich Weiterentwicklungen anschlussfähig sein,
- Bestehende Transferstrukturen werden genutzt (insbesondere Transferstelle Cybersicherheit und Mittelstand-Digital Zentren).

Geförderte Themen der Fokusprojekte werden vier Monate vor den in Nummer 6.2 aufgeführten Fristen zur Einreichung der Skizzen auf der BMWK-Internetseite www.mittelstand-digital.de veröffentlicht. Auch zu weiteren relevanten praxisnahen und zielgruppenspezifischen Themenfeldern bzw. Problemstellungen im Bereich der IT- und Cybersicherheit können Skizzen eingereicht werden.

2.3 Randbedingungen der Förderung

Die genannten Aufgaben der Transferstelle Cybersicherheit sowie der Fokusprojekte werden unter Beachtung folgender Randbedingungen bearbeitet:

a) IT-Sicherheitskompetenz: Transferstelle Cybersicherheit und Fokusprojekte greifen auf Fachexpertise und ausgereifte, anwendungsbezogene Qualifikationen im Schwerpunkt der IT- und Cybersicherheit zurück. Zur Umsetzung der Arbeiten der Transferstelle werden Fachkompetenzen im technologischen, organisatorischen und arbeitsgestaltenden Kontext sowie ausgeprägte Transferkompetenz eingebracht. Insbesondere die eigene technische Cybersicherheitskompetenz soll es der Transferstelle ermöglichen, neue Bedrohungen und ihre Auswirkungen auf den Mittelstand eigenständig zu bewerten.

b) Infrastruktur: Die Transferstelle Cybersicherheit ist deutschlandweite Kontaktstelle für KMU, Handwerk und Startups und zusätzlich vor Ort durch regionale Anlaufstellen präsent. Sie ist daneben über das Internet und telefonisch erreichbar. Der Gedanke der Regionalität wird bei der Ausgestaltung der Kontaktmöglichkeiten berücksichtigt. Die Fokusprojekte adressieren eine IT-sicherheitsspezifische Problemstellung und müssen die notwendige Infrastruktur zur Bearbeitung ebendieser Problemstellung und des Transfers einbringen.

   Sowohl für die Transferstelle Cybersicherheit als auch für die Fokusprojekte kann eine überregionale Ansprache der Zielgruppe auf bestehende Demonstrationsbeispiele oder mobile Transferinstrumente gestützt werden. Vorhandene Infrastruktur der Zuwendungsempfänger kann in einem begrenzten Maße im Rahmen des Projekts weiterentwickelt werden, sofern es dem Erfolg dienlich ist.

c) Kooperation/Vernetzung: Die Abstimmung und Zusammenarbeit mit anderen relevanten Initiativen zur IT- und Cybersicherheit für Wirtschaft und Mittelstand ist verpflichtend, um den praxisorientierten Transfer von Informationen und Ergebnissen zu gewährleisten und eventuelle Doppelarbeiten auszuschließen. Ein aktiver gegenseitiger Austausch und Zusammenarbeit innerhalb der Initiative IT-Sicherheit in der Wirtschaft und mit dem Netzwerk der Mittelstand-Digital Zentren werden vorausgesetzt, um ein aufeinander abgestimmtes, zielgruppengerechtes Angebot zu gewährleisten. Die Transferstelle Cybersicherheit nimmt zur Intensivierung der Kooperation zudem an relevanten Vernetzungsveranstaltungen anderer Initiativen teil und bringt sich aktiv in die „Redaktionsgruppe“ des Netzwerks Mittelstand-Digital zum Thema „IT-Sicherheit“ sowie in weiteren relevanten Arbeitsgruppen der Mittelstand-Digital Zentren (z. B. AG IT-Sicherheit, AG Recht) ein. Die Transferstelle Cybersicherheit wirkt an Publikationen der Begleitforschung von Mittelstand-Digital mit.

   Die Fokusprojekte kooperieren innerhalb der Initiative IT-Sicherheit in der Wirtschaft miteinander und mit der Transferstelle Cybersicherheit und darüber hinaus den Mittelstand-Digital Zentren. Um interne und externe Kooperationen außerhalb von Mittelstand-Digital zu sichern, organisiert die Transferstelle Cybersicherheit eine themenspezifische Fachkonferenz pro Jahr. Die Zentren des Netzwerks Mittelstand-Digital und die Fokusprojekte werden bei der Konzeption berücksichtigt.

d) Begleitforschung: Transferstelle Cybersicherheit und Fokusprojekte arbeiten mit der durch das BMWK beauftragten Begleitforschung von Mittelstand-Digital zusammen. Diese ist für das Netzwerkmanagement verantwortlich, unterstützt die Evaluation und Öffentlichkeitsarbeit des Förderschwerpunkts Mittelstand-Digital sowie den Wissens- und Technologietransfer in die Fläche. Insbesondere für die Transferstelle Cybersicherheit wird daher vorausgesetzt, dass sie sich aktiv an Veranstaltungen der Begleitforschung und des BMWK, wie z. B. Messeauftritten und internen Vernetzungstreffen sowie gemeinsamen Arbeiten, beteiligt und der Begleitforschung alle zur Erfüllung ihrer Aufgaben notwendigen Informationen zur Verfügung stellt. Hierzu gehört u. a. die jährliche Bereitstellung einer summarischen Dokumentation ihrer Arbeitsaktivitäten und -ergebnisse auf Basis eines von der Begleitforschung bereitgestellten Fragebogens. Die Zuwendungsempfänger sollen die von der Begleitforschung bereitgestellte interne Zusammenarbeitsplattform aktiv nutzen.

e) Projektsteuerung: Transferstelle Cybersicherheit und Fokusprojekte werden bedarfsgerecht und agil gesteuert. Der Projektträger übernimmt die Erfolgskontrolle des jeweiligen Projekts und führt zu diesem Zweck u. a. Projektbesuche und Statusworkshops unter Beteiligung des BMWK und der Begleitforschung durch. Hier werden die Arbeitspläne gegebenenfalls zielgruppengerecht angepasst und mit dem Projektträger abgestimmt. Dazu sind die Bedarfe der Zielgruppe im Themenbereich IT-Sicherheit laufend zu erheben und nutzerorientiert in den Arbeitsplänen umzusetzen.

f) Monitoring/Erfolgskontrolle: Für Transferstelle und Fokusprojekte finden ein Monitoring und Befragungen statt, um das Angebot fortlaufend bedarfsgerecht auf die Bedürfnisse der Zielgruppen auszurichten (kontinuierlicher Verbesserungsprozess). Dabei werden sowohl Leistungskennzahlen (Aktivitäten, Output) als auch die Wirkung bei den Geförderten (Outcome) und Spill-Over bzw. Nachahmer-Aktivitäten erfasst. Die Basis für das Monitoring und die Erfolgskontrolle auf Projektebene bildet ein vom Zuwendungsempfänger zu erstellendes Konzept mit Meilensteinen, Zielen und Kennzahlen. Projektträger und Begleitforschung stellen zu dessen grundsätzlicher Ausrichtung, zur Methodik und den zu erhebenden Indikatoren eine Vorlage bereit. Erkenntnisse aus dem Monitoring bilden zudem die Grundlage für die bedarfsgerechte Anpassung der projektinternen Arbeitspläne.

g) Öffentlichkeitsarbeit (ÖA): Eine zielgruppengerechte Öffentlichkeitsarbeit und zum Ergebnistransfer ist die Grundlage für eine erfolgreiche Transferarbeit. Hierzu ist von der Transferstelle Cybersicherheit und den jeweiligen Fokusprojekten ein Konzept zu entwickeln, welches die ÖA systematisch darstellt. Als Grundlage für das Konzept der Transferstelle Cybersicherheit ist eine Vorlage zu verwenden, welche von der Begleitforschung und dem Projektträger bereitgestellt wird.

Die Zuwendungsempfänger haben bei allen Informations- und Kommunikationsmaßnahmen im Zusammenhang mit dem Vorhaben auf die Förderung durch das BMWK hinzuweisen. Hierbei sind das Förderlogo des BMWK, das Logo der Initiative „IT-Sicherheit in der Wirtschaft“ sowie das Logo des jeweiligen Projekts zu verwenden. Es wird erwartet, dass die Transferstelle Cybersicherheit wie auch die Fokusprojekte ihre geplanten Aktivitäten wie öffentliche Termine, Veranstaltungen oder Publikationen auf der eigenen Internetseite und über das Portal Mittelstand-Digital (www.mittelstand-digital.de) der Öffentlichkeit bereitstellen.

3 Zuwendungsempfänger und Zuwendungsvoraussetzungen

3.1 Zuwendungsempfänger

Antragsberechtigt sind ausschließlich öffentliche oder nicht gewinnorientiert arbeitende Institutionen wie Hochschulen, Forschungseinrichtungen, Vereine und Verbände, Wirtschaftsförderungseinrichtungen, Kammern sowie Körperschaften des öffentlichen Rechts und Gebietskörperschaften, die aufgrund ihrer bisherigen Erfahrungen und Tätigkeiten sowie ihres Auftrags in der Lage sind, IT- und Cybersicherheit fachlich kompetent und unter Beachtung der oben genannten Randbedingungen und Aufgaben an die Zielgruppe heranzutragen.

Es werden ausschließlich nichtwirtschaftliche Tätigkeiten der genannten Einrichtungen gefördert. Als nichtwirtschaftliche Tätigkeiten werden bei Forschungseinrichtungen gemäß Nummer 2.1.1 des FuEuI-Unionsrahmens z. B. die unabhängige Forschung und Entwicklung zur Erweiterung des Wissens und des Verständnisses, die Verbreitung der Forschungsergebnisse und die Ausbildung von mehr und besser qualifizierten Mitarbeitenden betrachtet. Auch der im Zusammenhang mit den nichtwirtschaftlichen Tätigkeiten betriebene Transfer technologischen Wissens gemäß Randnummer 15 Buchstabe V des FuEuI-Unionsrahmens durch Forschungseinrichtungen oder Forschungsinfrastrukturen gilt als nichtwirtschaftliche Tätigkeit, sofern die Gewinne daraus wieder in die primären Tätigkeiten der Forschungseinrichtung oder der Forschungsinfrastruktur reinvestiert werden.

Die Transferstelle Cybersicherheit und die Fokusprojekte dürfen nicht wirtschaftlich tätig sein. Zur wirtschaftlichen Tätigkeit zählen beispielweise die Individualberatung von Einzelnen, Forschungstätigkeiten in Ausführung von Verträgen mit der gewerblichen Wirtschaft (Auftragsforschung), die Vermietung von Forschungsinfrastruktur oder andere Dienstleistungen für gewerbliche Unternehmen.

Die Praxiskooperationen mit KMU (siehe Nummer 2.2 2.) stellen keine mittelbare staatliche Beihilfe dar, da die Ergebnisse weit verbreitet werden. Die Voraussetzungen von Randnummer 28 Buchstabe b des FuEuI-Unionsrahmens sind von den Praxisprojekten zu erfüllen.

Soweit dieselbe Einrichtung sowohl wirtschaftliche als auch nichtwirtschaftliche Tätigkeiten ausüben sollte, fällt die staatliche Finanzierung der nichtwirtschaftlichen Tätigkeiten nur dann nicht in Artikel 107 Absatz 1 AEUV, wenn zur Vermeidung von Quersubventionierungen die beiden Tätigkeitsformen eindeutig und in der Finanzbuchhaltung sowie der Kosten- und Leistungsrechnung nachgewiesen voneinander getrennt werden. Der Nachweis kann z. B. im Jahresabschluss erbracht werden.

Forschungseinrichtungen, die eine Grundfinanzierung von Bund und Ländern erhalten, können nur unter bestimmten Voraussetzungen (insbesondere Einhaltung des Besserstellungsverbots und Verbot der Quersubventionierung) eine Projektförderung für ihren zusätzlichen Aufwand erhalten.

3.2 Zuwendungsvoraussetzungen

Antragsteller müssen über die notwendige Fachkunde, Leistungsfähigkeit und Zuverlässigkeit zur Durchführung des Projekts verfügen. Sie müssen zudem die Gewähr für eine ordnungsgemäße Mittelverwendung bieten. Der Empfänger einer Zuwendung muss in der Lage sein, die zweckentsprechende Verwendung der Mittel nachzuweisen.

Die Projekte dürfen bei der Antragstellung weder ganz noch teilweise von anderen öffentlichen Stellen des Bundes, der Länder oder der Europäischen Union gefördert werden. Bereits geleistete Vorarbeiten und vorhandene Infrastrukturen müssen dargestellt bzw. nachgewiesen werden und sind nicht mehr förderfähig.

Projekte können gefördert werden, wenn sie hinsichtlich der Themenstellung die Förderziele dieser Förderbekanntmachung erfüllen und an der Bearbeitung des vorgeschlagenen (Teil-)Projekts ein erhebliches Bundesinteresse besteht.

3.3 Konsortien

Mehrere Antragsteller schließen sich zur gemeinsamen (interdisziplinären) Bearbeitung der Aufgabenstellung der Transferstelle Cybersicherheit in einem Konsortium zu einem überschaubaren und gut steuerbaren Verbundprojekt mit maximal fünf Partnern zusammen. Im Interesse des Förderziels ist auf ein ausgeglichenes Verhältnis zwischen wissenschaftlichen Partnern und Transferpartnern zu achten.

Daneben können weitere juristische und natürliche Personen im Unterauftrag eines Partners beteiligt werden. Unternehmen der gewerblichen Wirtschaft können über Unteraufträge zu Marktpreisen beteiligt werden. Assoziierte Partner können ohne Förderung in das Projekt eingebunden sein.

Verbundprojekte können gefördert werden, wenn die Verbundpartner abgestimmt arbeitsteilig und interdisziplinär die Aufgabenstellungen dieser Förderbekanntmachung mit dem Ziel bearbeiten wollen, die jeweiligen Ressourcen (Personalkapazität, spezifisches Know-how) effizient zu nutzen, Synergieeffekte zu erzielen und den Wissens-, Technologie- und Kompetenztransfer in Richtung KMU zu beschleunigen.

In dem Konsortium der Transferstelle Cybersicherheit müssen die fünf Rollen 1. Konsortialleitung/Gesamtprojektleitung, 2. Transferpartner, 3. Fachexpertise, 4. Öffentlichkeitsarbeit sowie 5. Vernetzung besetzt werden. Ein Partner kann dabei mehrere Rollen einnehmen. Die Verortung der Rollen und Aufgaben (Ablauf- und Aufbauorganisation) sowie die erforderliche Expertise ist bereits in der Skizze nachvollziehbar darzustellen.

Die konkreten Aufgaben und Verantwortlichkeiten innerhalb der jeweiligen Rolle werden nachfolgend dargestellt. Alle Partner müssen in Bezug auf den Wissens-, Technologie- und Kompetenztransfer eine neutrale Stellung hinsichtlich kommerzieller Anbieter aufweisen.

1. Konsortialleitung/Gesamtprojektleitung: Das Konsortium bestimmt eine Konsortialleitung, die über entsprechende Erfahrung im Management und in der Führung von institutionsübergreifenden Projekten verfügt. Die Rolle der Leitung ist durch einen geförderten Partner auszufüllen. Das für das Projekt bereitgestellte Leitungspersonal sollte schwerpunktmäßig für dieses Projekt eingesetzt werden und nach Möglichkeit nicht bzw. nur in einem geringeren Zeitumfang für andere Förderprojekte/Bereiche arbeiten. Zudem sind insbesondere folgende Aufgaben durch die Konsortialleitung wahrzunehmen:
   - Sie ist verantwortlich für das Gesamtprojektmanagement des Konsortiums. Hierzu sind entsprechende Werkzeuge zur ordnungsgemäßen Steuerung und Dokumentation des Projekts (Ressourcen, Zielerreichung) einzusetzen.
   - Sie ist für die Konsensbildung und Kommunikation im Konsortium verantwortlich und wirkt auf einen einheitlichen Auftritt des Konsortiums sowie der eingebundenen Partner nach außen hin.
   - Sie entwickelt in enger Abstimmung mit den Partnern eine Strategie zur Erreichung der Projektziele und stellt die Selbstevaluation des Projekts sicher.
   - Sie ist erster Ansprechpartner bzgl. des Projektstandes gegenüber Zuwendungsgeber, Begleitforschung und Projektträger und leitet relevante Informationen an das Konsortium weiter.
2. Transferpartner: Der Wissens- und Technologietransfer wird durch mindestens einen geförderten Partner unterstützt, der nachweisbare Expertise in der Erwachsenenbildung hat. Ausgewiesene Erfahrungen und Kenntnisse im praxisorientierten Wissens- und Technologietransfer sowie entsprechenden Werkzeugen und Methoden in Richtung KMU, Handwerksbetriebe und Start-ups sowie deren Beschäftigten sind vorhanden (beispielsweise durch Vorerfahrungen in anderen Projekten). Der Transferpartner agiert im engen Zusammenspiel mit dem Vernetzungspartner und ist darüber hinaus selbst gut mit den Anforderungen der Zielgruppen vertraut.
3. Fachexpertise: Die zu vermittelnden Inhalte des Themenbereichs IT- und Cybersicherheit werden durch (wissenschaftliche) Partner mit entsprechender Fachexpertise aufbereitet und zur Verfügung gestellt. Dies beinhaltet die eigenständige Bewertung von digitalen Gefahren für die Zielgruppen, präventiver, detektierender und reaktiver Maßnahmen und die bedarfsgerechte Zielgruppenansprache mit anwendungsorientierten und praxistauglichen Lösungen (siehe hierzu auch Randbedingung a „IT-Sicherheitskompetenz“). Aktuelle Entwicklungen und Trends werden aufgegriffen und fließen über die Fachexperten in die Instrumente und Angebote der Transferstelle Cybersicherheit ein.
4. Öffentlichkeitsarbeit (ÖA): Das Konsortium entwickelt einen strategischen Plan für eine zielgruppenorientierte Öffentlichkeitsarbeit. Dabei wird das Projekt selbst, aber auch das übergeordnete Ziel der Initiative IT-Sicherheit in der Wirtschaft berücksichtigt. Die Öffentlichkeitsarbeit ist durch einen geförderten Partner zu besetzen, der nachweisbare Erfahrungen im PR-Bereich (soziale Medien, Printmedien, Veranstaltungsmanagement, strategisches ÖA-Management/Projektmanagement) besitzt. Unterstützende ÖA-Leistungen können auch durch Unterauftragnehmer wie PR-Agenturen erbracht werden.

5. Vernetzung: Ein guter Zugang zur Zielgruppe, unterstützenden Multiplikatoren und der IT-Sicherheitscommunity ist unerlässlich für eine erfolgreiche Projektumsetzung, die durch einen Partner im Schwerpunkt „Vernetzung“ zu erfüllen ist. Mindestens ein Partner des Konsortiums verfügt bereits über einen direkten Zugang zu den zu adressierenden Zielgruppen und relevanten Akteuren der IT- und Cybersicherheit (z. B. Verbände, Kammern, Wirtschaftsförderungseinrichtungen). Ein ausgeprägtes Verständnis der Bedarfe der Zielgruppe ist vorhanden und wird in die Transferarbeit eingebracht, sodass bedarfsgerechte und zugeschnittene Angebote entwickelt und verbreitet werden können.

Die Fokusprojekte können als Einzel- oder Verbundprojekte durchgeführt werden. Entsprechend sind sowohl Skizzen durch einen Partner (Einzelprojekt) als auch durch ein Konsortium (Verbundprojekt) möglich, wobei die Anzahl der Partner eines Konsortiums im Regelfall nicht mehr als drei betragen sollte, um eine gute Steuerbarkeit zu gewährleisten. Die Antragsteller müssen hierbei die für das jeweilige Projekt notwendigen Vorerfahrungen, Kompetenzen und Infrastrukturen entweder als alleiniger Partner oder innerhalb des geplanten Konsortiums einbringen. Hierzu zählen insbesondere die Bereiche Wissenschaft/Fachexpertise, Transfer sowie Öffentlichkeitsarbeit. Gegebenenfalls können einzelne Schwerpunkte auch durch Unteraufträge abgedeckt werden. Entscheidend für die Konsortialstruktur ist die Fähigkeit des bzw. der entsprechenden Partner(s), das spezifische Themengebiet bearbeiten und zielgruppengerecht in die Breite transferieren zu können.

Die Partner eines Verbundprojekts regeln ihre Zusammenarbeit in einer Kooperationsvereinbarung, die nach Bewilligung der Förderung durch das BMWK geschlossen wird. Bei Einreichung des Projektvorschlags (Antrags) wird lediglich eine formlose Absichtserklärung über die gemeinsame Projektbearbeitung beigefügt.

4 Art und Umfang, Dauer und Höhe der Förderung

4.1 Art und Umfang der Förderung

Die Zuwendungen können im Wege der Projektförderung als nicht rückzahlbare Zuschüsse gewährt werden. Zuwendungsfähig sind die projektbezogenen Ausgaben bzw. Kosten zur Durchführung der Projektarbeiten einschließlich der notwendigen projekttypischen Koordinationsaufgaben.

4.2 Dauer der Förderung

Der Förderzeitraum für die Transferstelle beträgt maximal vier Jahre ab Bewilligung. Eine Verlängerung ist bei Vorliegen der zuwendungsrechtlichen Voraussetzungen bis zu zwei Jahre möglich. Die Laufzeit der Fokusprojekte soll sich in einem Rahmen von sechs bis zu maximal 36 Monaten bewegen.

4.3 Höhe der Förderung

Bemessungsgrundlage für Zuwendungen an die Antragsberechtigten gemäß Nummer 3.1 sind die zuwendungsfähigen projektbezogenen Ausgaben oder Kosten. Sofern Antragsteller nicht über ein geordnetes Kostenrechnungswesen nach den Leitsätzen für die Preisermittlung auf Grund von Selbstkosten (LSP) verfügen oder es die Bewilligungsbehörde festlegt, erfolgt die Förderung auf Ausgabenbasis.

Einrichtungen, die auf Kostenbasis (AZK) gefördert werden, müssen eine angemessene Eigenbeteiligung (mindestens 10 % der zuwendungsfähigen Vorhabenkosten) erbringen. Bei Helmholtz-Zentren und der Fraunhofer-Gesellschaft soll die Eigenbeteiligung mindestens 10 % der zuwendungsfähigen Vorhabenkosten betragen.

Einrichtungen, die auf Ausgabenbasis (AZA) abrechnen, können bis zu 100 % gefördert werden. Es sind nur Ausgaben des vorhabenbedingten Mehraufwandes zuwendungsfähig.

Nicht übernommen oder bezuschusst werden:

- Übliche Grundausstattung wie EDV-Ausstattung (Hard- und Software) und Mobiliar;
- Mieten für vorhandene Räumlichkeiten;
- Personalausgaben, die durch Dritte aus öffentlichen Haushalten gedeckt sind.

5 Sonstige Zuwendungsbestimmungen

Die Förderung der Vorhaben erfolgt auf der Grundlage der jeweils anzuwendenden Nebenbestimmungen des BMWK. Mit den Arbeiten am Projekt darf vor Bewilligung der Zuwendung noch nicht begonnen worden sein. Zwingende Voraussetzung für die Gewährung einer Bundeszuwendung ist der Nachweis der Sicherung der Gesamtfinanzierung des Projekts. Im Rahmen des späteren Bewilligungsverfahrens hat der Antragsteller gegebenenfalls nachzuweisen, dass er in der Lage ist, den nicht durch Bundesmittel gedeckten Eigenanteil an den gesamten Projektkosten aufzubringen und dass dies seine wirtschaftlichen Möglichkeiten nicht übersteigt (Bonitätsnachweis).

Das BMWK ist gemäß § 7 BHO und zugehöriger Verwaltungsvorschrift verpflichtet, eine begleitende und abschließende Erfolgskontrolle durchzuführen. Das BMWK kann eine Evaluation mit dem Ziel beauftragen, wesentliche Beiträge für die Erfolgskontrolle des Förderprogramms zu erheben. Zuwendungsempfänger sind zur Zusammenarbeit mit dem BMWK, dem Projektträger und gegebenenfalls vom BMWK beauftragten Evaluatoren verpflichtet und müssen unter Beachtung der datenschutzrechtlichen Regelungen alle für die Erfolgskontrolle bzw. die Evaluation der Förderung benötigten Daten bereitstellen und an den hierfür vorgesehenen Befragungen, Interviews und sonstigen Datenerhebungen teilnehmen. Dies gilt auch für Prüfungen durch den Bundesrechnungshof gemäß den §§ 91 und 100 BHO. Bei der Auswahl teilnehmender Mitarbeitenden hat der Zuwendungsempfänger darauf zu achten, dass diese zum relevanten Zuwendungsverfahren Auskunft geben können. Für die genannten Pflichten des Zuwendungsempfängers

gelten die in den Nebenbestimmungen genannten Fristen. Der Zuwendungsempfänger verpflichtet sich, die für die Bereitstellung von Daten Dritter gegebenenfalls erforderlichen Einwilligungserklärungen einzuholen.

6 Auswahl- und Förderverfahren

6.1 Einschaltung Projektträger

Mit der Betreuung der Transferstelle und der Fokusprojekte gemäß dieser Förderbekanntmachung ist beauftragt der

DLR Projektträger
Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)
Digitale Transformation Mittelstand – Mittelstand-Digital
Heinrich-Konen-Straße 1
53227 Bonn

Ansprechpartnerin:
Judith Hellhake
Telefon: 0228 3821 2452
E-Mail: judith.hellhake@dlr.de

Der Projektträger gibt im Auftrag des BMWK weitergehende Informationen zu Verfahrensfragen und berät bei Skizzen- und Antragstellung.

6.2 Bewerbungs- und Auswahlverfahren

Das Förderverfahren ist zweistufig angelegt. In der ersten Verfahrensstufe sind Skizzen einzureichen. Bei positiver Beurteilung der Projektskizze werden die Interessenten in der zweiten Verfahrensstufe aufgefordert, (bei Verbundvorhaben in Abstimmung mit dem vorgesehenen Projektkoordinator) einen förmlichen Förderantrag vorzulegen. Über die Förderung entscheidet das BMWK oder der beauftragte Projektträger nach abschließender Prüfung im Rahmen der zur Verfügung stehenden Haushaltsmittel.

Einreichung einer Projektskizze

Die Einreichung der Skizze erfolgt durch den Konsortialführer/Verbundkoordinator.

Die Projektskizzen für die Transferstelle Cybersicherheit und Fokusprojekte werden spezifisch eingereicht, d. h. eine Skizze bezieht sich immer auf eine der beiden geförderten Teilmaßnahmen der Initiative IT-Sicherheit in der Wirtschaft (siehe Nummer 2).

Die Einreichung erfolgt elektronisch beim Projektträger über die Internet-Anwendung PT-Outline unter der Adresse:

Skizzen „Transferstelle Cybersicherheit“:

https://ptoutline.eu/app/md_it_s

Skizzen „Fokusprojekte“:

https://ptoutline.eu/app/md_it-s_fokus

Die Internet-Anwendung erfasst in einem Formular zentrale Daten zu dem Projektvorschlag und ermöglicht den Upload der Projektskizze. Der Projektvorschlag liegt passwortgeschützt auf dem Server des DLR und kann bis zum Bewerbungsschluss bearbeitet werden. Die Datenübertragung erfolgt verschlüsselt.

Soweit in der Anwendung PT-Outline eine E-Mail-Adresse als Kontakt zu Verfügung gestellt wird, kann diese verwendet werden, um während der Phase der Erarbeitung der Projektskizzen an den Projektträger gerichtete Fragen in anonymisierter Form und die jeweiligen Antwortbeiträge des Projektträgers anderen potenziellen Projektteilnehmern zur Verfügung zu stellen.

Frist für die Online-Einreichung von Projektskizzen für die Transferstelle Cybersicherheit ist der 10. Dezember 2022, um 12 Uhr mittags.

Für die Einreichung von Skizzen für die Fokusprojekte gelten jährlich die Fristen 1. Februar und 1. August des jeweiligen Haushaltsjahres, ebenfalls 12 Uhr mittags. Erstmalig werden Skizzen zur Einreichungsfrist 1. August 2023 angenommen.

Zu diesen Zeitpunkten wird der Serverzugang geschlossen. Zuvor ist über die Internetseite eine Druckversion der Bewerbung zu erstellen. Die schriftlichen Bewerbungsunterlagen mit Unterschrift sind unverzüglich an die in Nummer 6.1 genannte Adresse zu schicken. Das DLR speichert die in den Projektskizzen gemachten Angaben in maschinenlesbarer Form. Sie werden zur Auswahl durch die Jury und zur Abwicklung des Projekts verarbeitet. Dabei bleiben die Belange des Daten- und Vertrauensschutzes gewahrt.

Für die Projektskizze der Transferstelle Cybersicherheit ist ein maximaler Umfang von 20 Seiten (Minimum Schriftgröße 10 und Zeilenabstand 1,5) einzuhalten. Für die Projektskizzen der Fokusprojekte beträgt der maximale Umfang zehn Seiten (Minimum Schriftgröße 10 und Zeilenabstand 1,5).

Vorgegebene Gliederungspunkte sind:

Für Skizzen zur „Transferstelle Cybersicherheit“

a) Ziele, Schwerpunkte und Angebote der Transferstelle Cybersicherheit mit konkretem Bezug auf die Ausgangslage und Herausforderungen der Zielgruppen im Bereich IT- und Cybersicherheit.

b) Darstellung des Konsortiums und seiner Partner bezogen auf
   - die in Nummer 3.3 genannten Rollen sowie deren Aufteilung,
   - Expertise und Kompetenz der jeweiligen Partner für die vorgesehene(n) Rolle(n) sowie Fachkompetenz im Themengebiet IT-Sicherheit,
   - einzubringende vorhandene Infrastruktur, wie z. B. (mobile) Demonstratoren, IT-Tools etc.,
   - Kompetenz in Wissens- und Technologietransfer hin zu KMU, insbesondere auch in der praxisnahen Zielgruppenansprache,
   - Kenntnis der Zielgruppe und (lokale, überregionale) Vernetzung mit der Zielgruppe,
   - Vernetzung mit der IT-Sicherheitscommunity und anderen relevanten Akteuren (Politik/Verwaltung, Kammern, Verbände, Wirtschaftsförderer etc.).

c) Konzepte hinsichtlich
   - Leistungsportfolio (inhaltlich, quantitativ, Praxisbezug mit regionaler und thematischer Ausrichtung, geplante Instrumente) und Wissenstransfer unter Berücksichtigung der methodischen Zielstellungen,
   - Spezifischer Adressierung der in Nummer 2.2 erläuterten Aufgaben,
   - Umsetzung der in Nummer 2.3 genannten Rahmenbedingungen,
   - Abgrenzung und Synergieeffekten mit dem Netzwerk Mittelstand-Digital sowie der Zusammenarbeit mit den weiteren Projekten der Initiative IT-Sicherheit in der Wirtschaft wie auch anderen Förderinitiativen,
   - Verwertung und Anschlussfähigkeit der Transferstelle Cybersicherheit und ihrer Angebote.

d) Geschätzte Gesamtkosten und Fördermittelbedarf pro Partner tabellarisch.

Für Skizzen der „Fokusprojekte“:

a) Ziele und Schwerpunkte des Projekts sowie Analyse der zugrundeliegenden Bedarfe der KMU
   - Darstellung des Ist-Zustands in Bezug auf die thematische Fokussierung des Projekts und der vorliegenden Herausforderungen der Zielgruppe,
   - Aufgreifen der aufgezeigten Bedarfe und Darstellung der entsprechenden Adressierung durch die zentrale Umsetzungsidee des Projekts,
   - Darstellung der (quantifizierten) Zielstellung des Projekts unter Berücksichtigung durchzuführender Angebote, resultierender Hilfestellungen und Potenziale für die Zielgruppe.

b) Methodische Umsetzung des Projekts mit Bezug zu den in Nummer 1.2.1 genannten Förderzielen.

c) Leistungsportfolio und Projektplan unter besonderer Berücksichtigung der
   - in Nummer 2.2 erläuterten Aufgaben, insbesondere der Transfer- und Breitenwirkung,
   - in Nummer 2.3 genannten Rahmenbedingungen,
   - langfristigen Perspektive: Verstetigung und weiterführende Nutzung der resultierenden Ergebnisse und Lösungen durch Projektpartner, KMU und Dritte.

d) Darstellung der Erfahrungen und Kompetenzen des Konsortiums in Bezug auf die Zielgruppe KMU, insbesondere hinsichtlich der Kompetenz in Wissens- und Technologietransfer sowie der Öffentlichkeitsarbeit.

e) Geschätzte Gesamtkosten und Fördermittelbedarf pro Partner tabellarisch.

Aus der Vorlage einer Skizze kann kein Rechtsanspruch auf eine Förderung abgeleitet werden.

6.3 Bewertung und Auswahlentscheidung

Die eingehenden Projektskizzen stehen im Wettbewerb. Die Auswahlentscheidung erfolgt nach den folgenden Bewertungskriterien:

- Ausrichtung am spezifischen Bedarf der Zielgruppe (Ausgangslage, Ziele, Schwerpunkte) bzw. im Hinblick auf Fokusprojekte entsprechende Adressierung eines ausgewählten Themenfokus,
- Leistungsfähigkeit und Kompetenz des Konsortiums unter Berücksichtigung der für die Transferstelle Cybersicherheit vorgesehenen Rollen (vgl. die Nummern 3.1 und 3.3), einzubringender Infrastruktur und Expertise im Themenfeld IT-Sicherheit,
- Leistungsportfolio (qualitativ und quantitativ) für den Wissens-, Technologie- und Kompetenztransfer, mit Bezug zu den in Nummer 1.2.1 genannten Zielen,
- Erfüllung der Aufgaben und der Erreichung der förderpolitischen Ziele sowie Vernetzung mit weiteren relevanten Akteuren,
- Verstetigung des Projekts bzw. der Projektergebnisse,
- Wirtschaftlichkeit des Mitteleinsatzes.

Nach erfolgter Auswahlentscheidung werden die Konsortialführer über das Ergebnis schriftlich informiert. Im Rahmen des Auswahlprozesses wird eine vom BMWK einberufene Jury beratend tätig.

6.4 Antrags- und Bewilligungsverfahren

Für die Bewilligung des Vorhabens ist folgender Verfahrensablauf vorgesehen:

- Information des potenziellen Antragstellers/Konsortialführers über die Auswahl.
- Beratung zur Antragstellung, Erörterung von Auflagen.
- Erarbeitung eines Förderantrags durch den Antragsteller/das Konsortium.
- Einreichung des Förderantrags beim Projektträger.
- Prüfung des Antrags durch den Projektträger und gegebenenfalls Bewilligung.

7 Veröffentlichung

Diese Bekanntmachung wird im Bundesanzeiger veröffentlicht. Mit der Einreichung einer Skizze werden die Teilnahmebedingungen dieser Bekanntmachung akzeptiert.

Berlin, den 15. September 2022

Bundesministerium
für Wirtschaft und Klimaschutz

Im Auftrag
Gesa Förster