Bundesanzeiger
Herausgegeben vom
Bundesministerium der Justiz
und für Verbraucherschutz
www.bundesanzeiger.de

Bekanntmachung
Veröffentlicht am Montag, 31. Dezember 2018
BAnz AT 31.12.2018 B2

Bundesministerium für Wirtschaft und Energie

Bekanntmachung IT-Sicherheit in der Wirtschaft

Vom 21. Dezember 2018

1 Zuwendungszweck, Förderziele, Rechtsgrundlagen

1.1 Zuwendungszweck

Das Bundesministerium für Wirtschaft und Energie (BMWi) hat mit der Digitalen Strategie 2025 aufgezeigt, wie ein erfolgreiches, digitales Deutschland möglich werden kann und das Ziel ausgegeben, die innovative Digitalisierung in Wirtschaft und Gesellschaft zu fördern sowie aktiv zu begleiten. Die Digitalisierung und die IT-Sicherheit sind ebenfalls wichtige Leitlinien im Koalitionsvertrag für die 19. Legislaturperiode und dort mit einer Reihe an Maßnahmen untersetzt.

Vor diesem Hintergrund möchte das BMWi insbesondere kleine und mittlere Unternehmen (KMU) für die Chancen der Digitalisierung sensibilisieren und Anwendungsmöglichkeiten aufzeigen. Einhergehend mit der Digitalisierung und Vernetzung wird jedoch die IT-Sicherheit immer wichtiger, beispielsweise bei den Themenfeldern Internet of Things, Industrie 4.0, Smart Cars/Cities oder Smart Home. KMU werden auch in der vernetzten Welt einen großen Teil der deutschen Wirtschaft ausmachen. Allerdings verfügen sie im Gegensatz zu großen Unternehmen meist über nur eingeschränkte Ressourcen für IT-Sicherheit. Wirtschaftliche Abläufe sind inzwischen ohne Digitalisierung nicht mehr vorstellbar. Für die verlässliche Nutzung dieser Abläufe ist eine diesbezüglich sichere Nutzung Voraussetzung für eine aktive Marktteilnahme. IT-Sicherheit wird so zu einem entscheidenden Faktor für den wirtschaftlichen Erfolg.

Die Studie „Aktuelle Lage der IT-Sicherheit in KMU“[1] zeigt: Trotz zunehmender Digitalisierung mangelt es immer noch am Bewusstsein für IT-Sicherheit. Selbst da, wo das eigene Risiko als hoch gilt, wird unzureichend für Schutz gesorgt. So geben zwei Drittel der kleinen KMU an, dass IT-Sicherheit für sie eine hohe Bedeutung hat, aber nur etwa 20 % von ihnen hat eine IT-Sicherheitsanalyse durchgeführt. Im Vergleich zu vor fünf Jahren hat sich die Lage der IT-Sicherheit in KMU noch nicht entscheidend verbessert. Mit Blick auf die erheblich gestiegenen Anforderungen stellt sich daher die Herausforderung umso eindrücklicher, die KMU dabei zu unterstützen, die bestehenden Defizite der Umsetzung mit Nachdruck anzugehen. Dass IT-Sicherheit zunehmend wichtiger wird, zeigt auch die polizeiliche Kriminalstatistik. Im Jahr 2016 wurden im Bereich Cybercrime über 80 000 Straftaten erfasst. Damit ist die Anzahl erfasster Straftaten im Vergleich zum Vorjahr um 80,5 % gestiegen[2].

Diese Förderbekanntmachung erweitert die existierende Initiative „IT-Sicherheit in der Wirtschaft“[3] des BMWi und schreibt diese fort. Die seit einigen Jahren laufende Initiative unterstützt vor allem KMU mit konkreten Maßnahmen und Hilfestellungen darin, beim Einsatz von IKT-Systemen ihre IT-Sicherheit zu verbessern. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung wird eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung der KMU beim Thema IT-Sicherheit zu stärken. Hierzu wurden Studien und Projekte gefördert, welche sich beispielweise mit Tools für sichere Internetseiten, IT-Sicherheit in Ausbildung und Berufsschulen oder mit Awareness und Sensibilisierung befassen.

Mit der neuen Förderbekanntmachung wird neben dem bisherigen Fokus auf einzelnen Projekten, welche die oben genannten Zielsetzungen adressieren, auch die Einrichtung und der Betrieb einer Transferstelle „IT-Sicherheit in der Wirtschaft“ gefördert. Sie bereitet die vielen existierenden Angebote zu Information und Weiterbildungen bei IT-Sicherheit zielgruppengerecht auf, überführt sie in ein allgemeinverständliches, bedarfsgerechtes Angebot und stellt den Transfer der Projektergebnisse sicher. Somit wird eine der Haupthürden bei der Einführung von IT-Sicherheit adressiert, namentlich die große Masse der Möglichkeiten und die Kleinteiligkeit der Angebote[1].

Mit der neuen Transferstelle wird IT-Sicherheit und nutzerfreundliche Sicherheitsfunktionen nicht als isoliertes Thema am Ende einer Prozesskette und on-top stehen, sondern von Beginn an mitgedacht – Stichwort: Security by Design. Neben den Hauptaufgaben des Wissens- und Technologietransfers in den Mittelstand, der Schaffung von Awareness sowie der Vernetzung mit Multiplikatoren und weiteren Initiativen wird durch die Transferstelle die Umsetzungslücke in KMU geschlossen.

Laut der Studie „Aktuelle Lage der IT-Sicherheit in KMU“ nennen mehr als die Hälfte der KMU Kostenaufwand, fehlende Qualifikation der Mitarbeiter oder Mangel an einschlägigem Personal als Grund für die aktuell unzureichende IT-Sicherheitslage bei KMU in Deutschland. Angebote wie Informationsbroschüren oder kostenlose Schulungen sind zwar teilweise vorhanden, oftmals allerdings fehlt die Übersicht, was für das eigene Unternehmen passt und wer diese Angebote verbreitet. Unübersichtlichkeit und eine komplexe Technik-Sprache schrecken KMU ab. Allem voran fehlt es aus

[1] WIK, Wissenschaftliches Institut für Infrastruktur 2017
[2] Aktuelle Lage der IT-Sicherheit in KMU, WIK Wissenschaftliches Institut für Infrastruktur 2017
[3] www.it-sicherheit-in-der-wirtschaft.de

Sicht vieler Experten trotz Digitalisierung und Vernetzung in KMU jeder Größe immer noch an Awareness für das Thema IT-Sicherheit im eigenen Unternehmen.

Zweck der neuen Förderbekanntmachung ist es daher, die Handlungsempfehlungen der Expertenbefragungen und der Studie in Projekten zu adressieren und über eine Transferstelle bundesweit und zielgruppengerecht zu verbreiten.

Die Projekte und die Transferstelle wird die KMU dort abholen, wo sie gerade stehen. Sei es, dass sie noch keinerlei Kenntnisse im Bereich IT-Sicherheit haben – hier wird die Transferstelle sensibilisieren und vorhandene Möglichkeiten aufzeigen, auch mit adressatengerechter Öffentlichkeitsarbeit. Sei es, dass mit ersten IT-Sicherheitsmaßnahmen schon begonnen wurde – dann wird über weitere technologische Innovationen und ihre konkrete Umsetzung im Unternehmen informiert werden.

Darüber hinaus wird die Förderbekanntmachung Aktivitäten fördern, welche die aktive gegenseitige Vernetzung und Zusammenarbeit mit anderen thematisch relevanten Förderinitiativen des Bundes und der Länder voranbringen. Hierzu zählen u. a. die Mittelstand 4.0-Kompetenzzentren, um ein aufeinander abgestimmtes Angebot für KMU zu gewährleisten.

1.1.1 Förderziele

Ziele der Initiative „IT-Sicherheit in der Wirtschaft“ sind:

- Sensibilisierung und Unterstützung von KMU und Handwerk beim Thema IT-Sicherheit im Zuge ihrer digitalen Transformation.
- Stärkung von Wettbewerbs- und Innovationsfähigkeit von KMU durch den sicheren Einsatz digitalisierter Prozesse und Geschäftsmodelle.
- Förderung technologischer, organisatorischer und arbeitsgestaltender IT-Sicherheitskompetenzen sowie Stärkung von Sicherheit und Vertrauen (Anbieter/Anwender) von IKT-Systemen inkl. Hard- und Software.
- Erhöhung des IT-Sicherheitsniveaus in KMU.
- KMU befähigen selbstständig kompetente IT-sicherheitsrelevante Entscheidungen zu treffen.

Aufgabe der Transferstelle und der Projekte ist der Technologie- und Wissenstransfer in KMU mit dem Ziel Bewusstsein zu wecken und über Aufklärung neutral über aktuelle Sicherheitsvorfälle und ihre Einfallstore zu berichten. Kosten-Nutzen-Abwägungen oder IT-Sicherheitsanalysen werden als Leistungen angeboten. Konkrete Umsetzungen in KMU erarbeiten Best-Practices und Fallbeispiele als Leuchtturmprojekte, welche zum Nachahmen im eigenen Unternehmen anregen. Vorhandene und eigene Angebote zu IT-Sicherheit werden didaktisch aufbereitet und zielgruppengerecht in verständlicher Sprache eines Unternehmers aus dem KMU-Bereich angeboten. Die Nachhaltigkeit der Angebote und der Qualifikationsmaßnahmen wird durch permanentes, bedarfsgerechtes Anpassen an die sich wandelnden Herausforderungen der Digitalisierung und IT-Sicherheit sichergestellt. Die geförderten Partner vernetzten sich darüber hinaus mit bereits bestehenden Mittelstand 4.0-Kompetenzzentren innerhalb des Förderschwerpunkts „Mittelstand-Digital“, um Synergien zu bilden und branchenübergreifende IT-Sicherheitsfragen der Digitalisierung besser abdecken zu können.

1.1.2 Rechtsgrundlagen

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

Die Förderung erfolgt auf Grundlage der Nummern 2.1.1 und 2.2.2 des Unionsrahmens für staatliche Beihilfen für FuEuI[4] (FuEuI-Unionsrahmen (ABl. C 198 vom 27.6.2014, S. 1), soweit die Zuwendungsempfänger die Voraussetzungen einer Einrichtung für Forschung und Wissenstransfer im Sinn von Nummer 1.3 Doppelbuchstabe ee des Unionsrahmens für staatliche Beihilfen für FuEuI erfüllen. Es werden Wissenstransfermaßnahmen gefördert, die als nichtwirtschaftliche Tätigkeiten der Zuwendungsempfänger einzustufen sind.

Falls diese Voraussetzungen nicht erfüllt sind, 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.

Die Maßnahme unterlieget einer begleitenden Erfolgskontrolle nach Maßgabe von § 7 Absatz 2 BHO und zugehöriger Verwaltungsvorschriften.

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

[4] FuEuI = Forschung, Entwicklung und Innovation

2 Gegenstand, Aufgaben und Randbedingungen der Förderung

2.1 Gegenstand der Förderung

Das BMWi beabsichtigt die Förderung von zwei Handlungsfeldern.

Handlungsfeld 1:

Einrichtung und Betrieb einer Transferstelle „IT-Sicherheit in der Wirtschaft“

Gefördert wird die Einrichtung und der Betrieb einer bundeweiten Transferstelle IT-Sicherheit in der Wirtschaft für drei Jahre. Sie kann durch regionale Schaufenster unterstützt werden. Diese wird als Verbundprojekt von Partnern unterschiedlicher, komplementärer Expertise gemeinsam umgesetzt. Hauptaufgabe ist der Wissens- und Technologietransfer und die Adressierung der in Nummer 1 genannten Herausforderungen über eine Vielzahl an zielgruppengerechten Angeboten und Öffentlichkeitsmaßnahmen. Die spezifischen Aufgaben sind in Nummer 2.2 beschrieben.

Handlungsfeld 2:

Projekte, welche mindestens eines der in Nummer 1.2 genannten Förderziele adressieren.

Gefördert werden Einzel- oder Verbundprojekte, welche durch ihre Arbeiten und Ergebnisse aktiv zur Sensibilisierung und Unterstützung von KMU und Handwerk beim Thema IT-Sicherheit beitragen, welche Hilfestellungen und Unterstützungsleistungen zum sicheren Einsatz digitalisierter Prozesse und Geschäftsmodelle zielgruppengerecht aufbauen oder welche zur Förderung technologischer, organisatorischer und arbeitsgestaltender IT-Sicherheitskompetenzen in KMU beitragen. Alle Projekte müssen durch ihre Ergebnisse nachweislich zu einer Erhöhung des IT-Sicherheitsniveaus in KMU beitragen und übertragbare Lösungen für den breiten, bundesweiten Transfer entwickeln. Als weiteres Instrument zur Verbreitung der Ergebnisse dient die im Handlungsfeld 1 genannte Transferstelle „IT-Sicherheit“. Die Projekte können ebenfalls selektive Aufgabenfelder aus dem Handlungsfeld 1 (siehe Nummer 2.2) übernehmen und für den Einsatz in der Transferstelle aufarbeiten. Hierbei wird eine enge Koordination zwischen Projekten und Transferstelle vorausgesetzt.

2.2 Aufgaben der Förderung

Aufgaben Handlungsfeld 1:

Einrichtung und Betrieb einer Transferstelle IT-Sicherheit in der Wirtschaft

a) Für KMU werden praxisorientierte, zielgruppengerechte Informations-, Transfer- und Unterstützungsangebote, welche dazu geeignet sind, die IT-Sicherheit im Unternehmen nachhaltig zu verbessern – auch in Kooperation mit öffentlichen Institutionen oder Verwaltungen – aufbereitet und intensiv für den Wissenstransfer genutzt. Multiplikatoren wie Verbände, Gewerkschaften, Kammern oder Wirtschaftsförderer werden ebenfalls adressiert und unterstützen die regionale sowie bundesweite Umsetzung und Kooperation. Für die Zielgruppe der IT-Dienstleister wie beispielsweise Beratungsunternehmen werden gezielt Informations- und Qualifikationsangebote aufbereitet, damit sie den Bedürfnissen der mittelständischen Klientel besser gerecht werden können.

b) Praktische mobile Anschauungs- und Erprobungsmöglichkeiten unterstützen den Wissenstransfer in die Fläche und forcieren den Abbau der Umsetzungsdefizite im IT-Sicherheitsbereich in KMU.

c) Interdisziplinäre Unterstützungsnetzwerke (z. B. aus Forschung, Vereinen, Dienstleistern oder Verbänden und Gebietskörperschaften) werden aufgebaut, um die Arbeit der Transferstelle in ihrer Wirkung zu verstärken und Querschnittsfragen zu beleuchten. Hierbei übernimmt die Transferstelle auch eine Lotsenfunktion.

d) Für Zwecke des Wissenstransfers und zur Gewinnung von Erkenntnissen für erfolgreiche Implementierung von IT-Sicherheitsaspekten im Zuge der digitalen Transformation entwickelt und identifiziert die Transferstelle während der Förderlaufzeit fortlaufend qualitativ hochwertige Best Practice-Beispiele in Umsetzungsprojekten mit KMU. Die hierbei zu beteiligenden KMU erhalten keine eigene Förderung. Die Aufwände seitens der Transferstelle werden durch die Projektförderung abgedeckt. Die Erfahrungen und Erkenntnisse aus diesen Umsetzungsprojekten werden für die Transferarbeit in geeigneter Form aufbereitet und öffentlich kommuniziert.

e) Während der Projektlaufzeit werden neue Entwicklungen sowie aktuelle Themen im Umfeld von IT-Sicherheit aufgegriffen. Dazu beobachten die Projektbeteiligten laufend das wissenschaftliche und wirtschaftliche Umfeld, greifen und bereiten jeweils aktuelle und für den Transfer geeignete Inhalte auf und verwenden diese für den Informationstransfer und den Know-how-Aufbau in den Unternehmen.

f) Die Transferstelle nutzt und transferiert Werkzeuge, Materialien, Best-Practice-Beispiele und weitere Ergebnisse und Erkenntnisse insbesondere aus den im Handlungsfeld 2 geförderten Projekten mit unterschiedlichen Maßnahmen der Öffentlichkeitsarbeit und sorgt somit für eine hohe Sichtbarkeit aller Ergebnisse dieser Initiative.

Aufgaben Handlungsfeld 2:

Projekte welche mindestens eines der in Nummer 1.2 genannten Förderziele adressieren.

Gefördert werden Einzel- oder Verbundprojekte, welche durch ihre Ergebnisse aktiv zur Sensibilisierung und Unterstützung von KMU und Handwerk bei Thema IT-Sicherheit beitragen, welche Hilfestellungen und Unterstützungsleistungen zum sicheren Einsatz digitalisierter Prozesse und Geschäftsmodelle zielgruppengerecht aufbauen oder welche zur Förderung technologischer, organisatorischer und arbeitsgestaltender IT-Sicherheitskompetenzen in KMU beitragen.

Hierbei können u. a. folgende Herausforderungen und Arbeiten adressiert werden:

a) Kosten-Nutzen-Abwägungen: Informations- und Schulungsangebote als Einstieg oder erste IT-Sicherheitsanalysen.

b) Aus- und Weiterbildung stärken und an die neuen, sich verändernden Herausforderungen der Digitalisierung und IT-Sicherheit anpassen.

c) Defizite in der Qualifikation der Mitarbeitenden im Unternehmen.

d) Defizite bei der prozessorientierten IT-Sicherheitsstrategie im Zuge der Digitalisierung.

e) Defizite bei der Akzeptanz für IT-Sicherheitsmaßnahmen im Unternehmen.

f) Awareness und Hilfestellungen schaffen für existierende Bedrohungen und gesetzliche Vorgaben (beispielsweise der Datenschutz-Grundverordnung).

g) Kompetenzvermittlung zur eigenständigen Durchführung von IT-Sicherheitsanalysen.

Sämtliche Ergebnisse und Angebote müssen öffentlich zugänglich sein.

Um möglichst bald nach Projektbeginn operativ tätig werden zu können, kommen für die Förderung insbesondere Konsortien in Betracht, die

– über Expertise im Bereich der IT-Sicherheit verfügen und schon vor Projektbeginn über geeignete Anschauungs-/Demonstrationsmöglichkeiten verfügen. Diese können gegebenenfalls für die Arbeit der Transferstelle weiterentwickelt werden,

– Expertise in Digitalisierung der Dimensionen Mensch-Technik-Organisation besitzen,

– Erfahrungen bei Wirtschaftlichkeitsbetrachtungen (z. B. Kosten-Nutzen-Einschätzungen), Projektevaluation und Geschäftsmodellentwicklung aufweisen,

– ausgewiesene Erfahrungen und Kenntnisse im Wissens- und Technologietransfer und seinen Werkzeugen und Methoden in Richtung KMU und Handwerk nachweisen,

– ein überzeugendes Konzept nachweisen, wie der Wissenstransfer praxisnah auch außerhalb von Ballungszentren, gegebenenfalls mobil, erfolgen und somit eine Breitenwirkung in ganz Deutschland erreicht werden kann, und

– in Bezug auf den Wissenstransfer eine neutrale Stellung (hinsichtlich kommerzieller Anbieter) und ein interdisziplinäres Konzept aufweisen, das dem Charakter der vernetzten Digitalisierung gerecht wird.

2.3 Randbedingungen der Förderung

Die genannten Aufgaben werden unter Beachtung folgender Randbedingungen bearbeitet:

a) Kooperation

Die Abstimmung und Zusammenarbeit mit anderen thematisch im Kontext von IT-Sicherheit in der Wirtschaft relevanten Förderinitiativen des Bundes und der Länder ist verpflichtend, um den praxisorientierten Transfer von Informationen und Ergebnissen zu gewährleisten und eventuelle Doppelarbeiten auszuschließen. Ferner werden ein aktiver gegenseitiger Austausch und eine Zusammenarbeit mit der Initiative „Mittelstand-Digital“ vorausgesetzt, um ein aufeinander abgestimmtes, zielgruppengerechtes Angebot zu gewährleisten. Um die interne Kooperation und den Wissenstransfer mit Experten außerhalb des geförderten Projekts zu sichern, organisiert die Transferstelle mindestens eine große Fachkonferenz.

b) Projektsteuerung

Während der Projektdurchführung soll mindestens einmal jährlich ein Status-Workshop unter Beteiligung des BMWi und des beauftragten Projektträgers durchgeführt werden. Hier werden die Arbeitspläne für das nächste Laufzeitjahr mit dem Projektträger abgestimmt und Zwischenergebnisse der Evaluation vorgestellt. Dazu sind die Bedarfe im Aktionsbereich IT-Sicherheit zu erheben und nutzerorientiert in den Arbeitsplänen umzusetzen.

c) Evaluation

Die Zuwendungsempfänger der Projekte bzw. Transferstelle sind verpflichtet, Beiträge und Daten für die Erfolgskontrolle bzw. eine Evaluation zu leisten.

d) Koordination und Organisation

Es wird erwartet, dass die Projekte ihre geplanten Aktivitäten (wie öffentlichen Termine, Veranstaltungen oder Publikationen) mit der Transferstelle der Initiative IT-Sicherheit koordinieren und über deren Internetseite der Öffentlichkeit zur Verfügung stellen. Somit erhöht und multipliziert sich die Reichweite.

e) Wissens- und Technologietransfer

Die Transferstelle erstellt ein geeignetes Konzept zum adressatengerechten Wissens- und Technologietransfer in die Öffentlichkeit mit allen dazugehörigen Aktivitäten und Materialien. Dazu zählen auch Medien- und Öffentlichkeitsarbeit sowie Instrumente zum Transfer der Ergebnisse aus den Projekten im Handlungsfeld 2 (siehe Nummer 2.1).

3 Zuwendungsempfänger und Zuwendungsvoraussetzungen

Antragsberechtigt sind ausschließlich öffentliche oder nicht gewinnorientiert arbeitende Institutionen wie Hochschulen, außeruniversitäre Forschungseinrichtungen, Vereine und Verbände, Wirtschaftsförderer, Kammern sowie Körperschaften des öffentlichen Rechts und Gebietskörperschaften, die aufgrund ihrer bisherigen Tätigkeit und ihres Auftrags in der

Lage sind, Digitalisierung und das Thema IT-Sicherheit 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 Mitarbeitern betrachtet. Auch der im Zusammenhang mit den nichtwirtschaftlichen Tätigkeiten betriebene Transfer technologischen Wissens gemäß Randnummer 15 Buchstabe v des FuEuI-Unionsrahmens gilt als nichtwirtschaftliche Tätigkeit, sofern sämtliche Einnahmen daraus wieder zugunsten von nichtwirtschaftlichen Tätigkeiten eingesetzt werden. Für vergleichbare Institutionen gelten diese Vorgaben entsprechend.

Wirtschaftliche Aktivitäten sind keine Aufgabe der Projekte der Initiative IT-Sicherheit in der Wirtschaft. Hierzu zählen beispielweise die Beratungstätigkeit im Einzelfall, Forschungstätigkeiten in Ausführung von Verträgen mit der gewerblichen Wirtschaft (Auftragsforschung), die Vermietung von Forschungsinfrastruktur oder andere Dienstleistungen für gewerbliche Unternehmen.

Die Umsetzungsvorhaben der Transferstelle in mittelständischen Firmen (Nummer 2.2 Buchstabe d) 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 Umsetzungsprojekten zu erfüllen.

Soweit dieselbe Einrichtung sowohl wirtschaftliche als auch nichtwirtschaftliche Tätigkeiten ausüben sollte, fällt die staatliche Finanzierung der nichtwirtschaftlichen Tätigkeiten nur dann nicht unter Artikel 107 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union, 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 Besserstellungsverbot und Verbot der Quersubventionierung) eine Projektförderung für ihren zusätzlichen Aufwand erhalten.

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.

Mehrere Antragsteller können sich zur gemeinsamen (interdisziplinären) Bearbeitung des Themas in einem Konsortium zu einem überschaubaren und gut steuerbaren Verbundprojekt zusammenschließen. 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 mit dem Ziel bearbeiten wollen, die jeweiligen Ressourcen (Personalkapazität, spezifisches Know-how) effizient zu nutzen, Synergieeffekte zu erzielen und den Wissens- und Technologietransfer in Richtung KMU zu beschleunigen.

Die Partner eines Verbundvorhabens regeln ihre Zusammenarbeit in einer Kooperationsvereinbarung, die nach Bewilligung der Förderung durch das BMWi geschlossen wird. Bei Einreichung des Projektvorschlags (Antrags) wird lediglich eine formlose Absichtserklärung über die gemeinsame Projektbearbeitung beigefügt. Für das Konsortium wird ein Konsortialführer bestellt, der sowohl das Projektmanagement des Gesamtprojekts übernimmt als auch Ansprechpartner in allen Fragen seitens des Fördermittelgebers oder seines Verwaltungshelfers ist.

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

Vorhaben können gefördert werden, wenn sie hinsichtlich der Themenstellung den Rahmen der dargestellten Fördermaßnahme erfüllen und an der Bearbeitung des vorgeschlagenen (Teil-) Projekts ein erhebliches Bundesinteresse im Sinne der Maßnahme besteht.

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 ist der projektbezogene Aufwand zur Durchführung der Projektarbeiten einschließlich der notwendigen projekttypischen Koordinationsaufgaben.

4.2 Dauer der Förderung

Die Umsetzung der Vorhaben wird für einen Zeitraum von maximal drei Jahren ab Bewilligung gefördert, im Handlungsfeld 1 mit einer Option auf Verlängerung um maximal zwei Jahre.

4.3 Höhe der Förderung

Bemessungsgrundlage für Zuwendungen an die nach Nummer 3 genannten Antragsberechtigten sind die zuwendungsfähigen projektbezogenen Ausgaben oder Kosten. Sofern Antragsteller nicht über ein geordnetes Kostenrechnungswesen 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.

Grundsätzlich nicht übernommen oder bezuschusst werden:

- übliche Grundausstattung wie IT-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 BMWi. Mit den Arbeiten am Projekt darf 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 dies seine wirtschaftlichen Möglichkeiten nicht übersteigt (Bonitätsnachweis).

Die genannten Bestimmungen können zum Zeitpunkt der Erteilung des Bescheids durch Nachfolgeregelungen ersetzt sein.

6 Auswahl- und Förderverfahren

6.1 Einschaltung Projektträger

Mit der Betreuung der Förderprojekte ist beauftragt das

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

Ansprechpartner Dr. Sven Nußbaum

Telefon: 02 28/38 21 23 90
E-Mail: sven.nussbaum@dlr.de

Der Projektträger gibt im Auftrag des BMWi weitergehende Informationen zu Verfahrensfragen und berät bei Skizzen- und Antragstellung. Vordrucke für Förderanträge, Richtlinien, Merkblätter, Hinweise und Nebenbestimmungen können ebenfalls dort angefordert werden.

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 BMWi nach abschließender Prüfung im Rahmen der zur Verfügung stehenden Haushaltsmittel.

Einreichung einer Projektskizze

Die Einreichung der Skizze erfolgt durch den Konsortialführer/Verbundkoordinator.

Die Projektskizzen werden Handlungsfeld-spezifisch eingereicht, d. h. eine Skizze bezieht sich immer auf eines der beiden geförderten Handlungsfelder (siehe Nummer 2).

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

Skizze Handlungsfeld 1:

Einrichtung und Betrieb einer Transferstelle IT-Sicherheit in der Wirtschaft

https://ptoutline.eu/app/it_sidw

Handlungsfeld 2:

Projekte welche mindestens eines der in Nummer 1.2 genannten Förderziele adressieren.

https://ptoutline.eu/app/itsidwh2_201902

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 das Handlungsfeld 1 ist der 28. Februar 2019, um 12.00 Uhr. Für das Handlungsfeld 2 gelten jährlich die Fristen 28. Februar und 1. August des jeweiligen Haushaltsjahres, ebenfalls 12.00 Uhr.

Zuvor ist über die Internetseite eine Druckversion der Bewerbung zu erstellen. Damit eine Online-Bewerbung Bestandskraft erlangt, muss sie schriftlich bestätigt werden. Die schriftlichen Bewerbungsunterlagen mit Unterschrift müssen spätestens eine Woche nach Einreichungsfrist beim DLR eingehen. Einreichungen per Telefax oder E-Mail können nicht berücksichtigt werden.

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 ist ein maximaler Umfang von 20 Seiten (Minimum Schriftgröße 10 und Zeilenabstand 1,5) einzuhalten.

Skizze Handlungsfeld 1:

Einrichtung und Betrieb einer Transferstelle IT-Sicherheit in der Wirtschaft

Vorgegebene Gliederungspunkte sind:

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

b) Darstellung des Konsortiums und seiner Partner bezogen auf
   - einzubringende vorhandene Demonstrations- und Anschauungsinfrastruktur,
   - wissenschaftliche und praktische Expertise im Thema IT-Sicherheit bei der Digitalisierung der Dimensionen Mensch, Technik und Organisation wie auch in ökonomischen Zusammenhängen und den gewählten Schwerpunkten,
   - Kompetenz in Wissens- und Technologietransfer hin zu KMU. Dazu gehört insbesondere die praxisnahe Zielgruppenansprache,
   - Erfahrung bei Wirtschaftlichkeitsbetrachtungen (z. B. Kosten-Nutzen-Einschätzungen) und Geschäftsmodellentwicklung,
   - Kenntnis der Unternehmen im Adressatenkreis und Vernetzung mit diesen,
   - Vernetzung mit anderen Akteuren (Politik/Verwaltung, Kammern, Verbände, Wirtschaftsförderer, Standardisierungs- und Normungsgremien etc.).

c) Konzepte zu
   - Leistungsportfolio (inhaltlich, quantitativ, Praxisbezug mit regionaler und thematischer Ausrichtung, geplante Instrumente) und Wissenstransfer,
   - Evaluation (Zielerreichung, Wirkungs- bzw. Wirtschaftlichkeitskontrolle),
   - Nachhaltigkeit des Zentrums.

d) Geschätzte Gesamtkosten und Fördermittelbedarf pro Partner tabellarisch.

Handlungsfeld 2:

Projekte, welche mindestens eines der in Nummer 1.2 genannten Förderziele adressieren.

Vorgegebene Gliederungspunkte sind:

a) Beschreibung der vorgeschlagenen Maßnahme und Zielstellung des Projekts
   - Bedarfsanalyse/Ist-Zustand der anvisierten Zielgruppe/Defizitanalyse
   - Projektkonzept, Projektschwerpunkte/zu transferierende Themen mit Bezug zu Nummer 2.2
   - Innovation und Attraktivität des Lösungsansatzes für die Zielgruppe

b) Breitenwirkung und Nutzen des Projekts
   - Chancen/Risiken bei der Projektumsetzung (soweit absehbar)
   - Kosten-/Nutzenaspekte und Zielvorgabe
   - Plausibel ausgearbeitetes, bundesweites und auf eine definierte Zielgruppe ausgerichtetes Transfer- und Umsetzungskonzept
   - Nachhaltigkeit nach dem Auslaufen der Förderung, Aussage zu Möglichkeiten zur Verankerung bei der Zielgruppe

c) Grober Projektplan mit vorläufiger Zeit- und Meilensteinplanung

d) Darstellung der Erfahrungen und Kompetenzen des Konsortiums in Bezug auf die Zielgruppe KMU und das Thema der Ausschreibung

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 folgenden Bewertungskriterien:

- Ausrichtung am spezifischen Bedarf der adressierten Zielgruppe (Ausgangslage, Ziele, Schwerpunkte),
- Leistungsfähigkeit und Kompetenz des Konsortiums, einschließlich bundesweiter Mobilisierung und Vernetzung,
- Leistungsportfolio (qualitativ und quantitativ) für den Wissens- und Technologietransfer und der Zieleerreichung der förderpolitischen Ziele sowie Konzepte zur Evaluation der Leistungen und Nachhaltigkeit des Zentrums,
- Wirtschaftlichkeit des Mitteleinsatzes.

Nach erfolgter Auswahlentscheidung werden die Konsortialführer über das Ergebnis schriftlich informiert. Im Rahmen des Auswahlprozesses wird eine vom BMWi 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.

Mit der Einreichung einer Skizze werden die Teilnahmebedingungen dieser Bekanntmachung akzeptiert.

Berlin, den 21. Dezember 2018

Bundesministerium
für Wirtschaft und Energie

Im Auftrag
Frank Fischer