IT-Förder-Newsletter

Fördermöglichkeiten

Datensicherheit in der digitalisierten Wirtschaft

Dezember 2016

House of IT

TransMIT
Gesellschaft für
Technologietransfer mbH

Inhaltsverzeichnis

1 Vorwort

„Datendiebstahl bei Yahoo: 500 Millionen betroffene Nutzer.“

„Passwörter und E-Mails von 117 Millionen Nutzern bei LinkedIn ausgespäht“

„Hackerangriff auf Deutschen Bundestag.“

Liebe Leser,

diese Schlagzeilen der letzten Monate erzeugen bei manch einem Entscheider in zweierlei Hinsicht eine zweifelhafte Wirkung: Zum Einen entsteht der Eindruck, dass es nur die Global Player trifft, zum Anderen wird in der Berichterstattung der Fokus ausschließlich auf das Ausspähen von Daten gelegt. Beides könnte zu dem fatalen Schluss verleiten, dass KMU eigentlich kein Problem haben. „Zuerst trifft es die Großen und wenn etwas passiert, haben wir ja nichts zu verbergen!“ lautet die oft folgenreiche Fehleinschätzung.

Dass es nicht nur die Großen trifft und Datenklau nur die Spitze des Eisbergs darstellt, zeigt die weltweite Kaspersky-Studie „Corporate IT Security Risks 2016“. Im Durchschnitt kostete ein Krypto-Malware-Angriff mittelständische Unternehmen im vergangenen Jahr 99.000 US-Dollar. Bei dieser Art von Angriffen werden Datenbestände ohne Vorankündigung verschlüsselt und damit unbrauchbar gemacht. Die Täter geben vor, gegen die Zahlung eines Lösegelds die Daten wieder frei zu geben. Und dies ist nur eines von vielen Bedrohungsszenarien: Automatisierte Angriffe gegen Netzwerke sind an der Tagesordnung. Trojaner, die Daten ausspähen und verändern oder gleich Ihre Server kapern, werden ganz einfach über das Öffnen verseuchter E-Mail-Anhänge eingeschleust. Die fortschreitende Digitalisierung fördert diese Entwicklung: Jedes zusätzliche System eines Unternehmens, das mit dem Internet verbunden ist, stellt eine potenzielle Bedrohung dar. Das gilt insbesondere für mobile Endgeräte wie Notebooks, Tablets und Smartphones.

Sollten wir uns also der Digitalisierung verweigern? Auf keinen Fall, denn in den allermeisten Fällen dürfte uns dann der Wettbewerb abhängen. Es braucht vielmehr gerade in KMU einen offensiven Umgang mit potenziellen Sicherheitsrisiken. Ein Teil Ihres IT-Budgets sollte daher dauerhaft und regelmäßig in das Thema Sicherheit fließen. Natürlich gibt es keine 100%ige Sicherheit, aber schon einfache Maßnahmen können Ihre Sicherheit deutlich erhöhen.

Wenn Sie einen kurzen Sicherheits-Check Ihres Netzwerkes machen möchten, schauen Sie einfach gleich in das Kapitel 2 „IT-Sicherheits-Check – Einstieg leicht gemacht“ des Newsletters. Wer professionelle Einstiegsunterstützung sucht, wird in Kapitel 3 „Geförderte Einstiegsberatungen“ fündig ebenso wie unsere FuE-Interessierten Leser/-innen in Kapitel 3 „Gezielte FuE-Förderungen für IT-Sicherheitsthemen“.

Viel Spaß beim Lesen!

Ihr

Dr. Peter Stumpf
Geschäftsführer TransMIT GmbH

Dr. Robert Heinrich
Geschäftsführer House of IT e.V.

2 IT-Sicherheits-Check – Einstieg leicht gemacht

Der Einstieg in die digitale Sicherheit muss nicht künstlich hoch stilisiert und verkompliziert werden. Prüfen Sie doch einfach anhand kostenloser Sicherheitschecks den aktuellen Stand Ihrer bisherigen Sicherheitsarchitektur und –struktur.

Dazu empfehlen wir Ihnen den DsiN-IT-Sicherheitscheck. Dieser wird in Kooperation des Bundesministeriums für Wirtschaft und Energie sowie dem Bundesministerium des Innern im Rahmen der Initiative „Deutschland sicher im Netz“ bereitgestellt.

Der Check umfasst 20 Fragen und ist demnach zeitlich recht überschaubar. Als Ergebnis erhält man dafür eine recht ausführliche Übersicht der einzelnen Sicherheitsbereiche und kann damit konkret und gezielt etwaige sicherheitsrelevante Bereiche angehen.

2 Geförderte Einstiegsberatungen

Häufig leiden „interne Projekte“ unter der „Verschieberitis“ im Terminkalender und rücken somit an die letzte Stelle. Denn verständlicherweise werden eingehende Aufträge bevorzugt abgearbeitet und der notwendige Umsatz erwirtschaftet. Ein weiteres Hemmnis könnte die Unsicherheit hinsichtlich IT-Sicherheitskenntnissen sein, für das man sich erst einmal in Ruhe widmen möchte. Beide Argumente könnten zu fatalen Folgen mit Reputationsverlust und hohen Schadensummen führen.

Dabei können gerade KMUs von geförderten Einstiegsberatungen zum Thema IT-Sicherheit enorm profitieren und externe Beratung bezuschusst bekommen. Damit kann das Thema parallel durch externe IT-Experten zum wichtigen laufenden Geschäft bearbeitet und vorbereitet werden. Wir wollen Ihnen zwei wichtige Möglichkeiten vorstellen.

2.1 Go-Digital – ab 2017 voraussichtlich bundesweit möglich

Gemäß Ankündigung auf der Webseite des BMWi wird beabsichtigt, das bisher regional begrenzte Förderangebot Go-Digital ab 2017 nach erfolgreicher Evaluierung bundesweit zugänglich zu machen. Es lohnt sich jetzt, regelmäßig einen Blick auf die Webseite von Go-Digital zu werfen!

Ziel der Förderung ist es, KMUs und Handwerksunternehmen bei der Entwicklung und Einführung von ganzheitlichen IT-Geschäftskonzepten und organisatorischen Maßnahmen in den Bereichen

- IT-Sicherheit,
- Internet-Marketing und
- Digitalisierte Geschäftsprozesse

zu unterstützen, um mit der zunehmenden Digitalisierung des Geschäftsalltags Schritt halten zu können.

Antragsberechtigt sind Unternehmen mit technologischem Potenzial mit maximal 100 Mitarbeitern und einem Jahresumsatz oder einer Jahresbilanzsumme von höchsten 20 Mio. Euro, die eine Betriebsstätte in Deutschland haben.

Gefördert werden

Leistungsstufe	Inhalt	Max. Beratertage	max. Förderwert
LS 1	Analyse/Grobkonzept	6	6.600 EUR
LS 2	Feinkonzept/Umsetzung	23	25.300 EUR

Abbildung 1: Geplante Leistungsstufen und Fördersummen in Go-Digital ab 2017

Die Förderquote beträgt für Unternehmen mit weniger als 50 Mitarbeitern 75 % und mit Betrieben mit 51 bis 100 Mitarbeitern 50 % der vorhabenbezogenen Ausgaben.

Darüber hinaus können sich Unternehmen mit entsprechender fachlicher Expertise als Beratungsunternehmen akkreditieren lassen, um ihren Kunden entsprechende Dienstleistungen anbieten zu können. Weiterführende Informationen finden Sie hier.

2.2 Förderung unternehmerischen Know-hows

Verständlicherweise überlegt man es sich gründlich, ob man in neue Technologien und Verfahren zur Digitalisierung und potenziellen Verbesserung der betrieblichen Abläufe durch im digitalen Zeitalter investieren soll. Die eingangs angesprochene Kosten-/Nutzen-Analyse zur betriebswirtschaftlichen und technischen Entscheidungsfindung muss nicht komplett aus eigener Tasche bezahlt werden.

Gerade die voranschreitende Digitalisierung des Geschäftsbetriebs birgt Fragestellungen im Bereich der organisatorischen Unternehmensführung, bei der externe Experten die wegweisenden Voraussetzungen, Implikationen und Handlungsoptionen aufzeigen können. Externe Beratung kostet jedoch zunächst Geld, sodass viele KMUs, junge Unternehmen und Start-ups sich diesen Schritt zweimal überlegen.

Die bei der BAFA (Bundesamt für Wirtschaft und Ausfuhrkontrolle) seit 2016 angesiedelte Förderung unternehmerischen Know-hows richtet sich genau an solche Beratungsanliegen und ist für den Einstieg in dieses Thema durchaus geeignet. Auch wenn es nur eine kleine Beratungsförderung ist, kann dieses Programm für den Einstieg in das Thema „IT-Sicherheit“ im organisatorisch-betriebswirtschaftlichen Kontext helfen.

2.2.1 Fördervoraussetzung

Mit der Förderung unternehmerischen Know-hows werden Unternehmen mit Sitz in der Bundesrepublik Deutschland unterstützt, welche die KMU-Definition für kleine und mittlere Unternehmen der Europäischen Kommission entsprechen:

- Max. 250 Mitarbeiter (Vollzeitäquivalente)
- Entweder ein Jahresumsatz von höchstens 50 Mio. EUR oder eine Jahresbilanzsumme von höchstens 43 Mio. EUR

2.2.2 Inhalt der geförderten Beratung

Es können Beratungen zu allgemeinen Themen der Unternehmensführung durchgeführt werden wie z. B.

- Wirtschaftliche Fragen
- Finanzielle Fragen
- Personalalthemen
- Organisatorische Fragen

Dies ist sehr offen und nicht eingrenzend zu verstehen, sodass der Themenkomplex der Einführung digitaler Produktionsprozesse im allgemeinen Beratungsbereich der Organisation zu sehen ist.

Darüber hinaus besteht die Möglichkeit, sich in weiteren speziellen Themengebieten beraten zu lassen. Dies umfasst vor allem Beratungen zum Ausgleich struktureller Ungleichheiten (Stichwort „Gleichstellung“) oder auch Fachkräftegewinnung.

2.2.3 Beratungszuschuss

Die Höhe des Zuschusses orientiert sich an den maximal förderfähigen Beratungskosten sowie dem Standort des Unternehmens:

Fördersätze: 80 % neue Bundesländer (ohne Berlin und ohne Region Leipzig), 60 % Region Lüneburg, sonst 50 %, 90 % Unternehmen in Schwierigkeiten unabhängig von Alter und Standort			
Unternehmensart	**Bemessungsgrundlage**	**Fördersatz**	**maximaler Zuschuss**
Junge Unternehmen nicht länger als 2 Jahre am Markt	4.000 Euro	80 %	3.200 Euro
		60 %	2.400 Euro
		50 %	2.000 Euro
Bestandsunternehmen ab dem dritten Jahr nach Gründung	3.000 Euro	80 %	2.400 Euro
		60 %	1.800 Euro
		50 %	1.500 Euro
Unternehmen in Schwierigkeiten	3.000 Euro	90 %	2.700 Euro

Abbildung 2: Beratungszuschuss "Förderung unternehmerischen Know-hows"[1]

2.2.4 Beraterauswahl

Sie können Ihren Wunschberater selber auswählen. Wie bzw. nach welchen Kriterien ein geeigneter Berater bzw. Beratungsunternehmen ausgewählt werden kann, gibt die Broschüre der BAFA „Hinweise für KMU zur Beraterauswahl“.

Um den Beratungszuschuss auch zu erhalten, muss der Berater bei der BAFA registrieren sein und bestimmte Voraussetzungen mitbringen. Im Wesentlichen müssen die Berater

[1] Quelle: http://www.bafa.de/bafa/de/wirtschaftsfoerderung/foerderung_unternehmerischen_know_hows/, zuletzt abgerufen am 9.5.2016

- selbstständig sein;
- überwiegend beratend tätig sein (>50% des Umsatzes aus Beratungstätigkeit erzielen);
- über erforderliche Befähigung verfügen;
- zuverlässig sein;
- ein geeignetes QM-Instrument eingeführt haben und dies auch leben;
- eine ordnungsgemäße Geschäftsführung gewährleisten, insbesondere eine richtlinienkonforme Durchführung der Beratung.

Weitere Einzelheiten können Sie dem Dokument „Berater/-in – Anforderung“ entnehmen. Der Nachweis der Beratereignung muss spätestens zum Zeitpunkt der Bewilligung des Zuschusses, also nach Vorlage des Verwendungsnachweises, vorgelegt werden. Insofern ist es empfehlenswert, die Registrierung vor der Beratung durchzuführen, damit der Beratungszuschuss auch gewährt werden kann.

Die TransMIT GmbH bietet Ihnen im Bereich ITK und Digitalisierung entsprechende Beratungsmöglichkeiten. Bitte sprechen Sie uns hierzu gerne direkt an.

2.2.5 Antragsverfahren

Anträge werden online gestellt: https://fms.bafa.de/BafaFrame/unternehmensberatung.

Jungunternehmen, bis 2 Jahre nach Gründung sowie Unternehmen in Schwierigkeiten müssen ein kostenloses Informationsgespräch bei einem regionalen Ansprechpartner über die Zuwendungsvoraussetzungen führen. Etablierte Unternehmen können direkt den Antrag stellten.

Antragssteller und Zuwendungsempfänger ist das beratene Unternehmen. Die Anträge werden seitens der regionalen Leitstellen/Regionalpartner geprüft und eine unverbindliche Inaussichtstellung der Förderung versendet. Erst danach kann der Beratungsauftrag erteilt werden und im bewilligten Förderzeitraum durchgeführt werden.

3 Gezielte FuE-Förderungen für IT-Sicherheitsthemen

3.1 IT-Sicherheit in der Wirtschaft

Die zunehmende Digitalisierung der Wirtschaft erweckt zum einen Wachstumshoffnungen durch die Erschließung neuer Märkte und der Optimierung betrieblicher Abläufe. Wer sich dieser allgemeinen Entwicklung verschließt, läuft sprichwörtlich Gefahr, abgehängt und verdrängt zu werden. Die Nutzung und der Umgang mit den neuen digitalen Technologien bergen auch Sicherheitsgefahren.

KMUs sind ein zentraler Bestandteil der Wertschöpfungskette. Die Notwendigkeit der Nutzung digitaler Technologien können sich Unternehmen nicht verschließen und können gleichzeitig, mit den steigenden Anforderungen in der IT-Sicherheit nur schwer Schritt halten.

3.1.1 Antragsberechtigte und Ziel der Förderung

Die hier vorgestellte Fördermaßnahme richtet sich primär an aktive Akteure im Bereich der IT-Sicherheit – insbesondere Hochschulen als **Kompetenzpartner**, Unternehmen aus der IT-Sicherheitsbranche als **Anwendungspartner** und Multiplikatoren/Interessenvertretungen als **Transferpartner**.

Gefördert werden „zielgruppengerechte Aufklärungskampagnen bzgl. Modellvorhaben, die der Verbesserung der Cyber-Sicherheit in KMU dienen.“ Die Verbundprojekte zwischen Kompetenzpartnern, Anwendungspartner und Transferpartnern sollen darauf abzielen,

wissenschaftlich fundierte und neueste technische Erkenntnisse und Verfahren (z.B. Best-Practice) im Bereich der IT-Sicherheit mit geeigneten praktischen Hilfestellungen und Anleitungen KMUs zugänglich zu machen. Dies können folgende Maßnahmen sein:

- Innovative Formen des Wissensaustauschens zur Stärkung der Netzwerkarbeit, die KMU zugutekommen.
- Breit angelegte und nachhaltige wirkende Transfermaßnahmen zur Verbesserung des IT-Sicherheitsniveaus der Geschäftsprozesse in KMU
- Aufbau geeigneter Transferverbünde zur Vorbereitung und modellhaften Erprobung

Interessenten sollten die eigene Projektidee darauf hin prüfen, ob

a) genügend Vor- und Fachkenntnisse vorhanden sind,

b) die Zielgruppe (z.B. KMU einer spezifischen Branche) bekannt ist, und

c) der Zugang zur Zielgruppe (quantitativ und qualitativ) dargestellt werden kann,

d) das zielgruppenspezifische Problem analysiert und dargestellt ist und

e) das Vorhaben mit technischem sowie wirtschaftlichem Risiko derart verbunden ist, dass ohne Förderung eine Umsetzung nicht realistisch erscheint.

3.1.2 Umfang der Förderung

Die Verbundprojekte werden als nicht rückzahlbarer Zuschuss gefördert. Die Gesamtkosten des Verbundvorhabens sollen 1,5 Mio. EUR nicht überschreiten. Für die modellhafte Erprobung von Transferverbünden besteht eine Obergrenze von 300.000 EUR. Die Projektlaufzeit darf maximal 3 Jahre betragen.

Beteiligte Hochschulen werden mit bis zu 100% der zuwendungsfähigen Kosten gefördert. Die Zuwendungen an Verbände und Multiplikatoren können mit bis zu 80% projektbezogener Ausgaben gefördert werden. Für gewerbliche Unternehmen wird eine Eigenbeteiligung von grundsätzlich mindestens 50% zuwendungsfähiger Projektkosten vorausgesetzt. Beteiligten KMU können zusätzliche Aufschläge als Bonus gewährt werden.

3.1.3 Antrag und weitere Informationen

Das Antragsverfahren ist zweistufig aufgebaut. Projektskizzen können laufend eingereicht werden. Nach erfolgreicher Bewertung werden wird ein Antragsverfahren eingeleitet.

Weitere Informationen sind der Bekanntmachung zu entnehmen oder direkt bei der

Geschäftsstelle Initiative „IT-Sicherheit in der Wirtschaft“ im BMWi
Villemombler Str. 76
53123 Bonn
Mail: it-sicherheit-in-der-wirtschaft@bmwi.bund.de

3.2 KMU-Innovativ – Themenfeld IKT – IT-Sicherheit

Für forschungstreibende und innovative kleinere und mittlere Unternehmen, welche z. B. eine konkrete Idee zur Digitalisierung und Virtualisierung von Produktionssystemen realisieren möchten. Sofern sich diese von dem bisherigen Stand der Technik deutlich abhebt, kann das umfangreiche Förderprogramm „KMU-Innovativ“ interessant sein.

Mit KMU-Innovativ fördert das BMBF ganz allgemein Spitzenforschung in wichtigen Zukunftsbereichen. Diese sind:

- Biotechnologie
- Medizintechnik
- Informations- und Kommunikationstechnologien
- Materialforschung
- Photonik
- Produktionsforschung
- Ressourceneffizienz und Klimaschutz
- Forschung für die zivile Sicherheit
- Elektroniksysteme; Elektromobilität

Gerade im Themenbereich „Informations- und Kommunikationstechnologien“ können in unterschiedlichen Branchen und Anwendungsfeldern innovative Projekte zum Thema „IT-Sicherheit“ gefördert werden.

Dabei sind die Exzellenz und Innovationsgrad des geförderten Projekts sowie hohe Verwertungschancen wichtiger als die korrekte Zuordnung zu einem der oben genannten Themenfelder. Für die „richtige“ Einordnung der Projektidee hilft der Lotsendienst für Unternehmen (Tel.: 0800/2623-009 oder lotse@kmu-innovativ.de).

Weiterführende Informationen zum Themenfeld „Informations- und Kommunikationstechnologien“ finden Sie unter diesem Link.

3.2.1 Fördervoraussetzungen und -höhe

Antragsberechtigt sind KMUs entsprechend der Definition der EU-Kommission. Darunter fallen Unternehmen mit weniger als 250 Beschäftigten, einem Jahresumsatz von höchstens 50 Millionen Euro oder eine Jahresbilanzsumme von höchstens 43 Millionen Euro.

Im Rahmen von Verbundprojekten mit mehreren Projektpartnern können auch Hochschulen, außeruniversitäre Forschungseinrichtungen und Unternehmen, die nicht die KMU-Kriterien erfüllen, eingebunden werden.

Die Förderquote für KMUs beträgt 50 % der zuwendungsfähigen Kosten. Das maximale Projektvolumen ist vom Leistungsvermögen der beteiligten KMUs abhängig. Hochschulen und außeruniversitäre Forschungseinrichtungen werden individuell mit bis zu 100 % gefördert.

3.2.2 Antragsverfahren

Das Antragsverfahren ist zweistufig, d. h. jeweils zum 15. April bzw. 15. Oktober eines Jahres können Projektskizzen über das Online-Skizzentool eingereicht werden. Zwei Monate nach dem Stichtag werden die Antragssteller benachrichtigt, die für eine Förderung vorgesehen werden. Innerhalb von weiteren zwei Monaten nach der dann vorzunehmenden Einreichung der vollständigen Antragsunterlagen über das elektronische Antragssystem „easy-online“ erfolgt die Erteilung der Förderbewilligung sodass nach ca. 4 Monaten mit dem Projekt begonnen werden kann.

3.3 Horizon 2020 – Digitale Sicherheit im Arbeitsprogramm Sichere Gesellschaften

Abschließend möchten wir Ihnen auch Förderoptionen der Europäischen Kommission im Förderschwerpunkt III „Gesellschaftliche Herausforderungen“ vorstellen. Hier bietet der Call „Digital Security Focus Area“ im Arbeitsprogramm „Sichere Gesellschaften“ für unsere europäisch-kooperationsinteressierten Leser aktuell sehr interessante Förderbekanntmachungen (Calls), die Ende 2016 bzw. Anfang 2017 zur Antragsstellung geöffnet werden.

Drei Calls möchten wir Ihnen im hier dargestellten Kontext der IT-Sicherheit kurz vorstellen. Weitere Informationen erhalten Sie durch Klick auf den jeweiligen Call-Titel:

Call Titel	Call-ID	Antrag ab	Frist
Cryptography	DS-06-2017	08.12.2016	25.04.2017
Addressing Advanced Cyber Security Threats and Threat Actors	DS-07-2017	01.03.2017	24.08.2017
Privacy, Data Protection, Digital Identities	DS-08-2017	01.03.2017	24.08.2017

Tabelle 1: Call-Ankündigungen im Themenfeld IT-Sicherheit unter Horizon 2020

Bitte beachten Sie, dass die hier vorgestellten EU-Förderungen i.d.R. nur Verbundprojekte mit mindestens drei Partnern aus drei unterschiedlichen EU-Mitgliedsstaaten bzw. anerkannten assoziierten Ländern gefördert werden. Nähere Informationen hierzu finden Sie unter den jeweiligen angegebenen Links der Calls.

3.3.1 Cryptography – Call-ID DS-06-2017

Im Kontext zunehmender Digitalisierung der Wirtschaft steigen auch die Bedürfnisse in der Leistungsfähigkeit von Verschlüsselungstechniken über die gesamten IKT-Ebenen. Ziele der Fördermaßnahme sind die Verbesserung der Vertrauenswürdigkeit, Leistungs- und technologischem Stand europäischer IKT-Dienstleistungen und –Produkte sowie der dadurch angestrebten Verbesserung der Konkurrenzfähigkeit insbesondere der Unternehmen in der Verschlüsselungs- sowie Smart-Card-Industrie. Darüber hinaus sollen Online-Dienste bei gleichzeitiger Einhaltung europäischer grundlegender Datenschutzrechte sicherer werden. Die geförderten Maßnahmen sollen auch neue Gefahren wie z.B. die Technologie der so-genannten Quantencomputer zur Zerlegung und Lösung extrem langer Algorithmen (kryptographischer Verfahren), adressieren.

Weitere Informationen entnehmen Sie bitte der Call-Ankündigung.

3.3.2 Addressing Advanced Cyber Security Threats – Call-ID DS-07-2017

Hackerangriffe auf Unternehmen, Organisationen und Regierungen nehmen zu und werden zunehmend ausgeklügelter, tückischer und vielschichtiger mit durchweg kriminellen Zielen. So können komplette IT-Infrastrukturen dadurch lahmgelegt werden, geheime Informationen und Daten werden gestohlen und missbraucht. In einer Gesellschaft, die immer stärker von der digitalen Infrastruktur abhängt, sind neue Technologien und Ansätze zur Gefahrerkennung und Widerstandsfähigkeit gefragt.

Die Förderung ist in zwei Kategorien untergliedert:

a) Research and Innovation Actions – Situational Awareness
   Der Fokus liegt auf der Entwicklung neuer Ansätze zur situationsbedingten Gefahrerkennung von IT-Sicherheitsrisiken sowie der Entwicklung von Schutzmechanismen für besonders gefährdete Organisationen/Institutionen.

b) Innovation Actions – Simulation Environments, Training
In dieser Kategorie werden Projekteideen gefördert, die innovative Trainings-Simulations-Umgebungen entwickeln, um die handelnden Personen innerhalb der besonders gefährdeten Organisationen/Institutionen zu schulen.

Weitere Informationen entnehmen Sie bitte der Call-Ankündigung.

3.3.3 Privacy, Data Protection, Digital Identities – Call-ID DS-08-2017

Durch Nutzung moderner Telekommunikationstechnologien und Online-Services bedarf es immer häufiger der Angabe personenbezogener Informationen. Die verbreitete Nutzung sozialer Netzwerke führt dazu, personenbezogene Daten preiszugeben. Wir hinterlassen bei jeder Internetrecherche eine Datenspur, mit der man persönliche Bewegungsprofile erstellen kann, um daraus wiederum Rückschlüsse ziehen zu können. Für viele Unternehmen sind diese technischen Möglichkeiten geschäftsentscheidend, führen detaillierte Nutzerkenntnisse zu einem vertieften Kundenwissen.

Doch wie steht es mit dem Schutz der Privatsphäre und dem Recht auf Datenlöschung, das in der neuen EU-Datenschutz-Grundverordnung am 14. April 2016 beschlossen wurde?

Mit dieser Förderung sollen diese grundlegenden Rechte der digitalen Gesellschaft unterstützt werden, damit das Vertrauen in den digitalen EU-Binnenmarkt gestärkt wird.

Projektanträge können daher in folgenden Bereichen eingereicht werden:

- Technologien zur Verbesserung der Privatsphäre
- EU-Datenschutz-Grundverordnung in der Praxis
- Sichere digitale Identitätssysteme

Weitere Informationen entnehmen Sie bitte der Call-Ankündigung.

4 Wie geht es weiter? Fördermittel beantragen leicht gemacht!

Sie fragen sich, wie etwaige Maßnahmen und Projekte finanziert oder gefördert werden können, und wissen nicht, wo und wie Sie anfangen sollen?

Bei der ganzen Fülle an Förderoptionen stehen ggf. berechtigte Fragen im Raum, wie zum Beispiel:

- Welches Förderprogramm passt nun zu meiner Projektidee?
- Wie entwickelt man eine passende Projektskizze?
- Wie finde ich passende Kooperationspartner?
- Welchen Stand der Technik hat meine Erfindung/Projektidee?
- Wie setze ich den administrativen Teil der Beantragung, Projektdurchführung und –abwicklung mit den Projektträgern durch?
- Welche rechtlichen und finanziellen Rahmenbedingungen müssen beachtet werden?
- Welche Auswirkung hat das ggf. auf mein Geschäftsergebnis?
- Wie geht man mit Erfindungen in einem Verbundprojekt um?
- Was muss man bei Kooperationsverträgen beachten?
- u.v.m.

Diese und weitere Fragen sollten im Vorfeld intern als auch mit etwaigen Projektpartnern im Rahmen der Projektentwicklung und -beantragung geklärt werden. Hierfür kann man sich an folgendem dargestellten Prozess orientieren:

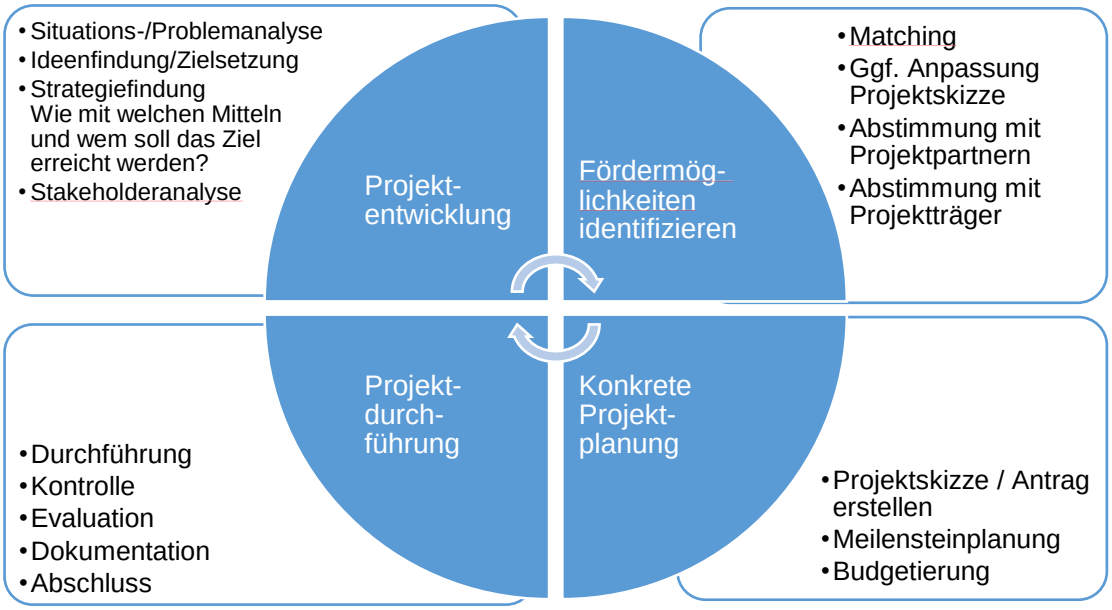

Abbildung 3: Prozess Entwicklung von Fördermittelprojekten

4.1 Kontaktdaten

Gerne stehen die Ansprechpartner des House of IT e.V. und der TransMIT GmbH für Ihre Rückfragen zur Verfügung:

House of IT e.V.

Gerald Münzl
Mornewegstr. 30
64293 Darmstadt

Tel.:0171/76 94 644

E-Mail: muenzl@house-of-it.eu

TransMIT
Gesellschaft für Technologietransfer mbH
Fördermittelberatung
Herr Michael Haberland
Kerkrader Str. 3
35394 Gießen

Te.l: 0641/94364-50

E-Mail: michael.haberland@transmit.de

4.2 **Mögliche Partner – wie und wo finde ich diese?**

Weitere Ansprechpartner für folgende Förderprogramme sind:

Förderprogramm	**Projektträger/Institute**	**Kontakt**
Horizon 2020 und SME-Instrument	Enterprise Europe Network	www.een-hessen.de F+E-Programmberatung, Kooperations-vermittlung: Herr Adrian Stypka Tel.: 0611/95017-8494 Mail: adrian.stypka@htai.de
	Nationale Kontaktstelle IKT	www.nks-ikt.de IKT-Strategien und EU-Synergien Projektträger im DLR Programmkoordination Dr. Friedhelm Gillessen Tel: 02203/601-3403 Mail: friedhelm.gillessen@dlr.de
	Nationale Kontaktstelle KMU	www.nks-kmu.de Projektträger DLR Programmkoordination Dr. Petra Oberhagemann Tel: 0228/3821-1643 Mail: petra.oberhagemann@dlr.de
Bundesförderprogramme des BMBF und BMWi etc.	Förderberatung „Forschung und Innovation“ des Bundes	www.foerderinfo.bund.de Tel.: 0800/2623-008 Mail: beratung@foerderinfo.bund.de
	Lotsendienst für Unternehmen KMU-Innovativ	Tel.: 0800/2623-009 Mail: lotse@kmu-innovativ.de
Landesförderung Hessen	Hessen Agentur	www.innovationsfoerderung-hessen.de Allgemeine Fragen: Dr. Claudia Männicke Tel: 0611/95017-8691 Mail: claudia.maennicke@hessen-agentur.de IT und Software Hendrik Terstiege Tel: 0611/95017-8962 Mail: hendrik.terstiege@hessen-agentur.de

Das EEN Hessen unterstützt Sie bei der Suche nach Kooperationspartnern aus Europa und steht auch für Fragen zur EU-Förderung zur Verfügung.

4.3 Förderprogramme im Überblick

Geldgeber	Programmname	Fristen	Förderart/-Nr.
EU	Cybersecurity: Cryptography	25.4.2017	Zuschuss
EU	Cybersecurity: Addressing Advanced Cyber Security Threats and Threat Actors	24.8.2017	Zuschuss
EU	Cybersecurity: Privacy, Data Protection, Digital Identities	24.8.2017	Zuschuss
EU	Eurostars (deutsch) Eurostars	2.3.2017	Zuschuss
BMBF	KMU-Innovativ - Themenfeld Informations- und Kommunikationstechnologie	14.4. und 15.10. eines Jahres	Zuschuss
BMWi	Smart Service Welt II	9.2.2017	Zuschuss
BMWi	IGF - Industrielle Gemeinschafts-forschung	lfd.	indirekter Zuschuss durch Forschungsergebnis
BMWi	Go-Digital	Bundesweit ab voraussichtlich 2017	Beratungszuschuss
BMWi	Go-Innovativ	Lfd.	Beratungszuschuss
BMWi	WIPANO – Patentförderung für Unternehmen	Lfd.	Beratungszuschuss
BAFA	Förderung unternehmerischen Know-hows	Lfd.	Beratungszuschuss
HMWK	LOEWE 3	15.12.2016, 23.2.2017, 20.4.2017	Zuschuss